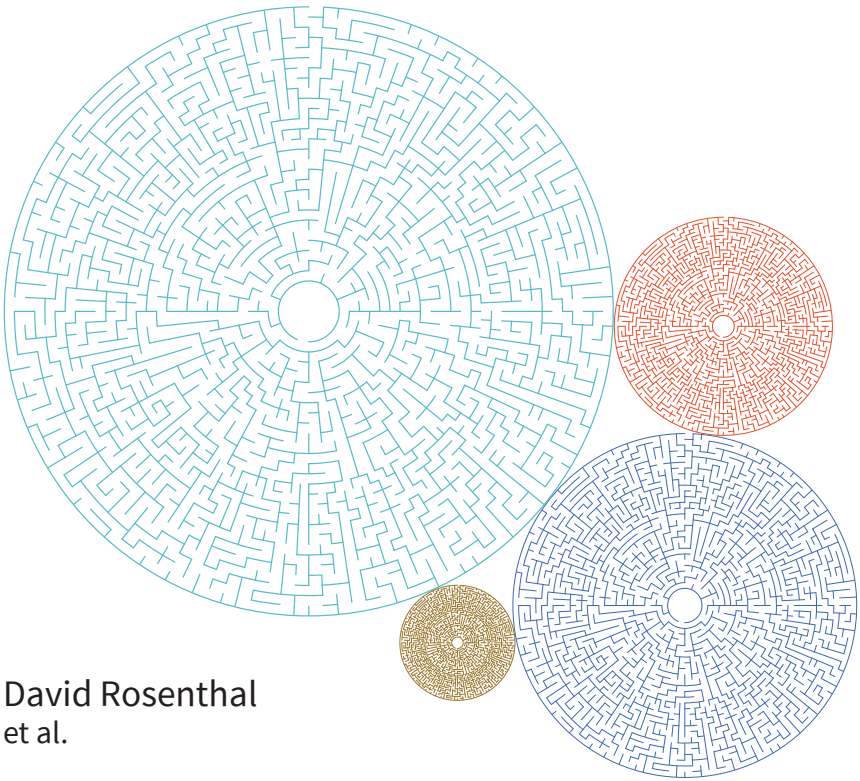
VISCHER

EDITIONS WEBLAW

Praxishandbuch für interne Untersuchungen und eDiscovery.

Release 1.01



David Rosenthal
et al.

Release History:

Mai 2021	Release 1.01

Autor: David Rosenthal

Mitarbeit: Marisa Di Francesco sowie für Fachfragen Felix W. Egli, Marc Ph. Prinz, Jonas D. Gassmann, Adrian Briner und Nadia Tarolli.

Ein herzliches Dankeschön (in alphabetischer Reihenfolge):

- für die wertvollen Inputs und Feedbacks geht u.a. an Matthias Grossenbacher (Ernst & Young), Lars Hauser (Julius Bär), Christoph Jörg (BKW), Sandra Middel (Clariant), Adrian Ott (Ernst & Young), Josef Sachs, Peter C. Stelzer (Privatdetektei Ryffel), Rogier Teo (SwissFTS), an eine Person, die leider nicht genannt werden darf, sowie an alle Personen, denen ich zu diesem Thema schon begegnet bin und die mir zu meinen Erfahrungen verholfen haben.
- für die aufschlussreichen Gedanken zwischen den Kapiteln an Zoé Baches, Philipp Becker, Susan Emmenegger, Claudius Gelzer, Sabine Gless, Damian K. Graf, Christoph Jörg, Alexander Lacher, Sandra Middel, Nicolas Passadelis, Alain Pfäffli, Josef Sachs, Eveline Saupper, Annette Schüller, Michael von Felten und Christian Zeunert.
- für die wunderbare Unterstützung bei diesem Projekt seitens VISCHER an Rolf Auf der Maur, Geraldine Bless, Livia Camenisch, Nicole Grob, Seraina Paradiso, Inge Rother und Tiia Vogel, sowie an das Team von Weblaw.

Labyrinth-Grafik auf dem Titelbild: Gordon Johnson von Pixabay

Verlegt von VISCHER AG, Zürich/Basel/Genf, www.vischer.com, gemeinsam mit Editions Weblaw, Bern, www.weblaw.ch

ISBN: 978-3-03916-069-3

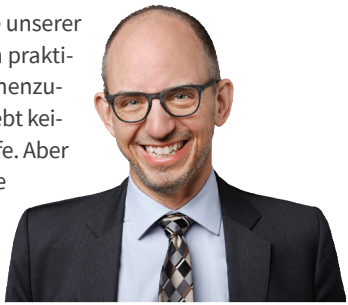
Zitiervorschlag: David Rosenthal et al., Praxishandbuch für interne Untersuchungen und eDiscovery, Release 1.01, Zürich/Bern, 2021, S. xx

Vorwort

Es war kurz nach der Jahrhundertwende. Mein erster Fall begann mit einer Due Diligence, noch bei meiner früheren Kanzlei. Wir entdeckten, wie eine Medizinalgerätefirma Ärzte mit Säcken voller Bargeld bestach. Klassisch. E-Mail-Reviews waren damals für die meisten ein Fremdwort. Es gelang uns auch ohne einen solchen Review den Fall aufzuklären, ihn mit einer Selbstanzeige und Strafzahlung ans Department of Justice (DoJ) in den USA aus der Welt zu schaffen – und hierzulande mit dem Grundsatz *ne bis in idem* ein Strafverfahren zu verhindern.

Seither hat sich in der Welt der internen Untersuchungen vieles verändert. Die Verstösse sind vielfältiger geworden, es wird besser getarnt, doch auch die Toleranzschwelle in den Unternehmen ist deutlich gesunken. Vor allem aber hat die digitale Revolution die Branche voll im Griff – ein Fluch und Segen zugleich. Einerseits kommen laufend neue Datenquellen hinzu, andererseits neue Werkzeuge und Methoden, um sie noch besser aufzuarbeiten. Derweil lernten Behörden zuerst in den USA, dann hier, interne Untersuchungen zu schätzen: Lassen Unternehmen potenzielle Compliance-Verstösse gleich selbst untersuchen, hat jeder etwas davon – der Staat spart Geld und Ärger, das Unternehmen verliert nicht völlig die Kontrolle und die Anwälte und Dienstleister machen ein gutes Geschäft.

Inzwischen herrscht Ernüchterung. Viele erkannten: Nicht immer ist es sinnvoll, mit der grossen Kelle anzurühren. Verhältnismässigkeit ist angesagt, und die vollmundigen Versprechungen der Datendienstleister werden kritisch hinterfragt. Das ist gut so. Gleichzeitig ist der Bedarf an internen Untersuchungen gestiegen und neue Bedürfnisse sind entstanden, etwa des Datenschutzes wegen. Auskunftsersuchen, *Privacy Redactions* und *Data Breaches* sind nur drei Stichworte.



Die Idee zu diesem Handbuch kam mir, als mich ein Kollege unserer Kanzlei bat, für einen seiner Klienten ein Papier mit einigen praktischen Hilfestellungen zu internen Untersuchungen zusammenzustellen. Ich entschied, dieses Handbuch zu verfassen. Es erhebt keinen Anspruch auf Vollständigkeit oder wissenschaftliche Tiefe. Aber die vielen Merkpunkte und Tipps vermitteln hoffentlich einige wertvolle Praxiserfahrungen, auf die es im Alltag ankommt.

David Rosenthal
drosenthal@vischer.com

Inhalt

Fragen und Antworten

Gedanken zum Thema.

Wirtschaftskriminalität beginnt im Kopf. Bevor der Täter zur Tat schreitet, spielt er seine Pläne tausendmal in der Fantasie durch. Er ist von kriminellen Ideen fasziniert, verwirft sie wieder und lässt sie dann erneut auferstehen. Indem er so denkt, sinkt die Hemmschwelle, die kriminelle Handlung verliert ihren Schrecken. Doch wer eine schwere Straftat begeht, kann die damit verbundene Belastung oft nicht für sich behalten. Zur Entlastung werden bei Drittpersonen oder in sozialen Foren vage Andeutungen über die Taten platziert. Diese Andeutungen werden *Leakings* genannt und sind für den aufmerksamen Beobachter erkennbar.

Josef Sachs
Forensischer Psychiater

1. Einleitung

Mit diesem Handbuch will ich Sie bei der komplexen Thematik der internen Untersuchung unterstützen und Ihnen ein praktisches Hilfsmittel an die Hand geben. Sie können dieses Handbuch als Ganzes lesen oder nur die Teile, die Sie interessieren. Ich präsentiere Ihnen praktische und konkrete Antworten auf Fragen, mit denen Sie bei einer internen Untersuchung oder in einem eDiscovery-Projekt typischerweise konfrontiert werden, gestützt auf die Erfahrungen von mir und all den anderen Personen, die an diesem Handbuch mitgewirkt haben. Dabei werden nicht nur rechtliche, sondern auch technische, organisatorische und psychologische Aspekte diskutiert, auch wenn sich zu jedem Thema mit Sicherheit noch mehr sagen lässt.

Zur Vereinfachung der Formulierung wird der Leser dieses Handbuchs mit „Sie" angesprochen. Aus Gründen der Lesbarkeit wird im Text nur die männliche Form verwendet, nichtsdestotrotz beziehen sich alle Angaben auf Angehörige sämtlicher Geschlechtsidentitäten. Sofern das vorliegende Handbuch Bezug nimmt auf das schweizerische Datenschutzgesetz, wird auf die geltende Fassung Bezug genommen. Zu beachten ist, dass voraussichtlich 2022 das revidierte Datenschutzgesetz in Kraft treten wird. Wo angezeigt, wird auf wesentliche Neuerungen hingewiesen.

So gar nicht!

Dieses Buch behandelt ein vielschichtiges und heikles Thema. Ich habe darum viele Teile zusätzlich einem *Peer-Review* unterzogen. Trotz meines Anspruchs, Klartext zu reden, soll das Buch ausgewogen und fair sein. Falls Sie der Meinung sind, ein Aspekt fehlt, etwas sei falsch gewichtet oder ganz verkehrt, dann sagen Sie es mir, damit ich falls notwendig Korrekturen und Ergänzungen vornehmen kann.

Jedes Kapitel ist gleich aufgebaut: Es gibt eine Einleitung, die das Thema zusammenfasst und positioniert. Die wichtigsten Anwendungsfälle werden dargelegt und danach Schritt für Schritt erklärt, was zu tun ist, mit Hinweisen aus der Praxis und Hintergrundinformationen, um die Dinge besser einordnen zu können.

Ein Fingerzeig-Symbol (☝) weist Sie auf praktische Hinweise (wie Beispiele) oder Überlegungen hin, die Sie beachten sollten. In jedem Kapitel sind auch diverse Fragen und Antworten zum Thema aufgeführt, die entsprechend ihrer Nummer referenziert sind. Ein Verzeichnis davon findet sich am Anfang dieses Handbuchs. Am Ende des Buchs ist ein Glossar; die orangen Begriffe verweisen darauf.

Der eine oder andere wird mir vielleicht vorhalten, dass das Handbuch auch den Tätern wertvolle Hinweise liefern kann, wie Unternehmen vorgehen, um deren Fehlverhalten aufzudecken, und dass die Täter das Wissen nutzen können, um zukünftige „Fehler" zu vermeiden. Ich bin mir diesem Risiko bewusst, bin jedoch der Ansicht, dass der Vorteil einer möglichst fundierten und praxisnahen Vermittlung von Wissen in diesem Bereich überwiegt. Ich habe in meiner über 15-jährigen Karriere im Bereich der internen Untersuchung bisher keinen Fall erlebt, in welchem eine interne Untersuchung bei vorhandenen Verdachtsmomenten nicht zu hinreichend handfesten Ergebnissen geführt hat, wenngleich Fälle auch unerwartete Wendungen nehmen können. Selbst in einem kürzlichen Fall, in welchem die gesamte Belegschaft in das Fehlverhalten einer Führungsperson involviert war und die Untersuchung nach Strich und Faden sabotiert wurde, kam die Wahrheit letztlich heraus. Der Grund dafür liegt darin, dass immer Menschen am Werk sind, und Menschen machen Fehler, hinterlassen Spuren und haben (wenn auch nicht immer) ein Gewissen oder ab einem bestimmten Zeitpunkt die Einsicht, dass sich Offenheit und Einsicht lohnt. Auf Seiten des Untersuchenden braucht es allerdings Geduld, Beharrlichkeit und Fingerspitzengefühl. Vielleicht kann dieses Handbuch einen Täter möglicherweise sogar überzeugen, dass Kooperation die bessere Option ist, wenn eine Sache erst einmal aufgeflogen ist.

Zwischen jedem Kapitel finden sich einige Gedanken von Personen, die alle auf irgendeine Weise mit dem Thema zu tun haben, ob als Verwaltungsrätin, Wirtschaftsredaktorin, General Counsel, eDiscovery-Spezialist, Compliance-Verantwortlicher, Staatsanwalt, Gewerkschaftspräsident, Richter oder Professorin für Strafrecht.

Die Abläufe und Vorgehensweisen entsprechen internationalen Standards. In rechtlicher Hinsicht gehe ich jedoch primär auf das Schweizer Recht ein. Auch wenn ich versuche, die Rechtslage möglichst klar darzustellen, kann dieses Handbuch eine Rechtsberatung für den konkreten Fall nicht ersetzen. Wenden Sie sich hierfür an den Rechtsberater Ihres Vertrauens oder an uns.

Dieses Handbuch ist als eBook kostenlos verfügbar und wird nachgeführt. Sie können die aktuellste Fassung über mich oder via www.vischer.com/investigations beziehen. Dort können Sie sich auch auf einen Verteiler setzen lassen, um jeweils beim Erscheinen einer neuen Fassung informiert zu werden.

Falls Sie Ideen für Ergänzungen haben (Fragen, Literatur, Hinweise, etc.), Mängel feststellen oder Sie sonst reagieren möchten, schreiben Sie mir auf drosenthal@vischer.com!

Gedanken zum Thema.

Bekommt der Verwaltungsrat Kenntnis von Unregelmässigkeiten oder Verstössen, muss er schnell handeln. Das ist häufig einfacher gesagt als getan. Wer geht der Sache nach? Wer ist allenfalls auch noch involviert? Ist der Vorwurf berechtigt oder versucht jemand, einen Kollegen oder Chef auf diese Art loszuwerden? Wie reagieren wir, wenn der Fall, bevor er geklärt ist, nach aussen dringt? Und wie die Aufarbeitung anpacken? Drei Dinge helfen Ihnen da weiter: Sie brauchen eine Vertrauensperson im Unternehmen. Sie brauchen jemanden, der das nicht zum ersten Mal macht. Und Sie brauchen Mut zur Lücke und Gelassenheit, weil Sie letztlich nie auf alle Fragen eine befriedigende Antwort erhalten werden.

Eveline Saupper
Verwaltungsrätin

2. Die richtige Vorbereitung

Kurz gesagt

- Regeln Sie die Zuständigkeiten für die Untersuchung (und zwar so, dass Interessenkonflikte vermieden werden) und klären Sie vorgängig ab, von welchen externen Stellen Sie im Fall der Fälle rasch Unterstützung erhalten wollen.
- Informieren Sie die Mitarbeiter, wohin sie sich mit Hinweisen auf Compliance-Verstösse wenden können und welche Untersuchungsmassnahmen (z.B. Zugriff auf E-Mails) Sie ergreifen können.
- Gehen Sie allen Meldungen nach und geben Sie Feedback, damit die Mitarbeiter wissen, dass sie mit ihren Anliegen ernst genommen werden.

Worum es geht

Eine → **interne Untersuchung** wird früher oder später jedes Unternehmen ab einer gewissen Grösse durchführen wollen oder müssen. Denn in jedem Unternehmen kann es zur Verletzung von internen Regeln, öffentlich-rechtlichen Bestimmungen oder sogar Strafnormen kommen. Als „interne Untersuchung" wird eine systematische, vertiefte Ermittlung und Beurteilung der Fakten bezüglich eines solchen Fehlverhaltens bezeichnet, die durch das Unternehmen selbst durchgeführt wird (im Gegensatz zu einer behördlichen Untersuchung). Mit der Untersuchung werden in der Regel interne Funktionen beauftragt, in heikleren oder grösseren Fällen, oder wenn das Management selbst beteiligt sein kann, werden jedoch Externe betraut, die nicht in den Vorfall involviert waren oder sind. Zuständig ist i.d.R. Compliance, Human Resources (HR) oder der Rechtsdienst. In heikleren und grösseren Fällen erfolgt der Auftrag oft direkt von der Geschäftsleitung, dem Verwaltungsrat oder des → **Audit Committee**.

Die interne Untersuchung ist von operativen Kontrollen (*First Level of Defense*, teilweise *Second Level of Defense*), Audits (*Third Level of Defense*), der Vorbereitung auf einen Zivilprozess oder der Beantwortung von behördlichen Anfragen zu unterscheiden. Auch in diesen Fällen kommt es natürlich zu internen Abklärungen. Die interne Untersuchung ist mithin ein Führungsinstrument des Verwaltungsrats oder des Managements.

Worauf zu achten ist

- Die Mitarbeiter sind anzuweisen, wie sie sich korrekt zu verhalten haben und dass Fehlverhalten sanktioniert werden kann.
- Es sind Massnahmen zu treffen, um im täglichen Betrieb Fehlverhalten zu entdecken.
- Die Mitarbeiter müssen wissen, an wen sie sich wenden können und sollen, wenn sie merken, dass etwas nicht stimmt oder sich jemand nicht korrekt verhalten hat – und zwar ohne Angst vor Repression.
- Die Verantwortlichkeit, besser noch ein Prozess zur Durchführung interner Untersuchungen, sollte festgelegt sein, und zwar so, dass keine Interessenkonflikte entstehen und die Unabhängigkeit gewahrt bleibt.

Die Themen?

- Vermögensdelikte
- Korruption
- Kartellrecht
- Ungetreue Geschäftsführung
- Kapitalmarktrecht
- Steuerdelikte
- Datenschutz
- Sanktions- und Exportrechtsverstösse
- Sexuelle Belästigung, Mobbing
- Diskriminierung
- Geheimnisverrat
- Datendiebstahl

- Den Mitarbeitern muss klar sein (Reglement, Hinweis), dass ihr Arbeitgeber auf ihre persönlichen Daten (Postfach, Internet-Surfverhalten, persönliches Notebook) zugreifen kann, falls dies erforderlich sein sollte.
- Das Unternehmen muss im Fall der Fälle die für eine Untersuchung erforderlichen Daten sofort sichern können, damit keine Beweismittel verloren gehen.
- Vergessen Sie nicht Feedbacks an den oder die Hinweisgeber („Wir nehmen Euch ernst!“).

Liegen ernstzunehmende Hinweise auf Gesetzesverstösse vor, müssen diese grundsätzlich untersucht werden, damit laufende Verstösse beendet und künftige Verstösse durch das Treffen entsprechender Massnahmen verhindert werden können (zur internen „Verjährung“ → **Q17**); dies kann auch durch deren Sanktionierung erfordern. Dies ergibt sich im **Gesellschaftsrecht** aus der Pflicht des Verwaltungsrats und der Geschäftsleitung, die Interessen des Unternehmens zu wahren und ihre Aufgaben mit aller Sorgfalt zu erfüllen (Art. 717 Abs. 1 → **OR**). Dabei hat der Verwaltungsrat die Oberaufsicht über die Geschäftsleitung (Art. 716a Abs. 1 Ziff. 5 OR). Bereits 2007 hielt das Bundesgericht fest, dass bei Hinweisen auf eine falsche oder unsorgfältige Geschäftsführung – wozu auch die Verletzung von Gesetzen zählt – der Verwaltungsrat verpflichtet ist, „sogleich die erforderlichen Abklärungen zu treffen, nötigenfalls durch Beizug von Sachverständigen“

(BGer 4C.358/2005 vom 12. Februar 2017, E. 5.2.1). Auch die **arbeitsrechtliche Schutzpflicht** des Arbeitgebers und seine Schutzpflicht nach **Gleichstellungsgesetz** können zur Durchführung einer internen Untersuchung verpflichten, wenn Hinweise auf ein Fehlverhalten gegenüber Arbeitnehmern bestehen. Schliesslich kann ein Tolerieren von Fehlverhalten und das Nichtergreifen von Massnahmen zur Verhinderung weiterer Delikte auch zu einer **strafrechtlichen Verantwortlichkeit** und **zivilrechtlichen Haftung** der Geschäftsführung führen (vgl. BGE 142 IV 315, E. 2 ff.; Art. 11, 29 und 102 → **StGB**; Art. 6 Bundesgesetz über das Verwaltungsstrafrecht). Das **Aufsichtsrecht** erwartet im Rahmen des Grundsatzes der einwandfreien Geschäftsführung ebenfalls, dass Unregelmässigkeiten abgeklärt werden. Für gewisse Verstösse bestehen auch Meldepflichten (z.B. Art. 29 → **FINMAG**), die wiederum zu einer impliziten Pflicht führen können, die erforderlichen Abklärungen zu treffen.

Wie vorzugehen ist

1. **Weisen Sie die Mitarbeiter an, wie sie sich zu verhalten haben.** Dazu kann ein genereller Verhaltenskodex (sog. → **Code of Conduct**) gehören, aber auch spezifische Weisungen zu speziellen Themen (z.B. Korruption, sexuelle Belästigung, Kartellrecht, Export- und Sanktionsrecht, Berufsgeheimnis, Datensicherheit und Datenschutz). Die Mitarbeiter müssen wissen, welches Verhalten von ihnen erwartet wird und, dass Verstösse gegen die Regeln sanktioniert werden können.
In gewissen Bereichen lohnen sich auch Schulungsveranstaltungen (z.B. Umgang mit Dienstleistern und Geschäftspartnern zur Vermeidung von Vorwürfen der Korruption oder unerlaubter Absprachen).

Die Hitliste …

… der Verurteilungen im Bereich Wirtschaftsstrafrecht führte 2020 in der Schweiz die ungetreue Geschäftsführung und Veruntreuung an, gefolgt von Versicherungs- und Sozialhilfebetrug. Mehr zur KPMG-Studie: → **Q13**.

2. **Sorgen Sie dafür, dass die Einhaltung im Betrieb überwacht wird.** Ein Unternehmen sollte nicht nur Regeln erlassen, wie sich die Mitarbeiter zur Einhaltung von Gesetzen und anderen internen Vorgaben zu verhalten haben. Es sollte auch Massnahmen treffen, um die Einhaltung proaktiv sicherzustellen, also nicht erst auf Hinweise hin reagieren. Dazu gehören Massnahmen wie Protokolle, definierte Prozesse (die z.B. bei Dienstleistern eine bestimmte → **Due Diligence** erfordern), das Vier-Augen-Prinzip in heiklen Angelegenheiten, systematische oder stichprobenartige Prüfungen durch Mensch und Maschine (z.B. automatisierte Prüfung von Computerlogs, Finanztransaktionen, etc. auf verdächtige Muster). Dokumentieren

Sie diese Massnahmen; kommt es zu Unregelmässigkeiten, die durch die Maschen schlüpfen, können Sie immerhin zeigen, dass sich das Unternehmen sorgfältig organisiert hat.

> Gerade bei flächendeckenden, systematischen Überwachungen kommt dem **Datenschutz** eine besondere Rolle zu. Wer überwachen will, sollte möglichst viel automatisch dem Computer überlassen, so dass der Mensch nur bei Verdachtsmomenten, die sich anders nicht lösen lassen, Einblick nehmen muss. Überwachungen sollten angekündigt sein, mindestens in allgemeiner Form (z.B. über ein Reglement oder Hinweise). Sie müssen zeitlich und sachlich begrenzt sein. Vgl. auch → **ÜBERWACHUNGSMASSNAHMEN**.

3. **Schaffen Sie Meldestellen für Hinweise auf Missstände.** Die Mitarbeiter, unter Umständen aber auch Geschäftspartner, Kunden und andere externe Stellen, sollen wissen, an welche Stelle sie sich hinwenden können, wenn sie Hinweise auf Verstösse gegen geltendes Recht (oder ggf. auch unethisches Verhalten) haben. Gemeint ist ein Meldekanal im Unternehmen ausserhalb der üblichen Dienstwege, über den vermutete oder konkrete Missstände gemeldet werden können, damit das Unternehmen ihnen nachgeht (sog. → **Whistleblowing-Hotlines**). Für den Bereich der sexuellen Belästigung sollten innerbetrieblich besondere Anlaufstellen (sowohl ein Mann als auch eine Frau) kommuniziert werden. In grösseren Unternehmen werden häufig externe Dienstleister mit dem Betrieb eigener Kontaktstellen beauftragt, was aber auch für KMU sinnvoll sein kann (→ **Q7**). Es sollte ein Dienstleister gewählt werden, der eine anonyme Kommunikation mit dem Hinweisgeber ermöglicht (über ein Postfachsystem). Die Erfahrung in der Schweiz zeigt zwar, dass solche Kontaktstellen bei 40 bis 50 Prozent der Unternehmen kaum benutzt werden. Sie sind trotzdem ein wichtiges Instrument, um die Bemühungen eines Unternehmens zur Sicherstellung der Compliance zu demonstrieren. Mehr zum Nutzen von und der Erfahrung mit Meldestellen → **Q5**, zu den datenschutzrechtlichen Vorgaben → **Q6** und zur EU-Hinweisgeber-Richtlinie → **Q8**. Letztere sollten auch alle Schweizer Unternehmen mit Betrieben in der EU kennen. Weitere praktische Hinweise enthalten auch die in Kürze erscheinenden ISO-Empfehlung (kein Standard) für ein Whistleblowing Management System (ISO 37002).

Verbreitet

In einer Umfrage der HTW Chur von 2019 in der Schweiz, Deutschland, Frankreich und Grossbritannien gaben 59 Prozent der Unternehmen an, über eine Meldestelle zu verfügen. Je grösser das Unternehmen, desto eher besteht eine: → **Q5**.

Ein wichtiges Thema ist die **Möglichkeit anonymer Hinweise**. Sie können Meldungen fördern, aber erhöhen auch die Gefahr unberechtigter Vorwürfe. Datenschützer sehen sie daher kritisch und einige wenige Länder untersagen sie sogar. In der Schweiz sind sie erlaubt und die Erfahrung zeigt, dass Anonymität selten missbraucht wird. Anonyme Hinweise, jedenfalls ohne Belege, haben den Nachteil, dass sie schwieriger aufzuklären sind, wenn bei Fragen mit dem Hinweisgeber nicht kommuniziert werden kann. Oft erfolgt nur der Ersthinweis anonym und die Identität des Whistleblowers wird im Laufe der Untersuchung aufgedeckt (→ **Q5**). Es gibt auch technische Lösungen zur anonymen Kommunikation.

4. **Schaffen Sie Regeln zum Schutz von Hinweisgebern.** Besondere arbeitsrechtliche Bestimmungen zum Schutz von Hinweisgebern gibt es in der Schweiz zwar bisher nicht.[1] Unternehmen können trotzdem dafür sorgen, dass in guten Treuen handelnde Whistleblower geschützt werden. Dazu gehört, dass intern klar kommuniziert wird, dass Repressalien gegen Hinweisgeber sanktioniert werden. Auch ihre Anonymität sollte – soweit möglich – gewahrt werden. Ein Unternehmen wird jedoch nie Anonymität unter allen Umständen wahren können und sollte diese daher auch nie absolut zusichern. Insbesondere im Falle einer rechtlichen Auseinandersetzung wird die Identität des Whistleblowers mitunter offengelegt werden müssen, sowie bei bösgläubigen Anschwärzungen.

Nicht nur Repressalien gegen Hinweisgeber sind zu sanktionieren. Auch **missbräuchliche Meldungen** müssen geahndet werden. Die Erfahrung zeigt, dass weniger Missbrauch vorkommt, wenn das Unternehmen klar kommuniziert, dass es gegen einen solchen vorgehen wird. Gemäss einer Studie aus dem Jahr 2018 lag der Anteil missbräuchlicher Meldungen in Schweizer Meldestellen bei rund fünf Prozent (→ **Q5**).

5. **Schaffen Sie einen Prozess und Zuständigkeiten für interne Untersuchungen.** Liegt dem Unternehmen ein Hinweis für eine Unregelmässigkeit vor, muss klar sein, wer für dessen Bearbeitung zuständig ist, wer entscheidet, ob eine interne Untersuchung stattfindet, wer sie durchzuführen hat und an wen in welcher Form rapportiert wird. Es sollte ein alternativer Prozess bestehen, falls die Unregelmässigkeit die normalerweise in den Prozess involvierten Stellen betrifft. Häufig wird der Bereich Compliance mit der Durchführung von internen Untersuchungen beauftragt, mit Bezug auf Arbeitsplatzverhalten allenfalls das Personalwesen. Sind untere Hierarchiestufen oder klarerweise nur einzelne Per-

1 Eine entsprechende Gesetzesvorlage wurde vom Parlament zuletzt 2020 abgelehnt.

sonen betroffen, erfolgen interne Untersuchungen oft auf Entscheid und unter Aufsicht der Geschäftsleitung, doch wo auch diese selbst betroffen sein kann, wird typischerweise der Verwaltungsrat bzw. das → **Audit Committee** aktiv, um Interessenkonflikte zu vermeiden (→ **Q2**, auch zu Interessenkonflikten und zu ungewollten Informationsflüssen beim Untersuchenden). In solchen Fällen kann es sich aus demselben Grund auch empfehlen, für die Durchführung der Untersuchung auf externe, nicht der Geschäftsleitung unterstehende Spezialisten zurückzugreifen.

Extern geben?

Die wichtigsten Gründe für die Beauftragung externer Berater mit einer Untersuchung:

- Komplexität
- Ressourcen
- Unabhängigkeit, speziell, wenn das Management involviert sein könnte
- Glaubwürdigkeit
- Imagerisiko
- Anwaltsgeheimnis

Auch wenn einem *internen* Untersuchenden formal die Unabhängigkeit zugesichert wird, wird es für ihn häufig schwierig sein, potenziell auch gegen seine Vorgesetzten zu ermitteln. Das gilt erst recht, wenn noch nicht klar ist, ob und wer in der Geschäftsleitung in einer Sache möglicherweise involviert ist (→ **Q3**). Ob beim Einsatz externer Experten für eine interne Untersuchung auf Anwälte und Berater zurückgegriffen wird, die für das Unternehmen auch sonst bereits tätig gewesen sind (und es daher kennen) oder auf völlig unabhängige Dritte (auch ohne bekannte persönliche Beziehungen), muss von Fall zu Fall entschieden werden. Ist die Unabhängigkeit einer internen Untersuchung wichtig, etwa in medienträchtigen Fällen, empfiehlt es sich allerdings, *nicht* die Hauskanzlei, sondern eine unabhängige Stelle mit der internen Untersuchung zu beauftragen.

Wer für die Durchführung interner Untersuchungen zuständig ist, läuft mitunter Gefahr, im Unternehmen als die **interne „Polizei"** wahrgenommen zu werden. Das kann dem Aufbau einer offenen Unternehmenskultur entgegenstehen und die Umsetzung der Haupttätigkeit (z.B. für Compliance zu sorgen) entgegenstehen.

6. **Schaffen Sie ein Reglement für interne Untersuchungen.** Die Mitarbeiter sollten wissen, dass es zu internen Untersuchungen kommen kann und wie diese ablaufen, insbesondere mit welchen Mitteln untersucht werden kann (z.B. Einsichtnahme in E-Mails eines Mitarbeiters) und welche Rechte die verschiedenen Personen haben. Dies ist auch aus datenschutzrechtlicher Sicht wichtig (zu den Grenzen vgl. auch → **ÜBERWACHUNGSMASSNAHMEN**). In diesem Reglement kann auch der Umgang bzw. Schutz von Hinweisgebern geregelt werden.

7. **Sorgen Sie für einen sicheren Arbeitsbereich.** Wenn Sie eine Meldestelle für Hinweisgeber betreiben oder interne Untersuchungen durchführen, werden Sie einiges an sensiblen Informationen erhalten und verwalten müssen. Dazu brauchen Sie die nötige IT-Infrastruktur um diese sicher und vor dem Zugriff durch andere geschützt aufzubewahren. Sie sollten sich sogar überlegen, ob die sonst üblichen Zugriffsrechte seitens der IT-Abteilung in Ihrem Fall nicht eingeschränkt werden sollte. Sie müssen sicher per E-Mail kommunizieren können (d.h. bei Bedarf auch verschlüsselt) und Sie müssen über eine eigene Dateiablage verfügen. Sind Sie gut ausgerüstet, werden Sie auch über eine Geschäftsverwaltung bzw. ein System zur Verwaltung der Hinweise verfügen. Auch Ihre Büros sollten so gestaltet sein, dass Sie ungestört und vertraulich telefonieren können. Ein Grossraumbüro, das Sie mit anderen, nicht mit Untersuchungen betrauten Personen teilen, ist dafür nicht unbedingt geeignet.

   ☝ Vorsicht beim Versenden von E-Mails und Dokumenten mit sensiblen Informationen. Sie können versehentlich an den falschen Empfänger gelangen und auch der Zugriff auf fremde Postfächer des eigenen Unternehmens ist – wie Sie vielleicht aus eigener Erfahrung aus Untersuchungen wissen – technisch nicht sehr kompliziert. Arbeiten Sie vorzugsweise mit **Codenamen** und formulieren Sie Ihre E-Mails im Team oder im Verkehr mit Ihren externen Experten so, dass ein Aussenstehender damit möglichst wenig anfangen kann. Mitunter lohnt es sich auch einfach zum Telefon zu greifen. Dokumente mit sensiblen Inhalten werden vorzugsweise mit einem **Codeschutz** versehen; versenden Sie mehrere Dateien, bietet sich der Einsatz eines Passwort-geschützten ZIP-Files an.

8. **Sprechen Sie sich mit der Buchhaltung, Audit, etc. ab.** Unregelmässigkeiten werden dem Unternehmen oft nicht durch anonyme Tipps über eine Whistleblowing-Hotline bekannt, sondern indem im Rahmen der üblichen Kontrollen Verdachtsmomente auftauchen, z.B. im Rahmen einer Buchprüfung, der Ausführung von Zahlungen, einer Kontrolle von Lagerbeständen oder einem Personalgespräch. Daher sollten Mitarbeiter an entsprechenden Stellen im Betrieb (z.B. Audit, Buchhaltung) darin geschult werden, dass sie auf gewisse „*Red Flags*“ achten und wissen, wohin sie sich bei Verdachtsmomenten wenden können. Erfahrungsgemäss erhalten Compliance-Verantwortliche sehr viele Hinweise direkt in persönlichen Gesprächen (auch wenn diese nicht den Charakter von „Meldungen“ haben).

   ☝ Grössere Unternehmen und Unternehmen mit besonderen Risiken (z.B. für Korruption) sollten sich nicht nur auf die Aufmerksamkeit der Mitarbeiter verlassen, sondern auch technische Systeme einsetzen, welche **Unregelmässigkeiten** (z.B. im Zahlungs- oder E-Mail-Verkehr) **automatisch aufspüren** und entsprechende Hinweise geben können.

9. **Etablieren Sie Kontakt zu den erforderlichen Experten.** Kommt es zu einer internen Untersuchung, muss normalerweise rasch gehandelt werden und es bleibt keine Zeit, ein Auswahlverfahren für die nötige externe Unterstützung durchzuführen. Sie sollten daher bereits wissen, welchen Anwalt oder sonstigen Experten[2] Sie im Bedarfsfall kontaktieren und welche IT-Forensiker sie beiziehen, wenn es gilt, Beweise zu sichern oder elektronische Ermittlungen zu unternehmen. IT-Forensiker können Ihnen auch helfen, Ihre Systeme so vorzubereiten, dass eine Sicherung der Daten einfach möglich ist. Bei der Auswahl eines Anwalts ist nebst der Praxiserfahrung im Bereich interner Untersuchungen vor allem sein Augenmass wichtig, denn eine Kostenkontrolle ist für den Klienten oft schwierig bis unmöglich, will er sich doch nicht den Vorwurf einhandeln, die Untersuchung behindert zu haben. Viel wichtiger als eine Diskussion von Stundensätzen ist es daher ein Gefühl dafür zu bekommen, welche Untersuchungsmassnahmen ein Anwalt kennt und einsetzt – ob er beispielsweise jeweils gleich einen umfangreichen → **Review** von Dokumenten anordnet (= erheblicher Kostentreiber) oder stattdessen prüft, ob es andere Ermittlungsmethoden gibt, die schneller und günstiger zum Ziel führen. In formaler Hinsicht sollten Sie im Falle des Beizugs von Anwälten, Audit-Firms und anderen Beratern, ferner deren Vertragsbedingungen frühzeitig klären (und ggf. Anpassungen vornehmen, etwa was die Möglichkeit der Verwendung der Arbeitsergebnisse betrifft, die Vertraulichkeit und die Haftung) sowie in Erfahrung bringen, wie sie mit der Prüfung von Interessenkonflikten umgehen. Letztere kann insbesondere bei grossen Beratungsgesellschaften und Kanzleien eine gewisse Zeit dauern, welche Sie im Fall der Fälle vielleicht nicht haben und daher eine Alternative benötigen.

> **IT-Support?**
>
> Die meisten Unternehmen sind nicht in der Lage, eine grössere interne Untersuchung IT-mässig zu unterstützen, da diese in der Regel spezielle Systeme für die Aufbereitung und Sichtung von Daten erfordern.

> Für viele Unternehmen in der Schweiz ist das **Anwaltsgeheimnis** der Grund, warum sie mit der Durchführung einer internen Untersuchung einen Schweizer Anwalt und nicht ein sonstiges Beratungsunternehmen beauftragen. Genau genommen geht es um das in Schweizer und ausländischen Prozessgesetzen festgehaltene sog. → **Legal Privilege**, welches davor schützt, dass Korrespondenz mit dem eigenen Anwalt oder dessen Arbeitsprodukte in einem allfälligen Verfahren offengelegt werden müssen.

2 Neben einem Anwalt bzw. einer Anwaltskanzlei kann es sich ebenfalls anbieten einen anderen Untersuchungsspezialisten (z.B. einen Wirtschaftsprüfer) oder eine spezialisierte Investigation-Boutique zu beauftragen.

Das *Legal Privilege* gilt bei einem herkömmlichen Berater nicht. Allerdings hat die Rechtsprechung in der Schweiz inzwischen betont, dass Korrespondenz und Arbeitsprodukte von Anwälten nur im Rahmen der *anwaltstypischen* Tätigkeit diesen Schutz geniessen (und diese sehr eng verstanden wird) und zum Beispiel nicht, wenn eine Anwaltskanzlei lediglich die Funktion der ausgelagerten Geldwäschereistelle einer Bank erfüllt (→ **Q10**); die Anwälte müssen zudem nach → **BGFA** zugelassen sein. In den USA wird wiederum regelmässig zwischen Rechtsrat und Ermittlung des Sachverhalts unterschieden. Was im Rahmen einer Untersuchung von den Anwälten an E-Mails sichergestellt wird, geniesst kein *Legal Privilege*, wie die Anwälte die einzelnen E-Mails bewerten hingegen schon.

10. **Bereiten Sie sich in technischer Hinsicht vor.** Kommt es zu einer internen Untersuchung, wird es sehr häufig zu einer Sichtung von E-Mails und anderen elektronischen Daten kommen. Solche mutmasslichen Beweismittel müssen zu Beginn sehr schnell gesichert (*"preserved"*) werden, damit sie nicht vernichtet werden können oder sonst verloren gehen. Darum sollten Sie wissen, wo und wie Sie bei Bedarf veranlassen können, dass E-Mails bestimmter Personen und andere elektronische Daten (z.B. Dokumentenablage, Kommunikationsaufzeichnungen) so lange gesichert werden, bis klar ist, dass sie nicht mehr benötigt werden. Klären sie auch, ob und wie diese Daten für eine Sichtung eingesammelt und bereitgestellt werden können (d.h. über Funktionen für ein sog. → **eDiscovery** verfügen; zu Microsoft 365 vgl. → **Q55**). Entsprechende Möglichkeiten sollten bereits bei der Anschaffung neuer Systeme (z.B. E-Mail-Services in der Cloud, Kommunikationssysteme wie z.B. Chats, Messaging, Videokonferenzen, neue *Tools*) berücksichtigt werden, da manche dieser Systeme noch nicht in verwertbarer Form dokumentieren, wer sie wie und wozu benutzt hat (→ **WERKZEUGE FÜR EDISCOVERY**). Nicht zu vergessen sind auch mobile Systeme, die den Mitarbeitern zur Verfügung gestellt oder von diesen selbst mitgebracht werden, und ebenfalls relevante Daten enthalten können. Sie sollten sich daher mit Ihren Spezialisten Gedanken darüber machen, wie Sie im Fall der Fälle auch bei diesen Geräten an Ihre Daten kommen (vgl. auch → **Q20**).

Wilde Systeme

Sorgen Sie mit Weisungen und Sperren dafür, dass Mitarbeiter am Arbeitsplatz keine „wilden", von Ihnen nicht kontrollierten Systeme für geschäftliche Daten einsetzen (z.B. Systeme für den Datenaustausch wie DropBox). Die Verhinderung solcher Schattensysteme ist allerdings oft eine Herausforderung.

Im angelsächsischen Rechtsraum müssen Unternehmen immer dann, wenn vernünftigerweise mit einem Rechtsstreit zu rechnen ist, dafür sorgen, dass im Unternehmen keine potenziellen Beweismittel mehr vernichtet werden. Dies wird durch eine firmeninterne Anordnung eines **Vernichtungsstopps** (sog. → **Legal Hold**) umgesetzt, was in grösseren Unternehmen heute automatisiert möglich ist (z.B. um mehrere parallele *Legal Holds* zu verwalten oder die Kenntnisnahme sicherzustellen und zu dokumentieren). Ähnliches wird auch im Falle von Behördenanfragen oder internen Untersuchungen erwartet. Bei internen Untersuchungen ist teils von einem ***„Investigation Hold"*** die Rede. Weitere Informationen zum *Legal Hold* befinden sich in Kapitel 3 Ziff. 15.

11. **Filtern Sie relevante Fälle.** Verdachtsmeldungen in Bezug auf Unregelmässigkeiten und Fehlverhalten wird es immer wieder geben. Allerdings sind bei weitem nicht alle davon relevant. Eine interne Untersuchung ist grundsätzlich nur dann erforderlich, wenn ein konkreter Hinweis auf einen Verstoss gegen geltendes Recht oder gegen interne Regeln vorliegt. Um dies abzuklären, kann eine kleine „Voruntersuchung" angezeigt sein, sofern sie sich ohne grossen Aufwand, in kurzer Zeit und diskret durchführen lässt. In deren Rahmen wird geprüft, ob sich ohne Weiteres weitere Anhaltspunkte für oder gegen ein Fehlverhalten ergeben (z.B. durch eine Nachfrage in der Buchhaltung, ob eine angebliche Zahlung tatsächlich erfolgt ist) und ob vorgelegte Beweismittel authentisch sind (z.B., ob ein Beleg tatsächlich aus dem Unternehmen stammt). Dabei ist zu bedenken, dass Anschuldigungen oder Verdächtigungen – bewusst oder unbewusst – unberechtigt und damit rufschädigend sein können. Falls sich zeigen sollte, dass ein Mitarbeiter zu Unrecht angeschwärzt wird und dies bösgläubig oder regelmässig erfolgt (z.B. über ein sich hartnäckig haltendes Gerücht), muss das Unternehmen aufgrund seiner arbeitsrechtlichen Treuepflicht ebenfalls Massnahmen zum Schutz der betreffenden Person ergreifen. Zur Frage, ob Sie einem Hinweis nicht nachgehen müssen, weil die Sache zu lange zurückliegt („interne Verjährung") vgl. → **Q17**.

Sofort prüfen

Geht ein Hinweis ein, sind umgehend Sofortmassnahmen zum Schutz von Arbeitnehmern oder des Unternehmens zu prüfen. Aber Vorsicht vor einer Vorverurteilung!

Führen Sie ein **Protokoll** über die Hinweise auf Unregelmässigkeiten, wie Sie damit umgegangen sind und was sich ergeben hat – auch wenn es nicht zu einer internen Untersuchung kommt. Das kann später wichtig werden, wenn es darum geht, dass Sie Ihren Pflichten nachgekommen sind. In kleinen Verhältnissen können Sie dazu eine zugriffsgeschützte Excel-Datei benutzen, in grösseren Unternehmen lohnt sich unter Umständen der Einsatz eines Case-Management-Systems.

12. **Gehen Sie auch anderen Hinweisen nach.** Nicht immer wird Ihnen ein Verdacht von einer involvierten Person gemeldet werden. Hinweise können Ihnen auch anders zu Ohren kommen, sei es über betriebsinterne Gerüchte oder Berichte in den Medien. Auch solchen Hinweisen sollte, wenn sie nicht aus der Luft gegriffen erscheinen oder zum „üblichen" Tratsch gehören, nachgegangen werden. Dies sollte ergebnisoffen geschehen: Es geht nicht nur um die Erhärtung eines Verdachts. Die arbeitsrechtliche Treuepflicht gebietet ebenso, falsche Gerüchte bezüglich konkreter betroffener Arbeitnehmer zu entkräften, wenn diese die Person in ihrer Persönlichkeit verletzen.

13. **Geben Sie Feedback.** Ein Unternehmen wird nur dann Hinweise auf Unregelmässigkeiten erhalten, wenn die betreffenden Mitarbeiter und anderen Hinweisgeber den Eindruck haben, dass das Unternehmen sie ernst nimmt. Darum ist es wichtig, dass auf entsprechende Meldungen schnell reagiert wird und die Hinweisgeber – soweit dies möglich ist – ein Feedback erhalten, auch wenn dies zu Beginn in der Sache nicht möglich sein wird. Betreiber von professionellen → **Whistleblowing-Hotlines** bieten hierzu bidirektionale, aber anonyme Kommunikationsmöglichkeiten. Damit können dem Hinweisgeber auch Fragen gestellt werden, wenn seine Meldung nicht genügt, um festzustellen, ob ein Fehlverhalten vorliegt. Ein Feedback nach Abschluss einer Untersuchung ist ebenfalls wichtig und sinnvoll, auch wenn hier natürlich auch die Datenschutzinteressen der Beschuldigten berücksichtigt werden müssen.

Die **beschuldigte Person** sollte bei gewichtigen oder sonst ernstzunehmenden Anschuldigungen aus Gründen des Persönlichkeitsschutzes auch dann informiert werden, wenn sich die Anschuldigungen **als falsch erweisen** und es gar nicht erst zu einer internen Untersuchung kommt. Kommt es zu einer internen Untersuchung, wird sie ohnehin angehört werden müssen.

14. **Erstatten Sie regelmässig Bericht.** Auch wenn es zu keiner internen Untersuchung kommt, sollte die Unternehmensführung – Geschäftsleitung und Verwaltungsrat – wissen, wie es um die → **Compliance** des Unternehmens steht und wie es mit etwaigen Verstössen gegen solche umgeht. In der Praxis bewährt hat sich z.B. in grösseren Unternehmen, dass die Compliance-Stelle dem Verwaltungsrat

jährlich Bericht über Hinweise und etwaige Untersuchungen von gewichtigeren Unregelmässigkeiten und Verstössen erstattet.

15. **Bereiten Sie sich auch auf die persönlichen Herausforderungen einer internen Untersuchung vor.** Sie werden damit rechnen müssen, Druck von allen Seiten ausgesetzt zu sein und manchen schwierigen Situationen begegnen. Mehr zu den persönlichen Herausforderungen: → **Q1**.

Do's	Don'ts
• Hinweise auf Unregelmässigkeiten sind zum Schutz aller Beteiligter streng vertraulich zu behandeln. • Vermeiden Sie Bezeichnungen, welche das Ergebnis einer Untersuchung bereits vorwegnehmen wie z.B. „Täter" oder „Opfer", wie dies oft bei angeblichem Mobbing oder angeblicher sexueller Belästigung geschieht. Sie können von „Beschuldigtem", „Hinweisgeber", „Melder" oder „anschuldigender Person" sprechen. • Wenn strittig ist, ob untersucht werden soll, dann sichern Sie sich ab: Zu entscheiden hat am Ende der Verwaltungsrat. • Stellen Sie sicher, dass in internen Reglementen oder Hinweisen auf die Möglichkeit von Überwachungs- und Untersuchungsmassnahmen (z.B. Einblick in E-Mails) in allgemeiner Form hingewiesen wird. • Sichern Sie sich und ihre Arbeit mit den nötigen Reglementen ab – eine interne Untersuchung führt meist zu Spannungen und unangenehmen Situationen, und Sie sind mittendrin.	• Versprechen Sie Mitarbeitern oder anderen Personen nie absolute Geheimhaltung oder Anonymität. Sie werden ein solches Versprechen nicht unbedingt einhalten können. • Die Behandlung von Hinweisen auf Unregelmässigkeiten gehört nicht in die Linienorganisation des jeweiligen Bereichs – ihr fehlt die nötige Unabhängigkeit. • Lassen Sie Hinweise auf Unregelmässigkeiten nicht liegen. • Beauftragen Sie in heiklen Fällen nicht Ihre Hauskanzlei oder sonst eine Kanzlei, zu welcher enge persönliche Beziehungen bestehen. Dies wird in der Öffentlichkeit sehr kritisch aufgenommen und schadet letztlich der Glaubwürdigkeit aller Beteiligten.

Do's	Don'ts
• Erhalten Sie Verdachtsmeldungen auf Verstösse, so prüfen Sie, ob Sofortmassnahmen zum Schutz betroffener Arbeitnehmer (z.B. Versetzung an einen anderen Arbeitsplatz) oder des Unternehmens (z.B. Beweissicherung, Zahlungsstopp) nötig sind. • Persönlichkeitsverletzende Gerüchte über bestimmte Arbeitnehmer können den Arbeitgeber verpflichten, an ihrer Entkräftung mitzuwirken. • Sorgen Sie dafür, dass Ihre Informationen und Ihre Kommunikation zu einer internen Untersuchung auch betriebsintern vor fremden Zugriffen geschützt sind (z.B. durch sichere Dateiablagen). Verwenden Sie Codenamen und Verschlüsselungen bzw. einen Passwortschutz für Dokumente.	

Wann Sie externe Unterstützung beiziehen sollten

- Für **grössere oder komplexere Fälle**, für welche Ihnen die Expertise oder die Ressourcen fehlen.
- Für **internationale Fälle**, in denen es Anwälte in verschiedenen Rechtsordnungen zu koordinieren gibt.
- In Fällen, in denen sich **möglicherweise (auch) das Management falsch verhalten hat** und es daher nötig ist, dass jemand den Fall untersucht, der den betreffenden Personen nicht unterstellt ist (Unabhängigkeit).
- In Fällen, in denen die **Unabhängigkeit der Untersuchung** wichtig ist, insbesondere wo Aufsichtsbehörden oder die Öffentlichkeit involviert sind.
- Wenn Sie noch **nie eine interne Untersuchung** durchgeführt haben, jetzt aber mit einer solchen konfrontiert sind, die sich nicht wirklich zum Üben eignet.

- Wenn Sie sich intern auf diese Weise besser **absichern** können.
- Für die **forensische Sicherung von Beweisen** (z.B. Spiegelungen von Notebooks).
- Für den **Betrieb von eDiscovery-Systemen** (d.h. Systeme zur Durchführung von Dokumenten-Reviews).
- Wenn Sie **rechtlichen oder technischen Rat** benötigen.
- Wenn sich der Beizug eines externen Untersuchers aus **taktischen Gründen** aufdrängt (weil er z.B. effektivere Befragungen durchführen kann oder er der Untersuchung mehr Gewicht verleiht).
- Wenn Sie von unabhängiger Seite prüfen lassen wollen, ob Sie hinreichend vorbereitet sind oder **Unterstützung bei der Vorbereitung** benötigen.
- Wenn Sie eine **Whistleblowing-Hotline** betreiben lassen wollen.

Häufige Fragen und Antworten

Q1. Welche persönlichen Herausforderungen erwarten mich im Rahmen einer internen Untersuchung?

A: Vorweg lässt sich sagen: Es werden sich im Rahmen einer internen Untersuchung zahlreiche Herausforderungen stellen. Eine interne Untersuchung hat viele „Mitspieler". Einige davon verfolgen ihre höchstpersönlichen Interessen, andere handeln im Interesse des Unternehmens oder eines Dritten. Dabei wird Ihnen kaum einer der Personen mitteilen, worum es ihm oder ihr wirklich und ausschliesslich geht. Oder Sie werden der Person nicht glauben (können). Sie werden im Verlauf der internen Untersuchung rasch realisieren: Eine interne Untersuchung kann für erhebliche Verunsicherung in einem Betrieb sorgen und viele Personen dazu verleiten, sich still und unauffällig oder einfach mal „anders" zu verhalten. Dieses Verhalten kann in genereller Weise auftreten oder sich auch direkt gegen Sie als Person richten.

Auch wenn allen Beteiligten klar ist, dass es in gewissen Situationen ohne ihre Mitwirkung nicht geht, sind interne Untersuchungen – ausser vielleicht für jene Personen, die sie durchführen – eine normalerweise unangenehme und lästige Erscheinung: Solche Untersuchungen fressen Zeit, sie bergen persönliche Risiken und sie können Aussagen oder Massnahmen erforderlich machen, die jeder von uns gerne vermeiden möchte. Und überdies kosten sie sehr viel Geld, das im Budget üblicherweise nicht vorgesehen war.

Sie als untersuchende Person stehen im Zentrum der Aktivitäten und „zwingen" die Beteiligten dazu, sich mit einer unangenehmen Sache auseinanderzusetzen. Sie dürfen sich nicht wundern, wenn Ihnen keine Freude entgegenschlägt oder Sie unter Umständen sogar als interne „Polizei" wahrgenommen werden. Wundern Sie sich auch nicht, wenn Ihre Tätigkeit Angst und Stress verursacht (→ **Q41**).

Gewisse Personen können sehr gut damit umgehen, dass ihre Tätigkeit für negative Gefühle sorgt, anderen bereitet es wiederum selbst Mühe, denn sie wollen zwar ihre Arbeit richtig machen, aber unangenehmen Themen, Begegnungen und Massnahmen aus dem Weg gehen. Es ist für viele beispielsweise nicht einfach,

- einem Mitarbeiter zu erklären, dass Sie nun seine persönliche Mailbox sichten müssen,
- jemanden zu einer möglicherweise sexuellen Verhaltensweise gegenüber einer anderen Person am Arbeitsplatz befragen zu müssen, oder
- einen Mitarbeiter mit Beweisen für ein Fehlverhalten zu konfrontieren, welches ihn voraussichtlich nach langjährigem, treuem Einsatz für die Firma seinen Job kosten und in eine tiefe, persönliche Krise stürzen wird.

Sie selber wissen in dem Moment (noch) nicht in welcher, vielleicht schwierigen Lebenslage sich Ihr Gegenüber befindet.

Es ist allerdings erfahrungsgemäss gut, wenn Ihnen dies nicht allzu leicht von der Hand geht, denn Mitgefühl oder Empathie, d.h. die Fähigkeit, sich in die Gefühlslage des anderen hineinversetzen zu können, sind wichtige Voraussetzungen für den richtigen Umgang mit anderen Menschen – und damit auch für eine erfolgreiche interne Untersuchung. Diesem Aspekt wird leider nach wie vor zu wenig Aufmerksamkeit geschenkt. Denn ungeachtet der vielen technischen Hilfsmittel, geht es in einer internen Untersuchung immer um Menschen und ihr allzu menschliches Verhalten. Gehen Sie zwar hart in der Sache, aber trotz allem umsichtig und respektvoll mit den beteiligten Personen – auch der beschuldigten Person – um. So wird es auch Ihnen selbst viel einfacher fallen, Ihre Arbeit korrekt, unvoreingenommen und ohne eigene Beeinträchtigungen durchzuführen. Zudem haben auch Sie „ein Berufsleben nach der Untersuchung“ in Ihrem Unternehmen. Wer aufrichtig, korrekt, ethisch erklär- und vertretbar handelt, stärkt je nach Situation seine Wahrnehmung sogar.

Sie werden womöglich damit konfrontiert werden, dass die menschlichen Herausforderungen nicht nur den Umgang mit der beschuldigten Person betreffen können, sondern weit darüber hinaus zu gehen vermögen. Das trifft vor allem dort zu, wo ein Fall grössere Kreise zieht. Als untersuchende Person können Sie – je nach Dimension und Virulenz des Falls – zahlreichen externen und internen Einflüssen ausgesetzt sein:

- Inländische, womöglich aber auch ausländische Aufsichtsbehörden erwarten von Ihrem Arbeitgeber, dass er einen Fall aufklärt. Unter Umständen haben sich bereits Strafverfolgungsbehörden eingeschaltet. Alle wollen so rasch wie möglich informiert und bedient werden, senden Ihrem Unternehmen ihre Fragen und verlangen die Herausgabe von Unterlagen. Und alle wollen prioritär (und sicher nicht erst nach den anderen Behörden) bedient werden. Es werden Fristen gesetzt. Das Management gibt den Druck an Sie weiter.

- Die Medien haben vom Fall Wind bekommen. Informiert Ihr Arbeitgeber nicht offen und ehrlich, oder glauben die Journalisten, dass er dies nicht tut, werden die Medien selbst ermitteln und sich Quellen suchen, die bereit sind zu „plaudern". Und eines ist gewiss: Die Medienschaffenden werden dabei fast immer fündig werden. In der Folge kommen neue Details ans Licht, was wiederum neue Fragen von Behörden und der Öffentlichkeit provoziert. Schaltet sich die Politik ein, steigt der Druck zusätzlich. Das Management gibt den Druck an Sie weiter, will ebenfalls wissen, ob das, was da in den Medien zu lesen ist, richtig ist und wie diese davon erfahren konnten.
- Brennt es, will auch das Management des Unternehmens wissen, woran es ist. Dieses will eine Krise möglichst schnell hinter sich bringen, will handeln und Massnahmen treffen. Dazu bedarf es Fakten. Gewisse Personen im Management werden verstehen, dass eine saubere Aufklärung ihre Zeit braucht. Andere werden nicht so lange warten wollen und Sie zu vorschnellen Antworten und Einschätzungen drängen, auf deren Basis gehandelt wird. Sie verlieren möglicherweise mehr Zeit in Diskussionen mit dem Management als mit ihrem Team, welches die Untersuchung durchführen soll – falls Sie überhaupt eines haben.
- Vielleicht will das Management aber nichts wissen, hält Sie für übereifrig oder überkorrekt. Auf dem Papier (oder in einer E-Mail) wird Ihnen zwar niemand sagen, dass Sie beide Augen zudrücken sollen. Für Sie ist jedoch klar, dass vom Management ein Schönwetterbericht verlangt und eine vertiefte Untersuchung als Zeitverschwendung beurteilt wird. In Geschäftsleitungsprotokollen wird das Thema möglicherweise bewusst nicht oder kaum verzeichnet (Stichwort *"plausible deniability"*). Sie sind selbst hin- und hergerissen, denn Ihre Einschätzung der Rechts- oder Risikolage ist eine andere als jene des Managements. Es stellen sich zahlreiche Fragen: Was tun Sie in einer solchen Situation? An wen wenden Sie sich? Wie gehen Sie mit Ihren Bedenken und Empfehlungen karriereverträglich *"on record"*, damit Ihnen später kein Vorwurf gemacht werden kann, falls die Bombe explodieren sollte?
- Einzelne Personen werden eine interne Untersuchung möglicherweise auch als gute Gelegenheit für eigene, innenpolitische Manöver betrachten und Sie mehr oder weniger geschickt zu instrumentalisieren versuchen.
- Merken Ihre Kollegen im Unternehmen, dass Sie ermitteln und sich die Ermittlung möglicherweise gegen jemand aus ihrer Mitte richtet oder gegen eine ganze Gruppe von Personen, wird man Sie dies spüren lassen. Ist der Betrieb hinreichend gross, wird Sie das nicht stören. Nichtsdestotrotz macht es Ihre Arbeit nicht leichter, wenn sich das Umfeld der beschuldigten Person mit ihr solidarisiert und unter Umständen Ihre Untersuchung zu sabotieren versucht. Im schlimmsten Fall können Sie selbst zum neuen Feindbild werden.

- Auch jene, die nichts zu „befürchten“ haben, werden keine Freude an Ihnen haben. Der IT bescheren Sie womöglich einiges an Zusatzaufwand, weil dieses für Sie alle Arten von Daten bereitzustellen hat – und zwar umgehend. Die Vorgesetzten der von einer internen Untersuchung betroffenen Personen werden wiederum nicht goutieren, dass ihre Mitarbeiter aufgrund dessen abgelenkt werden oder nicht mehr vollständig verfügbar sind, um ihre tägliche Arbeit zu erledigen.
- Ist eine Person freigestellt, so leiden die verbliebenen Personen, denn sie müssen deren Arbeit nun ebenfalls übernehmen. Dabei kommt womöglich die Frage auf: Wen trifft es als nächstes?
- Und bei jeder Person, welche Sie um Auskunft oder Mitwirkung auffordern, werden Sie sich die Frage stellen müssen, ob diese Sie aufrichtig und ehrlich unterstützt oder, ob Sie Ihnen etwas „vorspielt“ – sei es, um sich selbst zu schützen, jemand anderen oder weil Sie Ihnen einfach nicht vertraut.

Hinzu kommt der Druck, den Sie sich selbst machen oder machen müssen, wenn Sie im Rahmen einer Untersuchung unter Zeitdruck Entscheide treffen müssen, die gewichtige Konsequenzen haben können – sei es in der Sache, sei es finanzieller Art (z.B. wenn über die Durchführung eines linearen Reviews entschieden werden muss). Hierbei können Aspekte übersehen werden, eine Situation wird falsch eingeschätzt oder es geschehen Fehler. All dies ist bis zu einem gewissen Grad normal, sorgt aber für Druck.

Wohlgemerkt: Diese Beschreibung zeichnet ein negativeres Bild, als es manche (hoffentlich) in diesem Metier erleben werden. Ob und wie vielen solcher negativen Erfahrungen Sie in Ihrem eigenen Unternehmen tatsächlich ausgesetzt sein werden, hängt letztlich stark von dessen Unternehmens, Compliance- und Führungskultur ab. Die Bandbreite ist in der Praxis erfahrungsgemäss gross. Dies ändert aber nichts daran, dass Sie im Rahmen von internen Untersuchungen immer einigem Druck ausgesetzt sein werden – von oben, unten und von der Seite. Es ändert auch nichts daran, dass Sie jederzeit damit rechnen müssen, dass interne und externe Personen Sie zu manipulieren oder instrumentalisieren versuchen werden.

Vor diesem Druck sind auch externe Untersuchende, wie etwa Anwälte, nicht gefeit. Der zuständige Partner in der eigenen Kanzlei hat Erwartungen an seine Mitarbeiter, die Klienten haben Erwartungen an ihre Anwälte. Das mag vielleicht nicht ausgesprochen werden, aber kann zweifellos in jenen Fällen ein Thema sein, in welchen eine Kanzlei nicht nur für die betreffende Untersuchung beigezogen, sondern regelmässig für diesen Klienten tätig wird. Aber selbst dort, wo dies nicht der Fall ist, gibt es oftmals Druck: Der Klient will Ergebnisse sehen, lieber früher als später, auch wenn sich gut erklären lässt, dass eine fundierte Untersuchung ihre Zeit braucht.

Mit all dem müssen Sie lernen umzugehen. Hierzu ist es erforderlich, sich selbst hinreichend gut zu kennen, zu verstehen, wie Sie mit einem politischen Umfeld (welches ein

Unternehmen zumindest auf der Führungsebene immer bis zu einem gewissen Masse ist) umgehen können und welche Strategien für Sie funktionieren. Seien Sie sich jedoch auch bewusst, dass Sie selber „nur" ein Mensch sind, der unterschiedlichen Tagesformen sowie Gefühl- und Gemütszuständen unterworfen ist. Sie werden sich auch nie nur „auf die Sache" konzentrieren können. Das ist allerdings heutzutage in grösseren Unternehmen und ab einer gewissen Hierarchiestufe normal. Rechnen Sie jedenfalls damit, dass Sie auch im Bereich der internen Untersuchungen sowohl Himmel- als auch Höllegefühle erleben werden. Und trotzdem, Sie werden in kaum einer anderen Situation die Möglichkeit haben, so viel auf einmal zu erleben und zu lernen. Nehmen Sie sich deshalb nach einer Untersuchung Zeit für eine Reflexion und Feedbacks.

Q2. Wer ist für den Entscheid über interne Untersuchungen zuständig – die Geschäftsleitung oder der Verwaltungsrat?

A: Für die tatsächliche Zuständigkeit des Entscheids über eine interne Untersuchung sind die jeweiligen **Verhältnisse des Unternehmens** im Einzelfall (Grösse, rechtliche Ausgestaltung, Risikoprofil, Geschäftstätigkeit sowie Tragweite des Vorfalles) zu beachten.

Ist das Unternehmen als **Aktiengesellschaft** ausgestaltet, kommt dem Verwaltungsrat die **Pflicht zur Oberleitung** über das Unternehmen zu (Art. 716a Abs. 1 Ziff. 1 OR). Der Verwaltungsrat ist in seinem Handeln stets dem **Interesse des Unternehmens** verpflichtet. Missstände oder Norm- bzw. Gesetzesverstösse, welche das reibungslose Funktionieren des Unternehmens beeinträchtigen, sind entsprechend aufzuklären. Obschon der Verwaltungsrat das Tagesgeschäft der Geschäftsleitung delegieren kann, verbleibt die Oberaufsicht über die Geschäftsführung beim Verwaltungsrat (Art. 716a Abs. 1 Ziff. 5 OR). Der Verwaltungsrat haftet für die Verletzung seiner gesetzlich auferlegten Pflichten (Art. 754 OR).

Aufgrund seiner umfassenden Pflichten gegenüber dem Unternehmen, ist es letztlich der **Verwaltungsrat**, der über die Durchführung einer internen Untersuchung entscheidet (bzw. dies seinem → **Audit Committee** überlässt). Das gilt insbesondere dann, wenn nicht klar ist, ob und inwieweit die Geschäftsleitung in die Angelegenheit involviert ist oder ihr bzw. ihren Mitgliedern ein Fehlverhalten anzulasten ist oder ein Interessenkonflikt bestehen könnte. Handelt es sich um einen weniger komplexen Fall, insbesondere dort, wo klar ist, dass es um das Fehlverhalten einer einzelnen Person geht (z.B. Datendiebstahl, sexuelle Belästigung, Mobbing am Arbeitsplatz), kann die Geschäftsleitung über eine interne Untersuchung entscheiden.

Auf **Interessenkonflikte** ist freilich nicht nur beim Entscheid über die interne Untersuchung zu achten, sondern auch bei der Stelle, die mit deren Durchführung betraut wird. Ein Beispiel: Der Rechtsdienst ist im normalen Tagesgeschäft mit der Prüfung von Verträgen von Lieferanten und Dienstleistern betraut. Im Falle einer Korruptions-

untersuchung, welche solche Lieferanten oder Dienstleister betrifft, kann sich u.a. die Frage stellen, ob deren Verträge hinreichend genau geprüft worden sind. Für die Korruptionsuntersuchung wird es nicht ratsam sein, eben diesen Rechtsdienst damit zu beauftragen. Zu beachten sind auch **ungewollte Informationsflüsse** im Büro. Wer eine interne Untersuchung durchführt, wird dies vor seinem Büronachbarn kaum verheimlichen können. Darum ist auch in technischer und organisatorischer Hinsicht dafür zu sorgen, dass die nötige Vertraulichkeit gewahrt bleiben kann.

Literatur:

Götz Staehelin, Claudia Unternehmensinterne Untersuchungen, Zürich/Basel/Genf 2019

Romerio, Flavio/Bazzani, Claudio/Groth, Stephan: Interne und regulatorische Untersuchungen – Einführung und Auslegeordnung / III. Entscheid über die Eröffnung einer Untersuchung (Konstituierung I), in: Romerio, Flavio/Bazzani, Claudio (Hrsg.), Interne und regulatorische Untersuchungen, Zürich 2015

Q3. Wenn die Geschäftsleitung potenziell involviert ist, soll dann zuerst „frei ermittelt“ werden?

A: Nein, der Sachverhalt ist so zu ermitteln, wie es in der Sache angezeigt ist. Steht nicht ein Fehlverhalten der Geschäftsleitung im Vordergrund, sondern „nur“ die Beteiligung bzw. das Mitwissen einzelner ihrer Exponenten, so wird der Sachverhalt ohnehin zuerst an anderer Stelle ermittelt werden müssen (z.B., ob es systematisch zur Verletzung bestimmter gesetzlicher Vorgaben gekommen ist). Erst wenn der Sachverhalt feststeht, wird sich normalerweise die Frage stellen, welches Mitglied der Geschäftsleitung worüber informiert war und ob und in welcher Weise zum Fehlverhalten aktiv oder passiv beigetragen hat.

Q4. Welche besonderen Vorkehrungen sind im Zusammenhang mit sexueller Belästigung zu treffen?

A: Der Arbeitgeber hat im Zusammenhang mit → **sexueller Belästigung** gewisse Vorkehrungen im Unternehmen zu treffen. Dies folgt aus seiner gesetzlich verankerten Fürsorgepflicht (Art. 328 OR) und dem → **Gleichstellungsgesetz** (welches in Art. 4 die Diskriminierung durch sexuelle Belästigung regelt).

- **Präventionsmassnahmen:** Zunächst einmal hat der Arbeitgeber sexuelle Belästigung zu verhindern. Es sind präventive Massnahmen zu treffen um die Mitarbeiter vor sexueller Belästigung zu schützen. Der Arbeitgeber hat dafür zu sorgen, dass im Unternehmen, eine **Unternehmenskultur** herrscht, welche sexuelle Belästigung gar nicht erst aufkommen lässt.

Die Mitarbeiter müssen darüber **aufgeklärt** werden, dass sexuelle Belästigung nicht mit der Unternehmenskultur vereinbar ist und somit nicht toleriert wird (Grundsatz der „Null-Toleranz!"). Ferner sind die Mitarbeiter darüber zu informieren, welche Rechte und Pflichten ihnen im Zusammenhang mit sexueller Belästigung zukommen und wie im Verdachtsfall vorzugehen ist. Die Aufklärung kann z.B. über das **Personalreglement** oder über die Abgabe von **separaten Merkblättern** bei Unterzeichnung des Arbeitsvertrages erfolgen.

Der Arbeitgeber sollte eine **Meldestelle** einrichten, um bei Verdacht des Vorliegens sexueller Belästigung Meldungen in anonymer Form zu ermöglichen. Das Meldeverfahren (involvierte Personen, Zuständigkeiten) sollte strikt geregelt sein.

Zentral sind auch regelmässige **Schulungen** namentlich der Vorgesetzten und Personalverantwortlichen, mit dem Ziel, dass diese sexuelle Belästigung möglichst früh erkennen und möglichst verhindern können.

- **Reaktive Massnahmen:** Um auf sexuelle Belästigung reagieren zu können, hat der Arbeitgeber reaktive Massnahmen zu treffen. Der Arbeitgeber hat bei Verdacht auf sexuelle Belästigung eine rasche, faire und diskrete Abklärung vorzunehmen. Die betroffene Person ist vor weiteren Nachteilen und Belästigungen zu schützen (z.B. durch Änderung der Arbeitsabläufe, interne Versetzung in neues Team). Gegen den belästigenden Mitarbeiter sind geeignete **Sanktionen** zu ergreifen. Je nach Schwere des Vorwurfs müssen unter Umständen die **Strafbehörden** eingeschaltet werden.

  Der Arbeitgeber kann bei Vorliegen eines Schadens **schadenersatzpflichtig** werden, falls er keine oder unzureichende Massnahmen ergriffen hat.

> **Literatur:**
>
> Götz Staehelin, Claudia/Huber, Melanie: Pflichten der Arbeitgeberin in der #MeToo-Ära, Recht relevant. für Compliance Officers (RR-COMP), 5 ff.

Q5. Lohnt sich eine Meldestelle für vermutete oder konkrete Missstände?

A: Zum eigentlichen Durchbruch verhalf den Meldestellen für Missstände (→ **Whistleblowing-Hotlines**) der US-amerikanische **Sarbanes-Oxley Act**, der 2002 die davon betroffenen Unternehmen verpflichtete, Stellen für „vertrauliche, anonyme Meldungen von Mitarbeitern" über zweifelhafte Buchführungs- oder Buchprüfungspraktiken vorzusehen. Der Fokus war damals inhaltlich beschränkt, aber er führte dazu, dass US-börsenkotierte Unternehmen auch in ihren europäischen Niederlassungen Whistleblowing-Hotlines einführten.

In Europa gab es mit wenigen Ausnahmen (z.B. *UK Bribery Act*) über lange Zeit keine gesetzliche Pflicht, solche Meldestellen zu betreiben. Das änderte sich erst jetzt mit der 2019 verabschiedeten **EU Whistleblowing-Richtlinie** und deren nationalen Umsetzung

(→ **Q8**). In der Schweiz gibt es nach wie vor keine entsprechende Pflicht, jedenfalls nicht in der Privatwirtschaft.

Das Instrument solcher Meldestellen hat sich allerdings inzwischen bereits etabliert. Wie eine **Umfrage der Hochschule für Technik und Wirtschaft HTW Chur aus dem Jahre 2019** ergab, verfügen bereits fast 60 Prozent der befragten Unternehmen über eine Meldestelle für Missstände. Ein Drittel der Unternehmen ohne Meldestelle plante oder diskutierte die Einführung in den nächsten zwölf Monaten.

Whistleblowing Report 2019

Die Hochschule für Technik und Wirtschaft HTW Chur hat in Zusammenarbeit mit der EQS Group eine umfassende **Studie zur Thematik des Whistleblowings** durchgeführt und dessen Ergebnisse im Whistleblowing Report 2019 festgehalten. Dabei wurden insgesamt 1392 Unternehmen (KMUs sowie Grossunternehmen) in vier Ländern (Deutschland, Frankreich, Grossbritannien und Schweiz) und aus unterschiedlichsten Branchen (z.B. Baugewerbe, Banken- und Versicherungswesen, Öffentliche Verwaltung und Industrie) befragt. Die Gesamtergebnisse der Studie können unter nachstehendem Link abgerufen werden: https://whistleblowingreport.eqs.com/de/resultate/management-summary

Interessant ist freilich, dass Unternehmen mit Meldestellen diese offenbar **primär aus Imagegründen** eingeführt haben: Die Stärkung des eigenen Images als ethisches und integres Unternehmen wurde in der Umfrage als wichtigster Grund genannt. Erst an zweiter und dritter Stelle wurde die Vermeidung finanzieller Schäden und die Überzeugung vom Nutzen und der Effektivität einer Meldestelle genannt.

Die meisten Unternehmen gehen denn auch nicht soweit, dass sie für Meldungen spezialisierte Kanäle vorsehen (z.B. eigene Call-Center oder Melde-Apps), sondern sie beschränken sich auf die **kostengünstigeren traditionellen Meldekanäle**, wie einer eigenen E-Mail-Adresse, einer Telefonnummer oder der Möglichkeit des persönlichen Besuchs. Eine spezielle telefonische Hotline hatten gemäss der Umfrage nur 30 Prozent der Grossunternehmen (und halb so viele KMUs), ein webbasiertes Meldesystem etwas mehr als 36 Prozent der Grossunternehmen und eine App knapp unter 10 Prozent.

Organisatorisch angesiedelt ist die Meldestelle in der Schweiz besonders häufig in der **Personalabteilung**, der Geschäftsleitung oder der Compliance-Abteilung, zuweilen bei der Rechtsabteilung oder dem Verwaltungsrat, selten hingegen bei der internen Revision oder dem *Audit Committee*.

Bei Unternehmen mit Meldestellen gingen gemäss der Umfrage 2018 über alle vier Länder hinweg betrachtet **im Schnitt 65 Meldungen bei Grossunternehmen** und 16 Meldungen bei KMUs ein. Allerdings fällt auch auf, dass bei 40 Prozent der Schweizer

Grossunternehmen mit Meldestellen im Jahre 2018 gar keine Meldungen eingingen, bei den KMUs mit Meldestellen blieben sogar 53 Prozent ohne Hinweis.

Spannend sind auch die Erkenntnisse zu **anonymen Meldungen**: Wo anonymes Melden möglich war, wurden über die Hälfte der Erstmeldungen anonym eingereicht, wobei bei mehr als einem Drittel die Identität des Hinweisgebers im Verlauf des Prozesses bekannt wurde. Einen Einfluss der Möglichkeit anonymer Meldungen auf den Anteil missbräuchlicher Meldungen konnte die Studie nicht feststellen.

Gemäss der Studie stuften die Unternehmen rund fünf Prozent der eingegangenen Meldungen als **missbräuchlich** ein. Die Möglichkeit, Meldungen anonym einzureichen, hatte – wie bereits gesagt – auf den Anteil missbräuchlicher Meldungen offenbar keinen Einfluss. Rund 48 Prozent der Meldungen erwiesen sich wiederum als **nicht relevant**. Als Beispiele für solche nicht relevanten Meldungen nennt die Studie individuelle Beschwerden bezüglich des Führungsstils von Personen oder Hinweise auf technische Betriebsprobleme.

Die Studie zeigt schliesslich auch, dass die über die Meldestellen eingegangenen Hinweise für die Unternehmen **nutzbringend waren**: Von den Unternehmen, die 2018 Missstände mit einem finanziellen Schaden hatten, konnten zwischen 21 und 60 Prozent dieses Schadens aufgedeckt werden, weil das Unternehmen einen entsprechenden Hinweis erhielt. Über alle Länder hinweg betrachtet konnten rund ein Drittel der befragten Unternehmen mehr als 60 Prozent des erlittenen finanziellen Gesamtschadens dank der Meldestelle aufdecken.

Q6. Worauf ist bei der Implementation einer Meldestelle für Hinweisgeber in datenschutzrechtlicher Hinsicht zu achten?

A: Durch das Betreiben einer Meldestelle werden in der Regel → **Personendaten** der gemeldeten und ggf. auch der meldenden Person bearbeitet, jedenfalls soweit eine Meldung nicht vollständig anonym und ohne Namen erfolgt, was in der Schweiz zulässig und möglich ist (wenngleich aus Sicht des Untersuchenden tendenziell ungünstig). Daraus folgt, dass bei der Datenerhebung und -bearbeitung die → **Grundsätze der Datenbearbeitung** des Datenschutzgesetzes zu beachten sind.

Das Datenschutzrecht schreibt mitunter vor, dass die Beschaffung der Personendaten sowie der Zweck ihrer Bearbeitung von der betroffenen Person **erkennbar** sein müssen. Entsprechend sind die Mitarbeiter vor der Implementation einer Meldestelle über deren Zweck und über die zu erhebenden Daten sowie die Art der Datenbearbeitung **zu informieren** (z.B. über eine interne Richtlinie, dem *Code of Conduct*). Es sollte für die Mitarbeiter auch klar sein, zu welchen Themen sie Meldungen vornehmen können. Namentlich, ob es nur um bestimmte Gesetzesverstösse geht, alle Gesetzesverstösse oder darüber hinaus auch Verstösse gegen interne Weisungen oder unethisches Verhalten. Es sollte klar kommuniziert werden, dass **ein Geschäftsbezug erforderlich** ist.

Unklar ist, ob ein **genereller Hinweis** auf die Möglichkeit einer Datenbearbeitung im Rahmen eines *Whistleblowing* genügt (z.B. über eine Richtlinie oder Datenschutzerklärung) oder ob im Falle eines Hinweises die davon betroffenen Personen separat zu informieren sind. Die EU-Datenschutzbehörden sind der Ansicht, dass auch ein **spezifischer Hinweis** nötig ist, sobald es der Fall zulässt – jedenfalls was die beschuldigte Person betrifft. In der Praxis ist dies von beschränkter Relevanz, da die betroffene Person – sollten sich die Vorwürfe erhärten – schon aus arbeitsrechtlichen Gründen früher oder später angehört (und damit auch informiert) werden muss. Eine spezifische Information aller Personen, über die im Zusammenhang mit einem Hinweis (oder einer Untersuchung) Personendaten bearbeitet werden, geht indes zu weit. Hier genügt eine generische Information, soweit diese den gesetzlichen Vorgaben entspricht.

Eine Whistleblowing-Meldestelle kann **auch für Dritte** (z.B. Lieferanten) zugänglich gemacht bzw. diesen kommuniziert werden. Bestimmte Unternehmen verpflichten ihre Vertragspartner in ihren Verträgen sogar zu Meldungen, etwa im Bereich der Korruption oder Kartellabsprachen.

Der Umgang mit Meldungen ist vorzugsweise in einem **Reglement** zu regeln. Dieses sollte auch festhalten, wer die Meldungen bearbeitet, sowie die Abläufe und Zuständigkeiten festlegen. Hierbei ist sicherzustellen, dass keine Interessenkonflikte entstehen, die Vertraulichkeit und der Persönlichkeitsschutz der betroffenen Personen gewährleistet sind und eine faire Vorgehensweise gegenüber allen Beteiligten sichergestellt ist. Dies umfasst nicht nur den Schutz der meldenden, sondern auch der gemeldeten Person. Meldungen können auch falsch, unbegründet oder sogar bösgläubiger Natur sein. Es empfiehlt sich der Hinweis im Reglement, dass sowohl missbräuchliche Meldungen wie auch Repressalien gegen Hinweisgeber sanktioniert werden.

Anonyme Meldungen sind in der Schweiz zulässig und können die meldende Person schützen. Erfahrungsgemäss wird die Identität des Melders jedoch häufig bekannt. Der Arbeitgeber sollte sie schützen und sicherstellen, dass gutgläubige Meldungen keine negativen Konsequenzen haben. Der Nachteil eines anonymen Melders ist selbstredend, dass im Laufe einer Untersuchung keine Kommunikation mit ihm möglich ist, weder bezüglich Rückmeldungen noch Rückfragen. Dieses Problem lässt sich jedoch mit anonymen Postfächern und ähnlichen Kommunikationssystemen von Anbietern von Whistleblowing-Meldestellen beheben. Das Unternehmen sollte einem Melder jedoch **nie Anonymität garantieren**, da es etwa im Rahmen eines Rechtsstreits gezwungen sein kann, die Identität offenzulegen. Die Erfahrung zeigt, dass viele Meldungen zu Beginn anonym erfolgen, im Laufe der Untersuchung aber die Identität des Melders bekannt wird. Nimmt ein Unternehmen Dokumente mit Hinweisen auf einen Whistleblower in die **Personalakte** eines beschuldigten Mitarbeiters, so sollten die Hinweise vorab geschwärzt werden. Dies erhöht den Schutz im Falle eines Auskunftsbegehrens[3]. Zu Aufbewahrungsfrist: → **Q47**.

3 Vgl. dazu den Fall vor dem Landesarbeitsgericht Baden-Württemberg vom 20. Dezember 2018, Az. 17 Sa 11/18.

Das Unternehmen hat die notwendigen organisatorischen und technischen Massnahmen zu treffen, um die **Datensicherheit** zu gewährleisten (Art. 7 Abs. 1 → **DSG**). Das Datenschutzgesetz schreibt ferner vor, dass private Personen → **Datensammlungen** anmelden müssen, wenn regelmässig → **besonders schützenswerte Personendaten** oder → **Persönlichkeitsprofile** bearbeitet werden (Art. 11a Abs. 3 DSG), was typischerweise vorkommt. Daher ist es üblich, dass die Datensammlung, die hinter einer Meldestelle steht und mit welcher die Meldungen bzw. Fälle verwaltet werden, angemeldet wird. Die Anmeldepflicht wird allerdings unter dem revidierten Datenschutzgesetz abgeschafft.

Je nach Ausgestaltung der Whistleblower-Meldestelle sind zudem weitere datenschutzrechtliche Aspekte zu beachten. Soll ein **externer Dienstleister** mit dem Betrieb einer Kontaktstelle für Hinweisgeber beauftragt werden, was in grösseren Unternehmen regelmässig der Fall ist, ist vertraglich sicherzustellen, dass dieser die datenschutzrechtlichen Vorgaben einhält und die Datensicherheit muss gewährt werden (ausführlich dazu → **Q7** sowie → **Q22**). Befindet sich der externe Dienstleistungsanbieter im **Ausland** was gerade bei Konzernverhältnissen der Fall sein kann, sind die Vorgaben zum → **Datenexport** einzuhalten (dazu → **Q21**).

Schutz der Hinweisgeber

Die Arbeitsgruppe „Whistleblowing" der Ethics and Compliance Switzerland (ECS) (dazu → **ORGANISATIONEN**) hat 2019 in einem *Whitepaper* gewisse *Best Practices* für eine effektive und moderne Whistleblowing-Regulierung im privaten Sektor formuliert. Während das Schweizer Gesetzgebungsprojekt, um das es dabei ging, zwischenzeitlich gescheitert ist, enthält das Dokument einige Hinweise, wie Unternehmen den Schutz von Whistleblowern ausgestalten können: https://bit.ly/3sxPUrC

Unter dem revidierten DSG werden Unternehmen für den Betrieb einer Whistleblowing-Hotline eine Datenschutz-Folgenabschätzung durchführen und die dazugehörige Datenbearbeitung in ihr Bearbeitungsverzeichnis aufnehmen müssen.

Literatur:

Rieder, Stefan: Whistleblowing als interne Risikokommunikation, Zürich/St. Gallen 2013

Rüedi, Marco: Whistleblowing in der Praxis, in: von Kaenel, Adrian (Hrsg.), Whistleblowing – Multidisziplinäre Aspekte, Bern 2012, 99 ff.

Zimmermann, Anita/Pärli, Kurt: Whistleblowing und Datenschutz, Zeitschrift für Datenrecht und Informationssicherheit (digma) 2016, 18 ff.

Q7. Wann macht der Beizug eines externen Dienstleisters für eine Meldestelle für Hinweisgeber Sinn?

A: Der Beizug eines externen Dienstleisters macht zunächst dort Sinn, wo **spezialisierte Meldekanäle** angeboten werden sollen, d.h. die Hinweisgeber sich nicht direkt bei der für die (allenfalls notwendige) interne Untersuchung der Hinweise zuständigen Stelle melden sollen. Gemeint ist z.B. der Betrieb eines Internet-basierten Meldesystems, der Betrieb eines *Call Centers* oder auch einer Melde-App. Solche spezialisierten Kanäle generieren erfahrungsgemäss mehr Meldungen als die allgemeinen Kanäle (wie etwa eine E-Mail).

Sinnvoll kann der Beizug eines externen Dienstleisters auch sein, um die für die interne Untersuchung zuständige Stelle **operativ zu entlasten**.

Ein wichtiger Grund für einen externen Dienstleister ist schliesslich, dass auf diese Weise **anonyme Meldungen einfacher und zuverlässiger** möglich sind, einschliesslich der Möglichkeit einer anonymen (Rück-)Kommunikation mit dem Hinweisgeber.

Wenig erstaunlich setzen vor allem grössere Unternehmen solche Dienstleister ein, insbesondere auch dann, wenn eine **internationale Abdeckung** erforderlich ist und der Betrieb einer Meldestelle schon sprachlich und logistisch ohne externe Unterstützung nicht vernünftig möglich ist. Externe Whistleblowing-Stellen bieten teilweise einen 24-Stunden Telefonservice an sieben Tagen in der Woche und dies in unterschiedlichen Sprachen an. Die externen Stellen verfügen bereits über die notwendigen **Ressourcen** und das entsprechende **Know-How**. Sie bieten auch Dienstleistungen, wie z.B. die Möglichkeit anonymer Zwei-Weg-Kommunikation mit Hinweisgebern, d.h. die Personen können über ein Internet-basiertes System mit dem Unternehmen kommunizieren und Fragen beantworten oder informiert werden, ohne dass sie sich identifizieren müssen.

Die **eigentliche Befassung mit einer Meldung** (also die Erstbewertung, Triage, Untersuchung, Nachverfolgung) muss notabene weiterhin durch eine Stelle *innerhalb* des Unternehmens erfolgen und koordiniert werden, auch wenn das Unternehmen im Einzelfall einen externen Experten mit der Aufklärung eines Hinweises beauftragen wird.

Ob der Beizug eines externen Dienstleisters bei **kleineren und mittleren Unternehmen** mehr oder weniger Sinn als bei grossen Unternehmen macht, ist umstritten: Einerseits erhalten KMUs im Schnitt deutlich weniger Meldungen, andererseits kann es in einem KMU aufgrund der Überschaubarkeit der Verhältnisse umso wichtiger sein, anonyme Meldungen zu ermöglichen – oder weil die Ressourcen für eine unabhängige interne Stelle fehlen.

Für spezifische Themen oder für Unternehmen **in besonders heiklen Situationen** (z.B., wenn das Vertrauen in die Geschäftsleitung eines Unternehmens angeschlagen ist) kann es sich aufdrängen, einen externen Dienstleister mit dem Betrieb von (zusätzlichen) Meldekanälen zu beauftragen. Dies muss nicht immer ein spezialisierter

Dienstleister sein. In Frage kommen auch andere Vertrauensstellen wie z.B. eine Anwaltskanzlei, welche die Fälle dann auch gleich untersuchen kann[4].

Aus **datenschutzrechtlicher Sicht** ist das Betreiben einer externen Whistleblowing-Stelle zulässig, auch im Ausland (jedenfalls soweit keine Geschäftsgeheimnisse auf dem Spiel sind, die aufgrund von Art. 273 StGB nicht ins Ausland kommuniziert werden dürfen). Vom externen Anbieter der Whistleblowing-Stelle sind ebenfalls die Grundsätze der Datenerhebung bzw. -bearbeitung zu beachten. Verantwortlicher bleibt das Unternehmen, der Anbieter ist in der Regel Auftragsbearbeiter, mit welchem ein entsprechender Vertrag abzuschliessen ist, der gewissen datenschutzrechtlichen Vorgaben zu entsprechen hat (zum Ganzen → **Q22**).

Literatur:

Rieder, Stefan: Whistleblowing als interne Risikokommunikation, Zürich/St. Gallen 2013

Q8. Was sind die Vorgaben der EU Whistleblower-Richtlinie?

A. Am 16. Dezember 2019 trat in der Europäischen Union die sog. EU Hinweisgeber-Richtlinie (EU) 2019/1937 (umgangssprachlich auch „Whistleblower-Richtlinie" genannt) in Kraft und muss von den EU-Mitgliedsstaaten **bis 17. Dezember 2021** im jeweiligen nationalen Recht umgesetzt werden.

Kerninhalte der Richtlinie sind Vorgaben zum Schutz von Whistleblowern (in der Richtlinie als „Hinweisgeber" bezeichnet) sowie Vorschriften zur zwingenden Implementierung eines Whistleblowing-Systems ab einer gewissen Unternehmensgrösse.

Zwar findet die Richtlinie grundsätzlich nur auf **Unternehmen in den Mitgliedstaaten der EU** Anwendung. Dies können jedoch auch Zweigniederlassungen oder Tochtergesellschaften von Schweizer Unternehmen sein. Die Richtlinie findet Anwendung auf private Unternehmen **mit 50 oder mehr Arbeitnehmern** sowie auf Betriebe der öffentlichen Hand. Sie müssen interne Meldekanäle für Verstösse gegen Unionsrecht einrichten (siehe nachfolgende Box). Die Mitgliedstaaten können auch kleinere Unternehmen in bestimmten (besonders gefährdeten) Branchen dieser Pflicht unterstellen. Die Umsetzung muss bis zum Inkrafttreten des Rechts des jeweiligen Mitgliedstaats erfolgen, also grundsätzlich bis spätestens zum 17. Dezember 2021. Unternehmen mit weniger als 250 Arbeitnehmern wird allerdings eine zusätzliche Frist von zwei Jahren bis zum 17. Dezember 2023 gewährt.

4 So geschehen im Fall des Westschweizer Fernsehens, wo 2020 Vorwürfe sexuelle Belästigung und Machtmissbrauch im Raum standen. Die Mitarbeiter wurden aufgefordert, sich bezüglich etwaiger weiterer Fälle bei einer Anwaltskanzlei zu melden, was rund 200 Personen taten – allerdings nur als Zeugen, nicht als direkt Betroffene. Neue Belästigungsfälle wurden offenbar nicht gemeldet. Vgl. dazu den Bericht des Bundesrats auf einen parlamentarischen Vorstoss NR 20.4462 hin: https://bit.ly/3gn8tw1.

Die Richtlinie selbst bezieht sich **nur auf EU-Recht** (z.B. EU-Kartellrecht, DSGVO; ein Anhang der Richtlinie listet die Erlasse auf zehn Seiten auf), jedoch können die Mitgliedstaaten die entsprechenden Pflichten auch auf Verstösse gegen nationales Recht erweitern (was in Deutschland z.B. der Fall sein soll). Nationales Umsetzungsrecht (z.B. Umsetzung von Richtlinien) gilt als EU-Recht.

Massgebliche Vorgaben der EU Hinweisgeber-Richtlinie sind:

- Zwingende **Implementation interner Meldekanäle** sowie Definition eines Meldeverfahrens bei Unternehmen mit 50 oder mehr Beschäftigten. Grundsätzlich muss jedes Unternehmen (d.h. jede Rechtseinheit, auch im Konzern) seine eigenen Kanäle haben; lediglich Unternehmen mit maximal 249 Beschäftigten können sich ein Meldesystem (einschliesslich der Nachverfolgung der Meldungen) teilen, was in vielen Konzernen nicht dem Standard entspricht. Dabei gibt die Richtlinie **gewisse Mindeststandards** zur Ausgestaltung der Meldekanäle und deren Handhabung vor, mitunter:
  - Die Meldungen müssen in **schriftlicher** oder **mündlicher** Form vorgenommen werden können, oder in beiden Formen (hingegen haben Behörden die Pflicht, sowohl schriftliche als auch mündliche Meldungen zu ermöglichen). Mündlich bedeutet, dass eine Telefonnummer oder ein Sprachmitteilungssystem angeboten werden muss, und ebenso ein persönliches Vorsprechen. Etwaige Transkripte oder Besprechungsprotokolle dürfen vom Melder verifiziert werden.
  - Die Meldekanäle sind **nicht nur den Mitarbeitern** eines Unternehmens zugänglich zu machen, sondern einem „breiteren Publikum“ (z.B. auch Stellenbewerbern, unabhängigen Beratern).
  - Dem Hinweisgeber muss **innert sieben Tagen** nach Eingang der Meldung eine Eingangsbestätigung zugehen.
  - Es muss eine **unbefangene Person** oder Abteilung bestimmt sein, welche den Meldungen nachgeht.
  - **Spätestens drei Monate** nach Eingangsbestätigung ist der Hinweisgeber über etwaige getroffene Massnahmen zu informieren und es muss in diesem Zusammenhang ein Ansprechpartner angegeben werden. Solche Massnahmen können z.B. die Einstellung mangels Beweisen, die Durchführung einer internen Untersuchung oder eine Meldung an die zuständige Aufsichtsbehörde sein. Details sind nicht erforderlich, allerdings wird das Unternehmen ein Interesse an hinreichender Information haben, um zu vermeiden, dass der Hinweisgeber sich auch noch an andere Stellen wendet.

  - Es muss eine **Behörde angegeben** werden, bei welcher sich der Hinweisgeber nötigenfalls melden kann. Das kann im internationalen Kontext schwierig sein, weshalb es sich empfiehlt, den Hinweis jeweils im Rahmen des Feedbacks zu einer Meldung zu spezifizieren.
  - Wahrung der **Vertraulichkeit** über die Identität des Whistleblowers sowie Dritter, die in der Meldung erwähnt werden. Die Richtlinie sieht aber keinen absoluten Schutz der Identität des Hinweisgebers vor.

- **Dokumentationspflicht** für alle eingehenden Meldungen, wobei auch hier stets die Vertraulichkeit sowie die datenschutzrechtlichen Grundsätze der Datenbearbeitung zu wahren sind. Eine konkrete Aufbewahrungsfrist gibt die Richtlinie aber nicht vor. Dazu: → **Q47**.
- **Keine vorgegebene Kaskadenordnung**, d.h. der Whistleblower muss sich grundsätzlich nicht zuerst an interne Stellen des betroffenen Unternehmers wenden. Er kann direkt zu einer Behörde gehen.
- Massnahmen zum **Schutz des Hinweisgebers**, z.B. Verbot der Androhung von Repressalien (wie beispielsweise Verweigerung der Beförderung, der Weiterbildung, Lohnerhöhung, Versetzungen). Kommt es zur Repression, muss sie verfolgt werden. Schutz erhalten allerdings nur Personen, die einen nachvollziehbaren Grund hatten (*"reasonable grounds"*), dass die von ihnen gemeldete Information zum damaligen Zeitpunkt wahr war (auf ihre Motive kommt es allerdings nicht an). Sie sind auch dann geschützt, wenn sie mit ihrem Hinweis z.B. Vertraulichkeitsverpflichtungen gegenüber dem Unternehmen verletzen würden oder beispielsweise verbotenerweise Unterlagen entfernen oder kopieren, die sie für ihre Meldung nutzen (inwieweit die Begehung von Straftaten geschützt ist, bestimmt das nationale Recht). Die Nationalität des Hinweisgebers ist irrelevant. Es muss sich auch nicht um Arbeitnehmer handeln. Zu schützen sind z.B. auch Verwandte und Bekannte des Hinweisgebers. Kein Schutz soll erhalten, wer bereits öffentlich bekannte Informationen meldet oder bei der Meldung von unsubstantiierten Gerüchten oder bei Hörensagen. Ein absoluter Schutz von Arbeitnehmern besteht auch nicht; arbeitsrechtliche Massnahmen, die nicht durch den Hinweis ausgelöst worden sind, sind weiterhin erlaubt.

- Es gilt eine **Beweislastumkehr**, d.h. wird gegenüber einem Whistleblower eine benachteiligende Massnahme erhoben, muss das Unternehmen beweisen, dass diese Massnahme in keinem Zusammenhang mit der Hinweisabgabe steht.

- **Sanktionen:** Dem nationalen Gesetzgeber wird die Pflicht auferlegt Sanktionen für natürliche und juristische Personen festzulegen, welche z.B. Meldungen verhindern oder behindern oder ungerechtfertigt Repressalien gegen den Whistleblower ergreifen.

  Anzumerken ist, dass die Vorgaben der EU Whistleblower-Richtlinie von den einzelnen Mitgliedstaaten umzusetzen sind. Diese können in ihrer Regulierung noch weitergehen und z.B. einen stärkeren Schutz für den Whistleblower vorsehen.

  Der Richtlinien-Text kann hier heruntergeladen werden: https://bit.ly/2Rz3QVc

Die Richtlinie lässt **anonyme Hinweise** zu, doch sind solche in der EU nach wie vor umstritten. Das deutsche Umsetzungsgesetz sieht im gegenwärtigen Entwurf beispielsweise vor, dass Unternehmen anonymen Hinweisen nicht nachgehen müssen.

Die Verletzung der Richtlinie wird – wie erwähnt – über das Recht der Mitgliedsstaaten sanktioniert. In Deutschland ist beispielsweise eine Busse von **bis zu EUR 100‘000** vorgesehen, was im Vergleich zu den Bussen für die Verletzung der DSGVO ein vergleichsweise geringer Bussenrahmen ist.

Die Richtlinie regelt nicht nur die Unternehmens-interne Meldung, sondern auch die **Meldungen an Behörden** und **Medien bzw. die Öffentlichkeit** (letzteres dann, wenn Hinweise an die internen und externen nicht-öffentlichen Kanäle nicht weiterführen). Die Mitgliedsstaaten können Behörden bestimmen, welche Meldungen von Hinweisgebern entgegennehmen (z.B. wo nicht bereits Aufsichtsbehörden bestehen).

Literatur:

Erlenbach, Kimberly: Die Regelungen der EU-Hinweisgeberrichtlinie und ihre Auswirkungen auf deutsche Unternehmen, Compliance Berater (CB) 2020, 284 ff.

Hahn, Anne-Catherine: Die neue EU Whistleblower-Richtlinie – Handlungsbedarf für Schweizer Unternehmen? Recht relevant. für Compliance Officers (RR-COMP), 1/2020, 2 ff.

Q9. Können Mitarbeiter zur Meldung von Fehlverhalten verpflichtet werden?

A: Mitarbeiter können nicht generell zur Meldung von Fehlverhalten anderer Mitarbeiter verpflichtet werden bzw. eine solche Verpflichtung wäre grundsätzlich nicht durchsetzbar. Bei höhergestellten Arbeitnehmern ist eine Meldepflicht denkbar, soweit das Fehlverhalten einen Arbeitsplatzbezug und eine gewisse Schwere aufweist oder hierarchisch tiefergestellte Arbeitnehmer betrifft.

Sind die Interessen des Arbeitgebers jedoch erheblich gefährdet oder verletzt, kann sich auch aus der allgemeinen Treuepflicht nach Art. 321a OR eine Meldepflicht erge-

ben, die selbst gleichrangige Arbeitnehmer betrifft (vgl. BGE 113 IV 68, E.6, E.7, m.w.H.). Eine Meldepflicht kann sich allenfalls auch aus einer Garantenstellung des Arbeitnehmers ergeben, so etwa, wenn ihm die Verwaltung des vom Fehlverhalten betroffenen Vermögens des Arbeitgebers anvertraut worden ist.

Q10. Wie weit gilt das Anwaltsgeheimnis in der Schweiz noch?

A: Das geschützte Rechtsinstitut des **Anwaltsgeheimnisses** ist das Vertrauensverhältnis zwischen dem Anwalt und dessen Klient. Das schweizerische Prozessrecht sieht vor, dass Anwälte Auskünfte über Geheimnisse verweigern können, die sie in Ausübung ihrer Tätigkeit wahrgenommen haben. Grundsätzlich deckt das Anwaltsgeheimnis sämtliche Informationen, die der Anwalt vom Klient erhält und welche zur Wahrung seiner Interessen notwendig sind.

Unterlagen (Anwaltskorrespondenzen, Arbeitsprodukte des Anwaltes) sowie Gegenstände dürfen von Aufsichts- bzw. Strafbehörden nicht beschlagnahmt werden und müssen daher in einem etwaigen Prozess nicht offengelegt werden, vorausgesetzt diese unterliegen dem Anwaltsgeheimnis. Im Strafverfahren sind entsprechende Unterlagen und Gegenstände zu siegeln (Art. 248 → **StPO**).

Mandatiert ein Unternehmen aufgrund dieses sog. → **Legal Privilege** im Rahmen einer internen Untersuchung einen Anwalt oder eine Anwaltskanzlei, ist aber Vorsicht geboten. Denn durch das Anwaltsgeheimnis wird das Unternehmen vor Eingriffen der Aufsichts- und Strafbehörden nicht absolut geschützt; das Bundesgericht hat hier einschränkend eingegriffen. Hinzu kommt, dass **Aufsichts- und Strafbehörden** ein gewisses Interesse entwickelt haben, die Ergebnisse von internen Untersuchungen für ihre eigenen Zwecke zu nutzen, weil ihnen dies Arbeit abnimmt. Sie warten dann mit entsprechenden Verfahren, bis die internen Untersuchungen abgeschlossen sind und verlangen danach die Berichte.

Geschützt durch das Anwaltsgeheimnis wird lediglich die **typische Anwaltstätigkeit**, nicht aber die sog. **anwaltliche (akzessorische) Geschäftstätigkeit.** Darunter zu verstehen sind (nicht abschliessend) die Geschäftsführung, die Verwaltung einer Gesellschaft oder die Vermögensverwaltung. Wird eine Anwaltskanzlei in einer solchen Funktion mandatiert, kann sich das Unternehmen folglich nicht auf das Anwaltsgeheimnis berufen. Auch materielle Beweismittel für die Straftat (insbesondere solche, die der Beschuldigte bei seinem Verteidiger in Sicherheit zu bringen versucht hat), fallen nicht unter das Anwaltsgeheimnis. Entsprechende Unterlagen sind in einem Prozess offenzulegen.

Obschon die Tätigkeiten bei der Durchführung einer **internen Untersuchung** (Erstellung des rechterheblichen Sachverhalts und rechtliche Würdigung) zum Grossteil als **anwaltstypische Tätigkeiten** zu qualifizieren sind, legt die Entwicklung der bundesgerichtlichen Rechtsprechung nahe, dass das Anwaltsgeheimnis enger zu fassen ist.

Gemäss bundesgerichtlicher Rechtsprechung kann sich das Unternehmen bei **gemischten Mandaten** nicht integral auf das Anwaltsgeheimnis stützen. Es ist jeweils im **Einzelfall** zu prüfen, ob es sich um eine typische Anwaltstätigkeit handelt oder eben nicht. Ferner hat das Bundesgericht entschieden, dass kein Schutz durch das Anwaltsgeheimnis besteht, wenn ein Finanzinstitut **Compliance-Aufgaben** an eine Anwaltskanzlei auslagert. Die Compliance-Pflichten sowie dazugehörige Dokumentationspflichten sind aufsichtsrechtliche Pflichten eines Finanzinstituts und können nicht durch Mandatierung eines Anwalts und anschliessende Berufung auf das Anwaltsgeheimnis unterlaufen werden.

☝ Diese Praxis des Bundesgerichts prägten bisher zwei Entscheide des Bundesgerichts aus den Jahren 2016 und 2018 (BGer 1B_85/2016 vom 20. September 2016, BGer 1B_433/2017 vom 21. März 2018). Das enge Verständnis des Bundesgerichts dafür, was als „anwaltstypische" Tätigkeit gilt, sorgte allerdings für viel Kritik, da es die Tätigkeit des Anwalts auf den Bereich des Anwaltsmonopols reduziert. In beiden Fällen kam das Bundesgericht zum Schluss, dass ein „Mischmandat" vorliegt, d.h. das Mandat nicht nur rechtsberatende Anteile, sondern auch deutliche Anteile eines nicht anwaltsspezifischen bankrechtlichen *Controllings* und *Auditings*, der von der Bank einzuhaltenden Compliance-Vorschriften im Bereich der Geldwäschereiabwehr enthält, mit der m.a.W. genauso ein Nicht-Anwalt hätte mandatiert werden können. Für das Bundesgericht war insbesondere nicht klar, warum ein umfangreicher E-Mail-Review und die Befragungen diverser Mitarbeiter durch Anwälte zu erfolgen hat (BGer 1B_433/2017 vom 21. März 2018, E. 4.16).

Mit anderen Worten: Was ein Unternehmen unabhängig von einer internen Untersuchung abgeklärt und dokumentiert haben muss, soll es nicht unter dem Titel des Anwaltsgeheimnisses zurückhalten können, indem es die Aufgabe einem Anwalt überträgt. **Könnte eine Sachverhaltsabklärung auch von einem Nicht-Anwalt vorgenommen werden**, soll sie nach der Praxis des Bundesgerichts selbst dann nicht vom Anwaltsgeheimnis erfasst sein, wenn sie für eine Rechtsberatung nötig ist. Ob diese Praxis auch für interne Untersuchungen ausserhalb der Geldwäscherei-Compliance bzw. aufsichtsrechtlich vorgeschriebener Compliance-Aufgaben gilt, bleibt abzuwarten.

Das betroffene Unternehmen kann in diesem Zusammenhang zumindest einige Vorkehrungen treffen. So empfehlen sich eine genaue **Mandatsumschreibung** im Kontext der internen Untersuchung (als Beispiel: Vorbereitung auf Zivilprozess bzw. zivilrechtlicher Forderungen, Abklärung zwecks Einleitung eines Strafverfahrens, Vorbereitung der Verteidigung in einem Aufsichts- oder Strafverfahren gegen das Unternehmen, auch wenn ein solches noch nicht absehbar ist, weil die Behörden bewusst oder unbewusst die interne Untersuchung abwarten). Bei Finanzinstituten ist eine klare **Trennung der gesetzlichen Compliance-Pflichten** (z.B. Abklärungen im Bereich der Geldwäscherei, Buchführungspflicht) von der internen Untersuchung sinnvoll.

Viele interne Untersuchungen zielen traditionell nur auf die Abklärung des relevanten Sachverhalts ab. Solche Aufträge laufen Gefahr, integral nicht als anwaltstypische Tätigkeit qualifiziert zu werden. Dem kann entgegengewirkt werden, wenn das Unternehmen dem Anwalt stattdessen einen **Auftrag zur Rechtsberatung- und -vertretung gibt**, und den dazu erforderlichen Sachverhalt selbständig aufarbeitet.

Ferner sollte genau erwogen werden, welche **Beweismittel** zur Unterlegung der Untersuchungsergebnisse (relevante Dokumente, Protokolle von Befragungen, etc.) dem Unternehmen übergeben werden, da mit ihrer Beschlagnahmung gerechnet werden muss.

In besonders heiklen Fällen kann es sich auch anbieten, dass der mit einer Untersuchung beauftragte Anwalt **gar keinen schriftlichen Bericht** mehr erstattet oder einen solchen nach der Präsentation wieder einsammelt. Dies wäre eine Rückkehr zur Praxis in der Zeit vor der Einführung des heutigen *Legal Privilege* in den Prozessgesetzen. Allerdings kann dies einer allfälligen aufsichtsrechtlichen Pflicht des Unternehmens zur Dokumentation seiner Geschäfte zuwiderlaufen.

Nicht viel Spielraum für Unternehmen lässt das Bundesgericht auch unter dem Titel der aufsichtsrechtlichen Mitwirkungspflichten (in regulierten Märkten) und in Bezug auf einen **Zwang zur strafrechtlichen Selbstbelastung** (*nemo-tenetur*-Grundsatz) durch die Herausgabe von Unterlagen. Das strafprozessuale Verbot des Selbstbelastungszwangs gelte grundsätzlich auch für beschuldigte juristische Personen. Doch sei dieser Grundsatz in dem Sinne restriktiv zu handhaben, so dass ein aufsichtsrechtlicher und strafprozessualer Zugriff auf Unterlagen, welche das beschuldigte Unternehmen aufgrund verwaltungsrechtlicher Gesetzesvorschrift erstellen, aufbewahren und dokumentieren müsse, nicht unterlaufen werden könne (Entscheid des BGer 1B_249/2015 vom 30. Mai 2016, E. 8.3).

Ungeachtet der Ausgestaltung des Mandats des Anwalts sollte das Unternehmen davon ausgehen, dass **seine Unterlagen zum Sachverhalt** nicht vor dem Zugriff etwaiger Behörden geschützt sind, auch wenn sie vom Anwalt bzw. seinem Forensik-Dienstleister (und damit seiner Hilfsperson) sichergestellt worden sind, wie z.B. E-Mails und Dokumente. Sie gehören dem Unternehmen und müssen diesem vom Anwalt auf Verlangen (und gestützt auf den mit ihm abzuschliessenden Auftragsbearbeitungsvertrag, → **Q23**) wieder herausgegeben werden. Immerhin ist es mit einem modernen → **Review-System**[5] ohne Weiteres möglich, die darin enthaltenen Dokumente auch ohne die → **Tags** oder Kommentare des Anwalts (als dessen Arbeitsprodukt) herauszugeben.

5 Zu den Review-Systemen siehe → **WERKZEUGE FÜR EDISCOVERY**.

Solche Abgrenzungsfragen kennt nicht nur das Schweizer Recht. Auch im Ausland, so etwa in den **USA**, gilt das *Legal Privilege* nicht für sämtliche Inhalte in den Händen des Anwalts. Es unterscheidet unter anderem zwischen der Kommunikation mit dem Anwalt und der vom Anwalt erteilten Rechtsberatung, die ebenfalls geschützt ist. Hingegen ist eine reine Sachverhaltsdarstellung, auch wenn vom Anwalt erstellt, nicht geschützt.

Anders als in der Schweiz ist das *Legal Privilege* in den USA jedoch in persönlicher Hinsicht weiter gefasst: Es schützt auch **unternehmensinterne Juristen**, was in der Schweiz nach wie vor nicht der Fall ist. Spielt das Anwaltsgeheimnis in einem konkreten Fall somit eine Rolle, sollte der (externe) Anwalt in die Kommunikation einbezogen sein und bleiben. Immerhin ist in den Räten derzeit eine parlamentarische Initiative hängig, welche die Einführung eines Zeugnis- und Editionsverweigerungsrechts für Unternehmensjuristen in der Zivilprozessordnung anstrebt[6].

Literatur:

Fritsche, Claudia M./Studer, Nadine: Arbeitsprodukte interner Untersuchungen, Aktuelle Juristische Praxis (AJP) 2018, 168 ff.

Götz Staehelin, Claudia: Unternehmensinterne Untersuchungen, Zürich/Basel/Genf 2019

Huber, Roman: Interne Untersuchungen und Anwaltsgeheimnis, Gesellschafts- und Kapitalmarktrecht (GesKR) 2019, 65 ff.

Q11. Was muss beim Beizug ausländischer Anwälte beachtet werden?

A: Das *Legal Privilege* des schweizerischen Rechts kommt nur bei Anwälten, welche dem → **BGFA** unterstehen zur Anwendung. Arbeitsprodukte, selbst wenn diese aus einer anwaltstypischen Tätigkeit herrühren, sind nicht geschützt, wenn ausländische Anwälte diese hervorgebracht haben. So können Anwaltskorrespondenzen mit ausländischen Anwälten durchaus beschlagnahmt und in einem Verfahren offengelegt werden. Beim Beizug von ausländischen Anwälten sind idealerweise stets Schweizer Anwälte, welche dem BGFA unterstehen, federführend.

Literatur:

Romerio, Flavio/Bazzani, Claudio/Groth, Stephan: Interne und regulatorische Untersuchungen – Einführung und Auslegeordnung / V. Rechtsanwälte als Untersuchungsbeauftragte, in: Romerio, Flavio/Bazzani, Claudio (Hrsg.), Interne und regulatorische Untersuchungen, Zürich 2015, 62 ff.

6 15.409 Pa.Iv. Markwalder „Berufsgeheimnisschutz für Unternehmsjuristinnen und -juristen“.

Q12. Welche neuen Herausforderungen stellen sich durch das Home-Office im Zusammenhang mit internen Untersuchungen?

A. Durch das Home-Office verlagert sich die Arbeitstätigkeit des Mitarbeiters ganz oder zumindest teilweise in dessen eigene vier Wände und weg vom traditionellen Arbeitsplatz. Das Unternehmen sieht sich einerseits mit **neuen Formen der Pflichtverletzung** konfrontiert. So können vertrauliche Dokumente auf dem privaten Computer abgespeichert werden oder dem Berufsgeheimnis unterliegende Dokumente landen im Hausmüll anstatt im Schredder. Selbstredend können solche Pflichtverletzungen auch ohne Home-Office stattfinden, doch nach alter Weisheit macht Gelegenheit Diebe. Dem Mitarbeiter werden also Freiheiten eingeräumt, die er im schlimmsten Fall zum Nachteil des Arbeitgebers ausnutzt. Erschwerend kommt dazu, dass das Unternehmen weniger **Kontrolle** über die Situation vor Ort hat. Dies ergibt sich bereits aus der geografischen Distanz zum Arbeitsplatz. Vorgesetzte haben einen weniger guten Überblick darüber, was der Mitarbeiter den ganzen Tag macht. Verdachtsmomente können unter Umständen erst zu spät geäussert werden. Auch die IT-Systeme können im Home-Office weniger überwachen, wenn der private Computer zur Arbeit genutzt wird.

Daneben stellen sich Herausforderungen bezogen auf die eigentliche Durchführung der internen Untersuchung. Zum einen kommen **neue Datenquellen** hinzu. Zwar bleibt der Review von E-Mails vorderhand noch zentral, doch in der Praxis kommt es zu Fällen, in welchen neue „Datenquellen" vom Neben- zum Hauptakteur werden (z.B. Zoom, Teams, Chats, etc.). Der Arbeitgeber muss sicherstellen, dass im Falle einer internen Untersuchung auch auf solche Datenquellen zugegriffen werden kann, was sich durchaus als Herausforderung erweisen kann, da viele dieser *Tools* bzw. deren Anbieter eine solche Möglichkeit noch gar nicht vorsehen. Dies bedeutet, dass sich zwar Teile der Kommunikation auf diese neuen Plattformen verlagert, sie dort aber nicht oder nicht vollständig nachvollzogen werden kann. So gibt es Kommunikationsplattformen, auf denen zwar Chats protokolliert werden, jedoch ohne etwaige Emoticons (die wichtig sein können) oder Beiträge nur in der letzten Fassung (d.h. nachträgliche Änderungen sind möglich). Mehr dazu: → **WERKZEUGE FÜR EDISCOVERY**; zu Microsoft 365 → **Q55**.

Ferner kann der Mitarbeiter zwar aufgefordert werden, physisch zu einer Befragung zu erscheinen, jedoch kann unter Umständen auch eine **virtuelle Befragung** sinnvoll oder sogar angezeigt sein (dazu → **Q39**). Zudem stellt sich die Frage, inwiefern und auf welche Art **Geschäftsdokumente aus dem Home-Office** herausverlangt werden können (dazu → **Q20**) oder, ob ein → **Review** von Dokumenten ebenfalls aus dem Home-Office erfolgen kann (dazu → **Q25**).

Home-Office der Mitarbeiter steht einer internen Untersuchung allerdings nicht im Wege. Es stellen sich aber neue **Fragen** und **Herausforderungen**, die vom Arbeitgeber zu berücksichtigen bzw. zu bewältigen sind. Und dies bereits vor Durchführung einer internen Untersuchung als auch bei deren eigentlichen Vornahme.

Literatur:

Naber, Sebastian/Ahrens, Tim: Remote Investigations: Die Aufklärung von Compliance-Verstössen im New Normal, Compliance Berater (CB) 2020, 465 ff.

Q13. Welche Delikte im Bereich des Wirtschaftsstrafrechts kommen besonders häufig vor?

A: Gemäss dem aktuellen „KPMG Forensic Fraud Barometer 2020“[7] lag die Deliktssumme im Bereich *White Collar Crimes*[8] gemessen an den Verurteilungen durch Schweizer Gerichte im Jahr 2020 mit CHF 355 Mio. ungefähr auf dem Niveau des Vorjahres; die Zahl der Verurteilungen war mit 52 (im Vorjahr: 48) leicht höher. Dies ergibt eine durchschnittliche Deliktssumme von knapp CHF 7 Mio. pro Fall.

Eine Analyse der Täterstrukturen zeigt, dass professionelle Täter mit 36 Prozent die grösste Gruppe ausmachten, gefolgt von privaten Einzeltätern (25 Prozent), dem Management (23 Prozent), Mitarbeitern (8 Prozent) und einer Kombination von Management und Mitarbeitern (6 Prozent). Auf das organisierte Verbrechen entfielen nur 2 Prozent.

Am häufigsten wurden öffentliche Institutionen Opfer (39 Prozent), gefolgt von privaten Einzelpersonen (23 Prozent), Unternehmen der Privatwirtschaft (19 Prozent), Kunden (15 Prozent) und Finanzinstitutionen (2 Prozent).

Die häufigsten Verurteilungen erfolgten 2020 wegen ungetreuer Geschäftsführung und Veruntreuung (je 19 Prozent), Versicherungs- und Sozialhilfebetrug (15 Prozent), anderen Betrügereien (13 Prozent), Geldwäscherei (8 Prozent), Steuerbetrug (6 Prozent), Korruption und Investmentbetrug (je 4 Prozent).

7 https://home.kpmg/ch/en/home/insights/2021/04/forensic-fraud-barometer-2020.html.
8 Erfasst werden nur Fälle mit einem Schaden von mindestens CHF 50‘000.

Gedanken zum Thema.

In den letzten Jahren hat ein Paradigmenwechsel stattgefunden, dem viele Akteure noch nicht genügend Rechnung tragen. Eine Firma muss heute möglichst unabhängige Experten beauftragen, interne Vorfälle zu untersuchen. Es können damit nicht mehr einfach die Hauskanzlei oder sonst vertraute Personen beauftragt werden. Selbst wenn solche auf den ersten Blick geeignet erscheinen, weil sie eine Firma bereits sehr gut kennen, ist die Aussenwirkung von Befangenheit und mangelnder Unabhängigkeit fatal. Das schadet dem Ergebnis, dem Unternehmen und der Kanzlei.

Zoé Baches
Wirtschaftsredaktorin
Neue Zürcher Zeitung

3. Erste Schritte

Kurz gesagt

- Sichern Sie zuallererst die Beweise, denn was weg ist, ist weg. Eine Sicherung elektronischer Daten (E-Mails, etc.) ist unbemerkt möglich; erst danach sollten Sie einen Vernichtungsstopp (*Legal Hold*) verhängen.
- Es gibt keine fixe Vorgehensweise, aber in vielen Fällen werden zuerst Unterlagen gesichtet und erst dann – mit entsprechender Aktenkenntnis – die involvierten Personen befragt; die beschuldigte Person ist oft zuletzt an der Reihe.
- Dokumentieren Sie jeden Schritt – und dokumentieren Sie auch, auf welche Massnahmen Sie verzichten und warum.

Worum es geht

Kommt es zu einer internen Untersuchung, ist meist nicht klar, wohin die Wege führen werden und wie gross die Sache werden wird. Klar ist, dass es konkrete Anhaltspunkte für einen möglichen Compliance-Verstoss gibt und das Unternehmen diesem, weshalb auch immer, auf den Grund gehen will. Ist dies nicht nur vorgeschoben, ist es daher wichtig, die interne Untersuchung richtig aufzugleisen, die richtigen Personen beizuziehen und die erforderlichen technischen und organisatorischen Sofortmassnahmen zu treffen. Dabei muss rasch und diskret gehandelt werden.

Worauf zu achten ist

- Jede interne Untersuchung braucht einen Leiter, intern und extern.
- Unabhängigkeit. Nur Personen ohne eigene Interessen (inklusive Loyalitätskonflikte oder Beisshemmungen) in der Angelegenheit sollten eine Untersuchung durchführen.
- Vertraulichkeit. Alle sind zu Stillschweigen zu verpflichten. Die Vertraulichkeit ist auch in der Kommunikation zu beachten (wer hat Zugriff auf E-Mails?).
- Halten Sie darum den Kreis der eingeweihten Personen möglichst klein. Nicht alle, die zur Untersuchung beitragen, müssen wissen, worum es geht.

Das Ziel?

Das primäre Ziel einer internen Untersuchung ist die neutrale Abklärung des Sachverhalts – so gut dies dem Unternehmen mit den ihm legal zur Verfügung stehenden Mitteln geht. Die rechtliche Einordnung und Empfehlung der zu treffenden Massnahmen folgt erst später.

- Für die Untersuchung relevante Personen (Beschuldigte, Auskunftspersonen, Zeugen) definieren – das braucht es auch für die Beweissicherung.
- Mit Thesen arbeiten und diese prüfen, aber ergebnisoffen bleiben – die Dinge können anders sein, als sie auf den ersten Blick erscheinen.
- Mögliche elektronische und physische Beweise sind sofort zu sichern, wo angezeigt ist ein → **Legal Hold** auszusprechen.
- Ein *"Early Case Assessment"* durch einen Spezialisten bei elektronisch sichergestellten Daten kann rasch erste Eindrücke liefern.
- Laufende interne und externe Berichterstattung und Standortbestimmung regeln.
- Kostenkontrolle – sich auf das beschränken, was im Moment wirklich nötig ist.
- Erstellen Sie bei Bedarf einen Plan Ihrer Untersuchung („*Investigation Plan*"), passen Sie ihn bei Bedarf an und dokumentieren Sie Ihre Schritte.

Geben Sie einer internen Untersuchung einen **Codenamen**. Er sollte allerdings keine Rückschlüsse auf die Natur, den Inhalt oder die Beteiligten der Untersuchung liefern. Ein Codename erleichtert die vertrauliche Kommunikation – und er motiviert das Team.

Wie vorzugehen ist

1. **Stellen Sie Ihr internes Team zusammen.** Auch wenn Sie die Untersuchung durch eine externe Stelle durchführen lassen, braucht es jemanden, der diese Stelle überwacht und intern die nötigen Hebel ziehen kann, damit die externe Stelle ihre Arbeit machen kann. Es braucht immer jemanden, der den Betrieb kennt, weiss, an welche Information wo zu gelangen ist, wer welche Aufgabe hat und wie diese Person „tickt" – und der sich um die Schnittstelle zur Geschäftsleitung und die administrativen Dinge wie z.B. das Budget, den Zutritt zum Gebäude oder die Räumlichkeiten kümmert.

   Die interne Stelle kann die Leitung der Compliance-Stelle, des Rechtsdienstes aber auch ein Vertreter der Geschäftsleitung sein. Es muss jedoch jemand sein, der den Betrieb kennt, nicht in die Sache involviert ist und über die nötigen Kompetenzen verfügt. Auch ist auf Interessenkonflikte und etwaige „Beisshemmungen" zu achten: Kann die Untersuchung auch vorgesetzte Stellen betreffen, ist es oft angezeigt, die Führung der Untersuchung einer externen Person anzuvertrauen und dieser intern lediglich zuzudienen.

2. **Bestellen Sie Ihr externes Team.** Falls Sie die Untersuchung von einer externen Person durchführen lassen wollen, werden Sie im Fall der Fälle Ihre Vertrauensperson anrufen, ihr den Fall mitsamt Kontext schildern und ihr die Beweismittel liefern. Diese Person wird dann ihrerseits ein Team zusammenstellen, soweit dies erforderlich ist. Sprechen Sie auch den Beizug von weiteren Dienstleistern ab. In den meisten Fällen braucht es Spezialisten, die IT-Beweise sichern und auswerten können und die die sichergestellten Daten für Untersuchungszwecke bereithalten können. Wird die Untersuchung von einem Anwaltsbüro geleitet, hat sich bewährt, dass dieses die Dienstleister unter Vertrag nimmt (die damit zu seinen Hilfspersonen werden und dem Anwaltsgeheimnis unterstehen), während das Unternehmen sich im Vertrag direkt zur Übernahme der Kosten verpflichtet, so dass diese nicht über das Anwaltsbüro abgerechnet werden müssen. Werden Anwälte ausserhalb Europas involviert, so wird mit diesen ausserdem eine spezielle Datenschutzvereinbarung getroffen werden müssen[9] (→ **Q21**), da das Schweizer Datenschutzrecht (wie auch das EU-Recht) den → **Datenexport**[10] in Länder ohne angemessenen gesetzlichen Datenschutz (wie z.B. die USA) ohne spezielle Vorkehrungen nicht zulässt. Wird eine externe Stelle mit einem Review beauftragt, so muss unter Umständen ein → **Auftragsbearbeitungsvertrag** abgeschlossen werden (→ **Q23**). Dasselbe gilt für eDiscovery-Provider (→ **Q22**). Soweit Sie Anwälte, Audit-Firms oder andere Berater beiziehen, sollten Sie sich bewusst sein, dass diese vor einer Annahme eines Mandats prüfen müssen, ob allenfalls ein Interessenkonflikt vorliegt. Das kann je nach Organisation eine gewisse Zeit dauern. Liegt ein Konflikt vor, werden Sie ein anderes Unternehmen beauftragen müssen. Darauf sollten Sie vorbereitet sein.

Spezialisten

- Anwälte
- IT-Forensiker
- eDiscovery-Provider
- Forensic Accountants
- Scandienste
- Kredit- und Wirtschaftsauskunfteien
- Privatdetektive
- Bewachungsdienste

9 Typischerweise die Standardvertragsklauseln (SCC) der Europäischen Kommission.
10 Hierzu zählt auch der blosse Fernzugriff auf Systeme mit elektronischen Dokumenten in Europa.

Für Anwälte, Berater und eDiscovery-Dienstleister sind interne Untersuchungen attraktiv. Sie sind inhaltlich spannend, bringen oft einiges an Arbeit mit sich und es liegt in der Natur der Sache, dass diese Mandate unter geringerem Kostendruck stehen als andere Fälle; normalerweise kommt ein Kostendach nicht in Frage. Zudem sind viele Klienten in diesem Bereich nicht sehr erfahren und – im Fall der Fälle – auch unter Druck. Trotzdem werden Sie intern in der Regel ein **Budget** beantragen müssen und die **Kosten kontrollieren** wollen. Die Kostenkontrolle beginnt bereits bei der Auswahl des richtigen Partners, der eine interne Untersuchung nicht als „Lizenz zum Gelddrucken" versteht, sondern ungeachtet der Notwendigkeit der Aufklärung des Sachverhalts auch die Kostenfolgen seines Wirkens zur Wahrung der Verhältnismässigkeit im Auge behält. Auch ein seriöser, kostenbewusster Untersucher wird Ihnen nicht im Voraus sagen können, was die Untersuchung kostet. Für die Aufklärung eines kleinen Datendiebstahls durch einen externen Anwalt wird womöglich ein Budget von CHF 10k genügen, während eine Korruptionsuntersuchung auch in einem KMU ohne Weiteres einige CHF 100k kosten kann. **Kostentreiber** sind typischerweise systematische Dokumenten-Sichtungen (→ **Review**), die systematische Aufarbeitung von Transaktionen und Befragungen von Zeugen. Ob es solche braucht bzw. in welchem Umfang, steht zu Beginn jedoch selten fest. Je besser ein Fehlverhalten getarnt wurde oder wird, desto aufwändiger ist seine Enttarnung. In praktischer Hinsicht hat sich bewährt, intern zu Beginn ein Budget einzuholen, das eine gute Einschätzung der Lage und die ersten Schritte erlaubt (z.B. CHF 10-20k), und zugleich das *Expectation Management* zu betreiben, dass da einiges mehr folgen kann. Parallel ist mit den externen Anwälten und Beratern ein Kosten-Reporting und **vor kostenträchtigeren Schritten Rücksprache** zu nehmen. Sind sie kostenbewusst, werden sie das sowieso tun. Es ist aber darauf zu achten, dass sie alle Entscheide über Untersuchungsschritte mittragen, so dass sie später bestätigen können, dass sie alle erforderlichen Untersuchungshandlungen vornehmen konnten. Anders ticken Anwälte aus dem **angelsächsischen Rechtsraum**. Sie sind sich gewohnt, interne Untersuchungen völlig selbständig vorzunehmen und mit grösserer „Kelle" anzurühren, als dies eine Schweizer Kanzlei typischerweise tun würde. Entsprechend hoch können die Kosten ausfallen. Hier kann es sich erfahrungsgemäss lohnen, eine erfahrene hiesige Kanzlei in leitender Stellung miteinzubeziehen, um die Verhältnismässigkeit aus Schweizer Sicht zu wahren.

3. **Definieren Sie das Untersuchungsmandat.** Jede interne Untersuchung folgt einem Mandat, sei es an eine interne Stelle, sei es an einen externen Beauftragten. Dieses Mandat sollte den Auftraggeber definieren, die zu beantwortenden

Fragen, das erwartete Arbeitsergebnis, die Stellung des Untersuchenden und ggf. die ihm zur Verfügung stehenden Mittel und die Organisation. Zu den Fragen, die es zu beantworten gilt, siehe Schritt 5, zur Berichtsform → **BERICHTERSTATTUNG**. Soweit Sie eine Schweizer Anwaltskanzlei mandatieren und in der Schweiz vom Schutz des Anwaltsgeheimnisses profitieren wollen, sollten Sie darauf achten, dass das Mandat eine anwaltstypische Tätigkeit umfasst (z.B. Vorbereitung der Verteidigung oder Durchsetzung von Rechtsansprüchen) und nicht nur die blosse Aufklärung des Sachverhalts (dazu: → **Q10**). Sie sollten sich auch Gedanken darüber machen, wer innerhalb des Unternehmens das Mandat erteilt, wem in welcher Form berichtet werden soll und welchen Grad der Unabhängigkeit und Freiheit der Untersuchende haben soll. Unterstützt der externe Beauftragte lediglich, nimmt er einzelne Abklärungen (z.B. Befragungen) unter Leitung des Unternehmens wahr oder führt *er* die Untersuchung? In letzterem Falle werden Sie wollen, dass der Untersuchende am Ende bestätigt, dass er jede ihm sachgerecht erscheinende Untersuchungshandlung hat vornehmen können und jede von ihm verlangte Unterstützung des Unternehmens erhielt. Dementsprechend müssen Sie ihm auch entsprechende Freiheiten überlassen. Bezüglich des Auftraggebers ist insbesondere auf mögliche Interessenkonflikte zu achten: Richtet sich die Untersuchung möglicherweise gegen einzelne Mitglieder der Geschäftsleitung, wird es angezeigt sein, wenn der Auftrag gerade nicht aus der Geschäftsleitung, sondern dem Verwaltungsrat oder seinem *Audit Committee* erteilt wird und auch diesem zunächst Bericht erstattet wird. Selbst in einer solchen Konstellation ist es ohne Weiteres möglich, einen Mitarbeiter des Unternehmens (z.B. Compliance-Verantwortlicher) als Bindeglied zum Unternehmen einzusetzen. Der externe Untersuchende wird darauf angewiesen sein, dass es eine solche Person gibt, um an Unterlagen zu gelangen, Termine zu vereinbaren und Informationen über Interna zu erhalten. Sie wird jedoch im Rahmen der Untersuchung in der Sache nicht oder nur beschränkt an die Geschäftsleitung rapportieren.

Soweit die Untersuchung intern durchgeführt werden soll, leitet sich die „Mandatierung" der untersuchenden Stelle (z.B. Compliance-Abteilung) in der Regel aus einem internen Reglement (z.B. Untersuchungsreglement, Organisationsreglement) oder einem individuellen Auftrag der Geschäftsleitung oder anderer Stelle ab.

4. **Legen Sie die Projektorganisation fest.** Führen Sie eine Untersuchung nicht alleine durch, sollte mindestens klar sein, wer das Projekt „managed", wie miteinander kommuniziert wird und wer worüber zu informieren ist. Besonderes Augenmerk ist dabei auf die Wahrung der Vertraulichkeit zu legen, d.h. wie sichergestellt werden kann, dass auf die im Team ausgetauschten Informationen keine anderen Perso-

nen Zugriff erhalten. Die Teammitglieder im Unternehmen sollten die Zugriffsberechtigungen für Ihre Postfächer, die Ablageordner und das allenfalls benutzte Dokumenten-Management-System überprüfen. Falls das *Legal Privilege* bzw. Anwaltsgeheimnis von Relevanz ist (→ **Q10**), sprechen Sie sich mit dem Anwalt ab, wie die Kommunikation zu erfolgen hat und Arbeitsprodukte zu bezeichnen sind; in sämtliche Kommunikation sollte ein Vertreter seines Teams einkopiert sein. Selbst wenn mit externen Stellen verschlüsselt kommuniziert wird (die meisten Unternehmen können das inzwischen[11]), sollten sich die Beteiligten bewusst sein, dass diese Verschlüsselung meist nur vor Zugriffen von aussen schützt, nicht unbedingt firmenintern.

Cloud

Immer mehr Unternehmen betreiben ihre IT-Infrastruktur in der Cloud durch internationale Provider. Das birgt das Risiko eines ausländischen Behördenzugriffs. In der Praxis ist dieses aber erfahrungsgemäss sehr gering. Trotzdem sollte bewusst entschieden werden, wo Daten aus der Untersuchung gespeichert werden.

5. **Definieren Sie die Fragen, die es zu beantworten gilt.** Jede interne Untersuchung soll im Ergebnis auf eine oder mehrere Fragen entsprechende Antworten liefern. Dies können Fragen zum Sachverhalt, zur rechtlichen Einordnung (nicht nur nach inländischem oder ausländischem Recht, sondern auch internen Regeln oder Vorgaben der Selbstregulierung) und zu möglichen Abhilfe- und Verbesserungsmassnahmen sein. Hat ein bestimmter Mitarbeiter gegen die vom Arbeitgeber und Gesetz definierten Regeln im Umgang mit seinen Mitarbeitern verstossen? Hat der Arbeitgeber seine Aufsichtspflichten verletzt? Ist es im Rahmen der Rückerstattungspraxis an Kunden zu systematischen Unregelmässigkeiten gekommen? Welcher Natur waren die an eine bestimmte Person getätigten Zahlungen? Wurde in der Vergabe eines Projektauftrags gegen die gesetzlichen Bestimmungen des Schweizer Korruptionsrechts verstossen? Gegen den US *Foreign Corrupt Practices Act* (FCPA)? Gegen den UK *Bribery Act*? Falls es zu Unregelmässigkeiten gekommen ist, wer war daran beteiligt? Treffen die Vorwürfe des Whistleblowers zu? Wie sind sie rechtlich zu werten? Welche Umstände (Organisationsmängel) haben die Tat begünstigt? Welche Umstände haben die Aufdeckung der Unregelmässigkeiten erschwert? Welche Ansprüche stehen dem Unternehmen gegen etwaige Dritte zu? Welche Ansprüche stehen Dritten gegenüber dem Unternehmen zu? Welche Schritte werden dem Unternehmen in Bezug auf eine Offenlegung gegenüber den Behörden empfohlen? Wie sollten die fehlbaren Mitarbeiter sanktioniert werden? Einige dieser Fragen können sich freilich auch erst im Verlaufe der internen Un-

11 Weitgehend Standard ist „TLS“, ein Verfahren zur Verschlüsselung der Verbindung von Server zu Server. Auch breit verfügbar, aber oft nicht standardmässig eingesetzt, ist „S/MIME“, ein Ver-fahren, um den Inhalt einzelner E-Mails zu verschlüsseln.

tersuchung oder nach ihrem Abschluss stellen und separat beantwortet werden. Mehr dazu in → **BERICHTERSTATTUNG** und → **WEITERE SCHRITTE**.

6. **Legen Sie eine Strategie fest, wie Sie die Fragen beantworten.** Es gibt kein Standardrezept, wie sich vermutete Unregelmässigkeiten in einem Unternehmen aufklären und Sie die gestellten Fragen beantworten lassen. Je nach Thema drängen sich jedoch bestimmte typische erste Untersuchungsschritte und ein bestimmtes Vorgehen auf. Steht der Vorwurf einer sexuellen Belästigung im Raum, stehen beispielsweise Befragungen im Vordergrund und allenfalls der Zugriff auf erfolgte Kommunikation, Inhalte in sozialen Medien und Reglemente. Geht es um Finanzdelikte, werden Daten aus der Finanzverwaltung des Unternehmens analysiert werden, bevor die Befragung der Hauptpersonen ein Thema ist. Im Falle eines Datendiebstahls werden Protokolle der IT-Systeme und E-Mails nach Hinweisen auf einen Datenabfluss geprüft werden müssen. In manchen Fällen führt eine Durchsuchung von E-Mails zu wichtigen Erkenntnissen, wobei hier verschiedene Methoden zur Verfügung stehen und häufig vergessen wird, dass es in vielen Betrieben auch noch andere, für eine Untersuchung sehr aufschlussreiche Datenquellen geben kann. Gefragt ist hier nicht juristisches Know-how (ausser bei der Frage, was an Massnahmen erlaubt ist), sondern Wissen über die Funktionsweise eines Betriebs, die Möglichkeiten der Technik und Ermittlungshandwerk – und viel Spürsinn. Das sollte daher bei der Auswahl eines Anwalts oder Beraters berücksichtigt werden. Die Erfahrung zeigt, dass in manchen internen Untersuchungen das Aufklärungspotenzial nicht ausgeschöpft wird, weil es am Wissen um oder Ideen über mögliche Informationsquellen oder Ermittlungsstrategien fehlt.

   ☝ **Begonnen** wird üblicherweise mit einer Befragung eines etwaigen Hinweisgebers, wenn eine solche möglich ist und seine Ausführungen nicht bereits hinreichend detailliert sind. Der nächste Schritt ist typischerweise die Sichtung von Daten und Dokumenten, um ein möglichst klares Bild der Sachlage zu erhalten. Es folgen in der Regel Befragungen, wo versucht wird, den im Rahmen der Sichtung gewonnenen Eindruck zu bestätigen, Lücken zu ergänzen und weitere Informationen zu gewinnen. Die beschuldigte Person wird häufig **zum Schluss** befragt, um sie mit den gewonnenen Erkenntnissen konfrontieren zu können.

7. **Erstellen Sie (bei Bedarf) einen Untersuchungs-Plan.** In der Literatur wird regelmässig empfohlen, einen *"Investigation Plan"* zu erstellen, d.h. einen Plan mit den einzelnen Schritten, die im Rahmen der Untersuchung durchgeführt werden sollen, um die gestellten Fragen zu beantworten. Dies empfiehlt sich vor allem für Personen, die mit internen Untersuchungen noch nicht viel Erfahrung haben oder in grösseren, komplexeren Fällen mit vielen Beteiligten. Im letzteren Fall dient er allerdings primär dem Projekt-Management. Sie werden rasch merken, dass es

viel wichtiger ist, an alles zu denken und die richtigen Fragen zu stellen (dabei hilft Ihnen dieses Handbuch), den richtigen Anfangspunkt für die Untersuchung zu finden und danach den Gang der internen Untersuchung flexibel den laufenden Erkenntnissen anzupassen, als die Untersuchung von Anfang an durchzuplanen und zu terminieren. Punkto Dokumentation kommt es primär darauf an, dass Sie das festhalten, was Sie tatsächlich getan haben und warum (dazu Schritt 20).

☝ Interne Untersuchungen sind erfahrungsgemäss effizienter und effektiver, wenn sie sog. **agil** erfolgen. Diese Vorgehensmethode hat bereits die Softwareentwicklung revolutioniert: Statt die zu entwickelnde Software von Anfang an vollständig zu spezifizieren, wird sie etappenweise definiert und entwickelt (in *"Sprints"*). Nach jeder Etappe findet eine erneute Standortbestimmung statt und die nächste Etappe wird festgelegt, um ans (grob) definierte Endziel zu gelangen. Auf eine interne Untersuchung angewandt bedeutet dies, dass nicht zuerst die Erhebung aller Beweise und dann die Auswertung aller Beweise erfolgt, sondern Erhebung und Auswertung von Beweisen sich laufend abwechseln und einander beeinflussen.

8. **Treffen Sie allenfalls nötige Sofortmassnahmen zum Schutz von Arbeitnehmern und des Unternehmens.** In gewissen Fällen liegt mit einem Hinweis bereits so viel vor, dass ein Unternehmen nicht den Ausgang der Untersuchung abwartet, bevor es Massnahmen trifft, um potenziell weiteren Schaden oder Rechtsverstösse zu vermeiden. Das kann Mitarbeiter betreffen (die z.B. intern versetzt werden oder von der Arbeit dispensiert werden müssen, um keiner weiteren sexuellen Belästigung oder keinem weiteren Mobbing ausgesetzt zu sein), aber auch das Unternehmen selbst (z.B. kann es angezeigt sein, verdächtige Zahlungen zu stoppen oder bei vermuteten Verstössen gegen Sanktions- und Exportkontrollbestimmungen weitere Lieferungen in bestimmte Länder einzustellen). Allerdings ist darauf zu achten, dass eine solche Massnahme keinen präjudizierenden Charakter hat, nicht ihrerseits zur Verletzung der Persönlichkeit anderer Arbeitnehmer führt (d.h. bestimmte Personen zum „Täter" abstempelt) oder das Ziel einer Untersuchung vereitelt (indem fehlbare Mitarbeiter merken, dass ihnen das Unternehmen auf die Schliche gekommen ist und Beweise vernichten).

9. **Bestimmen Sie, wer in die Sache involviert sein könnte.** Im Zentrum einer Untersuchung stehen in den meisten Fällen einzelne Personen, die gehandelt, zugelassen oder beobachtet haben. Der Kreis

Bleiben Sie …

… auch gegenüber sich selbst wachsam, wenn Sie über Zielpersonen nachdenken. Das gilt nicht nur für Personen, die Antipathien wecken, sondern auch solche, bei denen das Gegenteil der Fall ist.

dieser Personen kann sich im Laufe einer Untersuchung ausweiten, verengen oder verändern. Es geht hier nicht nur darum, mögliche *"Targets"* (Ziele) zu bestimmen, sondern auch andere Personen, die mit ihrem Wissen über Geschehnisse oder andere Dinge zur Untersuchung beitragen können.

☝ Werden elektronische Daten gesichert, so wird zwischen persönlichen Daten (z.B. ein Postfach, der Inhalt eines Notebooks oder persönlichen Laufwerks) und gemeinsamen Daten (z.B. Gruppenlaufwerke, Daten in Dokumentenmanagementsystemen, Daten in EPR-Systeme oder Branchenlösungen) unterschieden. Bei ersteren wird derjenige, dem die Daten zugeordnet sind, allgemein als → **Custodian** (Verwahrer) bezeichnet. Geht es darum, Daten zu sichern (d.h. vor einer Vernichtung oder Veränderung zu sichern), wird der Kreis der *Custodians* weit gezogen, während die Auswertung aus Kosten- und Zeitgründen zunächst auf die für den Fall wichtigsten *Custodians* beschränkt werden sollte.

10. **Überlegen Sie, wo es überall relevante Informationen haben kann.** Eine Untersuchung lebt von Beweisen, welche den Sachverhalt erhellen, und Sie werden diese finden müssen. Daher müssen Sie zunächst ein Verständnis für die möglichen Informationsquellen entwickeln. Hierbei ist nicht nur an E-Mails und elektronische Dokumentenablagen zu denken, sondern auch an sog. → **strukturierte Daten**[12] (z.B. in einer Buchhaltungslösung, in der Auftragsverwaltung oder in Logs von IT-Systemen und Zutrittskontrollen aller Art). Relevante Informationen kann es z.B. auch in Papierbelegen, in Aufzeichnungen von Sicherheitskameras, Messaging- und Chat-Diensten, Telefonaten und Videokonferenzen haben (allenfalls auch bei einem externen Provider) und natürlich auf den Notebooks und anderen mobilen Geräten der Mitarbeiter.

☝ Es zählt alles, **was dem Unternehmen gehört** oder von diesem kontrolliert wird. Das kann auch ein privates Mobiltelefon des Mitarbeiters sein (→ **Bring-your-own-Device**, BYOD), sofern es darin einen virtuellen, dem Unternehmen vorbehaltenen Bereich hat. Weil ein Zugriff auf ein **privates Gerät** jedoch die Privatsphäre des Mitarbeiters tangieren kann, stellt ein Unternehmen von Vorteil vorgängig klare Regeln auf, wie und in welchen Fällen es auf solche Geräte und die darin enthaltenen Daten zugreifen kann. Ein weitergehender Zugriff auf private Geräte (oder private Konten) eines Mitarbeiters bedarf einer genauen Klärung der Rechtslage, ist aber nicht per se ausgeschlossen (dazu → **Q19** und → **Q20**).

12 Zur Untersuchung solcher Daten: → **ANALYSE STRUKTURIERTER DATEN**.

11. **Erstellen Sie einen *Collection Plan*.** Die verschiedenen Datenquellen für die von Ihnen als potenziell relevant eingestuften Informationen sollten Sie in einem *"Collection Plan"* zusammentragen. Sie können diese über Zeit entsprechend ausbauen, falls weitere Datenquellen hinzukommen. Der *Collection Plan* hilft Ihnen, den Überblick zu bewahren und erlaubt Ihnen auch, die Sicherung und Beschaffung der Beweise und von weiteren Daten zu planen (z.B. Prioritäten festzulegen). Es gehen Ihnen auf diese Weise auch keine Datenquelle vergessen.

12. **Sorgen Sie für eine Sicherung der Beweise.** Sind die Quellen möglicherweise für den Fall relevanter Beweise identifiziert, müssen Sie sicherstellen, dass diese nicht mehr verloren gehen können, sei es im ordentlichen Geschäftsgang (z.B. Überschreiben von *Backups*, turnusgemässe Vernichtung von Daten), sei es mutwillig (durch Personen, welche Beweise verschwinden lassen, falsche Fährten legen oder ihre Spuren verwischen). Dabei ist sicherzustellen, dass die Beweiskraft erhalten bleibt (wie z.B. der Nachweis der Unverfälschtheit und Erhalt der Metadaten).

> **"Preservation"**
>
> So heisst die Sicherung im Fachjargon. Sie erfolgt *"in place"* (d.h. die Löschung und Veränderung wird vom System blockiert) oder durch Einsammeln (*"collect"*).

13. **Beginnen Sie mit der zentralen Sicherung.** Dort, wo die Informationsquellen zentral verwaltet werden, wird häufig auch die Möglichkeit bestehen, die Beweise zentral zu sichern, d.h. ohne Einbezug der *Custodians* und weiteren Benutzern der betroffenen Systeme. Sie werden diese Sicherung bestenfalls nicht einmal bemerken. Benutzt ein Unternehmen ein E-Mail-System in der Cloud, kann die Sicherung der Beweise mit einem Knopfdruck erfolgen; das System blockiert jede weitere Löschung oder Veränderung der Daten, aber das E-Mail-System läuft normal weiter. Wo dies nicht möglich ist, muss ggf. eine Kopie der Daten (z.B. des Postfachs) gezogen werden. Das hat den Nachteil, dass nur der bis dahin bestehende Datenbestand erfasst ist, d.h. ggf. später weitere Kopien vorgenommen werden müssen. Solche Sicherungen kann in der Regel die hausinterne IT problemlos machen. Sie kann auch beurteilen, ob eine Löschung von Daten drohen kann. In einem Buchhaltungssystem, wo Buchungen nicht nachträglich geändert oder gelöscht werden können und

> **Datenschutz?**
>
> Die Sicherung von Daten zu Beweiszwecken ist datenschutzrechtlich in der Regel unproblematisch und kann (oder muss aus ermittlungstaktischen Gründen) sogar geheim erfolgen. Der Zugriff auf die gesicherten Daten ist aber strikt zu beschränken.

hinzugefügte Buchungen als solche zu erkennen sind, sind besondere Sicherungsmassnahmen in der Regel nicht erforderlich.

14. **Sorgen Sie für die dezentrale Sicherung der Beweise.** Dort, wo physische Akten einzusammeln oder mobile oder lokale Geräte zu sichern sind (deren Inhalt nicht bereits *"remote",* d.h. aus der Ferne über ein Netzwerk gesichert werden konnte), sollten Sie dies erst tun, wenn die zentrale Sicherung sichergestellt wurde, da eine dezentrale Sicherung von Akten und Daten meistens bemerkt wird. Gesichert wird normalerweise, indem Kopien erstellt oder im Falle von Akten die Originale sichergestellt werden. Für das Erstellen von Datenspiegelungen gibt es IT-Forensiker, die das in einer solchen Form machen, dass später kein Vorwurf der Beweismanipulation erhoben werden kann (es wird dazu u.a. der sog. → **Hash-Wert** ermittelt und festgehalten, um die Beweisintegrität zu gewährleisten). Dies kann auch unbemerkt geschehen. Beweissicherungen von physischen Akten oder dort, wo es einen Zugangscode des *Custodians* braucht, sind natürlich schwerer oder nicht zu tarnen. Aus ermittlungstaktischen Gründen muss daher allenfalls entschieden werden, diesen Schritt zu verschieben. Dem steht natürlich das Risiko einer Beweisvereitelung durch einen aufgeschreckten Täter gegenüber.

> ☝ Wenn Sie **Aktenordner mitnehmen**, denken Sie daran, dass diese für den laufenden Betrieb möglicherweise gebraucht werden. Seien Sie sich bewusst, dass das Kopieren von Aktenordnern viel Zeit beanspruchen kann, da dies weitgehend Handarbeit darstellt. Müssen Dutzende von Ordnern kopiert oder gescannt werden, weil noch nicht klar ist, wo sich die relevanten Informationen befinden, benötigen dafür selbst Spezialfirmen mehrere Tage; die Kosten können sich je nach Vorlage (z.B. geheftete Belege) und Verarbeitungsart (Einzelscans) rasch auf weit über CHF 10k belaufen.

15. **Verhängen Sie einen Vernichtungsstopp.** Das Schweizer Recht verlangt dies zwar nicht, aber das Konzept des sog. → **Legal Hold** aus den USA gehört auch hierzulande zu den Sorgfaltspflichten einer internen Untersuchung (hier teilweise auch als „*Investigation Hold*" bezeichnet): Die Mitarbeiter, die möglicherweise relevante Unterlagen oder Daten haben, werden verbindlich angewiesen, diese Daten weder zu vernichten noch zu verändern. In der zu diesem Zweck verteilten sog. → **Legal Hold Notice** wird kurz der Anlass erläutert – auch das Thema, um das es geht – und es wird erläutert, was konkret erwartet wird. Der genaue thematische Umfang des *Legal Hold* sollte

Vereitelung?

Die Vernichtung oder Manipulation von Beweismitteln kann auch strafrechtliche Konsequenzen haben. Zu denken ist etwa an Begünstigung, Geldwäscherei, Unterdrückung von Urkunden, Urkundenfälschung und Datenbeschädigung.

mit den Anwälten abgesprochen sein. Je nach Fall kann dieser über längere Zeit bestehen, was betrieblich entsprechende Behinderungen mit sich bringen kann (und je nachdem viel Speicherplatz kostet). Der Kreis der Empfänger eines *Legal Hold* wird typischerweise breit gefasst und bedeutet nicht, dass gegen diese Personen ermittelt wird; möglicherweise haben sie lediglich relevante Informationen bei sich. Wer einen *Legal Hold* verletzt, muss wie bei sonstigen Weisungsverstössen mit arbeitsrechtlichen Folgen rechnen. Dokumentieren Sie daher den Zeitpunkt der Mitteilung bzw. Kenntnisnahme. Da mit einer *Legal Hold Notice* bezüglich der Durchführung einer internen Untersuchung die Katze normalerweise aus dem Sack ist, kann sie auch benutzt werden, um die Mitarbeiter über die mögliche → **Bearbeitung ihrer Daten** (z.B. Sichtung von E-Mails) aufzuklären. Dies ist aus datenschutzrechtlicher Sicht geboten, sofern keine ermittlungstaktischen Gründe es erfordern, dass die Information aufgeschoben wird.

Grössere Unternehmen erlassen und verwalten ihre *Legal Hold Notices* heute mit speziell **dafür programmierten Systemen**, welche u.a. protokollieren, welche Mitarbeiter die Hinweise wann erhalten und geöffnet haben.

16. **Sammeln Sie die benötigten Beweismittel ein.** Die Sichtung der gesicherten Daten und Unterlagen erfolgt jedenfalls bei unstrukturierten Daten normalerweise nicht vor Ort oder in den Systemen, in denen sie üblicherweise bearbeitet werden. Insbesondere E-Mails, Chats und elektronische Dokumente werden in spezielle sog. → **Review-Systeme** überführt, die spezifisch für die effiziente und effektive Auswertung solcher Daten entwickelt wurden (mehr dazu im Kapitel → **WERKZEUGE FÜR EDISCOVERY**). Unternehmen verfügen normalerweise nicht selbst über solche Review-Systeme oder nur in beschränkter Weise. Sind Daten erst einmal gesichert worden, werden sie normalerweise schrittweise eingesammelt und es wird entschieden, welche davon in die Review-Systeme zur weiteren Auswertung eingelesen werden. Weil dieser Vorgang mit Zeit und Geld verbunden ist, macht auch hier in aller Regel ein schrittweises Vorgehen Sinn; sie können dies in Ihrem *Collection Plan* entsprechend vermerken. Es werden nie gleich alle Daten eingelesen, sondern die Verarbeitung wird z.B. auf bestimmte Zeiträume oder → **Custodians** beschränkt. Mehr zur Durchführung von Reviews im Kapitel → **DOKUMENTEN-REVIEWS** und zur Analyse von strukturierten Daten im Kapitel → **ANALYSE STRUKTURIERTER DATEN**.

Collection Plan

Führen Sie den *Collection Plan* laufend nach und stimmen Sie ihn mit Ihrem eDiscovery-Provider ab. Sie können ihn auch zur Protokollierung der einzelnen Schritte benutzen.

Aus rechtlicher Sicht ist hier zunächst der **Datenschutz** zu beachten. Während das Sichern und Einsammeln von Daten datenschutzrechtlich normalerweise unproblematisch ist, sind im Rahmen der Auswertung bestimmte Vorgaben zu beachten. Diese dienen primär dem Schutz der Privatsphäre der Mitarbeiter, doch zu denken ist auch an andere Personen, die in den Daten vorkommen können. Der Zugriff auf private Daten ist z.B. nur eingeschränkt möglich. Auch muss generell die Auswertung auf das beschränkt werden, was für die Wahrung der legitimen Untersuchungsinteressen notwendig ist. Einzuschränken ist auch der Kreis der Personen, die Zugriff erhalten (z.B. soll der Vorgesetzte nicht in das persönliche Postfach des Mitarbeiters Einblick nehmen; dies sollte einer unbeteiligten Person vorbehalten sein). Mehr dazu in → **Q18** und → **Q19**. Zu beachten sind allerdings auch **Geheimhaltungsinteressen** des Unternehmens und von Dritten und insbesondere auch ein etwaiges **Berufsgeheimnis** (z.B. das Bankkundengeheimnis). In einer Untersuchung können sehr rasch sehr viele sensible Daten zusammenkommen (z.B. die gesamte Mailbox eines Geschäftsleitungsmitglieds). Dementsprechend muss die Vertraulichkeit und Datensicherheit bei den involvierten internen und externen Stellen sichergestellt werden (z.B. eDiscovery-Provider, Scandienstleister). Das bedingt auch die Klärung der Frage, wo in örtlicher Hinsicht die gesicherten Daten gespeichert werden können und dürfen (z.B. nur auf Servern in der Schweiz oder in Europa) und von wo aus Zugriffe möglich sein sollen (z.B. auch aus den USA für die dortigen Anwälte? → **Q21**). Diese Fragen sind rechtlich und vorgängig zur internen Untersuchung - unter Berücksichtigung der Umstände des Einzelfalles – zu klären.

17. **Lassen Sie ein *Early Case Assessment* durchführen.** Spielen E-Mails und andere elektronische Daten und Unterlagen im Fall eine relevante Rolle, so lohnt es sich erfahrungsgemäss, sich vor einer systematischen (und aufwändigen) Sichtung einen ersten Eindruck von den verfügbaren Daten zu schaffen und damit „zu spielen", um durch gezielte Suchläufe, Analysen und Auswertungen rasch relevante Hinweise auf den Sachverhalt zu erhalten. Dies setzt Übung mit solchen Recherchen und den diversen Funktionen der dafür benutzten Systeme voraus (mehr dazu im Kapitel → **WERKZEUGE FÜR EDISCOVERY**). Die so gewonnenen Informationen und Eindrücke erlauben es, die weiteren Untersuchungsschritte besser zu planen und gezielter anzugehen. Es kann z.B. ermittelt werden, mit wem bestimmte

Mailverteiler

Ist ein grösseres Team mit einer internen Untersuchung beschäftigt, so lohnt es sich, einen E-Mail-Verteiler für das Team einzurichten. So sind immer gleich alle informiert und Wechsel können leicht umgesetzt werden.

Zielpersonen in besonders engem Kontakt standen, welche Menge an Dokumenten es zu sichten gibt, in welcher Sprache sie abgefasst oder welcher Natur sie sind. Im günstigsten Fall können mit einigen Stunden Aufwand bereits auch erste Ermittlungsergebnisse (z.B. verdächtige E-Mail-Kommunikation) erzielt werden, die Ansatzpunkte für weitere Recherchen bieten. Ein *Early Case Assessment* ist auch wichtig, um die Suchstrategie für breiter angelegte Reviews festzulegen.

18. **Verfolgen Sie die Untersuchungsstrategie.** Eine Untersuchung ist häufig Fleissarbeit und braucht ihre Zeit. Neben dem Spürsinn, Genauigkeit und einem Blick für Details sowie für das grosse Ganze erfordert eine interne Untersuchung allerdings auch sehr viel Projektmanagement. Das Team will geführt und motiviert werden. Hierbei ist eine regelmässige Abstimmung im Team wichtig, was auch beinhaltet, dass die einzelnen Teammitglieder sich gegenseitig über ihre jeweiligen Erkenntnisse informieren, auch wenn auf den ersten Blick nicht klar ist, ob eine bestimmte neue Information zum Sachverhalt für alle Teammitglieder von Belang ist. Die Erfahrung zeigt allerdings, dass gut informierte Teammitglieder nicht nur motivierter, sondern dass die von ihnen zu verarbeitenden Daten und Unterlagen besser einzuordnen sind. Geht z.B. aus einer Information hervor, dass eine bestimmte Person mit einer anderen eine Liebesbeziehung unterhält, kann eine Transaktion zwischen den beiden Personen in einem anderen Kontext in einem völlig anderen Bild erscheinen.

19. **Bewerten Sie die Strategie regelmässig und passen Sie sie an.** Eine Untersuchung sollte ergebnisoffen durchgeführt werden. Das bedeutet aber auch, dass Sie bereit sein müssen, die gewählte Strategie und Stossrichtung bei Bedarf anzupassen. Es ist nicht ungewöhnlich, dass Untersuchungen ungewöhnliche Wendungen nehmen können. Aus dem Korruptionsverdacht eines einzelnen Mitarbeiters kann plötzlich ein gemeinsam geplantes Steuerdelikt werden, und eine Meldung über sexuelle Belästigung noch ganz andere Missstände ans Tageslicht bringen.

> ☝ Kommt es im Rahmen einer internen Untersuchung zu einem **Zufallsfund**, wird in der Regel separat entschieden werden müssen, ob und wie der Sache nachzugehen ist. Das betrifft auch die Vornahme weiterer rechtlicher Schritte, wie z.B. das Erstatten einer Strafanzeige. Eine rechtliche Pflicht hierzu hat ein Unternehmen normalerweise nicht.

20. **Dokumentieren Sie die Untersuchungsschritte.** Es macht natürlich einen Unterschied, ob Sie eine interne Untersuchung nur durchführen, damit das Unternehmen den Sachverhalt versteht und Massnahmen ergreifen kann, oder, ob gerichtsverwertbare Beweismittel für rechtliche Schritte gesammelt werden sollen. Davon kann abhängen, wie „forensisch sauber" Sie bei der Durchführung der Untersuchung vorgehen müssen, sprich wie gut Sie jeden Schritt dokumentieren oder dokumentieren lassen. Auch ein Untersuchungsbericht muss nicht nur die

Untersuchungsergebnisse darlegen, sondern auch, wie sie zustande gekommen sind. So oder so empfiehlt es sich aus Gründen der Nachvollziehbarkeit und damit Glaubwürdigkeit der Ergebnisse, dass die relevanten Untersuchungsmassnahmen in entsprechender Form dokumentiert werden. Dokumentiert werden sollte auch, warum bestimmte Schritte unternommen wurden und warum auf gewisse Schritte verzichtet wurde (z.B. weitergehende Datensichtungen, weil sie aktuell keine relevanten Erkenntnisgewinne versprechen, aber für den Fall der Fälle aufgrund der gesicherten Daten weiterhin möglich sind).

Sichern IT-Forensiker Daten von einem Notebook, Server oder sonst einem System, werden sie den physischen Besitz der dazu verwendeten Datenträger vom initialen Sicherungsvorgang an in einem **Protokoll dokumentieren**, so dass lückenlos nachvollzogen werden kann, wer den betreffenden Datenträger wann in seiner Hand hatte (*"chain of custody"* oder *"CoC"*). Was dabei aber im Einzelnen geschieht, kann damit aber nicht nachvollzogen werden. Es ist vielmehr eine Art Übergabeprotokoll. Zusätzlich zur Dokumentation sollten sichergestellte Daten wenn möglich in einem sog. **forensischen Container** abgespeichert werden, welcher sicherstellt, dass Daten während der Untersuchung nicht verändert werden. Arbeitskopien sollten mit dem Original verknüpft bleiben. Es gilt zu beachten, dass bereits ein Öffnen einer beweisrelevanten Datei zu Veränderungen gewisser Metadaten führen kann oder sich Dokumente in bestimmten Formaten (z.B. Excel) automatisch aktualisieren und das Dokument dadurch seine Beweiskraft verliert.

Do's	Don'ts
• Führen Sie eine interne Untersuchung ergebnisoffen und agil durch; seien Sie fair zu allen Beteiligten. • Dokumentieren Sie, was Sie wann tun und warum; dokumentieren Sie aber auch, worauf Sie verzichten und warum. Dazu gehört auch ein *Collection Plan* für die diversen Datenquellen.	• Rechnen Sie nicht damit, dass eine interne Untersuchung kostengünstig sein wird. • Lassen Sie sich durch Anwälte und Berater nicht blenden, vor allem nicht mit Werbung für irgendwelche *Tools* auf Basis „künstlicher Intelligenz"; viele halten nicht, was sie versprechen, und es kochen letztlich alle nur mit Wasser – auch die grossen Namen; viel wichtiger als die *Tools* ist die Erfahrung.

Do's	Don'ts
• Sorgen Sie dafür, dass ihre Anwälte und Berater kosten- und zeitintensive oder heikle Untersuchungshandlungen mit Ihnen absprechen. • Hinterfragen Sie kostspielige Massnahmen kritisch, z.B. warum sie im geplanten Umfang nötig sind und der Nutzen in einem vernünftigen Verhältnis zum Aufwand steht. • Beachten Sie den Datenschutz, sobald Sie es mit personenbezogenen Daten zu tun haben; er wird Ihnen letztlich meist nicht im Weg stehen. • Halten Sie den Kreis der im eigenen Unternehmen involvierten Personen möglichst klein. • Beim Sichern gilt lieber mehr als weniger, beim Auswerten geht Qualität vor Quantität: Die Nadel findet sich nicht einfacher, wenn der Heuhaufen grösser gemacht wird.	• Unterschätzen Sie nicht den psychologischen Druck, den eine interne Untersuchung auf Mitarbeiter haben kann. • Schieben Sie die Beweissicherung nicht auf, denn was weg ist, ist weg; für die Auswertung danach haben Sie in der Regel mehr Zeit. • Unterlassen Sie es nicht, ihre externen Berater vertraglich korrekt zu verpflichten – auch im Hinblick auf den Datenschutz und, wo relevant, auf das Anwaltsgeheimnis.

Wann Sie externe Unterstützung beiziehen sollten

- In den unter → **DIE RICHTIGE VORBEREITUNG** aufgezählten **Fällen** für den Beizug externer Personen für eine interne Untersuchung.
- Wenn sich zeigt, dass der Fall **grösser oder komplexer** ist, als Sie ursprünglich angenommen haben und Sie ihn nun doch nicht mehr selbst „stemmen" können.
- Wenn der Fall sich so entwickelt, dass die Leitung aus **taktischen oder innenpolitischen Gründen** einer externen Person übergeben werden muss.
- Weil Sie nur so den Untersuchungsaufwand auf die **Versicherung** oder **auf einen Dritten abwälzen** können.

- Falls Sie mit Anwälten oder Beratern arbeiten müssen, die es aber möglicherweise übertreiben werden, und Sie **Schützenhilfe** brauchen, um diese in Schach zu halten.
- Wenn Sie Mühe haben, **den richtigen Ansatz** für die Untersuchung zu finden.
- Wenn sich zeigt, dass Ihre eigenen IT-Fachkräfte doch nicht in der Lage oder Willens sind, die nötige **Sicherung und Aufbereitung der Daten** vorzunehmen, z.B. weil es plötzlich um sehr viel mehr Daten als ursprünglich angenommen geht oder die Fachkräfte nicht schnell genug handeln können.
- Wenn Sie sich **unsicher fühlen** oder eine **Zweitmeinung** benötigen.

Häufige Fragen und Antworten

Q14. Inwiefern müssen wir unsere Mitarbeiter über eine interne Untersuchung informieren?

A: Es besteht grundsätzlich **keine Pflicht des Arbeitgebers** die Mitarbeiter über eine interne Untersuchung zu informieren. Jedoch ist es teilweise sinnvoll, über einige Aspekte der internen Untersuchung aufzuklären, etwa um Gerüchten entgegenzuwirken und als vertrauensbildende Massnahme oder um weitere Hinweise zu erhalten. In diesem Zusammenhang sind mitunter Aspekte wie die **Schwere der Vorwürfe** und deren **Öffentlichkeit** (z.B., wenn bereits medial über die Vorwürfe berichtet wird) zu beachten.

Beim Entscheid, ob und inwieweit die Mitarbeiter über eine interne Untersuchung zu informieren sind, sind ferner **ermittlungstaktische Erwägungen** sowie **Vertraulichkeitsüberlegungen** miteinzubeziehen. Die Information der Mitarbeiter sollte die Ermittlungen nicht verhindern oder unnötig erschweren und die (Persönlichkeits-) Rechte des Einzelnen sind zu wahren. Auch muss berücksichtigt werden, dass je mehr Personen über die interne Untersuchung informiert werden, desto eher die Wahrscheinlichkeit besteht, dass die Information an die Öffentlichkeit gelangt. Auch die **externe Kommunikation** ist somit in den Entscheid miteinzubeziehen und idealerweise sind die interne und externe Kommunikation aufeinander abzustimmen.

Selbstredend sind jene Mitarbeiter über die interne Untersuchung zu einem geeigneten Zeitpunkt zu informieren, die von der internen Untersuchung **betroffen** sind, weil diese als Beispiel die entsprechenden Auskünfte erteilen müssen oder ein **Recht zur Stellungnahme** haben. Eine Information wird mindestens und spätestens dann erfolgen müssen, falls sich Vorwürfe gegen eine Person erhärtet haben und eine **Sanktion** oder andere Folgen im Raum stehen.

Zu prüfen ist auch, in welchem Umfang der Mitarbeiter zu informieren ist. Grundsätzlich sollte die Information darauf hinwirken, den Mitarbeiter von einer Kooperation zu überzeugen und sein Vertrauen zu gewinnen (ausführlich zur Aufklärung des Arbeitneh-

mers vor einer Befragung: → **Q33**). Nach unserer Erfahrung ist eine offene Kommunikation bezüglich der Aspekte, die klar sind und einen Mitarbeiter in seiner Aussage oder Situation direkt betreffen, vorteilhafter und vertrauensfördernder als Heimlichtuerei. Allerdings ist es wichtig, die verwendeten Worte sorgfältig zu wählen, um Entscheidungen und Einschätzungen nicht vorwegzunehmen oder den Eindruck einer Zusage zu erwecken, wo eine solche nicht gewollt ist. Der Befrager sollte auch darauf achten, dass er einer als Zeuge befragten Person nicht mehr über den untersuchten Verdacht verrät, als diese für ihre Aussage wissen muss. Der Arbeitgeber hat auch die Person des Beschuldigten zu schützen. Denn auch wenn alle befragten Arbeitnehmer zur Geheimhaltung verpflichtet werden können (→ **Q35**), lässt sich eine solche normalerweise nur beschränkt durchsetzen. Falls einem Mitarbeiter rechtliches Gehör (dazu → **Q15**) gewährt werden muss, sollte die Information jedenfalls alles umfassen, was für die angemessene Wahrnehmung dieses Gehörs notwendig ist.

Eine Information von Mitarbeitern lässt sich auch dort nicht vermeiden, wo eine → **Legal Hold Notice** erlassen, also ein **Vernichtungsstopp** angewiesen werden muss. Die Weisung beinhaltet regelmässig auch Angaben zum Anlass und Thema des Vernichtungsstopp. Auch gewisse **Untersuchungsmassnahmen** wie etwa die Sichtung von E-Mail-Postfächern erfordern an sich eine Information, auch wenn die Ermittlungstaktik es erforderlich machen kann, dass sie zunächst ohne Mitwirkung erfolgt. Allerdings tut ein Unternehmen gut daran, die Möglichkeit solcher Untersuchungsmassnahmen vorgängig **in allgemeiner Form bekanntzumachen** (z.B. in Reglementen, Weisungen, Datenschutzhinweisen).

Ist bekannt oder wird vermutet, dass eine interne Untersuchung stattfindet, kann dies **datenschutzrechtliche Auskunftsersuchen** zur Folge haben (→ **Q15**), die binnen 30 Tagen beantwortet werden müssen – wenngleich dies auch abschlägig erfolgen kann (→ **Q57**).

Was sich in aller Regel ab einer gewissen Zeitdauer, Schwere oder Grösse der Untersuchung nicht verhindern lässt, sind **Gerüchte und Klatsch**, was beides rasch ein Eigenleben entwickeln kann. Teilweise kann es sich daher lohnen, für die interne sowie auch externe Kommunikation **Experten** beizuziehen und mit der beschuldigten Person darüber zu sprechen, welchen Umgang sie in der Angelegenheit wünscht. Zur externen Kommunikation vgl. → **WEITERE SCHRITTE**.

Literatur:

Götz Staehelin, Claudia: Unternehmensinterne Untersuchungen, Zürich/Basel/Genf 2019

Wantz, Simona/Licci, Sara: Arbeitsvertragliche Rechte und Pflichten bei internen Untersuchungen, Jusletter vom 18. Februar 2019, Rz. 1 ff.

Q15. Wer kann Einblick in die Unterlagen einer internen Untersuchung nehmen?

A: Die Arbeitsprodukte interner Untersuchungen (Befragungsprotokolle, Aktennotizen, Untersuchungsberichte etc.) weisen einen reichen Informationsgehalt auf, weshalb diese für **Aufsichts- und Strafverfolgungsbehörden** von grossem Interesse sein können. Sowohl die Zivil- als auch Strafprozessordnung, sowie das Verwaltungsrecht sehen Möglichkeiten vor, Unterlagen zu beschlagnahmen bzw. deren Herausgabe zu verlangen. Grenze bildet hierbei stets das Anwaltsgeheimnis. Inwieweit Aufsichts- und Strafverfolgungsbehörden in solche Unterlagen Einblick erhalten können, hängt somit wesentlich davon ab, inwieweit diese vom **Anwaltsgeheimnis** geschützt sind; das Bundesgericht hat hier eine einschränkende Haltung eingenommen (→ **Q10**). Eine Kooperation kann immerhin aus taktischen Gründen sinnvoll sein. Gerade wenn es um die Einsichtnahme in beschlagnahmte E-Mails geht, was den Behörden je nach Konstellation ohnehin zusteht, macht es oftmals keinen Sinn, wenn die Behörden eine eigene Datenerhebung durchführen müssen, sondern auf derselben Datenbasis arbeiten, wie das Unternehmen zuvor auch – sofern diese forensisch korrekt sichergestellt worden ist. Ähnliches gilt für Befragungen: Strafrechtlich verwertbar sind sie nach herrschender Auffassung nur, wenn sie unter Wahrung der strafprozessualen Grundsätze erfolgt sind (→ **Q37**). Im Falle einer Offenlegung von Unterlagen gegenüber einer Behörde ist stets zu berücksichtigen, dass diese die Unterlagen unter Umständen wiederum **Dritten offenlegen** muss oder will, sei dies im Rahmen der Akteneinsicht, des datenschutzrechtlichen Auskunftsrechts oder der Amts- und Rechtshilfe.

Die **Mitarbeiter** haben keinen Anspruch auf eine umfassende Einsichtnahme in die Unterlagen einer internen Untersuchung. Soweit sie jedoch eines Fehlverhaltens verdächtigt oder beschuldigt werden, sind sie anzuhören und haben in diesem Zusammenhang auch Anspruch auf Einsicht in die relevanten Unterlagen zum Sachverhalt (arbeitsrechtlicher **Anspruch auf rechtliches Gehör**). Die Einsichtnahme muss nicht vor der ersten Befragung gewährt werden; sie kann – mit der Gelegenheit zur Stellungnahme – auch später erfolgen (→ **Q34**).

Ferner ergeben sich aus dem Datenschutzgesetz **Auskunftspflichten.** Beziehen sich Dokumente erkennbar auf eine bestimmte Person, besteht grundsätzlich ein Anspruch auf Auskunft. Der Arbeitgeber hat bei entsprechenden Anträgen innert Frist von 30 Tagen Einsicht zu gewähren (Art. 8 Abs. 5 DSG, Art. 1 Abs. 4 → **VDSG**). Falls solche Unterlagen Geheimhaltungsinteressen oder **Schutzinteressen Dritter** tangieren (z.B. anderer Mitarbeiter) hat der Arbeitgeber geeignete Schutzmassnahmen zu treffen, indem als Beispiel Schwärzungen vorgenommen werden (zum Auskunftsrecht generell: → **Q57;** zum Einblick des Beschuldigten in Beweismittel: → **Q34**; Einblick in Befragungsprotokolle: → **Q36**; zum Einblick in einen Untersuchungsbericht: → **Q44**).

Obschon der **Verwaltungsrat** Einsicht in die Unterlagen hat (typischerweise wird der Untersuchungsbericht dem Verwaltungsrat zugestellt), dürfen Verwaltungsratsmit-

glieder keine Einsicht in die Unterlagen erhalten, wenn diese von der internen Untersuchung selbst betroffen sind. Sie haben in Bezug auf die Beratung und der internen Untersuchung im Verwaltungsrat in den Ausstand zu treten.

> **Literatur:**
>
> Götz Staehelin, Claudia: Unternehmensinterne Untersuchungen, Zürich/Basel/Genf 2019
>
> Rudolph, Roger: Das Recht des Arbeitnehmers auf Einsicht in sein Personaldossier, Allgemeine Juristische Praxis (AJP) 2014, 1672 ff.

Q16. Können wir die Kosten einer internen Untersuchung auf Dritte abwälzen, z.B. eine Versicherung oder den Verursacher?

A: Der **Mitarbeiter** haftet für den Schaden, den er absichtlich oder fahrlässig dem Arbeitgeber zufügt (Art. 321e OR). Für die Haftung des Mitarbeiters muss mitunter ein Schaden vorliegen. Bei den Kosten für eine interne Untersuchung wird es sich primär um das **Anwaltshonorar** handeln (und das Honorar der weiteren involvierten Stellen wie z.B. eDiscovery-Provider).

Solche **vorprozessualen Anwaltskosten** können in einem Prozess auf Schadenersatz nur bei der Erfüllung gewisser Voraussetzungen geltend gemacht werden und somit auf den Verursacher bzw. dessen Haftpflichtversicherung abgewälzt werden.

Gemäss bundesgerichtlicher Rechtsprechung bilden vorprozessuale Anwaltskosten lediglich dann **Teil des Schadens**, wenn diese **gerechtfertigt, notwendig** und **angemessen** sind, der Durchsetzung der Schadenersatzforderung dienen und nicht bereits durch den Ersatz anderer Kosten gedeckt sind (Entscheid des BGer 4A_127/2011 vom 12. Juli 2011, E. 12.1). Möchte das Unternehmen solche Kosten in einem Schadenersatzprozess durchsetzen, ist dies zwar möglich, aber der Ersatzanspruch ist hinreichend zu **begründen**. Es bedarf mindestens eines **konkreten Anfangsverdachts** um die Notwendigkeit der durch die interne Untersuchung generierten Kosten zu legitimieren.

Die Durchsetzung eines Ersatzanspruches gegenüber dem Mitarbeiter kann unter Umständen auf dem Weg der **Verrechnung** mit dem Lohn erfolgen. Fand ein Fehlverhalten im Zusammenspiel mit Dritten statt, kann allenfalls auch auf diese Dritten und deren „*deep pockets*" zugegriffen werden, soweit sie mindestens die Stellung eines Teilnehmers am betreffenden Delikt hatten.

Versicherungen zur spezifischen Deckung der Kosten einer internen Untersuchung werden bisher kaum angeboten und sind vergleichsweise teuer, da eine Untersuchung rasch mehrere CHF 100'000 kosten kann. Ein deutscher Spezialversicherer, der die Kosten der internen Aufklärung bei Verstössen gegen das Wettbewerbsrecht, bei Korruption und bei Betrug oder Schädigung mit Hilfe der IT bezahlt, verlangt beispiels-

weise für eine Versicherungssumme von bis zu EUR 500‘000 bei einem Betrieb mit 250 Mitarbeitern eine Prämie von EUR 4‘500 pro Jahr, bei 1‘000 Mitarbeitern bereits EUR 12‘000. Erfolgt eine interne Untersuchung jedoch zur Geltendmachung von Ansprüchen gegenüber Dritten oder zur Abwehr von behördlichen oder strafrechtlichen Verfahren, können die Kosten teilweise bereits durch die herkömmlichen Rechtsschutzversicherungen abgedeckt sein.

Literatur:

Borle, Markus: Vorprozessuale Anwaltskosten – es führt kein Weg an der Substanziierung vorbei, in: Haftung und Versicherung (HAVE) 2012, 3 ff.

Jenne, Moritz/Schubert, Andreas: Kosten für interne Ermittlungen sind bei Compliance-Verstössen auch von Arbeitnehmern zu ersetzen, Compliance Berater (CB) 2020, 487 ff.

Q17. Gibt es so etwas wie eine „interne Verjährung“ für ein Fehlverhalten?

A: Nein, in dieser absoluten Form gibt es eine solche Verjährung nicht. Erfährt ein Unternehmen von einem tatsächlichen oder möglichen Fehlverhalten erst Jahre später, so kann die Frage, ob der Sache trotzdem noch nachgegangen werden muss, unter Berücksichtigung unterschiedlicher Perspektiven, beantwortet werden:

- **Die arbeitsrechtliche Sicht:** Auch wenn ein Mitglied der Geschäftsleitung Vermögenswerte der Firma vor 20 Jahren veruntreut hat, kann das Vertrauensverhältnis zerstört sein – und darauf kommt es arbeitsrechtlich in der Regel an, und nicht, ob das Fehlverhalten mehr als zehn Jahre zurückliegt oder weniger (die schuldrechtliche Verjährung). Sogar eine fristlose Kündigung kann deshalb – trotz einer solch langen Zeit – unter Umständen noch möglich sein. Umgekehrt sind viele Konstellationen denkbar, in welchen ein Mitarbeiter in der Vergangenheit zwar einen Fehltritt zu verantworten hatte, in der Zwischenzeit aber bewiesen hat, dass er des Vertrauens des Arbeitgebers würdig ist. Kommt nach zehn Jahren heraus, dass der heutige CFO des Unternehmens, seines Zeichens Familienvater von vier Kindern, von dem nichts Schlechtes bekannt ist, vor zehn Jahren als Bürochef eines kleinen Teams ein Verhältnis mit der 17-jährigen Praktikantin hatte, und will der sich von ihm eingeengt fühlende CEO diesen Vorfall nutzen, um ihn als „Charakterlump“ zu brandmarken und zu entlassen, so dürfte die Arbeitgeberfürsorgepflicht und das Persönlichkeitsrecht den CFO schützen. Eine Untersuchung der Sache kann trotzdem angezeigt sein. Das kann dazu dienen, die beschuldigten Mitarbeiter zu schützen, weil entsprechende Gerüchte im Betrieb die Runde machen. Es kann ebenfalls dazu dienen festzustellen, ob Vorwürfe einen Einzelfall (oder sogar nur eine einmalige Entgleisung) betreffen oder ein Fehlverhalten verbreiteter und gegenwärtiger Natur ist (und daher Massnahmen erforderlich sind). Nicht zuletzt kann eine interne Untersuchung auch angezeigt sein, um aus betriebshygienischen Grün-

den zu zeigen, dass der Arbeitgeber allfällige Missstände im Unternehmen nicht einfach ignoriert[13]. Siehe dazu auch den nächsten Punkt.

- **Die Compliance-Management-Sicht:** Hier geht es um das Risiko, dass das Unternehmen noch Mängel in der Organisation aufweist, die ein solches Fehlverhalten möglich machen oder dafür sorgen, dass es unerkannt bleibt. Es verhält sich wie bei der Software: Ein *"Bug"* oder gar eine „Hintertür" im System ist, was es ist und muss auch dann behoben werden, wenn es ihn bzw. sie schon seit Jahren gibt und bisher lediglich nicht aufgefallen ist. Hierbei stehen nicht zwischenmenschliche Verhaltensweisen im Vordergrund, sondern Missbräuche der Organisation für typischerweise vermögensorientierte Delikte (etwa Korruption, Betrug, Veruntreuung), d.h. für Fehlverhalten, welches dem Unternehmen schadet oder sogar zu einer strafrechtlichen Verantwortlichkeit des Unternehmens und seiner Geschäftsführer führen kann (→ **Q52**). Hier können Abklärungen angezeigt sein, um zu verstehen, was vorgefallen ist und wie es dazu kommen konnte, damit nötigenfalls Abhilfemassnahmen getroffen werden können und sich solche Vorfälle nicht wiederholen können. Dabei geht es nicht um die Sanktionierung der Mitarbeiter. Wurde die Organisation oder Technik zwischenzeitlich geändert, dürfte sich dieser Aufwand allerdings sowieso erübrigen.

- **Die Sicht der Buchführung:** Müssen frühere Geschäftsbücher und Abschlüsse eines Unternehmens nachträglich korrigiert werden, weil sich herausstellt, dass sie aufgrund eines Fehlverhaltens fehlerhaft sind? Die Antwort aus Sicht des „Praktikers" wird sein, dass ein zehn Jahre alter Jahresabschluss kaum mehr jemanden interessiert. Aber auch aus Sicht der internationalen Rechnungslegungsstandards ist ein Korrekturbedarf in den meisten Fällen nicht gegeben. Das kann zwar bei einem wesentlichen Fehler der Lehre nach anders sein, doch sind hier wiederum handelsrechtliche Einschränkungen zu beachten. Dazu → **Q54**.

- **Die steuerrechtliche Sicht:** Soweit eine Korrektur steuerrechtlich relevant ist und zu Rückforderungen (als Chance für das Unternehmen) oder Nachforderungen führen kann (als Risiko für das Unternehmen), ist die steuerrechtliche Verjährung entscheidend. Sie tritt spätestens nach zehn Jahren ein. Das Risiko einer Steuernachforderung dürfte für einen Unternehmer freilich primär ein Grund sein, eine alte Sache *nicht* zu untersuchen.

---

13 Vgl. etwa den Fall zu den Übergriffs- und Mobbingvorwürfen beim Westschweizer Radio- und Fernsehen, wo u.a. kritisiert wurde, dass das Verhalten am Arbeitsplatz gegenüber Mitarbeitern durch eine bestimmte Kaderperson nur während ihrer Zeit in ihrer Führungsposition und nicht schon zuvor untersucht wurde. Statt vieler: https://www.aargauerzeitung.ch/schweiz/belaestigungen-beim-westschweizer-fernsehen-der-chef-der-srg-stiehlt-sich-aus-der-verantwortung-ld.2126432, https://www.derbund.ch/um-den-kronzeugen-kuemmert-sich-niemand-833563805446, https://www.zuonline.ch/die-zeit-des-kuschens-ist-vorbei-967718432529, https://www.persoenlich.com/medien/tv-newschef-und-personalchef-verlassen-rts.

- **Die Sicht der Gegenwart:** Besteht die Möglichkeit, dass das Fehlverhalten noch anhält? In diesem Fall stellt sich die Frage der Verjährung gar nicht erst. Insbesondere im Bereich der Wirtschaftskriminalität können sich Delikte über viele Jahre hinwegziehen, wenn sie nicht entdeckt werden. Sind die Täter zunächst noch unsicher und fürchten Aufdeckung, gewinnen sie mit der Zeit zusehends an Sicherheit und Selbstvertrauen, was freilich auch das Risiko der (späten) Entdeckung erhöht.
- **Forderungen von und gegenüber Dritten:** Hier geht es um die Chance bzw. das Risiko, dass mit dem mutmasslichen Fehlverhalten verbundene schuldrechtliche Forderungen des Unternehmens (bzw. Dritter gegen das Unternehmen) bestehen, die geltend gemacht werden könnten. Vertragsrechtliche Schadenersatzansprüche (auch aus Arbeitsvertrag) verjähren in der Regel nach zehn Jahren. Deliktische Ansprüche verjähren nach drei Jahren. Im Falle von Personenschäden besteht allerdings inzwischen eine absolute Verjährungsfrist von 20 Jahren, was beispielsweise bei Verstössen gegen den Gesundheitsschutz im Betrieb (Stichwort „Asbestopfer“) relevant sein kann. Strafrechtlich liegen die Verjährungsfristen für die im Wirtschaftsbereich üblichen Delikte bei sieben oder 15 Jahren. Zu beachten ist in diesen Fragen, dass die Schwierigkeit der Erfüllung der Beweislast für den Beweisbelasteten mit zunehmender Sachverhaltsferne eher exponentiell als linear zunimmt.

Gedanken zum Thema.

So entscheidend E-Mail-Reviews für interne Untersuchungen mitunter sind, so herausfordernd können sie aus technischer und datenschutzrechtlicher Sicht sein. Das gilt vor allem in Fällen mit internationaler Dimension und hoher Dokumentenzahl. Hinzu kommt ein hoher Zeitdruck: Die Verantwortlichen erhalten kaum Zeit, alle Rechtsfragen im Vorfeld einer Untersuchung abschliessend und in Ruhe zu klären. Ohne einen risikobasierten Ansatz geht es darum nach meiner Erfahrung nicht. Hier braucht es gleichermassen innovative Lösungsansätze und professionelle, erfahrungsbasierte Einschätzungen.

Alexander Lacher
General Counsel
Generali

4. Dokumenten-Reviews

Kurz gesagt

- Das Sicherstellen, Aufarbeiten und Sichten von E-Mails und anderen Dokumenten kann in vielen Untersuchungen entscheidende Hinweise zum Sachverhalt liefern.
- Ein linearer Dokumenten-Review ist allerdings oft teuer, zeitraubend und unflexibel; daher sollten vorab Alternativen geprüft und der Review gut geplant werden.
- Durch geeignete Werkzeuge und Methoden (Suchmuster, etc.) kann die händische Sichtung stark reduziert werden, aber ganz ohne geht es weiterhin nicht.

Worum es geht

Die systematische Sichtung von Dokumenten – oft einfach nur als → **Review** bezeichnet – ist nebst Befragungen ein Kernelement vieler interner Untersuchungen. Ein Review bezieht sich in aller Regel auf den E-Mail-Verkehr (oder andere Kommunikation wie Chat-Protokolle) der Protagonisten einer Angelegenheit, der systematisch nach Hinweisen abgesucht wird, welche die vermutete Unregelmässigkeit aufklären können. Die Erfahrung zeigt: Viele Personen sind erstaunlich unvorsichtig, wenn sie über E-Mail oder andere elektronische Kanäle kommunizieren. Die Suche geschieht teilweise automatisch, teilweise von Hand. Aus taktischer Sicht finden Befragungen meist erst nach einem Review statt, damit die befragten Personen mit den Ergebnissen aus dem Review konfrontiert werden können und bereits ein Verständnis für die Interaktionen zwischen den Protagonisten und den Geschehnissen besteht.

Nebst den klassischen Reviews zwecks Sachverhaltsermittlung dienen Reviews heute auch noch diversen anderen Zwecken, namentlich der Suche und ggf. Schwärzung von Dokumenten, die eine Drittpartei benötigt (dazu → **SWISS SECRECY & PRIVACY REVIEWS** und → **DSAR-REVIEW**) und zur „fliessbandmässigen" Klassifikation von Dokumenten (dazu → **DATA BREACH REVIEW** und → **VERTRAGSREVIEW**). Hier nicht gesondert behandelt ist der in den USA übliche „*Privilege*"-Review.[14]

14 Er dient dazu, Anwaltskorrespondenz zu identifizieren, zu verzeichnen (in einem „*Privilege Log*") und auszusondern, bevor in einem Zivil- oder Behördenverfahren Unterlagen herausgegeben werden.

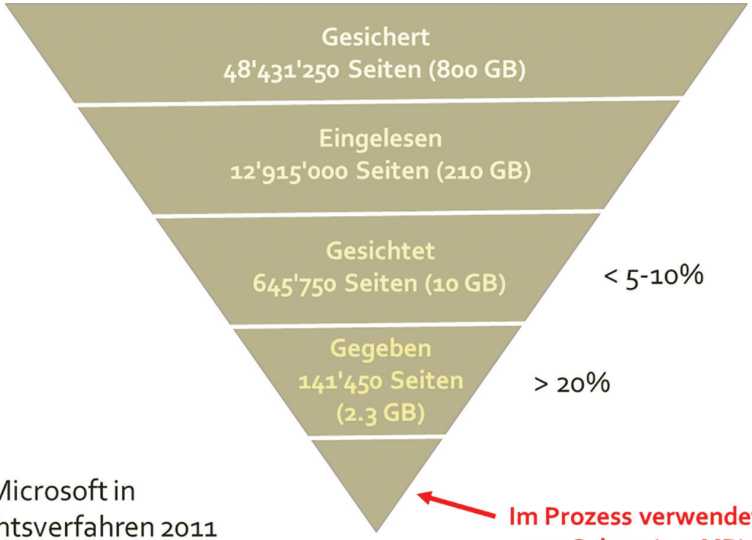
Worauf zu achten ist

- Ein Review ist wie ein Supertanker: Er braucht eine gewisse Zeit, um Fahrt aufzunehmen und bei einem späteren Kurswechsel geht viel Zeit und Weg verloren.
- Das operative Management eines Reviews ist anspruchsvoller und viel zeitintensiver als vermutet wird.
- Das gilt auch für das Definieren von Suchbegriffen und Verfassen guter Instruktionen und → **Coding-Panels**.

Tauglichkeit?

Reviews führen vor allem dort zum Erfolg, wo in einem Betrieb alltägliche Kommunikation elektronisch stattfindet und diese aufgezeichnet wird. Wo dies selten geschieht oder nicht kontrollierte Kommunikationskanäle genutzt werden (wie z.B. private E-Mail- und Messengerdienste) helfen Reviews dagegen kaum. Oft ist dies im Voraus aber nicht klar.

- Die manuelle Sichtung sollte auf ein Minimum reduziert werden (i.d.R. nicht mehr als 5-10% der Dokumente).
- Systematische Reviews benötigen zwingend eine Qualitätssicherung – und trotzdem sind sie nie fehlerfrei.
- Die Fähigkeiten „intelligenter" Systeme werden überschätzt, aber eine Kombination mit einem linearen Review kann sinnvoll sein.



Was Microsoft in Gerichtsverfahren 2011 im Schnitt zu verarbeiten hatte

Quellen: David Howard, Jonathan Palmer, & Joe Banks, Re: September 9, 2011 Committee Meeting on Preservation and Sanctions, MICROSOFT (Aug. 31, 2011) (gefunden unter: https://bit.ly/3ei65m7)

Das obige Diagramm illustriert, wie sich die **Mengenverhältnisse** in einem Review verändern. Die Zahlen beziehen sich auf US-Zivilprozesse, wo es üblich ist, vor einem Prozess alle Dokumente mit Themenbezug auszutauschen. Die absoluten Zahlen sind daher nicht repräsentativ; die meisten hiesigen internen Untersuchungen kommen mit wesentlich weniger Dokumenten aus. Die umgekehrte Pyramide zeigt aber, wie ein Review dazu benutzt wird, die Spreu vom Weizen zu trennen: Zuerst erfolgt eine maschinelle Aussortierung (mit Suchbegriffen, etc.); es bleiben im Schnitt 5-10% übrig. Dann erfolgt eine manuelle Sichtung, um die Dokumente mit Themenbezug zu identifizieren. Je besser die maschinelle Aussortierung, d.h. je weniger falsche Treffer sie erzeugt, desto höher ist der Anteil „relevanter" Dokumente im Rahmen der manuellen Sichtung. Was dann wirklich verwendet wird ist nochmals viel weniger.

Wie vorzugehen ist

1. **Einen eDiscovery-Provider buchen.** Unternehmen wie Anwaltskanzleien betreiben die Systeme für die Durchführung der Reviews in aller Regel nicht selbst. Es sind dies IT-Anwendungen, die speziell für diese Zwecke entwickelt wurden und daher in der Lage sind, sehr grosse Datenmengen aufzunehmen, zu durchsuchen und von ganzen Teams parallel bearbeiten zu lassen. Einige hundert E-Mails kann jeder in seinem Mail-Programm selbst anschauen, aber wenn es einige Tausend sind und diese noch durchsucht, klassifiziert oder gar noch geschwärzt werden müssen, geht das nicht mehr – ebenso nicht, wenn die Arbeit auf mehrere Personen verteilt werden muss. In solchen Fällen empfiehlt es sich, einen eDiscovery-Provider zu buchen, der die Daten in seine Systeme einliest und über eine sichere Internet-Verbindung Zugang dazu anbietet (*"Software-as-a-Service"*). Viele bieten für Reviews eine Basislösung an (z.B. „Relativity") und dazu diverse Umsysteme für spezifische Aufgaben (z.B. Analyse, Übersetzung, Wiederherstellung gelöschter Daten, Reviews von Dokumenten in besonderen Formaten wie Excel oder Audiodateien). Dazu: → **WERKZEUGE FÜR EDISCOVERY**.

   Die grundlegenden eDiscovery-Services sind heute weitgehend *Commodity*. Sie werden zu unterschiedlichen **Preismodellen** angeboten. Gebräuchlich ist ein Preis pro GB an verarbeiteten und gespeicherten Daten plus eine Entschädigung nach Aufwand (z.B. für das Einlesen von Daten) und Lizenzgebühren für Benutzer. Werden Daten mit Bedacht verarbeitet, sind die eDiscovery-Services in der Regel keine grossen Kostentreiber.

2. **Einen *Collection Plan* erstellen.** Soweit dies nicht bereits getan wurde (→ **ERSTE SCHRITTE**) sollten die relevanten Datenquellen für den Review (E-Mails, Dokumente

aus Dateiablagen, Chats, etc.) identifiziert werden und damit ein *"Collection Plan"* erstellt werden, damit keine relevanten Datenquellen vergessen gehen und wenn nötig priorisiert werden können.

3. **Dem Provider die Daten liefern.** Die zu sichtenden Daten müssen dem Provider in der einen oder anderen Form geliefert werden. Meist geschieht dies auf USB-Laufwerken oder Festplatten, seltener auf *Backup-Tapes*. Die meisten Provider können auch beauftragt werden, die Daten vor Ort auf ihre Systeme zu überspielen. Wo Unternehmen Cloud-Lösungen einsetzen, kann es einfacher sein, dem Provider den Zugang dazu zu geben, so dass er sich über die für eDiscovery vorgesehenen Schnittstellen die nötigen Daten direkt herunterladen kann. Denn: Jeder Zwischenschritt, jedes Umkopieren, Konvertieren oder Einlesen, kostet Zeit (und Geld). Wird z.B. ein ganzer Mailserver eines KMU kopiert, so kann das Extrahieren einzelner Postfächer ohne Weiteres einen Tag benötigen. Werden Daten aus der Cloud heruntergeladen, braucht dies auch Zeit, bei grösseren Mengen mitunter Tage.

Software

Der Softwaremarkt ist riesig. Die wenigsten decken alle Bereiche gleich gut ab. Oft werden sie kombiniert. Einige bekannte Namen:

- Relativity
- Nuix
- Luminance
- Brainspace/Reveal
- Encase
- AccessData/FTK
- Kira (für Verträge)
- Concordance
- Everlaw (Cloud)
- CS Disco (Cloud)

Werden **ganze Geräte** (z.B. das Notebook oder Mobiltelefon eines Mitarbeiters) **forensisch gesichert** (im Fachjargon: Es wird ein „*Image*" – ein Abbild – der Datenträger erstellt), so kann dies der eDiscovery-Provider auch tun, allerdings beinhalten diese *Images* sehr viel Daten, die nicht von Interesse sind. Hier muss also in der Regel manuell aussortiert werden, welche Verzeichnisse und Dateien (und allenfalls gelöschte Dateien) in den Review einfliessen sollen. Können Sie auf einen guten „*File Type*"-Filter zurückgreifen, ist der Aufwand überschaubar; er kann die diversen Dateitypen identifizieren und jene Dateien aussortieren, die keine verwertbaren Inhalte haben (z.B. Programmcodes oder Konfigurationsdateien). Falls der Verdacht besteht, dass **beweisrelevante Daten gelöscht** wurden, ist es wichtig, dass ein sogenanntes „physisches" Abbild des Arbeitsgeräts erstellt wird (im Gegensatz zum „logischen" Abbild, welches nur die Dateiordner und deren noch ganz vorhandenen Dateien enthält).

Beim physischen Abbild ist auch der *"unallocated Space"* (d.h. die auf dem Datenträger als gelöscht bzw. als frei markierten Stellen) durchsuchbar, in welchem sich oft Spuren von gelöschten E-Mails oder Dokumenten befinden können, welche sich unter Umständen ganz oder teilweise rekonstruieren lassen.

4. **Entscheiden, welche Daten wie aufbereitet werden sollen.** Gesichert und eingesammelt wird oft viel, aber oft macht es keinen Sinn, alles gleich so aufzubereiten, dass es gesichtet werden kann. Das kostet Zeit und angesichts der oft vom Datenvolumen abhängigen Preise auch Geld. Darum muss vor einem Review entschieden werden, welche Teile der elektronisch vorliegenden Daten für den Review aufbereitet – sprich *"processed"* – werden müssen, z.B. E-Mails nur bestimmter → **Custodians** und nur aus einer bestimmten Zeitperiode. Beim *Processing* finden wichtige Vorgänge wie etwa die → **Deduplizierung**, die Texterkennung[15] oder eine erste Dokumentenanalyse[16] statt. Je nach Bedarf können auch Zusatzfunktionen aktiviert werden, wie z.B. eine automatische Übersetzung. Es ist normalerweise problemlos möglich, nachträglich weitere Daten ins Review-System aufzunehmen.

Gelöschtes?

Meist ist es nicht nötig, gelöschte Daten durch Forensik-Tools auf einer Festplatte wiederherzustellen. Die Inhalte im "Papierkorb" eines Postfachs werden hingegen regelmässig mitverarbeitet. In der Microsoft-Cloud können Dokumente zudem bis zu 30 Tage lang nach der Löschung noch aufbewahrt werden.

5. **Problemfälle müssen gelöst werden.** Werden Daten in ein Review-System eingelesen und von diesem verarbeitet, kommt es immer zu Fehlern. Die meisten davon sind nicht schlimm (es fehlt in einer E-Mail eine Bilddatei mit dem Logo, ein exotisches Dateiformat wird nicht erkannt und kann nicht gelesen werden, eine Datei ist fehlerhaft, die Texterkennung funktioniert nicht, etc.). Der eDiscovery-Provider wird sich normalerweise darum kümmern, aber teilweise muss auch der Kunde entscheiden oder mitwirken. Typisches Beispiel sind verschlüsselte Dateien: Manchmal kann sie der Provider knacken, aber in vielen Fällen ist er darauf angewiesen, vom Kunden den Code zu erhalten – oder auf die Entschlüsselung zu verzichten.

6. **Review-Strategie festlegen:** Wie die gesammelten und verarbeiteten Daten gesichtet werden, müssen Sie oder der von Ihnen beauftragte Anwalt oder Berater

15 Damit Dokumente (z.B. PDFs) durchsuchbar werden.
16 So kann nach Sprachen, Sendern, Empfängern, Dokumententypen etc. gesucht und gefiltert werden.

festlegen. Das ist entscheidend – auch hinsichtlich der Kosten und der Zeit, die der Review beanspruchen wird. Auch hier zeichnet sich Erfahrung aus. Ein Review kann grundsätzlich **linear** oder **nicht-linear** erfolgen. Linear bedeutet, die Dokumente werden eines nach dem anderen abgearbeitet – zuerst werden sie nach Suchbegriffen durchsucht und gefiltert, dann manuell gesichtet. Nicht-linear bedeutet, die Reviewer gehen kreuz und quer durch die Dokumente durch und schauen sich nur jene an, die aufgrund von Begriffen, Mustern oder anderen Merkmalen als besonders vielversprechend gelten und bahnen sich anhand der gefundenen Informationen neue Wege durch die Masse der Dokumente (teilweise wird dies darum auch als „explorativer" Review bezeichnet). Auch Mischformen sind denkbar. Beide Methoden können durch geeignete Software unterstützt werden (*"Technology Assisted Review"*, TAR). Im linearen Review kann die Software z.B. Dokumente, die aufgrund der bisherigen Review-Ergebnisse als besonders relevant erscheinen, priorisieren oder gleich maschinell klassifizieren. Für den nicht-linearen Review gibt es z.B. Lösungen, welche Dokumente anhand darin verwendeter Wortkombinationen nach Themen gruppiert oder andere wiederkehrende Muster z.B. im Kommunikationsverhalten visualisiert. Mehr zu Möglichkeiten des TAR unter → **WERKZEUGE FÜR EDISCOVERY**.

Handarbeit?

Auch im eDiscovery ist "künstliche Intelligenz" ein grosses Schlagwort. Fast immer ist Mustererkennung gemeint. Richtig eingesetzt und bei genügend grossen Datenmengen kann sie viel helfen, aber ohne Handarbeit geht es in keinem Review.

7. **Suchfilter erarbeiten.** Auch heute noch ist der Einsatz von Suchbegriffen beim Review von Textdokumenten vor allem im linearen Review wichtig. Das Besondere an Review-Systemen ist, dass sie mit Dutzenden von Suchbegriffen und Kombinationen gleichzeitig arbeiten können. Das Zusammenstellen von guten Suchaufträgen ist wesentlich schwieriger, als die meisten sich dies vorstellen. Es geht nicht einfach darum, sich einige Begriffe zum Thema auszudenken, sondern mit Hilfe von Wortelementen, Synonymen, logischen und anderen „Operatoren" (AND, OR, NOT, WITHIN, etc. → **Boolean Search**) und Suchmusterbegriffen (→ **RegEx**) und weiteren Suchmethoden (→ **WERKZEUGE FÜR EDISCOVERY**) ein linguistisches „Schleppnetz" zu formulieren, in dem nur noch möglichst wenige irrelevante Dokumente hängen bleiben, aber keine relevanten Dokumente vorbeifliessen. Hat es in einem Topf mit 100'000 Dokumenten 500 re-

Culling

Als *"Culling"* wird der Vorgang bezeichnet, in welchem bewusst nach klar irrelevanten Dokumenten gesucht wird (z.B. Newsletter-Mails), um diese in globo von weiteren Suchläufen auszuschliessen und so die Dokumentenmenge zu reduzieren.

levante Dokumente, mag es für das Ergebnis keine Rolle spielen, ob hierzu 5 oder 10 Prozent der Dokumente manuell gesichtet werden müssen. Kann die Menge jedoch dank eines besseren Suchfilters auf 5 Prozent beschränkt werden, kostet der Review halb so viel und ist doppelt so schnell fertig. Es lohnt sich also, in gute Suchfilter zu investieren.

Suchfilter sollten nicht bloss einmalig zu Beginn definiert werden. Mit fortschreitendem Review ist es sinnvoll, die dabei gewonnenen Erkenntnisse über die Effektivität des Suchfilters in dessen **laufende Optimierung** einfliessen zu lassen. Das muss nicht unbedingt zu einer Einschränkung des Reviews führen. Ergeben sich aus dem Review neue Erkenntnisse, z.B. bestimmte neue Namen, Begriffe oder Redewendungen, können diese benutzt werden, um das Schleppnetz neu auszuwerfen und so relevante Dokumente zu erfassen, die bisher durch die Masche schlüpften.

8. ***Tagging*-Konzept festlegen.** Ein Review taugt kaum etwas, wenn das Ergebnis nicht festgehalten wird. Dies geschieht, indem jedes Dokument mit entsprechenden → **Tags** und ggf. auch Kommentaren versehen wird. *Tags* (mitunter ist auch von „Kodierungen“ oder „*Codes*“ die Rede) sind die elektronische Version eines Reiters oder einer Haftnotiz, mit welchem bzw. welcher jedes Dokument versehen und damit klassifiziert werden kann – zum Beispiel als „relevant“ (im Fachjargon: *“responsive“*), „möglicherweise relevant“ oder „*key*“. Es können so auch weitere Tags vorgenommen werden wie z.B. „enthält private Inhalte“ oder Namen betroffener Parteien, aber auch operative *Tags* wie „Fremdsprache“ (falls der Reviewer diese nicht versteht), „Technisches Problem“ (falls etwas mit einem Dokument nicht richtig funktioniert) oder „Weitere Fragen“ (falls das Dokument Fragen aufwirft, die noch zu klären sind). Auch die Workflows werden auf diese Weise gesteuert (z.B. das Zusammenspiel von Qualitätssicherung und den verschiedenen Reviewer-Ebenen). Die *Tags* haben den Vorteil, dass Dokumente später danach gesucht und gefiltert werden können; Statistiken sind so ebenfalls sehr einfach möglich. Für jeden Review und jede Review-Stufe werden die erforderlichen und optionalen *Tags* im → **Coding Panel** (oder *Tagging Panel*)

KISS

Ein häufiger Mangel von *Tagging*-Konzepten ist, dass den Reviewern zu viel abverlangt wird. Müssen sie bei jedem Dokument zu viele verschiedene Dinge klassifizieren oder beurteilen, nimmt die Fehlerquote deutlich zu und der Review wird stark gebremst. Reviews sind Fliessbandarbeit. Auch hier bewährt sich das KISS-Konzept – *Keep it simple, stupid!*

festgelegt, das rechts vom Dokument angezeigt wird und vom Reviewer für jedes Dokument ausgefüllt wird.

Werden Postfächer von Mitarbeitern gesichtet, so finden sich darin meistens auch **private Inhalte**, sei es als private E-Mails oder Bemerkungen privater Art in geschäftlichen E-Mails. Diese gehen den Arbeitgeber (normalerweise) nichts an. Gewisse Unternehmen haben den Umgang damit geregelt. Doch auch wo keine Regelung besteht, gilt heute, dass bei begründetem und berechtigtem Anlass eine Sichtung möglich ist, wenn die nötigen Vorkehrungen getroffen sind, um die Privatsphäre der Mitarbeiter so gut wie möglich zu schützen. Dazu gehört, dass sie über den Review informiert werden, sobald dies ohne Gefährdung der Untersuchung möglich ist (z.B. im Rahmen einer *Legal Hold Notice* → **ERSTE SCHRITTE** Schritt 15). Weiter sollten mit dem Review nur Personen betraut werden, die mit den *Custodians* (und weiteren betroffenen Personen) nicht in Verbindung stehen (d.h. nicht Arbeitskollegen, nicht Vorgesetzte). Schliesslich sollten die Reviewer angewiesen werden, auch dem Arbeitgeber der betroffenen Personen trotz seiner Stellung als Auftraggeber des Reviews, darüber keine Auskunft zu geben. Private Dokumente können zudem entsprechend kodiert werden, damit sie vor einer Weitergabe herausgefiltert bzw. geschwärzt werden können.

9. **Review-Team organisieren.** Je nach Art des Reviews werden zur Durchführung unterschiedliche Personen benötigt. Für non-lineare Reviews werden typischerweise mit dem Sachverhalt und der Problemstellung gut vertraute, aber in dieser Art der Suche erfahrene Personen benötigt. Für lineare Reviews, die häufig intellektuelle Fliessbandarbeit sind und in denen eine hohe Zahl von Dokumenten (10‘000, 50‘000 oder 100‘000 Dokumente) gesichtet müssen, werden meist weniger qualifizierte, dafür kostengünstigere Mitarbeiter eingesetzt. Es wird auch mit verschiedenen Stufen gearbeitet (*“levels“*). Ein klassisches Modell arbeitet mit drei Stufen:

   - Günstige *“1st level reviewer“* gehen die Dokumente rasch durch und nehmen eine Grobsortierung vor; alles was möglicherweise relevant ist, wird markiert.

Wie schnell?

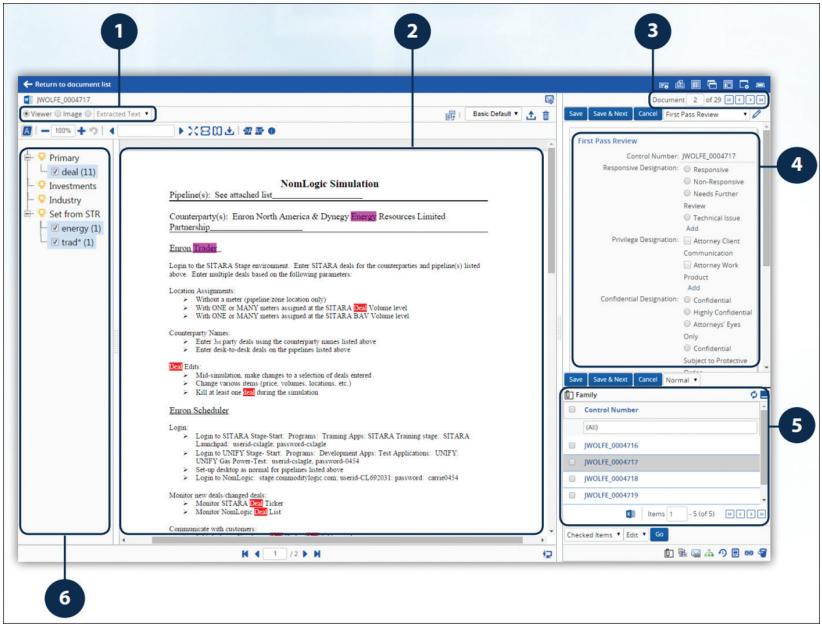
Ein geübter Reviewer kann nach einer Lernphase im Tag (8h) als Faustregel im Schnitt rund 400 Dokumente sichten. Die tatsächliche Zahl hängt von der Komplexität der *Tags*/Vorgaben und der Komplexität und Länge der Dokumente ab. Eine E-Mail mit 2-3 Seiten benötigt einen Bruchteil der Zeit im Vergleich zu einem Dokument mit 50 Seiten oder eine ausführliche Excel-Tabelle.

- In einer zweiten Stufe werden die (nun sehr viel weniger zahlreichen) Dokumente von einer Person mit höherer Seniorität, Fallkenntnis und Erfahrung genauer angeschaut.
- Die den Fall betreuenden Anwälte schauen sich dann an, was aus diesem *"2nd level review"* resultiert.

Auch für Reviewer gibt es einen Markt. **Schweizer Kanzleien** greifen auf ihr ständiges juristisches Personal (z.B. Substituten, junge Associates) zurück oder beschäftigen sog. Projekt-Mitarbeiter (typischerweise Jus-Studenten im Teilzeitpensum, die für spezifische Reviews angestellt werden; die Preise liegen hier bei 120 bis 150 Franken pro Stunde). Review-Teams bzw. *Managed Reviews* können aber auch bei spezialisierten **internationalen Dienstleistern** bezogen werden, die ihre Reviewer mitunter aus ganz Europa rekrutieren und bevorzugt ausserhalb der Schweiz durchführen (was teils deutlich tiefere Kosten erlaubt). Solche Teams können durchaus 50 Personen umfassen, die von einem oder mehreren *Review Leads* geführt werden. Üblich ist ein Stundenpreis, in gewissen Fällen werden aber auch Preise pro Seite oder Dokument angeboten. Die im Ausland tiefen Preise sind auf den ersten Blick verlockend und können sich – richtig geführt – auch lohnen. Sie sollten daher gerade in grösseren Vorhaben erwogen werden. Allerdings bestehen erfahrungsgemäss grosse Qualitätsunterschiede, und gute Führung ist sehr wichtig. Dass ein in England, den USA oder Indien für 50 bis 80 Franken in der Stunde angebotener Reviewer eine Anwaltszulassung hat oder angeblich auch Deutsch spricht, hat leider nicht viel zu bedeuten. Es gibt auch sehr grosse Unterschiede in der Führung von Review-Teams: In gewissen Teams bestehen streng hierarchische Strukturen – von den Reviewern wird erwartet, die Dokumente nach den Vorgaben der Review-Instruktion und des „Vorarbeiters" sklavisch im Akkord auszuführen; ihre Leistung wird laufend statistisch überwacht. Anderswo wird von Reviewern erwartet mitzudenken und sich einzubringen, etwa wenn ihnen relevante Dinge auffallen, die aber von den Anweisungen bisher nicht oder unpassend abgedeckt sind.

10. **Reviewer instruieren und schulen.** Wird ein linearer Review durchgeführt, muss das Team instruiert werden. Diese Instruktion muss schriftlich festgehalten werden. Erstens werden die Reviewer solche *Review Guidelines* während ihrer Arbeit brauchen, da sie mindestens zu Beginn immer wieder nachsehen müssen, wie mit bestimmten Konstellationen umzugehen ist. Zweitens kann damit im Sinne einer guten *Governance* dokumentiert werden, was getan wurde. Nicht nur klare Instruk-

tionen sind wichtig, damit das Review-Ergebnis richtig ist, sondern auch möglichst einheitlich. Dokumente sollen immer auf dieselbe Weise und nach denselben Kriterien beurteilt und klassifiziert werden. Je weniger Interpretationsspielraum die Instruktionen lassen, desto besser. Je mehr mögliche Konstellationen bezüglich der Inhalte, welche die Reviewer im Review mutmasslich antreffen, desto besser. In der Praxis lassen sich beide Ziele nie vollständig erreichen, weshalb es auch wichtig ist, die Review-Instruktionen mit zunehmenden Erkenntnissen weiterzuführen und nachzubessern. Taucht im Review eine neue Problemstellung auf, kann ihre Lösung über die Review-Instruktionen festgehalten werden. Nebst der schriftlichen Instruktion sollte auch eine mündliche Einführung in den Fall und den Review stattfinden, optimalerweise mit konkreten Beispielen (z.B. aus dem *Early Case Assessment*). Dabei können auch die Bedienung der Review-Systeme und die Organisation des Reviews vermittelt werden.



So sieht die **Arbeitsoberfläche eines Review-Systems** für einen Reviewer aus: ❶ Hier wählt er, wie das Dokument ihm angezeigt werden soll (z.B. als Text, als Bild). ❷ Dies ist das zu beurteilende Dokument. ❸ Jedem Mitarbeiter werden Stapel (*"Batches"*) zugeteilt. Hier sieht er, wo er steht. ❹ Das *Coding Panel* mit den *Tags*. ❺ Zum angeschauten Dokument zugehörende Dokumente (z.B. Anhänge, E-Mail). ❻ Dokumentensets, die für den Review zur Verfügung stehen.

Sog. ***Calibration Meetings*** oder ***Calibration Runs*** können hilfreich sein um zu prüfen, ob die Reviewer die Instruktionen richtig verstanden haben. Dabei werden zu Beginn von den Reviewern jeweils 20 bis 30 Dokumente gesichtet und bewertet. Die Resultate werden im Team besprochen und wo nötig Korrekturen angebracht.

11. **Review initiieren, durchführen und überwachen.** Reviews sind logistisch oft eine gewisse Herausforderung. Die Einsatzpläne der Reviewer müssen gemacht und koordiniert sowie ebenso die Arbeitsplätze zugewiesen werden. Es müssen Zugangscodes organisiert und die Arbeit passend verteilt werden. Die Reviewer müssen instruiert und eingeführt werden, auch die laufend neu hinzutretenden Personen (während längeren Reviews wird es immer wieder Wechsel geben). Läuft der Review, werden rasch viele inhaltliche und operationelle Fragen von Reviewern kommen, die kurzfristig beantwortet werden müssen. Und so gut die Technik heute ist, kommt es fast immer zu irgendwelchen kleinen oder grösseren technischen Problemen: Zugänge funktionieren nicht, Dokumente werden nicht richtig angezeigt, Daten sind nicht verfügbar, etc. Alles steht unter Zeitdruck, denn die Reviewer werden in der Regel auch fürs Warten bezahlt. Immer wieder müssen auch inhaltliche Entscheide getroffen werden, die folgenschwer sein können – so z.B. wie eine bestimmte inhaltliche Konstellation bewertet und *codiert* werden soll. Folgenschwer sind sie deshalb, weil ein späteres Zurückkommen unter Umständen bedeutet, dass viele tausende Dokumente nochmals angeschaut werden müssen, was viel Zeit und Geld kostet. Trotzdem sind Reviews nicht starr, sondern ständig in Bewegung und können und müssen den laufenden Erkenntnissen entsprechend ständig angepasst und neu austariert werden. Auch hier ist daher Erfahrung und gutes Projektmanagement gefragt, damit die Qualität am Ende stimmt und die Kosten nicht aus dem Ruder laufen. Der oder die mit dem Management der Reviewer und für die Qualitätssicherung zuständigen Personen müssen zudem stets die Motivation ihres Teams im Auge behalten, was gerade bei längeren Reviews nicht einfach ist.

Austausch

Reviews eignen sich auf den ersten Blick ideal fürs Alleinarbeiten. Die Erfahrung zeigt aber: Der Erfahrungsaustausch untereinander ist enorm wichtig. Selbst wenn im Homeoffice gearbeitet wird, sollte ein ständiger Austausch, auch im Review-Team, möglich sein. Tägliche Calls auch mit dem Auftraggeber, auch um Probleme festzustellen und rasch aus dem Weg zu räumen, sind wichtig.

Die meisten Reviews stehen im **Spannungsfeld zwischen Qualität und Quantität**, die es zu erzielen gilt. Hier kommt einerseits der Qualitätssicherung eine wichtige Rolle zu und wie sie bewerkstelligt wird. Die einfachste Variante ist das „Vier-Augen-Prinzip", das allerdings normalerweise nur bei Schwärzungen durchgängig angewandt wird (dazu → **SWISS SECRECY & PRIVACY REVIEWS**). In anderen Fällen wird mit Methoden wie Stichproben, dem Zweitreview von *Samples* (z.B. 10-20%) oder Plausibilisierungen aufgrund der erfolgten *Tags* und *Peer-Reviews* in einer Anfangsphase gearbeitet. Auch auf die Quantität kann Einfluss genommen werden, so z.B. wie die Dokumente auf die einzelnen Reviewer verteilt werden, etwa indem alle E-Mails einer Diskussion (→ **Thread**) oder einer → **Familie** (z.B. E-Mail mit Beilagen) zusammengehalten werden. Auch ähnliche Dokumente (→ **Near Duplicates**) können unter Umständen gesondert und rascher abgehakt werden (z.B. indem sie gruppenweise *codiert* werden).

12. **Den Fortschritt überwachen.** Ein Review muss auch seitens des Auftraggebers begleitet werden. Das betrifft zum einen inhaltliche und organisatorische Bedürfnisse des Reviews. Die Reviewer sind normalerweise nicht vom Fach, d.h. nicht wirklich vertraut mit den Themen, welche in den E-Mails und Dokumenten diskutiert werden und die sie zwecks Einschätzung mindestens ansatzweise verstehen müssen. Dies bedeutet, dass Personen, die mit diesen Themen vertraut sind, ihnen zur Seite stehen sollten. Das kann insofern herausfordernd sein, als dass es nicht Personen sein sollten, die Gegenstand der internen Untersuchung sind und nach Möglichkeit auch nicht Arbeitskollegen der betroffenen Personen. Zum anderen müssen auch die Zielerreichung, Fortschritt und Kosten im Auge behalten werden. Wird ein Review plötzlich langsamer, sollte z.B. abgeklärt werden, woran dies liegt und ob es allenfalls helfen kann, die Review-Instruktionen bzw. Anforderungen an die Reviewer zu vereinfachen. Die eDiscovery-Provider können mit Hilfe ihrer Systeme auch Statistiken dazu liefern. Allerdings ist hier auch der Datenschutz der Reviewer zu beachten.

Wochenenden

Auch Reviewer brauchen Pausen. Erhalten sie sie nicht, leiden die Qualität und Motivation. Allerdings sind insbesondere nebenberufliche Projekt-Mitarbeiter (z.B. Studenten) leicht auch für Wochenendarbeit zu gewinnen, weil sie dann Zuschläge zum Lohn erhalten. Bei Profi-Reviewern im Ausland ist das anders: Sie müssen oft ohnehin für hiesige Verhältnisse überlang arbeiten.

Die **Aussagekraft** der Statistiken ist teilweise sehr begrenzt. Wenn z.B. die Anzahl der gesichteten Dokumente pro Stunde gemessen wird, werden oft Äpfel mit Birnen verglichen, denn nicht alle Dokumente sind gleich lang und gleich komplex. Viele Review-Systeme können nicht mehr zählen als die Anzahl bearbeiteter Dokumente, nicht aber z.B. die gesichteten Seiten.

13. **Die Ergebnisse nutzen.** Auf die Ergebnisse des Reviews können Sie als Auftraggeber oft schon während des Reviews zugreifen, falls Sie die Untersuchung selbst durchführen. Aufgrund der *Tags* lassen sich die entsprechenden Dokumente rasch anzeigen. Es ist nicht unüblich, dass sogar bei von Anwälten geführten internen Untersuchungen die Klienten einen Zugang zum eDiscovery-System erhalten. Das erleichtert den Zugang zu Dokumenten – auch im Falle von Fragen. Jedes Dokument hat eine Nummer (*"Document ID"*), anhand welcher das Dokument eindeutig bestimmt und auch aufgerufen werden kann.

E-Mails und Dokumente sind verlockende Beweise, denn ihr Inhalt liegt Schwarz auf Weiss auf dem Tisch. Trotz allem ist auch die vermeintlich klare Aussage mitunter **interpretationsbedürftig** oder kann je nach Kontext und Person, von welcher sie stammt, unterschiedlich verstanden werden. Darum ist es in einer internen Untersuchung wichtig, nebst einem Dokumenten-Review die betroffenen Personen auch zu befragen (→ **BEFRAGUNGEN**). Bei wichtigen Dokumenten lohnt es sich auch, die bestehenden Datenbestände nach ähnlichen Dokumenten oder anderen Versionen eines bestimmten Dokuments abzusuchen. Die Review-Systeme können auch die → **Metadaten** von Dokumenten anzeigen, die allerdings nicht unbedingt verlässlich sind (z.B. muss der angegebene Autor eines Dokuments nicht dem tatsächlichen Autor entsprechen).

Do's	Don'ts
• Ein linearer Review ist sehr kostenintensiv – hinterfragen Sie, ob es diesen wirklich braucht, ob er allenfalls auch eingeschränkter (z.B. weniger *Custodians*) durchgeführt werden könnte oder ob es nicht Alternativen gibt. • Betrachten Sie die Reviewer nicht einfach als „Maschinen", sondern	• Rechnen Sie nicht damit, dass die Technik immer funktioniert und immer genügend Performance bringt. Sie ersparen sich damit viel Frust. • Fangen Sie nicht einfach irgendwo an mit dem Review, sondern überlegen Sie sich, ob es bestimmte Dokumente gibt, deren Review

Do's	Don'ts
lassen Sie sie mitreden, wenn es um die Verbesserung des Reviews geht – sie kennen die Dokumente in der Regel am besten. • Informieren Sie die Reviewer über die Entwicklungen im Fall, auch wenn sie dies nicht unbedingt zu wissen brauchen – das motiviert nicht nur, sondern kann auch zu besseren Ergebnissen führen. • Suchen Sie ständig nach Ansätzen, wie der Review schneller und besser gemacht werden kann. Fragen Sie die Reviewer und den Provider. Er sagt Ihnen auch, ob → **TAR**[17] in Ihrem Fall womöglich hilfreich sein könnte (z.B. → **Predictive Coding**). • Verwenden Sie genügend Zeit und „Denke" für die Definition der Suchbegriffe, die *Tags* und die Instruktionen. • Der Stundensatz bei Reviewern sollte nicht matchentscheidend sein, wenn die Qualität stimmen muss. Profi-Reviewer sind nicht zwingend besser. • Ist der Review durch, sollten Sie mit dem Provider über die Deaktivierung von Benutzern und die Archivierung der Daten sprechen. Damit können laufende Servicegebühren reduziert werden.	sich mehr lohnt oder leichter ist als bei anderen Dokumenten. • Fokussieren Sie sich nicht zu sehr auf lineare Reviews, weil sie zwar teuer, aber trotzdem der Weg des geringsten Widerstands sind. • Der Austausch unter Reviewern ist wichtig, aber lassen Sie „Schwatztanten" nicht im Team – sie bremsen das ganze Team ab. • Erwarten Sie nicht Perfektion; ein gewisses Mass an Fehlern ist bei einem Review normal. Das gilt auch für Inkonsistenzen: *Tagging*-Entscheide sind oft nicht 100% klar – der eine trifft sie so, der andere anders.

17 *Technology Assisted Review*, d.h. technische Verfahren, die einen Review effizienter oder effektiver machen können. → **WERKZEUGE FÜR EDISCOVERY.**

Do's	Don'ts
• Achten Sie darauf, dass Sie einen eDiscovery-Provider wählen, der ein transparentes *Pricing* hat und ihre Daten nicht als „Geisel" nimmt; klären Sie daher insbesondere die Bedingungen der Archivierung bereits im Voraus.	

Wann Sie externe Unterstützung beiziehen sollten

- Wenn Sie selbst **noch nie einen Review** durchgeführt haben.
- Wenn Sie den Review selbst machen wollen, aber **kein Review-System** haben.
- Wenn Sie **kurzfristig Reviewer benötigen**, weil Ihnen die Ressourcen fehlen.
- Falls Sie eine **Zweitmeinung** darüber benötigen, ob ein linearer Review angezeigt ist.
- Wenn Sie unsicher sind, ob ihre bisherige Anlaufstelle für Untersuchungen wirklich **auf der Höhe der Technik** ist, wenn es um den Einsatz moderner Analyse- und *Review-Tools* geht.
- Wenn Sie nicht sicher sind, ob und wie weit der **Datenschutz** und das Arbeitsrecht den Review wie geplant zulässt.
- Falls **private Inhalte** zu sichten sind. Das gilt auch, wenn Sie es auf geschäftliche Inhalte abgesehen haben, aber mit privaten Inhalten rechnen müssen.
- Wenn es um eine **sensible Angelegenheit** geht, in welcher die Unabhängigkeit des Reviews besonders wichtig ist.
- Wenn Sie sich bezüglich der Durchführung eines Reviews **unsicher fühlen** oder sich nicht selbst darum kümmern möchten.

Häufige Fragen und Antworten

Q18. Ist ein Review von persönlichen Postfächern überhaupt erlaubt?

A: Ja, doch nur unter gewissen Bedingungen und mit gewissen Restriktionen zum Schutz der Privatsphäre und Gesundheit der Mitarbeiter.

Die Inhalte persönlicher Postfächer[18] stellen → **Personendaten des Mitarbeiters** dar, da der Arbeitgeber einen Bezug zum Mitarbeiter herstellen kann. Deren Bearbeitung

18 Gemeint sind also Postfächer wie „max.muster@firma.ch" im Gegensatz zu „verkauf@firma.ch".

(worunter auch der blosse Zugriff fällt) untersteht damit den Grundsätzen des Datenschutzes sowie den durch das Arbeitsrecht vorgesehenen Grenzen. Das Arbeitsrecht schützt die Persönlichkeit des Mitarbeiters im Zusammenhang mit der Erhebung und Bearbeitung von Personendaten nochmals explizit. Gemäss (Art. 328b → **OR**) darf der Arbeitgeber Daten über den Mitarbeiter nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Es bedarf eines sog. **Arbeitsplatzbezuges**.

Nach der hier vertretenen Ansicht handelt es sich bei Art. 328b OR nicht um eine eigentliche Verbotsnorm, sondern lediglich um eine Konkretisierung des datenschutzrechtlichen **Verhältnismässigkeitsprinzips**. Mit anderen Worten wird der Zugriff auf persönliche Postfächer des Mitarbeiters automatisch gegen einen datenschutzrechtlichen Grundsatz verstossen, kann aber durch einen → **Rechtfertigungsgrund** legitimiert werden. Als Rechtfertigungsgrund kommen hier ein überwiegendes Interesse, eine gesetzliche Pflicht oder die Einwilligung des Mitarbeiters in Frage (wobei an die Gültigkeit einer Einwilligung seitens eines Mitarbeiters aufgrund seiner Abhängigkeit vom Arbeitgeber erhöhte Anforderungen bezüglich der Freiwilligkeit gestellt werden). Diese Ansicht ist allerdings umstritten. Teilweise wird Art. 328b OR auch strenger ausgelegt und eine Rechtfertigung nach Art. 13 → **DSG** ausgeschlossen (was aber zu unsinnigen Ergebnissen führt wie etwa die Rechtswidrigkeit des Einsatzes von Antivirenscannern, soweit diese auch ein- und ausgehende private E-Mails scannen und somit bearbeiten).

Auf **geschäftliche E-Mails** und Dokumente hat der Arbeitgeber einen Anspruch und kann diese auch jederzeit herausverlangen oder, falls dies nicht möglich ist, darauf zugreifen – und zwar ohne besonderen Hinweis. Die Schwierigkeit in der Praxis besteht darin, dass der Zugriff auf ein *persönliches* Postfach regelmässig auch den **Zugriff auf private Inhalte** eröffnet (soweit solche privaten Inhalte nicht untersagt sind und diese Regel auch gelebt wird) und die Auswertung der E-Mails eines Mitarbeiters im Rahmen eines Reviews auch eine (verpönte) **Überwachung des Verhaltens** eines Mitarbeiters darstellen kann (Art. 26 → **ArgV3**). Daher darf der Arbeitgeber nicht einfach beliebig in die Postfächer der Mitarbeiter Einblick nehmen.

In der Praxis ist der Zugriff des Arbeitgebers auf persönliche Postfächer unter folgenden Bedingungen grundsätzlich möglich:

- Er darf nur aus **begründetem Anlass** erfolgen, also z.B. aufgrund eines konkreten Verdachts. Eine elektronische „Rasterfahndung", bei dem z.B. alle Mitarbeiter-Postfächer nach bestimmten Inhalten durchsucht werden, ist normalerweise nicht erlaubt. Läuft eine interne Untersuchung wegen eines möglichen Fehlverhaltens im

Unternehmen, wird es am konkreten Verdacht in aller Regel nicht fehlen. Selbstverständlich muss der Anlass legitimer Natur sein und insbesondere einen Arbeitsplatzbezug aufweisen.

- Der Zugriff auf **private Inhalte** ist grundsätzlich nicht gestattet, wobei Ausnahmen die Regel bestätigen (dazu → **Q19**). Es muss daher sichergestellt sein, dass kein (relevanter) Zugriff auf private Inhalte erfolgt. Die Schwierigkeit in der Praxis liegt dabei in der Tatsache, dass sich heute unter die meisten geschäftlichen E-Mails, auf welche der Arbeitgeber einen Anspruch hat und auf die er auch zugreifen darf, auch private Inhalte mischen können. Sie müssen, sobald erkannt, logisch aussortiert werden (z.B. durch entsprechende → **Tags**)[19]; geht es nur um einzelne Teile einer geschäftlichen E-Mail, sollten diese Teile vor einer Weitergabe ggf. geschwärzt werden. Helfen kann es immerhin, dass in einer internen Weisung festgehalten wird, dass private E-Mails im E-Mail-Postfach gesondert abzulegen und auch als solche zu kennzeichnen sind. Letzteres ist wichtiger als ersteres, da in einem Review häufig über alle Ordner hinweg nach bestimmten Stichworten gesucht wird; der Reviewer sieht in seiner Anzeige primär die E-Mail und deren Betreffzeile, nicht aber den Ordner, aus welchem sie stammt. Je nach Fall ist auch darauf zu achten, dass private Ordner missbräuchlich genutzt werden können, um Beweise für ein geschäftliches Fehlverhalten vor einem Zugriff zu schützen.

- Es darf zu **keiner Überwachung des Verhaltens** kommen. Ebenso ist der Zugriff auf ein **Mindestmass** und auf das zu beschränken, was für die Untersuchung von Relevanz ist. Dies wird u.a. durch entsprechende Such- und Review-Strategien und entsprechende, mit den betroffenen Personen nicht in Berührung stehenden Review-Teams sichergestellt. Durch den Einsatz von externen Reviewern wird der Eingriff in die Privatsphäre zusätzlich abgeschwächt.

Ferner sind die Mitarbeiter über den Review ihrer E-Mails zu **informieren** (Grundsatz der Transparenz). Diese Information hat optimalerweise in allgemeiner Form vorab zu erfolgen (z.B. durch ein Reglement, eine Weisung oder eine Datenschutzerklärung), sollte aber auch im konkreten Fall geschehen, sobald es der Gang der Untersuchung zulässt, ohne diese zu gefährden (z.B. über eine → **Legal Hold Notice**, dazu → **ERSTE SCHRITTE**, Schritt 15). Natürlich kann eine solche Information eine Gegenreaktion zu provozieren, mit welcher umzugehen ist. Sie bedeutet freilich nicht das Ende eines

19 Vgl. einen Fall des gewerblichen Schiedsgerichts Basel-Stadt, in welchem der Arbeitgeber vor Gericht aus E-Mails vorlas, die durch den Betreff „Schatzi" als privat gekennzeichnet waren (Jahrbuch des Schweizerischen Arbeitsrechts, JAR, 2004, S. 441). Das Gericht erachtete dies als persönlichkeitsverletzend. Ob die E-Mails als Beweis zulässig waren (es ging um Überstunden), entschied das Gericht nicht. In einem anderen Fall des Arbeitsgerichts Zürich, in welchem die Arbeitgeberin auf dem Computer des Arbeitnehmers Viren entfernte, dabei aber auch mehrere private E-Mails öffnete und las, schloss das Gericht ebenfalls auf eine rechtswidrige Persönlichkeitsverletzung (JAR 2004, S. 607).

Reviews, da ein solcher z.B. gestützt auf ein überwiegendes Interesse je nach Situation trotz Widerspruch einer betroffenen Person möglich ist.

Ist eine Information in allgemeiner Form nicht erfolgt, schliesst dies eine Einsichtnahme in das Postfach eines Mitarbeiters selbst dann nicht aus, wenn darin mit privaten E-Mails zu rechnen ist. Auch in diesem Fall ist eine Interessenabwägung vorzunehmen. Würde eine vorherige Information den Untersuchungszweck vereiteln und steht genügend auf dem Spiel, kann eine Sichtung der E-Mails **auch ohne vorherige Information erfolgen** (vgl. zur heimlichen Überwachung Entscheid BGer 9C_785/2010 vom 10. Juni 2010; vgl. auch → **ÜBERWACHUNGSMASSNAHMEN**).

In Deutschland kommt als Restriktion erschwerend hinzu, dass dort der Arbeitgeber zusätzlich dem **Fernmeldegeheimnis** unterliegt, falls er seinen Mitarbeitern erlaubt, das firmeneigene E-Mail-System für private Zwecke zu nutzen. Es braucht diesfalls eine Einwilligung des Mitarbeiters für den Zugriff, die mitunter serienmässig eingeholt wird. In der Schweiz gilt diese Regel nicht.

Zu beachten ist schliesslich, dass ein persönliches Postfach nicht nur Personendaten des betreffenden Mitarbeiters enthält, sondern auch vieler **anderer betroffener Personen** (als Empfänger oder Sender oder aufgrund des Inhaltes der E-Mails). Sie werden im Rahmen der datenschutzrechtlichen Erwägungen in der Regel „ausgeblendet", d.h. es wird davon ausgegangen, dass sie einen Review auch ohne spezifische Information hinzunehmen haben und ohnehin erwarten müssen. Die Frage ihres Schutzes kommt in der Praxis daher kaum je auf. Sie stellt sich in konkreten Fällen vor allem dann, wenn es um die Offenlegung von Unterlagen gegenüber Behörden geht.

Literatur:

Hafner, Peter: Auswertung der E-Mails von Arbeitnehmern, Aktuelle Juristische Praxis (AJP) 2018, 1327 ff.

Rosenthal, David/Jöhri, Yvonne, Art. 328b OR, in: Rosenthal, David/Jöhri, Yvonne (Hrsg.), Handkommentar zum Datenschutzgesetz, Zürich/Basel/Genf 2008

Wantz, Simona/Licci, Sara: Arbeitsvertragliche Rechte und Pflichten bei internen Untersuchungen, Jusletter vom 18. Februar 2019, Rz. 1 ff.

Q19. Unter welchen Umständen ist der Zugriff auf private E-Mails erlaubt?

A: Es muss hierbei unterschieden werden zwischen dem unvermeidbaren Zugriff auf private E-Mails, der **als Nebeneffekt** auf der Suche nach geschäftlichen Inhalten geschieht, und der **Suche gezielt in privaten E-Mails**. Ersteres kann bei jedem Zugriff auf persönliche Postfächer oder andere persönliche Kommunikation vorkommen, selbst wenn sie an sich beruflicher Natur sind. Auch in geschäftlichen E-Mails können

private Inhalte vorkommen. Sie sind entsprechend auszusortieren oder zu schwärzen (→ **Q18**). Letzteres ist etwas heikler.

Der **Zugriff auf private E-Mails** ist zunächst nur dort ohne Einwilligung des Mitarbeiters möglich, wo sich diese in einem geschäftlichen Postfach oder sonst dem Arbeitgeber zugeordneten Bereich befinden, d.h. unter seiner Kontrolle stehen. Daten auf *privaten* Geräten (z.B. dem privaten Smartphone oder privaten Notebook) sind grundsätzlich tabu für den Arbeitgeber, mit Ausnahme des geschäftlichen Bereichs auf einem **"Bring-your-own-Device"-Gerät**, soweit dies vorgängig vereinbart worden ist oder der Mitarbeiter eingewilligt hat (z.B. indem er sein Gerät unter Hinweis auf etwaige Zugriffe zur Verfügung gestellt hat). Befinden sich private E-Mails jedoch im geschäftlichen Postfach, kann je nach den Umständen des Falles ein Zugriff darauf im Einzelfall zulässig sein. Ein solcher Fall kann z.B. die Untersuchung eines konkreten Verdachts auf Diebstahl oder den Verrat von Geschäftsgeheimnissen sein (z.B., wenn der Mitarbeiter sich mit seinem geschäftlichen E-Mail-Konto Dokumente mit Geschäftsgeheimnissen auf seine oder gar eine fremde private E-Mail-Adresse sendet).

Soll eine solche Untersuchung durchgeführt werden, gelten die Anforderungen für die Sichtung von persönlichen Postfächern (→ **Q18**) in erhöhtem Masse. Der **Zugriff muss auf wenige, externe Personen beschränkt sein** und es muss sichergestellt werden, dass der Arbeitgeber (oder Arbeitskollegen des Mitarbeiters) über die privaten Inhalte, welche diese externen Personen ggf. zur Kenntnis nehmen, nichts erfahren. Der Zugriff darf auch nur soweit gehen, wie dies für die Untersuchung unbedingt erforderlich ist und es darf **keine geeigneten, milderen Mittel** geben. In besonders heiklen Fällen ist zu prüfen, ob die Sichtung der privaten, von den geschäftlichen bereits abgesonderten E-Mails, nicht durch eine mit der rechtlichen Aufarbeitung des Falls nicht befassten Person vorgenommen werden sollte.

In rechtlicher Hinsicht erfolgt ein solcher Zugriff auf private E-Mails üblicherweise gestützt auf den **Rechtfertigungsgrund** der überwiegenden privaten Interessen. Das gilt vor allem dann, wenn der betreffende Mitarbeiter aus taktischen oder anderen Gründen nicht gefragt werden kann.

Es gibt jedoch erfahrungsgemäss auch Fälle, in denen Mitarbeiter durchaus bereit sind, sogar ihre **privaten Computer** für eine **Inspektion** zu öffnen. Dies können als Beispiel Mitarbeiter sein, die auf diese Weise einen Verdacht ausräumen möchten oder die auf ihrem privaten Computer Opfer eines Cyberangriffs geworden sind, der ebenfalls geschäftliche Daten betroffen hat, die korrekterweise oder inkorrekterweise auf diesem Gerät gespeichert waren. Um nachvollziehen zu können, was genau vorgefallen ist und wie gross der Schaden ist, kann es für einen Forensiker erforderlich sein, sich das gesamte (private) Gerät näher anzuschauen. Selbstverständlich kann ein Mitarbeiter in eine solche Untersuchung seines Geräts einwilligen und wird oft auch Interesse daran haben, dies zu tun. Die Einwilligung sollte jedoch schriftlich festgehalten werden, einschliesslich der genauen Vorgehensweise (z.B. mittels eines Protokolls).

In der Praxis kommen immer wieder Situationen vor, in welchen der Arbeitnehmer mit oder ohne Erlaubnis **private Konten für geschäftliche Kommunikation** nutzt. Zu denken ist an den Verkaufsmitarbeiter, der von seinem Kunden via WhatsApp auf seinem privaten Mobiltelefon angeschrieben wird, um mit ihm über einen Auftrag zu sprechen. Ein anderes Beispiel ist der persönliche (und in aller Regel nicht geschäftliche) LinkedIn-Account, der für geschäftliche Zwecke verwendet wird. Da diese Konten und Kanäle sich dem technischen Zugriff des Unternehmens i.d.R. entziehen, wird deren Einsatz für geschäftliche Belange häufig untersagt; auch die Verwendung persönlicher Konten für geschäftliche Aktivitäten in sozialen Netzwerken ist nicht sinnvoll (davon zu trennen ist die persönliche Beziehungspflege und im eigenen Namen erfolgende Eigen- und Fremdpromotion eines Arbeitnehmers). Findet trotzdem geschäftliche Kommunikation über diese Konten und Kanäle statt, kann der Arbeitgeber deren Herausgabe verlangen, denn sie steht grundsätzlich ihm zu.

Literatur:

Hafner, Peter: Auswertung der E-Mails von Arbeitnehmern, Aktuelle Juristische Praxis (AJP) 2018, 1327 ff.

Wantz, Simona/Licci, Sara: Arbeitsvertragliche Rechte und Pflichten bei internen Untersuchungen, Jusletter vom 18. Februar 2019, Rz. 1 ff.

Q20. Kann der Arbeitgeber auf Unterlagen im Home-Office zugreifen?

A. Geschäftliche Unterlagen sowie der Arbeitsplatz stehen im **Eigentum** des Arbeitgebers. Der Arbeitgeber ist dazu berechtigt sämtliche, geschäftliche Inhalte am Arbeitsplatz zu sammeln und zu bearbeiten. Der Mitarbeiter hat ferner gegenüber dem Arbeitgeber eine **Rechenschafts- und Herausgabepflicht**. Daraus folgt, dass der Mitarbeiter dem Arbeitgeber sämtliche Arbeitsprodukte herausgeben bzw. überlassen muss. Grundsätzlich hat der Mitarbeiter die Dokumente also dem Arbeitgeber zur Verfügung zu stellen, auch wenn sich diese in den persönlichen Räumlichkeiten befinden. Es handelt sich um eine Bringschuld.

Der Arbeitgeber kann nicht wissen, welche Unterlagen der Mitarbeiter zuhause aufbewahrt. Unter Umständen wird ein Arbeitgeber das Bedürfnis haben, eine **Durchsuchung des Home-Offices** veranlassen zu können. Obschon der Mitarbeiter aufgrund seines Arbeitsverhältnisses gewisse Pflichten gegenüber dem Arbeitgeber hat, legitimieren diese nicht automatisch zum Zutritt in die privaten Räumlichkeiten. Der Arbeitgeber hat vorgängig die Zustimmung des Mitarbeiters einzuholen. Teilweise wird diskutiert, ob ein solches **Zutrittsrecht** mit Blick auf das Home-Office vertraglich vereinbart werden kann. Im Normalfall würde eine solche Klausel in der Schweiz wohl kaum

geschützt werden und auch nicht zielführend sein. Zudem bedürfte der tatsächliche Zutritt noch immer der Zustimmung des Mitarbeiters. Da dies eine weitgehende Massnahme ist, die mit einem gewichtigen Eingriff in die Privatsphäre des Mitarbeiters verbunden sein kann, ist ein Modus zu wählen, der die Privatsphäre schützt. So sollte etwa der Zugang nicht durch den Vorgesetzten oder Arbeitskollegen erfolgen, sondern durch extern beigezogene Personen, die mit dem Mitarbeiter in keiner Beziehung stehen.

Der Mitarbeiter wird im Home-Office regelmässig auf seinem **privaten Gerät** arbeiten. Für den Arbeitgeber sind die Möglichkeiten auf solche privaten Geräte zuzugreifen beschränkt, jedenfalls wo es sich um mehr als ein Mobiltelefon handelt, welches über eine *Mobile-Device-Management*-Lösung kontrolliert werden kann. Arbeitet der Mitarbeiter in einem Cloud-System oder einer Remote-Session auf den Servern des Unternehmens, ergeben sich in der Praxis hierbei kaum Probleme, da vor Ort bei entsprechenden Sicherheitsvorkehrungen nichts gespeichert werden kann (der Computer übernimmt lediglich die Funktion des Bildschirms und der Tastatur mit Maus). Screenshots (und deren lokale Speicherung) sind immerhin meist noch möglich, und wenn die lokale Speicherung aus einer solchen Remote- oder Cloud-Session und Nutzung der Zwischenablage nicht unterbunden ist, dann können auch geschäftliche Dokumente lokal weiterverarbeitet werden. Dasselbe gilt, wenn ein E-Mail-Zugriff via Web-Client oder lokalem Mail-Client möglich ist; in letzterem Falle können umfassende E-Mail-Archive auf dem privaten Computer des Mitarbeiters gespeichert sein. Aus Sicht des Arbeitgebers ist es daher sinnvoll, sich diese Möglichkeiten vorab bewusst zu machen und entsprechende technische Vorkehrungen zu treffen – oder mit dem Risiko zu leben.

Immerhin: Ein **Recht zur Sichtung bzw. zur Kontrolle** des privaten Geräts kann rechtlich vorgesehen werden, jedenfalls wenn der Wunsch zum geschäftlichen Einsatz eines privaten Gerätes für geschäftliche Zwecke vom Mitarbeiter aus kommt (→ **Bring-Your-Own-Device**, BYOD). Solche Regelungen kommen insbesondere bei mobilen Geräten regelmässig vor, doch ist dem Arbeitgeber der Zugriff auch dann nur in Ausnahmefällen gestattet. Es ist denkbar, solche Regeln auch für den privaten Computer im Home-Office zu treffen. Der Mitarbeiter kann jedoch nicht gezwungen werden, dem Arbeitgeber den Zugriff darauf zu gestatten (davon zu unterscheiden ist der Zwang, dass sich der Arbeitnehmer selbst einen Computer für den *eigenen* Fernzugriff auf die Bürosysteme beschaffen muss, wenn von zu Hause gearbeitet werden soll). Praktisch erfolgt die Einwilligung in den Zugriff durch den Arbeitgeber entweder durch eine ausdrückliche Vereinbarung oder implizit dadurch, dass der Arbeitgeber ein BYOD-Reglement aufstellt oder entsprechende Hinweise erlässt, die einen Zugriff des Arbeitgebers (z.B. Lokalisierung und Fernlöschung im Falle eines Verlustes) vorbehält und der Mitarbeiter – im Wissen darum – sein Gerät mit der entsprechenden Software des Arbeitgebers ausstatten lässt. Die meisten BYOD-Reglemente regeln zudem nur den Fall des Verlusts des Geräts, nicht auch den Zugriff im Falle einer internen Untersuchung. Hierbei sind die auf solchen Geräten vorhandenen privaten Inhalte zu beachten, die

den Arbeitgeber normalerweise nichts angehen (dazu → **Q18** und → **Q19**), aber auch der Umstand, dass das Gerät und dessen Daten nicht im Eigentum des Arbeitgebers stehen. Hieraus können sich auch strafrechtliche Risiken ergeben. Zur Überwachung → **ÜBERWACHUNGSMASSNAHMEN**.

> **Literatur:**
>
> Birkhäuser, Nicolas/Hadorn, marcel: BYOD – Bring Your Own Device, Schweizerische Juristenzeitung (SJZ) 109/2013, 201 ff.
>
> Naber, Sebastian/Ahrens, Tim: Remote Investigations: Die Aufklärung von Compliance-Verstössen im New Normal, Compliance Berater (CB) 2020, 465 ff.
>
> Wantz, Simona/Licci, Sara: Arbeitsvertragliche Rechte und Pflichten bei internen Untersuchungen, Jusletter vom 18. Februar 2019, Rz. 1 ff.
>
> Wildhaber, Isabelle/Hänsenberger, Silvio: Bring Your Own Device (BYOD), Zeitschrift für Arbeitsrecht und Arbeitslosenversicherung (ARV) 2016, 151 ff.

Q21. Wir möchten in den Review eine Kanzlei in den USA einbeziehen. Ist es rechtlich zulässig, ihr einen Zugriff auf die Daten zu gestatten?

A: Der Zugriff auf ein Review-Tool durch eine ausländische Kanzlei ist grundsätzlich nicht verboten. Das Datenschutzgesetz sieht jedoch spezielle Bestimmungen für die **Bekanntgabe von Personendaten ins Ausland** vor. Unter die Bekanntgabe von Personendaten ins Ausland fällt auch der Fernzugriff vom Ausland auf inländische Personendaten („**Remote Access**").

Wird eine amerikanische Kanzlei der Zugriff gestattet, sind somit die datenschutzrechtlichen Vorgaben für den Transfer von Personendaten ins Ausland zu beachten. Die USA verfügt aus Perspektive des schweizerischen Datenschutzrechts über **kein hinreichendes Schutzniveau**. Das Unternehmen hat somit einen angemessenen Datenschutz sicherzustellen, z.B. durch die Verwendung von → **Standardvertragsklauseln** der Europäischen Kommission sowie entsprechenden Sicherheitsmassnahmen. Die Unterzeichnung entsprechender Verträge zwecks Durchführung von Reviews sind bei US-Kanzleien inzwischen allgemein akzeptiert.

In der Praxis stellt sich nebst dem Datenschutz vor allem die Frage, ob mit einer Zugriffsmöglichkeit aus den USA, das Risiko eines ausländischen Behördenzugriffs steigt. Sollte ein Schweizer Unternehmen beispielsweise mit einem **Herausgabebefehl einer US-Behörde** konfrontiert sein, wird die US-Behörde diesen in der Schweiz rechtlich normalerweise nicht ohne Weiteres durchsetzen können. Haben jedoch die US-Anwälte des Schweizer Unternehmens auf die verlangten Daten Zugriff, so können sie ihrerseits aus eigenem Recht verpflichtet sein, die ihnen zugänglichen Dokumente den Behörden offenzulegen – auch gegen den Willen ihres Klienten. Dieses Risiko kann es in besonderen Situationen erforderlich machen, den Zugang durch Anwälte in den USA (oder

sonst im Ausland) einzuschränken oder mindestens so auszugestalten, dass die Daten weiterhin in der Schweiz gespeichert sind und lediglich ein Fernzugriff besteht, der bei Bedarf auch gekappt werden kann.

Erfahrungsgemäss ist es auch „gefühlt" für viele Schweizer Unternehmen wichtig, dass ihre Daten – wenn sie schon für die Zwecke einer internen Untersuchung herausgegeben werden müssen – **in der Schweiz verbleiben**.

Zu beachten sind schliesslich auch allfällige **Geheimhaltungsvorschriften**, namentlich im Bereich des Berufsgeheimnisses. Dieses kann es erfordern, dass besonders geschützte Daten (z.B. Bankkundendaten) nur Personen in der Schweiz zugänglich gemacht werden, weil ihre Geheimhaltung ausserhalb der Schweiz nicht mehr kontrolliert werden kann oder weil das Unternehmen sich vertraglich gegenüber Dritten (um deren Geheimnisse es geht) verpflichtet hat, die Daten nicht ausser Landes zu geben. Dies kann den Beizug ausländischer Anwälte (und Dienstleister) erschweren oder verunmöglichen – oder erst nach einer Sichtung und Bereinigung der Unterlagen (→ **SWISS SECRECY & PRIVACY REVIEWS**).

Q22. Worauf muss ich aus Sicht des Datenschutzes im Vertrag mit meinem eDiscovery-Provider achten?

A: Bezieht ein Unternehmen Dienste von einem eDiscovery-Provider verbleibt die **Verantwortung** für die Datenbearbeitung in Einhaltung der einschlägigen Datenschutzbestimmungen in der Regel beim Unternehmen, welches die Personendaten weitergibt und letztlich die Parameter der Datenbearbeitung festlegt. Das Unternehmen bleibt sog. → **Verantwortlicher**, während der eDiscovery-Provider als → **Auftragsbearbeiter** gilt.

Die beiden Parteien haben einen → **Auftragsbearbeitungsvertrag** (ADV) abzuschliessen. Unter dem revidierten Datenschutzgesetz wird der Abschluss eines solchen Vertrages in schriftlicher Form **Pflicht** sein und das Fehlen eines solchen bei Vorsatz mit **Busse** sanktioniert. Der ADV wird in der Praxis als Teil des Dienstleistungsvertrages mit dem eDiscovery-Provider abgeschlossen (z.B. als Nachtrag zum Dienstleistungsvertrag) oder separat (z.B. als separater Vertrag, der mit dem Dienstleistungsvertrag verbunden ist).

Das **Schweizer Recht** regelt die zwingenden Inhalte eines ADV lediglich in seinen **Grundzügen**. Durch den ADV hat das Unternehmen sicherzustellen, dass der eDiscovery-Provider die Daten in der Form bearbeitet, wie das Unternehmen dies auch tun darf. Die Datenbearbeitung hat demnach nach den **Weisungen** des Unternehmens zu erfolgen. Der ADV sollte die **Datenbearbeitung** möglichst genau umschreiben, wobei sich die Datenbearbeitung aus dem restlichen Vertrag ergeben kann:

Checkliste

Details zur Bearbeitung sollten folgendes enthalten:

- Den Gegenstand der Bearbeitung
- Die Dauer der Bearbeitung
- Art und Zweck der Bearbeitung
- Die Arten der betroffenen Personendaten
- Die Kategorien der betroffenen Personen

Sinnvollerweise sind ausserdem Bestimmungen zur **Datensicherheit** sowie zu den **Unterstützungspflichten** (z.B. bei der Bearbeitung von Auskunftsersuchen) in den ADV aufzunehmen. Dies ist heute in der Regel völlig selbstverständlich. Befindet sich der eDiscovery-Provider im Ausland oder möchte er einen Teil Ihrer Daten im Ausland bearbeiten (z.B. Wartungszugriffe, Speicherung im Ausland), sind Bestimmungen zum → **Datenexport** in den Vertrag aufzunehmen, wie sie das Datenschutzrecht vorgibt. Auch dies ist heute weitgehend Standard.

Auf Ebene der **Europäischen Union** definiert die einschlägige → **EU-Datenschutz-Grundverordnung** (DSGVO) den genauen Inhalt einer solchen ADV. Es lohnt sich, sich an diesen Vorgaben zu orientieren. Die meisten eDiscovery-Provider tun dies ohnehin. Es ist aber darauf zu achten, dass sie nicht nur Referenzen auf die DSGVO aufweisen, sondern sich auch auf das Schweizer Datenschutzrecht beziehen:

Checkliste

Gemäss Art. 28(3) DSGVO müssen Bestimmungen zu nachfolgenden Punkten aufgenommen werden:

- **Weisungsrecht** in Bezug auf die Bearbeitung von Personendaten, einschliesslich in Bezug auf Datenexporte ins Ausland;
- Verpflichtung aller involvierten Parteien bezogen auf das **Datengeheimnis**;
- Angemessene **technische und organisatorische Massnahmen** im Zusammenhang mit der **Datensicherheit**;
- Regelung zum allfälligen Beizug von **Unterauftragsbearbeitern** (lediglich mit Genehmigung des Verantwortlichen zulässig, wobei für neue Unterauftragsbearbeiter eine Widerspruchslösung zulässig ist);
- Pflicht zur Unterstützung des Verantwortlichen bei der **Erfüllung der Rechte der betroffenen Person** (Auskunftsrecht, Löschrecht);

- Pflicht zur Unterstützung des Verantwortlichen bei **Erfüllung der Meldepflicht** bei Verletzungen gegen die Datensicherheit und Datenschutzfolgeabschätzungen;
- **Rückgabe bzw. Löschung der Daten** nach Ende der Auftragsbearbeitung;
- **Prüfrecht** des Verantwortlichen.

Ist ein Anwalt in die interne Untersuchung involviert, ist es sinnvoll, wenn der eDiscovery-Provider vom Anwalt beigezogen wird und somit als seine Hilfsperson dem **Anwaltsgeheimnis** unterstellt wird. Soweit es sich um Daten für eine anwaltstypische Tätigkeit handelt, die er bearbeitet, schützt dies auch vor einem Zugriff durch Schweizer Behörden (→ **Q10**). In der Praxis wird der Auftrag an den eDisvovery-Provider typischerweise vom Anwalt erteilt, der auch den entsprechenden Dienstleistungsvertrag unterzeichnet. Der Klient wird den Vertrag typischerweise auch unterzeichnen, jedoch nur in Bezug auf die Verpflichtung zur Bezahlung der anfallenden Kosten.

Literatur:

Rosenthal, David: Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, Jusletter vom 17. Juni 2019, Rz. 1 ff.

Q23. Müssen wir auch mit unserem Anwalt einen Vertrag über die Auftragsbearbeitung abschliessen?

A: Normalerweise ist dies nicht erforderlich, da ein Anwalt die ihm anvertrauten oder von ihm sonst für sein Mandat beschafften Personendaten als → **Verantwortlicher** bearbeitet. Führt er jedoch im Auftrag seines Klienten einen → **Review** durch, kann er diesbezüglich als → **Auftragsbearbeiter** gelten, jedenfalls wenn der Klient die Rahmenbedingungen des Reviews bestimmt, also die datenschutzrechtlichen Eckwerte festlegt. Ob dies der Fall ist, hängt von den Umständen ab, d.h. insbesondere der Frage, wie frei der Anwalt in der Durchführung des Reviews ist. Folgt er letztlich nur den Weisungen des Kunden, so wird er Auftragsbearbeiter sein und hat in diesem Falle auch einen → **Auftragsbearbeitungsvertrag** (ADV) abzuschliessen. Untersteht der Klient der DSGVO mit Bezug auf die zu sichtenden Personendaten, muss der ADV zudem den Anforderungen der DSGVO entsprechen. Zum Inhalt eines ADV → **Q22**.

Literatur:

Rosenthal, David: Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, Jusletter vom 17. Juni 2019, Rz. 1 ff.

Q24. Wir haben Dokumente auf Papier. Sollen und können wir diese in den elektronischen Review integrieren?

A: Technisch ist dies kein Problem. Review-Systeme können auch Scans von Papierdokumenten aufnehmen und diese auch einer Texterkennung (→ **OCR**) unterziehen (→ **WERKZEUGE FÜR EDISCOVERY**). Die Frage ist in der Praxis primär mit Blick auf die **Kosten** einer internen Untersuchung zu beantworten. Das Einscannen physischer Dokumente kann mitunter hohe Kosten verursachen, gerade wenn diese in grosser Zahl vorliegen. Sind diese in Ordnern vorhanden, allenfalls noch geheftet oder geklammert, ist viel Handarbeit erforderlich.

Des Weiteren ist das Einscannen sämtlicher physischer Dokumente auch aus dem Blickwinkel der **Effizienz** nicht immer sinnvoll. Es befinden sich darunter vermutlich mehr irrelevante Dokumente, als einschlägige. Sinnvollerweise sollte deshalb zunächst eine **Triage** der vorhandenen, physischen Dokumente vorgenommen werden und anschliessend lediglich die zentralen Dokumente in den elektronischen Review integriert werden.

Es ist möglich, dass die Umstände dazu zwingen Papierdokumente elektronisch in den Review zu integrieren. Dies kann z.B. der Fall sein, wenn die Dokumente vor Ort für das Tagesgeschäft des Unternehmens gebraucht werden und somit für den Review nicht mitgenommen werden können oder nur für kurze Zeit. Ist eine Beweissicherung von solchen Dokumenten nötig, sind grössere Unterbrüche für das Scannen jedoch oft unvermeidbar. Dies ist vorgängig zu erwägen.

Q25. Können Reviews auch im Home-Office durchgeführt werden?

A: Ja, das wird international auch so praktiziert. Solche Reviews bergen jedoch zusätzliche Herausforderungen.

Die erste Herausforderung ist die Wahrung der **Geheimhaltung**. Unbefugte dürfen keinen Einblick in die Unterlagen erhalten. Im Home-Office besteht jedoch das **Risiko**, dass andere Familienmitglieder und Mitbewohner (vielleicht auch unabsichtlich) Einblick in die Unterlagen erhalten können. Diese unterstehen ihrerseits keinem Berufs- bzw. Geschäftsgeheimnis. Das Unternehmen muss sich diesem Risiko bewusst sein, wenn ein Review im Home-Office in Betracht gezogen wird. Die Reviewer sind entsprechend zu instruieren. Eine Überprüfung ist jedoch schwierig.

Da die meisten Reviews heute erstens elektronisch stattfinden und der Zugang zweitens so gestaltet ist, dass auf dem vom Reviewer verwendeten Rechner keine Inhalte gespeichert werden, wird die **technische Absicherung** des Reviews in der Regel wenig Schwierigkeiten bereiten. Um sicherzustellen, dass ihre Mitarbeiter in einer vertraulichen Umgebung arbeiten, sind gewisse Review-Unternehmen dazu übergegangen, ihre Mitarbeiter mit Hilfe von Kameras sporadisch zu überwachen. Für Schweizer Verhältnisse sind solche Methoden jedoch nicht ohne Weiteres zulässig.

Die zweite Herausforderung besteht im **fehlenden Austausch der Reviewer** untereinander. Ein solcher leistet für die Qualität eines Reviews einen nicht zu unterschätzenden Beitrag, denn in jedem Review stellen sich jedenfalls zu Beginn sehr viele Abgrenzungs- und Ermessensfragen, welche die Reviewer durch einen gegenseitigen Austausch oft rascher klären können als über einen Austausch mit dem Klienten oder dem zuständigen Anwalt. Sie können sich untereinander auch über Erkenntnisse orientieren, die den anderen Reviewern helfen können. Sitzt jeder Reviewer für sich alleine vor dem Bildschirm, wird dieser Austausch schwieriger. Es sollte daher auf andere Weise eine einfache Kommunikation unter den Reviewern ermöglicht werden (z.B. über Gruppenchats).

Die **Produktivität** von Home-Office-Reviews ist erfahrungsgemäss nicht schlechter als herkömmliche Reviews. Sie lässt sich in beiden Fällen vergleichsweise gut messen. Die Kosten solcher Reviews sind tendenziell auch etwas tiefer, allerdings werden diese Einsparungen typischerweise nicht an die Endkunden weitergegeben.

Q26. Je länger wir zurückschauen, desto weniger E-Mails hat es im Review – wie kann das sein?

A: Wenn wir ausschliessen, dass dies an den von Ihnen gewählten Suchbegriffen liegt, so hat dies oft damit zu tun, dass die betreffenden Mitarbeiter die E-Mails in ihren Postfächern entweder manuell oder automatisch nach einer bestimmten Zeit löschen (z.B. nach 90 oder 180 Tagen) oder in Archive überführen.

Es ist daher wichtig zu prüfen, ob im betreffenden Betrieb allenfalls auch eine zentrale oder dezentrale Archivierung von E-Mails stattfindet, auf die nicht über das herkömmliche E-Mail-System zugegriffen wird. Wird in diesen Fällen das Postfach eines Mitarbeiters vom operativen Mail-Server gesichert, liegen für den Review nur die aktuellen E-Mails vor, nicht aber die archivierten. Selbst wenn das Unternehmen offiziell über keine E-Mail-Archivierung verfügt, ist es Mitarbeitern unter Umständen möglich, über Postfachdateien eigene E-Mail-Archive auf ihren lokalen oder persönlichen Laufwerken zu unterhalten. Diese müssen im Falle eines Reviews ebenfalls miteinbezogen werden.

Histogramme können dabei zur Plausibilisierung dienen, d.h. sie zeigen grafisch die Verteilung der Dokumentenmenge auf der Zeitachse an.

Gedanken zum Thema.

Durch die Konfrontation verdächtiger Personen in einer internen Untersuchung kann für ein Strafverfahren auch viel verloren gehen. Die Untersuchungsbeauftragten stellen hier den Erstkontakt her. Das ermöglicht es den Tätern, gegebenenfalls Beweismittel zu vernichten und sich untereinander abzusprechen, bevor die zur Abwehr derartiger Kollusionsgefahr gedachten strafprozessualen Zwangsmassnahmen veranlasst werden konnten. Entsprechend ist der Auftraggeber vor die Wahl gestellt: Will er eine möglichst wirksame Strafverfolgung oder eine möglichst vollständige interne Untersuchung?

Damian K. Graf
Staatsanwalt für Wirtschaftsdelikte
NW/OW/UR

5. Analyse strukturierter Daten

Kurz gesagt

- Sie zählen noch als „Geheimtipp“, weil viele in internen Untersuchungen nur an die Sichtung von E-Mails und Dokumenten denken und sich keine Gedanken machen, welche anderen Datenquellen weiterführende Hinweise liefern könnten.
- Die Auswertung erfordert oft Spezialkenntnisse in der Extrahierung, Aufbereitung und Analyse von Daten aus den in einem Unternehmen eingesetzten Systemen, wie z.B. der Buchhaltung, der Bestellverwaltung oder System-Logs.
- Der Auswertung von Sachdaten sind rechtlich kaum Grenzen gesetzt, aber sobald Daten einen Personenbezug haben, muss der Datenschutz und das Verbot der Verhaltensüberwachung beachtet werden – es muss soweit möglich informiert werden und Auswertungen sind sachlich und zeitlich zu begrenzen.

Worum es geht

In vielen internen Untersuchungen werden → **strukturierte Daten** als Informationsquelle noch zu wenig beachtet, weil viele sich auf Dokumenten-Reviews fokussieren. Je nach Fall kann die Analyse von strukturierten Daten allerdings ebenso wichtig oder sogar noch wichtiger sein. Im Vordergrund steht die Auswertung von Transaktionsdaten (Finanztransaktionen, Warentransaktionen, Bestellungen, Konten, etc.) und Daten über das Verhalten von Personen (z.B. Zutritte, Zugriffe, Logins, Telefonate, Sitzungen, Nutzung von Geräten wie z.B. Drucker, Standorte). Ein vorsichtiger Mitarbeiter wird zwar möglicherweise keine Spuren in Firmen-E-Mails hinterlassen, wenn er einen Beamten über einen Mittelsmann bestechen lässt, aber von irgendwoher muss das Geld kommen – und dies wird in der Regel Spuren hinterlassen.

Worauf zu achten ist

- Ist der deliktische *Modus Operandi* vermutet oder bekannt und betrifft er bestimmte geschäftliche Aktivitäten, so sollte versucht werden, diese datenmässig darzustellen und auf verdächtige Muster hin zu analysieren.
- Die dafür nötigen Daten gibt es normalerweise immer; die Herausforderung ist

Frühwarnsystem

Die Analyse strukturierter Daten kann nicht nur zur Aufklärung von Fehlverhalten beitragen, sondern frühzeitig auf Fehlverhalten hinweisen. Unternehmen setzen z.B. Warnsysteme ein, die vor Betrügern in ihren Online-Shops warnen oder in Vertriebs- und Finanzdaten nach Hinweisen auf Korruption suchen.

zu verstehen wo sie sind und wie an sie in einer maschinell auswertbaren Form heranzukommen ist.

- Oft hilft bereits eine Visualisierung von Daten, um verdächtige Muster zu erkennen; auch Computer-Analysen bedingen in der Regel Handarbeit eines Experten
- Bei Finanzdelikten sollte ein → **Forensic Accountant** beigezogen werden, der die typischen Vorgehensweisen der Täter kennt und daher weiss, worauf zu achten und welche Indizien zu suchen sind.
- Je mehr Computer und andere elektronische Geräte wir nutzen, desto mehr Spuren hinterlassen wir, die sich letztlich auch auswerten lassen.
- Sobald Verhaltensdaten im Spiel sind, sind der Datenschutz und das Arbeitsrecht zu beachten. In der Schweiz ist deren Auswertung (durch ein privates Unternehmen) nur in engen Grenzen erlaubt.

In heutigen Computersystemen wird jeweils **protokolliert**, wer was tut (sog. *Audit-Trails*). Allerdings sollte bedacht werden, dass Logins auch gestohlen oder inoffiziell aber mit Erlaubnis des Inhabers von anderen Personen (z.B. der Assistenz) genutzt werden können, so dass der angegebene Benutzer nicht dem tatsächlichen entspricht. Steht ein solcher Fall zur Diskussion, kann wiederum die Auswertung anderer Protokolle und Daten helfen, die Situation aufzuklären: Wer war am betreffenden Tag gemäss Badge-Log im Gebäude? War der Login-Inhaber zur selben Zeit separat eingeloggt, so bspw. via Internet über das E-Mail-Programm auf seinem Mobiltelefon, das wiederum über eine externe IP-Adresse mit dem Firmenserver verbunden war, was je nach IP-Adresse darauf hinweist, dass er sich an einem anderen Ort aufhielt? Lässt sich aus den Verbindungsnachweisen des hausinternen WLAN-Systems schliessen, ob eines der persönlichen Geräte, welche die in Frage stehenden Personen normalerweise auf sich tragen, vor Ort war? Allerdings gilt auch hier: Die Datenschutzfragen klären, bevor ausgewertet wird.

Wie vorzugehen ist

1. **Überlegen Sie, welche Informationen für Ihren Fall interessant sein könnten.** Sie müssen in einem ersten Schritt verstehen, welche Fragen Sie beantwortet haben möchten und welche Informationen es dazu braucht. Die Antworten finden Sie häufig am besten in einer Brainstorming-Sitzung im Team.
   - Geht es um einen möglichen Korruptionsfall in einer Unternehmen, so könnten z.B. die von ihr vorgenommenen Zahlungen, die dazugehörigen Freigaben, die Daten der Spesen- und Reisebelege, vergebene und erhaltene Bestellungen, die

Kontaktliste des → **CRM-Systems**, die persönlichen Kontakt- und Kalenderdaten und Einträge und Übersichten von Vertragsbeziehungen mit Dienstleistern von Relevanz sein.

- Wird einem Vorgesetzten ein systematisches Fehlverhalten gegenüber seinen Mitarbeitern vorgeworfen, so kann z.B. eine Aufstellung der HR-Abteilung über personelle Wechsel in der betreffenden Abteilung der letzten fünf Jahre von Relevanz sein, inklusive einer Liste der bestehenden und ehemaligen Mitarbeiter sowie eine Aufstellung bisheriger Beschwerden.
- Steht ein Datendiebstahl im Raum, kann z.B. relevant sein, auf welche Daten der Verdächtige in den letzten drei Monaten zugegriffen, welche er ausgedruckt oder allenfalls aus dem System heraus übermittelt hat sowie, ob er bestimmte Systeme für die Dateiübertragung nebst dem E-Mail benutzt hat.

Quellen?

- Buchhaltung
- ERP-Systeme
- BI-Systeme
- CRM-Systeme
- HR-Systeme
- Branchenlösungen
- Lagersysteme
- Spesenverwaltung
- Gebäudesysteme
- Zutrittskontrollen
- Logs von Servern
- WLAN-Protokolle
- Telefonzentralen
- Abrechnungen
- Archive
- Überwachungsgeräte
- Fahrzeugcomputer
- Mobile Geräte
- Anwendungen Dritter

2. **Identifizieren Sie mögliche Datenquellen.** Haben Sie Ihren Wunschzettel zusammengestellt, sollten Sie die möglichen Datenquellen identifizieren. Gewisse Daten werden sich in zentral betriebenen IT-Anwendungen befinden (z.B. Buchhaltungslösung, → **ERP-System**, → **Server-Logs**, CRM), andere nur lokal geführt (Excel-Sheet der Personalabteilung). Meist wird es sich um elektronische Daten handeln, aber das muss nicht sein. Nicht in jedem Betrieb werden z.B. die Spesenbelege bei der Erfassung in der Buchhaltung gescannt, aber je nach Fall kann es wichtig sein, auf diese Belege zugreifen zu können.

3. **Lassen Sie die Daten sichern.** Wie schon bei unstrukturierten Daten gilt auch hier: Sichern Sie frühzeitig die möglicherweise benötigten Daten. Das wird bei bestimmten Systemen nicht nötig sein, weil ihre Daten ohnehin längerfristig aufbewahrt werden (z.B. ein Buchhaltungssystem), aber z.B. *Logs* von Servern werden regelmässig überschrieben bzw. gelöscht, so dass die Daten unter Umständen nur ein bis drei Monate zurückreichen. Besteht die Möglichkeit, dass ein Fehlverhalten weiter andauert, stellt sich sogar die Frage zusätzlicher Überwachungsmassnahmen (dazu → **ÜBERWACHUNGSMASSNAHMEN**).

Ist es wichtig, auf frühere *Logs* zuzugreifen, die aber mittlerweile gelöscht sind, so bietet es sich allenfalls an, auf **Backups** der betreffenden Systeme zurückzugreifen, sofern es solche überhaupt gibt und sie länger als die *Logs* selbst aufbewahrt werden. Allerdings ist das Extrahieren solcher Daten mit einem gewissen Aufwand verbunden.

4. **Beschaffen Sie die Daten, die sie auswerten möchten, in einem passenden Format.** Dies kann unter Umständen schwieriger sein, als es auf den ersten Blick erscheint. Denn nicht alle Anwendungen bieten Zugang zu den von ihnen benötigten Daten in der passenden Form. Geht es nur um einige wenige Daten, die Sie „von Hand" auswerten können, kann ein simpler Ausdruck oder eine PDF-Datei genügen. Soll aber eine grössere Menge an Daten ausgewertet werden, so brauchen Sie diese nicht als Ausdruck oder in einem Bericht, sondern in roher, maschinell verwertbarer Form, d.h. als strukturierte Daten. Wo eine Anwendung keine entsprechenden sog. Export-Funktionen mit allgemein gängigen Formaten bietet, muss unter Umständen ein Spezialist beigezogen werden, welcher – allenfalls in Absprache mit dem Hersteller des jeweiligen Systems – direkt auf die Datenbank oder Datendateien des Systems zugreift und die Daten extrahiert.

Zeitsynchronität

Logs eines Computersystems können interessante Datenquellen sein, weil sie Vorgänge systematisch protokollieren. Bevor auf die genauen Zeitstempel abgestellt wird, sollte aber geprüft werden, ob die Uhren der Server richtig – und bei Abgleichen mehrerer *Logs* – synchron laufen. Auch die Zeitzone ist zu berücksichtigen.

5. **Verstehen Sie, was die Daten bedeuten und wie sie zusammenhängen.** Lassen Sie sich von den Spezialisten sagen, welche Daten in welcher Form vorliegen und was die Daten bedeuten (z.B. welche Informationen sich aus dem gesicherten Logbuch eines Druckers entnehmen lassen). Allenfalls werden Sie sich auch von den Personen, die im Unternehmen die jeweilige Anwendung normalerweise benutzen, deren Funktionsweise und Logik erklären lassen müssen, damit Sie die gewonnenen Daten richtig interpretieren können. Dies kann allerdings eine grosse Herausforderung sein, da Daten oft nur im Zusammenspiel mit der Applikationslogik der betreffenden IT-Lösung einen Sinn ergeben und interpretierbar sind. Sollen Daten mehrerer Systeme abgeglichen werden, sollten Sie prüfen, über welche Referenzfelder (z.B. eine Bestell-Nummer) eine Verknüpfung der Datensätze möglich ist.

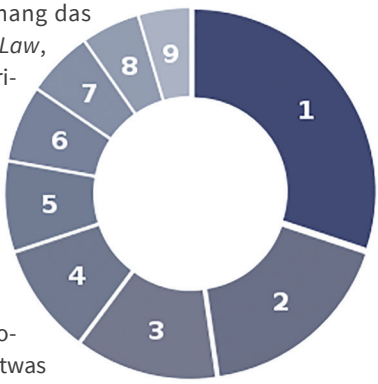
Interpretieren Sie Daten **systemübergreifend**. Versuchen Sie z.B. herauszufinden, wer Aktivitäten in einem System mit Gruppen-Account vorgenommen hat. D.h. dort, wo personenbezogene *Logs* fehlen, kann es helfen, die *Logs* anderer Systeme zu analysieren, in denen mit persönlichen Konten gearbeitet wird. Die dortige Aktivität einer bestimmten Person schliesst unter Umständen die gleichzeitige Aktivität im Gruppen-Account aus. Das andere System verschafft ihr also dank der übergreifenden Betrachtung ein „Alibi". Umgekehrt können parallele Nutzungen in zwei Anwendungen auf demselben System „*Copy+Paste*"-Kopiervorgänge von einem System ins andere indizieren. Ebenso können automatische Aktivitäten von Computersystemen (z.B. bei eingeloggtem, aber nicht anwesenden Benutzern) zu falschen Schlüssen führen.

6. **Definieren Sie, wonach in diesen Daten gesucht werden soll.** Sie können Ihre Daten nicht einfach in ein Computerprogramm „füttern" und es bitten nach Compliance-Verstössen zu suchen. Es gibt zu bestimmten Themen Software, die in strukturierten Daten nach typischen Warnhinweisen für Delikte sucht (z.B. Ausreisser bei den Vertriebspartnern gewährten Rabatten als Hinweis auf Korruption); diese dienen aber primär der frühzeitigen Erkennung. In einer internen Untersuchung liegen normalerweise bereits konkrete Hinweise auf ein mögliches Fehlverhalten vor. Bieten diese Anhaltspunkte für eine bestimmte deliktische Vorgehensweise? Wird eine Untersuchung z.B. wegen einer verdächtigen Zahlung an eine Privatperson ausgelöst und wird diese Zahlung danach mit einer Gutschrift an einen Kunden begründet, so macht es Sinn die Gutschriften an diesen Kunden zu analysieren. Zeigt sich dann, dass es zu fast jeder Bestellung sogleich eine Gutschrift gibt, lohnt es sich, nach anderen Kunden mit demselben Muster zu suchen. Kann auf diese Weise die Zahl der verdächtigen Transaktionen vervielfacht werden, steigt auch die Chance, dass anhand anderer Quellen (Belege, E-Mails, etc.) mehr über die Hintergründe ermittelt werden kann.

Visualisieren

Falls Sie nicht wirklich wissen, wonach Sie suchen, dann versuchen Sie es mit verschiedenen Visualisierungen der Daten. So fallen Ihnen möglicherweise Vorgänge, Beziehungen und andere Aspekte auf, die Ihnen sonst entgangen wären.

Das Suchen nach Unregelmässigkeiten in strukturierten Daten setzt erstens ein **Verständnis für die Machenschaften** voraus, um die es mutmasslich geht. Wer einen mutmasslichen Betrug aufdecken möchte, muss eine Vorstellung darüber haben, wie Betrüger vorgehen – auch um ihre Spuren zu verdecken. Stehen Finanzdelikte zur Diskussion, kann es daher sinnvoll sein, einen Experten hierfür beizuziehen. Zweitens muss derjenige, der eine Anomalie finden will, zunächst **verstehen, was normal ist**. Wer das nicht gut genug kennt und auf seine Datenbasis anwenden kann, findet zu viele → **false positives**, also vermeintliche Hinweise auf ein Fehlverhalten, die gar keine sind. Je nach Untersuchung kann diese Frage allerdings nur mit den Personen wirklich geklärt werden, welche die Untersuchung betrifft – eine Herausforderung.



Kennen sollten Sie in diesem Zusammenhang das **Benfordsche Gesetz** (*Newcomb-Benford's Law*, NBL), welches besagt, dass in einem empirischen, nicht manipulierten Satz von Zahlen tiefe Anfangsziffern häufiger vorkommen als hohe. Dabei kommen mit „1" beginnende Zahlen beispielsweise im Schnitt 6.6 Mal so häufig vor (30.1%) wie Zahlen, die mit einer „9" beginnen (4.6%). Erstaunlich viele numerische Datensätze folgen dieser Regel, egal ob Geldbeträge, Lagerwerte, Transaktionen, Flächen, Einwohnerzahlen oder sonst etwas gezählt wird. Das liegt vereinfacht gesagt daran, dass beim Zählen immer mit 1 begonnen werden muss, bevor 2, 3 oder 4 gezählt werden kann, und 10 gezählt werden muss, bevor 20, 30 oder 40 gezählt werden kann. Die Regel wird heute benutzt, um Unregelmässigkeiten in Zahlenbeständen aufzufinden, etwa wenn Bilanzfälschung, Betrug, Marktmanipulationen oder ganz generell gefälschte Daten zur Diskussion stehen – auch in der Wissenschaft. Die Aufdeckung der Bilanzmanipulationen bei Enron und Worldcom wird mitunter dem Einsatz von Methoden auf Basis des *Benfordschen Gesetzes* zugeschrieben. Wie Sie Zahlensätze mit Excel selbst nach dieser Regel überprüfen können: → **Q29**.

7. **Beauftragen Sie einen Experten mit der Umsetzung.** Ist klar, nach welchen Mustern Sie suchen, werden Sie häufig einen Spezialisten damit beauftragen müssen, die verfügbaren Daten entsprechend auszuwerten und in geeigneter Form darzustellen. Auch hierzu gibt es verschiedene Werkzeuge und Hilfsmittel. Meist ist hier eine gewisse Handarbeit erforderlich, z.B. um die aus den verschiedenen Datenquellen extrahierten Rohdaten zu verknüpfen und so darzustellen, dass sie von einem Menschen les- und interpretierbar sind.

8. **Bleiben Sie ergebnisoffen.** Datenanalysen können Ihnen erfahrungsgemäss nur (weitere) Hinweise auf ein Fehlverhalten liefern oder auf andere Weise Indizien zum Sachverhalt beitragen. Die (Hinter-)Gründe bestimmter Transaktionen oder anderer Sachverhalte, die sich in den Protokollen, Belegen oder sonstigen strukturierten Daten finden, erklären sie normalerweise nicht. So kann sich eine verdächtige Zahlung an eine Privatperson, die auf den ersten Blick als Korruptionsfall erscheint, bei näherer Untersuchung als mutmassliches Fiskaldelikt entpuppen, weil die Zahlung mit Wissen und Willen aller betroffenen Gesellschaften erfolgt ist. Darum kann auch die Analyse strukturierter Daten nur ein Teil des Puzzles liefern.

Do's	Don'ts
• Anders als im Dokumenten-Review gilt hier das Motto: Lieber mehr Daten als weniger. • Nicht jede technisch mögliche Auswertung von Daten über Mitarbeiter ist auch erlaubt – beachten Sie den Datenschutz. • Protokollieren Sie die Beschaffung der Daten, damit Sie später beweisen können, wie Sie an diese gelangt sind. • Denken Sie nicht nur an die eigenen Systeme, wenn Sie nach möglichen Datenquellen suchen. Bei der Analyse von Beziehungen können z.B. Daten aus Social-Media-Netzwerken weiterhelfen. Es gibt hierzu immer mehr *Tools*, die beim Sammeln solcher Daten helfen. • Lernen Sie mit Excel umzugehen. Strukturierte Daten lassen sich oft einfach in dieses Format überführen. So können Sie selbst damit „spielen" und können Betrachtungsweisen aufbauen, an die Sie zunächst gar nicht gedacht haben.	• Seien Sie nicht zu genau. Wenn es um die Erkennung von Mustern in strukturierten Daten geht, brauchen Sie „*fuzzy logic*", also eine gewisse Unschärfe. • Lassen Sie sich vom Datenschutz nicht abschrecken – es geht mehr, als viele glauben.

Wann Sie externe Unterstützung beiziehen sollten

- Wenn Sie **nicht wissen, wonach Sie suchen** sollen.
- Wenn Sie nicht wissen, wie Sie **an die von Ihnen gewünschten Daten gelangen** können oder, ob es diese überhaupt gibt.
- Wenn Sie nicht wissen oder sicher sind, ob Sie die Daten überhaupt **legal auswerten dürfen** und wie.
- Wenn die Daten sich nicht ohne Weiteres aus dem System **auslesen** lassen und daher Spezialwissen und Kontakte mit dem Hersteller erforderlich sind.
- Wenn es wichtig ist, dass der **Beweiswert der Daten und deren Analyse** gewahrt bleibt.
- Wenn es **mehr als nur Excel** zum Auswerten der Daten braucht und Sie intern keine Data-Analytics-Spezialisten haben.
- Wenn Sie **interne Spezialisten** aus taktischen Gründen nicht fragen wollen.
- Wenn Sie sich sonst **unsicher** fühlen oder Ihnen die **Ideen fehlen**.

Häufige Fragen und Antworten

Q27. Dürfen wir die Verhaltensdaten unserer Mitarbeiter auswerten, um mögliches Fehlverhalten frühzeitig zu erkennen?

A: Verhaltensdaten der Mitarbeiter dürfen bearbeitet bzw. ausgewertet werden, wenn diese **rechtmässig erhoben** wurden. Das Arbeitsrecht gibt die Grenzen der Überwachung von Mitarbeitern vor. Grundsätzlich dürfen Überwachungs- und Kontrollsysteme, die das Verhalten von Mitarbeitern am Arbeitsplatz überwachen nicht verwendet werden (Art. 26 Abs. 1 → **ArGV 3**). Überwachungs- und Kontrollsysteme dürfen nur eingesetzt werden, wenn sie anderen Zwecken dienen z.B. der Leistungs- bzw. Sicherheitsüberwachung und nicht permanent eingesetzt werden, d.h. eine **zeitliche und sachliche Begrenzung** erfolgt. Erfolgte die Erhebung der Daten bereits unzulässig, z.B. durch den mehrmonatigen Einsatz einer Spyware, können solche Daten grundsätzlich nicht rechtmässig bearbeitet werden (ob sie ein Gericht trotzdem als Beweis zulässt, ist eine andere Frage).

Begrenzt wird die Erhebung und Bearbeitung ebenfalls durch den Datenschutz. Aus dem datenschutzrechtlichen Grundprinzip der **Transparenz** ergibt sich, dass die betroffenen Mitarbeiter mittels Datenschutzerklärung oder internen Personalreglementen **vorgängig** allgemein über die Möglichkeit der Erhebung solcher Daten, die Art der Datenerhebung und den Bearbeitungszweck **informiert** werden müssen. Die Erhebung der Daten und deren spätere Bearbeitung müssen durch das **Interesse des**

Arbeitgebers gerechtfertigt sein. Die Verhinderung illegaler Aktivitäten stellt dabei einen legitimen Rechtfertigungsgrund dar.

Die eigentliche Auswertung hat im Rahmen des angegebenen Zweckes zu erfolgen, d.h. die Daten dürfen nur für den Zweck verwendet werden, der den Mitarbeitern mitgeteilt wurde. Es dürfen ferner nur Daten bearbeitet werden, die einen **Arbeitsplatzbezug** (vgl. Art. 328b OR) aufweisen. Es sind die Grundsätze der Datenbearbeitung einzuhalten, d.h. die Auswertung hat nach **Treu und Glauben** zu erfolgen und **verhältnismässig** zu sein.

Zur Überwachung von Mitarbeitern generell → **ÜBERWACHUNGSMASSNAHMEN**, mit weiteren Fallbeispielen und Hinweisen zur Gerichtspraxis.

> **Literatur:**
>
> Götz, Staehelin Claudia/Bertschi, Manuel: Grenzen der Mitarbeiterüberwachung, Recht relevant. für Verwaltungsräte (RR-VR) 3/2020, 5 ff.
>
> Wantz, Simona/Licci, Sara: Arbeitsvertragliche Rechte und Pflichten bei internen Untersuchungen, Jusletter vom 18. Februar 2019, Rz. 1 ff.

Q28. Wann dürfen wir auf die Positionsdaten von Mitarbeiter zugreifen?

A: Gleiches wie für Verhaltensdaten von Mitarbeitern (dazu → **Q27**) gilt für deren Positionsdaten. Diese müssen in den Grenzen des Datenschutzrechts und des Arbeitsrechts rechtmässig erhoben worden sein, damit der Arbeitgeber auf diese zugreifen kann. Die Ermittlung von Positionsdaten des Mitarbeiters bedarf einer **Rechtfertigung** durch den Arbeitgeber. Unerlaubt ist die ständige Echtzeitüberwachung per GPS. Der Arbeitgeber darf aber zum Beispiel Geschäftsfahrzeuge lokalisieren, um festzustellen, wie lange Einsätze des Mitarbeiters beim Kunden dauern. Wiederum hat die Bearbeitung nach den datenschutzrechtlichen Grundsätzen zu erfolgen.

Zur Überwachung von Mitarbeitern generell → **ÜBERWACHUNGSMASSNAHMEN**, mit weiteren Fallbeispielen und Hinweisen zur Gerichtspraxis.

> **Literatur:**
>
> Meier-Gubser, Stefanie: Mitarbeiterüberwachung: Rechte, Pflichten und Verbote, Der Treuhandexperte (TREX), 286 ff.
>
> Wantz, Simona/Licci, Sara: Arbeitsvertragliche Rechte und Pflichten bei internen Untersuchungen, Jusletter vom 18. Februar 2019, Rz. 1 ff.

Q29. Kann ich auch selbst einen Datensatz nach dem *Benfordschen Gesetz* analysieren?

A: Ja, das ist mit Excel ohne weiteres möglich. Sie können mit der Regel grundsätzlich jeden Satz an Zahlen analysieren, der **natürlich vorkommende Werte** aufweisen soll-

te, also beispielsweise die Buchungen aus der Finanzbuchhaltung, geschäftliche Transaktionen, bezahlte Preise, Spesenabrechnungen, Portfolios, Einträge in *Time-Sheets*.

Wichtig ist, dass die Regel nur dort gültig ist, wo im empirischen Datensatz grundsätzlich **jeder Anfangswert von 1 bis 9 vorkommen kann**. Wollen Sie die für ein bestimmtes Produkt bezahlten Preise analysieren, diese aber aufgrund anderer Umstände zwischen 50 und 80 liegen müssen, kann die Regel nicht funktionieren.

Sie sollten ferner darauf achten, dass Sie **möglichst viele Zahlen** haben. Je mehr, desto besser. Die Regel kann bereits bei Datensätzen mit 50 bis 100 Werten funktionieren bzw. relevante Abweichungen zeigen, aber besser sind Datensätze mit 500 oder mehr Werten.

Bedenken Sie zudem, dass eine Benford-Analyse **kein Beweis** für Fälschungen oder Manipulationen ist, sondern lediglich ein Hinweis.

Für die Auswertung benötigen Sie Excel:

- Fügen Sie in einer ersten Spalte die zu analysierenden Werte als Zahlen ein (z.B. Spalte B).
- Extrahieren Sie in der Spalte rechts davon (also z.B. Spalte C) die erste Ziffer jedes Werts mit der Funktion „=LINKS([Zelle];1)“.
- Jetzt müssen Sie Excel das Vorkommen der Ziffern von 1 bis 9 zählen lassen. Fügen Sie hierzu in einem separaten Bereich der Tabelle (z.B. in Spalte E) die Werte 1 bis 9 von oben nach unten auf (d.h. jeder Wert auf einer Zeile, also E2, E3, E4 etc.). Rechts neben der Zahl 1 (also im Feld F2) fügen Sie die Funktion „=ZÄHLENWENN ([Quellwerte];[Zelle mit der Zahl 1])“ ein. Die Referenz „[Quellwerte]“ bezieht sich auf die Spalte mit den Anfangsziffern, also z.B. $C$2:$C$2397, falls sich Ihre Zahlenwerte in Zelle C2 bis C2397 befinden. Verwenden Sie absolute Bezüge, damit sie sich beim Kopieren nicht verändern („$“ einfügen). Nun kopieren Sie die so erstellte „ZÄHLENWENN“-Funktion in derselben Spalte neben jeden Wert von 2 bis 9. Die Funktion Excel wird Ihnen in F2-F10 anzeigen, wie häufig jeder Anfangswert vorkommt.
- Zählen Sie alle Vorkommen mit der SUMME-Funktion zusammen und benutzen Sie diese, um in einer weiteren Spalte (E2-E10) den prozentualen Anteil zu berechnen („=D2/$D$11“, formatiert als Prozentwert, in der Annahme, dass D2 das Vorkommen der Zahl „1“ zeigt und D11 die Gesamtsumme enthält).
- Vergleichen Sie die Prozentwerte mit den Benford-Werten[20]. Eine grafische Auswertung kann Abweichungen noch deutlicher hervorheben.

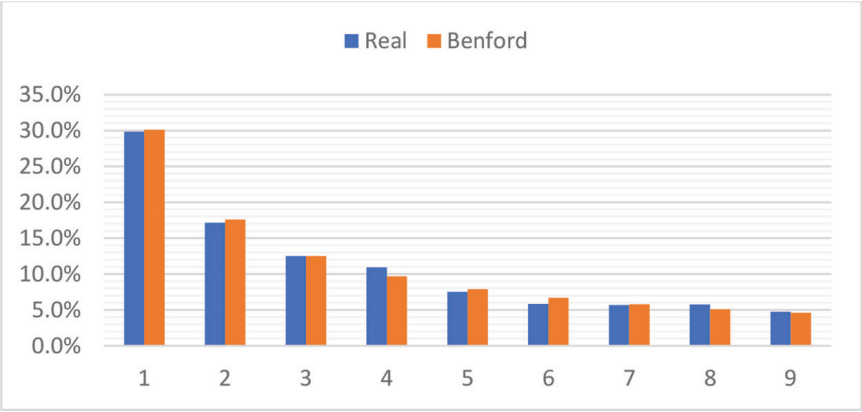
20 Nach Benford werden in einem tatsächlich empirischen, also nicht manipulierten oder auf Manipulationen beruhenden Datensatz 30.1% der Zahlen eine führende Ziffer 1 aufweisen, 17.6% eine 2, 12.5% eine 3, 9.7% eine 4, 7.9% eine 5, 6.7% eine 6, 5.8% eine 7, 5.1% eine 8 und 4.6% eine 9.

Führen Sie – zur Übung – die soeben beschriebene Analyse anhand von Musterdaten durch. Sie können allgemein verfügbare Daten verwenden, z.B. die Einwohnerzahlen aller Schweizer Gemeinden aus dem Jahr 2012.[21] Der nachfolgende Screenshot enthält das Ergebnis einer Excel-Auswertung dieser Zahlen. Auch hier zeigt sich, dass die reale Verteilung der Anfangswerte erstaunlich nahe an den Benford-Werten liegt:

D2 =ZÄHLENWENN($B$2:$B$2397;C2)

	A	B	C	D	E	F
1	Einwohner	Erstwert	Wert	Vorkommen	Real	Benford
2	1955	1	1	715	29.8%	30.1%
3	11276	1	2	411	17.2%	17.6%
4	5205	5	3	300	12.5%	12.5%
5	3376	3	4	262	10.9%	9.7%
6	3511	3	5	180	7.5%	7.9%
7	922	9	6	140	5.8%	6.7%
8	1982	1	7	136	5.7%	5.8%
9	641	6	8	138	5.8%	5.1%
10	4420	4	9	114	4.8%	4.6%
11	4833	4		2396		
12	2480	2				

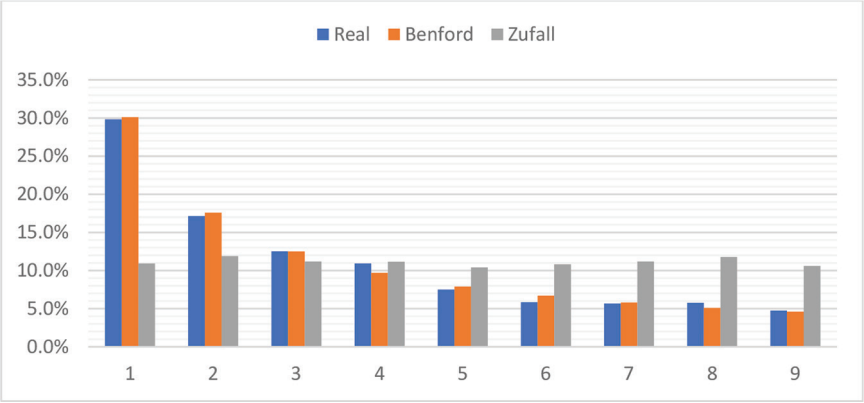
Grafisch dargestellt ist die Übereinstimmung noch deutlich sichtbarer:



Sie können auf dieselbe Weise beispielsweise auch die Transaktionen einer Buchhaltung, einer Verkaufsorganisation oder von Spesenabrechnungen analysieren. Dabei werden Sie vermutlich ein ähnliches Muster wie im obigen Beispiel entdecken. Ba-

21 Zu beziehen via opendata.swiss unter https://bit.ly/2QnPrej.

sieren die Zahlen hingegen auf **erfundenen oder durch Manipulationen erzeugten Werten**, wird die Darstellung womöglich eine andere sein. Wenn im obigen Beispiel statt der echten Bevölkerungsdaten der Gemeinden reine Zufallszahlen („=ZUFALLS-ZAHL()*10000“) verwendet werden, ergibt die Auszählung ein ganz anderes Ergebnis:



Der Balken rechts (grau) ist das Vorkommen der Anfangswerte und bewegt sich bei den Zufallszahlen in diesem Beispiel immer zwischen 10.4% und 11.9%. Dies ist ein starkes Indiz dafür, dass diese Zahlenreihe nicht „natürlichen“ Ursprungs ist, sondern von einem Computer generiert worden ist.

Erfindet jemand hingegen Nummern **von Hand**, so ist das Bild weniger gleichmässig, wobei das Ergebnis davon abhängt, ob er die Zahlenreihe über den Buchstaben oder den Zahlenblock rechts benutzt:

- Benutzt er die Zahlenreihe über den Buchstaben, so werden erfahrungsgemäss die Zahlen 4, 5, 6 und 7 häufiger vorkommen als die Zahlen am Rand der Reihe wie 1, 2, 8 und 9, weil diese mit dem kleinen Finger angeschlagen werden müssen. Dies wird sich auch in der Auswertung der Anfangswerte darstellen, nämlich in Form einer Glockenkurve.
- Benutzt er den Zahlenblock, sind verschiedene Muster zu erwarten, je nachdem, wie der Zahlenblock benutzt wird. Wer mit dem Zeigefinger und Mittelfinger die scheinbar zufälligen Zahlen eintippt, wird mit grösserer Wahrscheinlichkeit die Zahlen im linken Teil verwenden, also die 1, 4, 7, 8, 5 und 2, während die 9, 6 und 3 weniger häufiger vorkommen werden. Es kann aber auch sein, dass die Person sich auf andere Bereiche des Blocks fokussiert.

So oder so ist es jedoch höchst unwahrscheinlich, dass aus einer solchen Zahlenübung Zahlen resultieren, die tatsächlich eine Benford-Kurve ergeben. Das gilt auch dann, wenn sich jemand die Zahlen einfach ausdenkt. Hier zeigt die Erfahrung ebenfalls,

dass bestimmte Zahlen (aber nicht nur eine) besonders häufig benutzt werden, was wiederum zu einer völlig anderen Verteilung als bei Benford resultiert.

Beispiel eines Anwendungsfalls: Ein Mitarbeiter veruntreut Gelder einer Firma. Er weiss, dass Beträge ab CHF 10‘000 einer weiteren Unterschrift bedürfen. Um seine Machenschaft zu vertuschen, stückelt er die Deliktsbeträge daher so, dass sie jeweils deutlich unter CHF 10‘000 liegen und daher nicht auffallen. In der Auswertung aller Transaktionen tauchen Beträge in der Höhe von CHF 6‘xxx, 7‘xxx oder 8‘xxx übermässig häufig auf.

So faszinierend Benford-Analysen sein können, so ist doch zu beachten, dass sie **lediglich Hinweise** auf Unregelmässigkeiten liefern können. Auch ist zu prüfen, ob die Benford-Regel im vorliegenden Fall tatsächlich ihre Gültigkeit haben kann, etwa ob es andere, legitime Gründe geben kann, dass bestimmte Anfangswerte besonders häufig vorkommen können. Die gefundene Wertverteilung sollte mit der Wertverteilung bei Zahlenwerten verglichen werden, die bekanntermassen manipulationsfrei sind. Zahlen unterschiedlicher Perioden sollten ebenfalls verglichen werden, ebenso unterschiedliche Typen.

Hilfreich kann es schliesslich auch sein, Zahlen nicht direkt zu analysieren, sondern sie in ein **Verhältnis zu setzen**, z.B. Umsatz pro Tag statt Umsatz. Dies kann zu völlig anderen Einsichten führen.

Literatur:

Jackmuth, Hans-Willi/de Lamboy, Christian/Zawilla, Peter: Fraud Management in Kreditinstituten, Praktiken, Verhinderung, Aufdeckung, Frankfurt a.M. 2013

Gedanken zum Thema.

In den öffentlichen Diskussionen liegt der Fokus bei diesem Thema vor allem auf den grossen grundsätzlichen Fragen wie etwa der Gewähr der Unabhängigkeit einer internen Untersuchung durch passende Zuständigkeitsregeln in der Unternehmensführung. Doch im Alltag stellen uns vor allem die vielen vermeintlichen Kleinigkeiten vor Herausforderungen – wie etwa, einen Fabrikmitarbeiter in einem Land zu befragen, der kein Wort Englisch, Deutsch oder Französisch spricht und auch die Thematik nicht versteht, komplexe Datenschutzfragen, wenn verschiedene Nationalitäten in einem Land arbeiten und die Rechtsordnung des Landes der Niederlassung und die des Heimatlandes eines Untersuchungsteilnehmers beachtet werden müssen. Ausserdem ist es wichtig sich klarzumachen, dass man lokale Untersuchungen nicht von der Schweiz aus durchführen kann, sondern sich auf unbelastete Kontakte im lokalen Management verlassen können muss.

Annette Schüller
Head of Group Ethics & Compliance and ERM Givaudan

6. Befragungen

Kurz gesagt

- Befragen sollten Sie erst, wenn Sie die Beweismittel gesichtet haben und gut vorbereitet sind, so dass Sie die Personen mit den bisherigen Erkenntnissen konfrontieren können. Seien Sie aber ergebnisoffen – die Befragung wird Ihnen helfen, alles richtig einzuordnen.
- Arbeitnehmer sind verpflichtet, über geschäftliche Belange Auskunft zu erteilen, allerdings müssen sie korrekt aufgeklärt werden; beschuldigte Personen müssen sogar die Gelegenheit erhalten, zu den Vorwürfen Stellung zu nehmen.
- Befragungen sollten von unbeteiligten Personen vorgenommen werden und erfordern einiges Fingerspitzengefühl und Erfahrung.

Worum es geht

Befragungen spielen vor allem in internen Untersuchungen eine Rolle. Sie finden normalerweise dann statt, wenn die ersten Unterlagen gesichtet worden sind (→ **DOKUMENTEN-REVIEWS**) und ein erster Eindruck zum Sachverhalt besteht. Dieser Eindruck kann falsch oder unvollständig sein. Das erste Ziel einer Befragung ist es daher, den Sachverhalt weiter zu erhellen, die bestehenden Beweismittel einzuordnen und die Zusammenhänge besser zu verstehen. Das zweite Ziel einer Befragung ist es, den beteiligten Personen die Gelegenheit zur Stellungnahme geben zu können, insbesondere wenn ein Fehlverhalten im Raum steht. Ein solches „rechtliches Gehör" ist auch aus arbeitsrechtlicher Sicht wichtig. Auch wenn eine Befragung nur für die Zwecke einer internen Untersuchung durchgeführt wird, besteht immer auch die Möglichkeit, dass die Aussagen für zivil- und strafrechtliche Verfahren verwendet werden.

Worauf zu achten ist

- Befragungen setzen die Kenntnis der Sachlage voraus; daher sollten sie nach Möglichkeit erst nach einer Sichtung der vorliegenden Beweismittel stattfinden.
- Für die befragte Person kann eine Befragung hohen Stress erzeugen, selbst wenn ihr nichts vorgeworfen wird. Dies ist zu berücksichtigen.
- Personen sollten grundsätzlich einzeln und ohne Publikum befragt werden; oft ist es sinnvoller, dass kein Unternehmensvertreter dabei ist und die Zahl der Anwesenden tief gehalten wird.
- Befragungen sind zwar (mit Ausnahmen) zu protokollieren, aber nicht notwendigerweise aufzuzeichnen. Auch ein Wortprotokoll ist in der Regel nicht nötig.

- Die befragte Person muss über ihre Rechte und Pflichten vorgängig aufgeklärt werden; wird einer Person ein Fehlverhalten vorgeworfen, ist zu prüfen, ob ihr vorgängig Unterlagen zur Verfügung gestellt werden – bei der ersten Befragung ist dies allerdings nicht erforderlich.
- Arbeitnehmer sind dem Arbeitgeber zur Auskunft über geschäftliche Belange verpflichtet. Ob ein Verbot zum Zwang der Selbstbelastung besteht, ist umstritten (dazu → **Q37**). Ebenfalls umstritten ist, ob eine Person sich von einem Anwalt begleiten lassen darf. Steht eine Straftat im Raum kann dies jedoch angezeigt sein (dazu → **Q32**).

Eine erfolgreiche Befragung im Rahmen einer internen Untersuchung erfordert Erfahrung und psychologisches Geschick. Das gilt insbesondere dann, wenn die befragte Person selbst der Aufklärung des Sachverhalts entgegenstehende Interessen hat, sei es, weil sie eines Fehlverhaltens verdächtigt wird oder andere Personen nicht anschwärzen will. Solche Befragungen sollten von entsprechend erfahrenen Personen vorgenommen werden. Mehr zur Befragungstechnik und zu den Menschen, um die es geht: → **Q40**, → **Q41**.

Wie vorzugehen ist

1. **Erstellen Sie eine Liste derjenigen Personen, die Sie befragen wollen.** Sortieren Sie die Liste nach taktischen Gesichtspunkten: Wessen Aussage möchten Sie ggf. bei späteren Befragungen nutzen können? In der Regel wird mit den Personen begonnen, die entsprechende Hinweise auf ein Fehlverhalten geliefert haben – sofern sie überhaupt befragt werden können. In der Folge werden typischerweise Personen befragt, die selbst nicht im Fokus stehen, aber möglicherweise wichtige Hinweise oder Kontext liefern können. In einer internen Untersuchung geht es nicht immer nur um das Fehlverhalten selbst, sondern manchmal auch nur darum, ein Verständnis für Abläufe, Strukturen oder Systeme zu erlangen. Die beschuldigte Person wird aus taktischen Gründen tendenziell erst zum Schluss befragt, wenn sich bereits ein gutes Bild des Sachverhalts ergeben hat.

Hilfsmittel

- Text zur Aufklärung
- Fragen nach Themen vorbereiten, ergänzt um die wichtigsten Fakten
- Beweismittel, welche den Befragten bei Bedarf vorgelegt werden können
- Gerät zur Aufzeichnung der Befragung mit einem oder mehreren Mikrofonen
- Person, die protokolliert

Es ist ohne Weiteres möglich, eine Person **mehrfach zu befragen**. Dies betrifft insbesondere die beschuldigte Person. Wiederholte Befragungen sind teilweise auch erforderlich, weil zwischenzeitlich erste Aussagen validiert werden müssen. Seien Sie sich allerdings bewusst, dass die Dynamik und das Aussageverhalten zwischen einer ersten und den weiteren Befragungen, insbesondere einer beschuldigten Person, sich massiv verändern kann. Eine erste Befragung kann bei einer solchen Person, gerade wenn sie unerfahren ist, massiven Stress auslösen und sie einschüchtern, während ihre Stimmung im Nachgang kippen kann. Der beschuldigten Person werden sehr viele Dinge durch den Kopf gehen und sie wird sich sehr genau überlegen, mit welcher Strategie und Einstellung sie in ein zweites Gespräch gehen wird. Darum ist es wichtig, alle relevanten Fragen grundsätzlich **bereits im ersten Gespräch** zu stellen, um auf eine erste Aussage zurückgreifen zu können, die mutmasslich weniger überlegt sein wird als die Antworten in späteren Befragungen.

2. **Legen Sie die Rolle der Personen fest.** Gewisse Personen, mit denen Sie sich unterhalten, haben mit dem Fall nicht wirklich etwas zu tun, sondern geben Ihnen lediglich sachliche Auskünfte, etwa wie bestimmte Abläufe organisiert sind oder wie ein System funktioniert. Sie zu befragen ist unproblematisch und kann auch ohne besondere Aufklärung erfolgen; sie brauchen nicht einmal darauf hingewiesen zu werden, dass es sich um eine interne Untersuchung handelt. So kann der Kreis der wissenden Personen klein gehalten werden. Andere Personen sind möglicherweise über das Fehlverhalten informiert, haben daran bewusst oder unbewusst mitgewirkt oder sind ihm zum Opfer gefallen. Hier sind genauere Abklärungen nötig. Ein Generalverdacht gegenüber jedem und jeder bringt Sie nicht weiter, aber ein gesundes Misstrauen ist sinnvoll: Selbst bei jemandem, der sich selbst kein Fehlverhalten vorwerfen lassen muss, können persönliche Interessen im Spiel sein, die das Aussageverhalten der Person beeinflussen. In jedem Betrieb gibt es Freundschaften, Feindseligkeiten, Loyalitäten, Schadenfreude und andere Erscheinungen, die einer fairen Aufklärung in der einen oder anderen Form im Wege stehen können.

3. **Beschaffen Sie sich Hintergrundinformationen über die zu befragenden Personen.** Sie müssen eine Vorstellung der Personen haben, denen Sie begegnen werden, damit Sie mit ihnen psychologisch richtig umgehen. Sie müssen auch ihre Funktion und Kompetenzen kennen, um ihre Antworten richtig einschätzen zu können (z.B. ob sie etwas kennen müsste). Allerdings sollten Sie sich auch bewusst sein, dass auch der „kleine“ Buchhalter womöglich Vorgänge wahrgenommen hat, die sich weit über ihm abgespielt haben.

> Hintergrundinformationen lassen sich nicht nur vorab beschaffen, sondern auch in den Befragungen selbst. So kann ein Interview eine gute Gelegenheit sein, Fragen über die Persönlichkeit anderer Personen zu stellen, wobei die Antworten zwar sehr subjektiv ausfallen können, aber trotzdem wichtige Hinweise liefern. Wenn mehrere, nicht involvierte Mitarbeiter die rechte Hand des Beschuldigten als „aufrechte, aber sehr loyale Person" beschreiben, hilft Ihnen dies, nicht nur die Glaubwürdigkeit dieser Person einzuschätzen, sondern sie auch richtig anzupacken, damit sie ihre Beobachtungen trotz der Loyalität gegenüber ihrem Vorgesetzten offenlegt.

4. **Legen Sie den Kreis der an der Befragung beteiligten Personen fest.** Befragungen sollten nicht alleine durchgeführt werden, sondern mindestens zu zweit. Das gilt auch für rein interne Befragungen. Während Sie sich als Fragesteller auf die Fragen konzentrieren und genau zuhören können, kümmert sich die zweite Person um das Protokoll (falls es ein solches gibt), kann bei Bedarf Ergänzungsfragen stellen oder Klarstellungen verlangen oder einschreiten. Sie kann bei Bedarf auch den Verlauf des Gesprächs bezeugen. Ob es bei einer Befragung durch Anwälte oder andere externe Personen sinnvoller ist, Vertreter des Unternehmens „dabei" zu haben oder nicht, muss im Einzelfall entschieden werden. Gewisse Personen werden eingeschüchtert sein, wenn sie sich allein von Anwälten befragen lassen müssen, ohne irgendjemanden vom Unternehmen an ihrer Seite zu haben. Andere werden erst in dieser Situation zu einer offenen Aussage bewegt werden können. Ist ein Unternehmensvertreter anwesend, dann sollte dies grundsätzlich nicht der direkte Vorgesetzte sein, und ebenso keine direkten Arbeitskollegen, sondern etwa ein Vertreter des Rechtsdiensts (der die Rechte des Befragten kennt) oder der Personalabteilung. Bedenken Sie auch, dass die Zahl der teilnehmenden Personen nicht zu gross sein sollte, da auch dies einschüchternd wirken kann. Einschüchterung ist üblicherweise keine sinnvolle Taktik, auch bei der beschuldigten Person nicht. Allerdings lässt sie sich in manchen Situationen nicht vermeiden: Die meisten Arbeitnehmer sind sich interne Untersuchungen und erst recht Befragungen nicht gewohnt. Ihre Befragung kann auch dann Angst und Stress auslösen, wenn sie umsichtig und freundlich durchgeführt wird. Zur Frage, ob die betroffenen Personen selbst einen Anwalt oder eine andere Person beiziehen müssen: → **Q32**.

> Eine **einfühlsame Gesprächsführung** kann entscheidend dazu beitragen, dass Angst und Stress in einer Befragung abgebaut werden können. Beginnen Sie nicht gleich mit Fragen zur Sache, sondern erlauben Sie dem Gegenüber, Sie im lockeren Gespräch etwas kennenzulernen. Das hilft auch Ihnen, Ihr Gegenüber besser einzuschätzen. Nutzen Sie dazu harmlose Fragen,

für deren Beantwortung die befragte Person sich auf für sie sicherem Terrain bewegen kann und mit Ihnen ein Gespräch entwickelt. Sie können dabei durchaus Persönliches von Ihnen selbst preisgeben, wenn Sie mögen. Dies trägt erfahrungsgemäss wesentlich dazu bei, ein Vertrauensverhältnis zur Person aufzubauen: Reden Sie offen mit der Person (oder hat sie diesen Eindruck), ist die Wahrscheinlich höher, dass auch sie mit Ihnen offen spricht.

5. **Wählen Sie den passenden Ort für die Befragungen.** Auch hier kann es taktisch einen Unterschied machen, ob in den bekannten Räumlichkeiten des Unternehmens oder im Sitzungszimmer einer der Person unbekannten Anwaltskanzlei befragt wird. Letzteres kann die Ernsthaftigkeit der Angelegenheit untermauern, aber auch einschüchternd wirken; ersteres kann psychologisch insbesondere bei der Befragung des höheren Managements sinnvoll oder sogar erforderlich sein. Eine Befragung am Arbeitsplatz der befragten Person kann sich zwar unter Umständen anbieten, doch empfiehlt sich eine solche normalerweise nicht: Es kann zu Störungen kommen und üblicherweise wird es dort auch an der nötigen Diskretion fehlen. Sie wollen normalerweise – auch zum Schutz der betroffenen Person – nicht, dass jeder die Befragung mitbekommt. Wer abseits seines Arbeitsplatzes befragt wird, nimmt sich normalerweise auch mehr Zeit und ist mehr bei der Sache.

6. **Entscheiden Sie sich, ob aufgezeichnet werden soll.** Eine Aufzeichnung ist nicht erforderlich, wenn es nur um die Feststellung des Sachverhalts geht und die konkrete Aussage nicht bewiesen werden soll (wobei dies auch mit entsprechenden Protokollen, Notizen und Zeugenaussagen möglich ist). Eine Aufzeichnung kann abschrecken, aber meist vergessen die Befragten rasch, dass sie mitläuft. Sie erfordert in jedem Falle die Einwilligung der betroffenen Person, die auch auf der Aufzeichnung zu hören sein sollte. Eine Aufzeichnung nimmt ein Gespräch in seinen Ausprägungen natürlich sehr viel präziser auf, als dies selbst ein Wortprotokoll tut (welches auch bei Vollständigkeit, den Tonfall, Pausen und weitere non-verbale Elemente nicht wiedergibt). Die nachträgliche Niederschrift einer Aufzeichnung ist allerdings vergleichsweise aufwändig. Häufig lohnt sich dies erfahrungsgemäss nicht. In komplexen Fällen und

Nur Notizen?

Ein Wortprotokoll ist in der Praxis meist nicht erforderlich; ausführliche Notizen genügen in der Regel. Gleichen Sie diese unter den Teilnehmern nach der Befragung rasch ab, solange die Erinnerungen noch frisch sind. In gewissen Fällen kann es angezeigt sein, (zumindest während des Gesprächs) gar keine Notizen zu machen, etwa weil die Person es wünscht oder die Info besonders sensibel ist.

bei langen Befragungen kann eine Aufzeichnung nicht nur zu Beweiszwecken sinnvoll sein, sondern als Gedankenstütze – insbesondere dann, wenn eine frühere Befragung im Hinblick auf neu gewonnene Erkenntnisse nochmals angehört werden kann, weil gewisse frühere Aussagen in einem anderen Licht erscheinen mögen. Das kann insbesondere dann relevant sein, wenn an sich nur mit Notizen gearbeitet wird, die Aufzeichnung jedoch als *„Backup"* dient, sollten sich die Notizen als nicht ausreichend erweisen oder zunächst als irrelevant betrachtete (und daher nicht notierte) Aussagen nachträglich mehr Gewicht erhalten.

Eine Aufzeichnung kann auch die befragte Person schützen. Überlegen Sie sich vorher, ob und wie sie die Aufzeichnung bzw. eine Abschrift davon herausgeben wollen oder müssen, so insbesondere im Falle eines späteren zivil- oder strafrechtlichen Verfahrens. Sowohl die Gegenseite wie auch die Strafverfolgungsbehörden werden daran möglicherweise ein Interesse haben.

7. **Laden Sie die Personen zur Befragung ein.** Ein Arbeitnehmer muss dem Arbeitgeber über geschäftliche Belange Auskunft geben. Er kann ihn in diesem Umfang zur Teilnahme an einer Befragung verpflichten (Treuepflicht) und disziplinarisch sanktionieren, wenn der Arbeitnehmer sich weigert (→ **Q30**). In der Einladung sollte insbesondere dem eines Fehlverhaltens verdächtigten Mitarbeiter grundsätzlich angekündigt werden, worum es geht (grobe Themenangabe) – ausser, dies könnte die Untersuchung vereiteln. Weisen Sie die Person zur Vertraulichkeit an, auch wenn Sie diese nicht erwarten sollten (→ **Q35**). Sie müssen (auch) der beschuldigten Person jedenfalls vor der ersten Befragung keinen Einblick in die Unterlagen gewähren (→ **Q34**). Will ein Mitarbeiter aus gesundheitlichen oder anderen Gründen nicht vor Ort erscheinen, ist eine Befragung via Videokonferenz möglich (→ **Q39**). Zur Frage, was eine Befragung bei einer Person auslösen kann: → **Q41**.

Unter Umständen kann es sinnvoll sein, die Person zu bitten, aus ihrer Sicht relevante Dokumente zur Befragung mitzubringen (z.B. die eigene Agenda) oder sich vorgängig bereits Gedanken zu bestimmten Fragen zu machen, z.B. wenn Sie sich gewisse Abläufe erklären lassen wollen oder wenn Sie Auskünfte zu gewissen Geschehnissen haben wollen, die so weit zurückliegen, dass sich die Person möglicherweise nicht auf Anhieb erinnern wird. Muss sich die Person auf die Befragung nicht vorbereiten, wird Sie es Ihnen danken, wenn Sie ihr dies auch sagen.

8. **Bereiten Sie Ihre Befragung sorgfältig vor.** Sie sollten bezüglich der bisherigen Erkenntnisse sattelfest sein, die Akten und weiteren Fakten gut kennen. Sie müssen in der Lage sein, auf aktenwidrige Aussagen sofort reagieren zu können

und den Befragten nötigenfalls auch sofort mit den betreffenden Unterlagen zu konfrontieren (das gebietet auch die Fairness ihm gegenüber, da falsche Aussagen nicht zwangsläufig bösgläubig sind – der Mensch ist vergesslich). Daher ist es auch sinnvoll, Befragungen erst nach einer ersten Sichtung der Beweismittel durchzuführen. Es hat sich bewährt, eine Befragung zu strukturieren. Überlegen Sie sich hierzu eine Befragungsstrategie (z.B. nach Themenblöcken, nach Ereignissen, nach Dokumenten, vorwärts, rückwärts, durcheinander). Die Strukturierung hilft Ihnen auch, nichts zu vergessen.

Immer im Fluss

Eine gute Befragung ist nicht ein Spiel von Fragen und Antworten, sondern ein Gespräch, in welchem vor allem der Befragte zu Wort kommt. Es liegt an Ihnen, die dazu nötige vertrauensvolle, aber auch "es kommt alles ans Licht"-Atmosphäre zu schaffen und so sattelfest zu sein, dass es zu keinen Unterbrüchen kommt. Sind Sie nicht sattelfest oder sonst unsicher, erhöht sich auch das Risiko, dass Sie angelogen werden.

Ob Sie sich fertige Fragen notieren oder lediglich Punkte, die Sie geklärt haben möchten, hängt von Ihrer Erfahrung ab. Selbst wenn Sie sich Fragen notieren, sollten Sie nicht sklavisch abarbeiten, sondern bereit sein, auf die befragte Person und ihre Aussagen einzugehen. Sie müssen nicht jedes von ihr gelieferte Thema aufgreifen, aber seien Sie auf unerwartete Wendungen vorbereitet und nutzen Sie Gelegenheiten, die sich ihnen bieten. Das kann bedeuten, dass Sie Fragen umstellen oder spontan ergänzende Fragen formulieren müssen. Sie werden merken, dass Ihnen manche Fragen erst während dem Gespräch einfallen. Auf all diese Dinge müssen Sie eingehen können. Experimentieren Sie mit offenen und geschlossenen Fragen – beide haben ihren legitimen Zweck. In gewissen Fällen lohnt es sich, die Person erzählen zu lassen, in anderen ist eher ein Kreuzverhör angezeigt. Auch der persönliche Umgang mit der Person will gelernt sein – erfolgreiche Befrager können sich sehr gut in ihr Gegenüber hineinversetzen (Empathie) und wissen, wie sie Vertrauen gewinnen und auch ohne Aggression psychologisch die Führung erlangen – zwei Schlüsselelemente. Sie werden rasch merken, dass zielführende Befragungen ein sehr anspruchsvolles Handwerk sind, das Sie möglicherweise lieber einem Experten überlassen wollen. Stellen Sie nebst den Fragen auch *zwei* Sets der relevanten Unterlagen zusammen, eines für sich und eines, welches Sie der befragten Person vorlegen können (oder arbeiten Sie mit einer Projektion). Bereiten Sie ebenfalls einen geeigneten Einleitungstext vor (einschliesslich der nötigen Aufklärung: → **Q33**), ebenso, was Sie der Person zum Abschluss der Befragung mit auf den Weg geben wollen (z.B. Vertraulichkeit, nächste Schritte). Mehr Hinweise dazu, wie Sie erfolgreich befragen: → **Q40**.

In der Praxis hat sich bewährt, die Stichworte (Fragen bzw. Themen, Aktenverweise, Eckdaten und andere wichtige Fakten) für die einzelnen Themen oder Fragekomplexe auf jeweils einem Blatt gut lesbar festzuhalten, welches Sie während der Befragung vor sich haben und an dem Sie sich orientieren können. Auf diese Weise geraten Sie nicht aus dem Konzept, wenn Sie die Reihenfolge spontan umstellen müssen, können Aussagen rascher verifizieren und finden die Schlüsseldokumente sofort, falls Sie sie den Befragten damit konfrontieren müssen.

9. **Führen Sie die Befragung ungestört durch.** Sorgen Sie dafür, dass Sie die Befragung ohne externe Störung (Handys, Besucher, etc.) durchführen können. Der befragten Person sollte ein Getränk und etwas zum Schreiben angeboten werden; sodass sie sich an etwas „festhalten" kann, dies ist auch psychologisch wichtig. Der Psychologie entsprechend sollten Sie auch die Sitzordnung wählen. Planen Sie Pausen mit Bezug auf die zu besprechenden Themen geschickt. Halten Sie die Unterlagen, die Sie der befragten Person vorhalten wollen, in Kopie bereit. Achten Sie darauf, dass Sie sich in den Unterlagen rasch und sicher zurechtfinden. Sprechen Sie ihre Rollen ab, falls mehrere Personen die Befragungen durchführen. Die Atmosphäre sollte nicht feindselig sein; gehen Sie offen und freundlich auf die zu befragende Person zu und versuchen Sie, etwaige Anspannungen – vor allem bei der beschuldigten Person – abzubauen, etwa indem Sie ihr vermitteln, dass Sie sich der Anspannung und ihres Zustandes bewusst sind. Zum Abschluss der Befragung sollten Sie der befragten Person noch die Gelegenheit geben, sich zu bisher nicht angesprochenen Themen zu äussern und Fragen zu stellen.

Gefährdung

Eine Untersuchung kann einer beschuldigten Person schwer zusetzen oder sie kann das Gefühl gewinnen, es habe alles keinen Sinn mehr. Das kann zu einer Selbst- oder Fremdgefährdung führen. Seien Sie daher speziell bei Befragungen auf solche Fälle gedanklich und praktisch vorbereitet (Signale erkennen, medizinischer Notfallkontakt, z.B. Werksarzt Stand-by). Siehe auch → **Q41**.

Die das Protokoll führende Person sollte selbst keine Fragen stellen, ausser, sie hat etwas nicht verstanden oder will wissen, wie ein Name buchstabiert wird. Werden Dokumente gezeigt oder ausgetauscht, ist dies für die Protokoll führende Person laut zu sagen, damit diese Information protokolliert oder aufgezeichnet wird und später klar ist, in welchem Kontext eine Aussage stand.

10. **Sorgen Sie in der Befragung für ein klares Verständnis.** In Befragungen werden häufig Begriffe verwendet oder Vorgänge zusammenfassend beschrieben, die dem Zuhörer auf den ersten Blick vermeintlich klar sind, aber durchaus unterschiedlich verstanden werden können. Haken Sie in solchen Fällen nach. Erklärt der Befragte, sein Chef habe die Transaktion so „gewollt", so kann dies bedeuten, dass der Chef ihm im Einzelfall eine klare Weisung gegeben hat. Denkbar ist aber auch, dass nur eine Regelung in Grundzügen existierte, die der Mitarbeiter selbst interpretiert und angewandt hat, ohne dass der Chef im konkreten Fall davon wusste. Es kann ebenso sein, dass gar keine Vorgabe vorhanden war, sondern der Mitarbeiter lediglich aufgrund von Äusserungen oder anderen Umständen davon ausging, dass er mit Willen und allenfalls Wissen seines Vorgesetzten handelte. Werden Begriffe verwendet, lassen Sie sie vom Befragten definieren oder definieren Sie sie selbst. Wer z.B. einen Mitarbeiter in einer Untersuchung wegen unangemessenem Verhaltens am Arbeitsplatz dazu befragt, ob er eine „sexuelle Beziehung" zu einer bestimmten anderen Person hatte, sollte definieren, was in diesem Kontext unter sexueller Beziehung zu verstehen ist.[22] Ist die Definition wichtig, kann es sinnvoll sein, mit diesen Definitionen zu spielen und dieselbe Frage unterschiedlich zu stellen.

Wie lange?

Eine Befragung kann von einer halben Stunde bis zu mehreren Stunden dauern. Stellen Sie sicher, dass Sie alle wichtigen Punkte in der ersten Befragung abgedeckt werden – auch wenn das lange dauert.

Eine bewährte Technik ist es, eine erhaltene Antwort **in eigenen Worten neu zu formulieren** und sich das Verständnis vom Befragten bestätigen zu lassen. Diese Technik kann auch dazu benutzt werden, die Frage zuzuspitzen oder mit Varianten zu spielen und so der Sache näher zu kommen. Eine weitere Befragungstechnik besteht darin, den Sachverhalt **in möglichst kleine Teile aufzubrechen** und diese nacheinander abzuarbeiten. Diese Technik wurde für Kreuzverhöre entwickelt und sichert klare Aussagen. Sie fragen in diesem Fall nicht: „War es ein warmer Tag mit viel Publikum?" sondern fragen zuerst nach der Wärme und erst dann nach dem Publikum (und lassen sich, in diesem Beispiel, zusätzlich definieren, was der Befragte unter „viel" versteht, wenn er die Frage zuvor bejaht hat).

22 Vgl. dazu den sog. *Clinton-Lewinsky-Skandal* um den früheren US-Präsidenten Bill Clinton, der den Begriff so verstanden haben wollte, dass er Berührungen der Genitalien und bestimmter anderer Körperteile der Frau voraussetze, was er bestritt, da er von der betreffenden Frau „nur" oral befriedigt worden war, wie sich später herausstellte.

11. **Ein etwaiges Protokoll der Befragung muss nicht sofort abgegeben werden.** Das Protokoll der Befragung, soweit es eines gibt, wird häufig nicht unterzeichnet. Es wird der befragten Person aus Gründen der Vertraulichkeit und der Taktik auch nicht mitgegeben (etwa, weil sie das Befragungsprotokoll dazu benutzen kann, um sich bei späteren Befragungen nicht in Widersprüche zu verstricken oder anderen Personen zu erlauben, sich auf ihre eigene Befragung vorzubereiten). Rechtlich kann die Unterzeichnung und Abgabe der Befragung dort relevant sein, wo in anderen Verfahren (z.B. von Strafverfolgungsbehörden) darauf zurückgegriffen werden soll, was aber möglicherweise gar nicht im Interesse der befragten Person (und des Unternehmens) ist oder wo z.B. ihre Kündigung als Arbeitnehmerin im Raum steht (damit sie im Streitfall darauf behaftet werden kann). Ist Ihnen hingegen wichtig, dass Ihre Notizen die von der Person gemachten Aussagen wirklich richtig wiedergeben, etwa weil sie andere belasten (z.B. bei Zeugen), kann es sinnvoll sein, sie diesen Personen vorzulegen und bestätigen zu lassen, mit und ohne Unterschrift. Wollen Sie dies vermeiden, dann wiederholen Sie die Aussagen einer Person in Ihren eigenen Worten und lassen Sie sich bestätigen, dass Sie richtig verstanden haben. Das praktische Problem bei der Vorlage des Protokolls ist in der Regel, dass die während einer Befragung erstellten Protokolle und Notizen Rohfassungen sind, die zuerst einer Überarbeitung bedürfen[23]. Bedenken Sie schliesslich, dass jede Person im Rahmen des datenschutzrechtlichen Auskunftsrechts Anspruch auf Einsicht in die sie betreffenden Personendaten hat; diese kann allerdings in der Regel bis zum Abschluss der Untersuchung aufgeschoben werden. Mehr dazu: → **Q36**.

> **Auch als Zeuge?**
>
> Wird eine Person womöglich als Zeuge in einem späteren Zivilverfahren benötigt, sollte sie ihre Aussage nicht unterschreiben. Sie wäre ansonsten in ihrer Zeugenaussage vor Gericht nicht mehr frei und für eine solche womöglich gar disqualifiziert.

> Erlauben Sie der befragten Person, selbst Notizen zur Befragung zu machen. Rechnen Sie ohnehin damit, dass sie nach einer Befragung ihrerseits ein Gedächtnisprotokoll erstellen wird, insbesondere dann, wenn die Befragung für sie nicht gut lief.

12. **Fassen Sie bei Bedarf nach.** In Befragungen kommt es regelmässig vor, dass die befragte Person eine echte oder vorgetäuschte Gedächtnislücke hat oder auf irgend-

23 Die z.B. von Strafverfolgungsbehörden oder Gerichten praktizierte Alternative ist, jede Aussage gleich sauber ins Protokoll zu nehmen, was aber zu ständigen Pausen führt und eine effiziente und effektive Befragung tendenziell verhindert.

welche vorbestehenden Unterlagen verweist, die sie aber gerade nicht bei sich hat. Dies könnten Ausflüchte sein, aber auch berechtigte Hinweise auf weiterführende Beweismittel. Erstellen Sie während der Befragung eine Liste dieser Punkte, und vereinbaren Sie zum Schluss des Gesprächs, dass sich die befragte Person darum kümmert. Fassen Sie diesbezüglich nach – und sei es nur um zu zeigen, dass Sie nicht lockerlassen.

Do's	Don'ts
• Klären Sie jede Person vor einer Befragung über den Sinn und Zweck der Befragung und über ihre Rechte und Pflichten als Arbeitnehmer auf. • Versuchen Sie, auf die befragten Personen offen und unvoreingenommen zuzugehen und sich ihre Geschichte anzuhören; sprechen Sie sie auf Ungereimtheiten offen an und verlangen sie eine Erklärung. Sagen Sie ohne Vorwurf, wenn Ihnen etwas unglaubwürdig erscheint und warum. • Freundlichkeit und Empathie ist in einer Befragung oft hilfreicher als angsteinflössendes Auftreten. Treten Sie nicht wie Polizei oder Staatsanwalt auf. Sie dürfen allerdings durchaus vermitteln, dass früher oder später alles ans Licht kommt – dem ist nämlich meistens so. Zur Psychologie: → **Q40**, → **Q41**. • Wenn Personen sich nicht mehr erinnern können, kommen sie später auf das Thema zurück; wenn sie behaupten, sie müssten dazu in ihren Unterlagen nachschauen, erlauben Sie dies; geht dies nicht sofort, dann kommen Sie später darauf zurück.	• Sprechen Sie nicht zu viel, denn reden soll vor allem die befragte Person. • Geben Sie nicht zu viel über den Fall preis (wie z.B. den Namen der beschuldigten Person) – damit schützen Sie auch die beschuldigte Person vor Vorverurteilung und Gerüchten. • Zeichnen Sie nie ohne Einwilligung auf; die Einwilligung sollte auf der Aufzeichnung zu hören sein. • Zwingen Sie etwaige nicht im Unternehmen angestellte Personen nicht zu einer Befragung; Sie sind nicht der Staatsanwalt. Befragen Sie sie mit Einwilligung, so machen Sie klar, wozu diese Befragung dient. • Sie können eine Person letztlich nie zur Aussage oder Wahrheit zwingen. Drohen Sie ihr nicht mit Folgen, die unberechtigt sind; dies kann ansonsten eine strafbewehrte Nötigung darstellen. Sie dürfen eine Person aber darauf hinweisen, welchen Eindruck dies hinterlässt, welche Folgen dies haben kann und warum eine Antwort auch im Interesse der befragten Person sein kann.

Do's	Don'ts
• Lassen Sie einer Person genügend Zeit, ihr vorgehaltene Unterlagen genau zu studieren. Vergessen Sie nicht, zu protokollieren, was ihr zu welcher Frage vorgelegt worden ist (im Falle einer Aufzeichnungen sollten Sie das Dokument laut nennen, damit es „*on record*" ist). • Behalten Sie sich die weitere Befragung einer Person nach Möglichkeit vor.	• Versprechen Sie der Person nicht, dass Sie deren Aussagen nicht weitersagen. Sie sollten aber in guten Treuen handelnde Quellen so gut es geht schützen. • Lügen Sie nicht. Dies kann die Verwertbarkeit der Antwort beeinträchtigen. Aber Sie müssen nicht alles offenlegen, was Sie wissen.

Wann Sie externe Unterstützung beiziehen sollten

- Falls Sie **keine Erfahrungen** mit Befragungen haben und es sich nicht nur um einen kleinen, alltäglichen Fall handelt.
- Für **anspruchsvollere Befragungen**, welche Erfahrung und das Wissen um die rechtlichen Rahmenbedingungen erfordern.
- Für Befragungen, die aus **psychologischen Gründen** ausserhalb des Unternehmens, ausserhalb des üblichen Geschäftsbetriebs oder von Personen ausserhalb des Unternehmens erfolgen sollen.
- Für Befragungen, bei welchen die **Wahrung der Unabhängigkeit** und damit auch Glaubwürdigkeit der Untersuchung wichtig ist.

Häufige Fragen und Antworten

Q30. Können wir einen Mitarbeiter zur Teilnahme an einer Befragung verpflichten?

A: Ja, der Arbeitgeber kann den Mitarbeiter zur Teilnahme verpflichten. Dem Mitarbeiter kommt gegenüber dem Arbeitgeber eine **Treuepflicht** zu (Art. 321a Abs. 1 OR). Er hat die **berechtigten Interessen** des Arbeitgebers in guten Treuen zu wahren. Aus der Treuepflicht lässt sich die **Auskunfts- und Mitteilungspflicht** des Mitarbeiters ableiten, d.h. dem Arbeitgeber ist über sämtliche relevante Vorgänge und Tatsachen zu berichten, sowie über Missstände, Störungen und Gefahren (zur Pflicht, von sich aus Fehlverhalten anzuzeigen: → **Q9**).

Der Arbeitgeber kann den Mitarbeiter aufgrund seiner **Weisungsbefugnis** (Art. 321d OR) zur Teilnahme an einer Befragung verpflichten. Der Mitarbeiter muss aufgrund seiner Treuepflicht in der Befragung **wahrheitsgetreu, vollständig** und **rechtzeitig** Auskunft geben, vorausgesetzt es besteht ein genügender Bezug zum Arbeitsverhältnis, mithin hat der Mitarbeiter keine Fragen über sein Privatleben zu beantworten (in Ausnahmefällen kann das Privatleben freilich von geschäftlicher Relevanz sein, etwa wenn der Chef seine Mitarbeiterin im Ausgang belästigt und sie ihn aufgrund des Machtverhältnisses gewähren lässt). Aus taktischen Gründen kann es sinnvoll sein den Mitarbeiter darauf hinzuweisen, dass er **sich strafrechtlich nicht selbst belasten muss** (→ **Q37**). Es ist zudem üblich, Mitarbeiter vor einer Aussage im Rahmen einer Befragung über ihre Rechte und Pflichten aufzuklären (→ **Q33**).

Der **Termin (Ort und Zeit)** der Befragung kann vom Arbeitgeber festgelegt werden, soweit dies dem Mitarbeiter zumutbar ist. Dies muss nicht der Arbeitsplatz des Mitarbeiters sein; auch gewisse Reisen (z.B. zur Anwaltskanzlei, wo die Befragung stattfindet) können dem Mitarbeiter zugemutet werden. Es wird regelmässig sogar angezeigt sein, den Mitarbeiter nicht an seinem Arbeitsplatz zu befragen (Diskretion, keine Ablenkungen, mehr Aufmerksamkeit).

Die Pflicht zur Teilnahme an einer Befragung gilt lediglich für **gegenwärtige Mitarbeiter**. **Ehemalige Mitarbeiter** sind nicht verpflichtet an einer Befragung teilzunehmen. Dieser Umstand ist insbesondere im Falle einer fristlosen Entlassung eines fehlbaren Mitarbeiters zu beachten: Ist er per sofort freigestellt worden, besteht weiterhin ein Arbeitsverhältnis und der freigestellte Mitarbeiter hat entsprechende Rechte und Pflichten. Ist er hingegen entlassen worden, muss er für eine Befragung grundsätzlich nicht mehr zur Verfügung stehen.

Aus diesem Grund erwarten insbesondere auch **ausländische Untersuchungsbehörden**, die eine Person nicht aus eigenem Recht zur Befragung verpflichten können, dass potenziell fehlbare Mitarbeiter nicht einfach entlassen werden. Das Unternehmen würde sich dann der Möglichkeit rauben, den Mitarbeiter anzuweisen, sich der Behörde für Fragen zur Verfügung zu stellen, oder ihn selbst zu Aspekten zu befragen, über welche die Behörden Auskunft ersuchen.

Literatur:

Götz Staehelin, Claudia: Unternehmensinterne Untersuchungen, Zürich/Basel/Genf 2019

Rudolph, Roger: Interne Untersuchungen: Spannungsfelder aus arbeitsrechtlicher Sicht, Schweizerische Juristenzeitung (SJZ) 114/2018, 385 ff.

Wantz, Simona/Licci, Sara: Arbeitsvertragliche Rechte und Pflichten bei internen Untersuchungen, Jusletter vom 18. Februar 2019, Rz. 1 ff.

Q31. Mit welchen Konsequenzen muss der Mitarbeiter rechnen, wenn er sich weigert an der Befragung teilzunehmen?

A: Weigert sich der Mitarbeiter an einer Befragung teilzunehmen, verletzt er dadurch seine Treuepflicht, was **arbeitsrechtliche Konsequenzen** nach sich ziehen kann. Normalerweise wird zunächst eine **Verwarnung** oder ein **Verweis** ausgesprochen. Nach einer erneuten Verfehlung seitens des Mitarbeiters rechtfertigt sich die ordentliche oder sogar fristlose **Kündigung**[24] (zu den Sanktionen → **WEITERE SCHRITTE**).

Auch die Kosten für **nutzlose Aufwendungen** (z.B. das Warten auf den Mitarbeiter am Befragungstermin) können als Schadenersatz vom Mitarbeiter verlangt und unter den gegebenen Voraussetzungen mit seinem Lohn verrechnet werden.

Welche Bedeutung der Treuepflicht des Mitarbeiters eingeräumt wird, zeigt sich durch die Möglichkeit der **gerichtlichen Durchsetzung**. Die Erfüllung der Auskunfts- und Mitteilungspflicht kann gerichtlich erzwungen werden, wobei der Richter bei Renitenz eine Ordnungsbusse (Art. 292 → **StGB**) androhen kann.

> **Literatur:**
>
> Graf, Damian K.: Strafprozessuale Verwertbarkeit von Befragungsprotokollen interner Untersuchungen, forumpoenale 1/2016, 39 ff.
>
> Wantz, Simona/Licci, Sara: Arbeitsvertragliche Rechte und Pflichten bei internen Untersuchungen, Jusletter vom 18. Februar 2019, Rz. 1 ff.

Q32. Darf sich ein Mitarbeiter von einem Anwalt begleiten lassen? Wer trägt die Kosten für den Anwalt?

A: Der Mitarbeiter hat nicht immer Anspruch auf einen Rechtsbeistand. Bei der Frage, ob der Mitarbeiter sich von einem Anwalt begleiten lassen darf, ist die **Rolle des Mitarbeiters** bei der Befragung massgebend. Ist der Mitarbeiter lediglich Informationsträger und informiert in dieser Rolle nur über Geschäftsvorgänge, besteht kein Grund und somit auch kein Anspruch auf eine anwaltliche Vertretung.

Hingegen entspricht es der herrschenden Ansicht, dass der Mitarbeiter Anspruch auf einen Rechtsbeistand hat, wenn ihm **strafrechtlich relevantes Verhalten** vorgeworfen wird. Andere Stimmen wollen bereits dann anwaltlichen Beistand zulassen, wenn **zivilrechtliche Sanktionen** oder erhebliche Interessensgegensätze drohen oder stellen darauf ab, ob seitens des Unternehmens Anwälte oder andere „Profis" die Befragung durchführen. Möglich ist auch, dass vertragliche Richtlinien, interne Policies oder ein Gesamtarbeitsvertrag das Recht auf einen Rechtsbeistand vorsehen (zum Recht auf Aussageverweigerung: → **Q37**).

---

24 Zur fristlosen Kündigung aufgrund des Aussageverhaltens in einer internen Untersuchung: Entscheid BGer 8C_626/2020 vom 21. Dezember 2020.

Eingeschränkt werden kann der Beizug eines Anwalts, wenn **berufsgeheimnisgeschützte Daten** im Spiel sind, die dem Anwalt offengelegt werden müssen, damit er seine Aufgabe wahrnehmen kann. Hierzu ist der Mitarbeiter (z.B. einer Bank betr. Kundendaten) nicht ohne Weiteres befugt, denn die Offenlegung kann eine strafrechtlich sanktionierte Geheimnisverletzung darstellen. Eine mögliche Lösung sind Anwälte, die (auch) vom Arbeitgeber mandatiert und so dem Berufsgeheimnis unterstellt worden sind. Dieses Modell hat sich auch schon in anderen Situationen bewährt: Zeichnet sich in einem konkreten Fall ab, dass eine Vielzahl von Mitarbeitern persönlich rechtlichen Risiken ausgesetzt sein könnten (z.B. auch in Bezug auf behördliche Verfahren) oder könnten Mitarbeiter entsprechende Befürchtungen haben, kann es aus Sicht des Unternehmens sinnvoll sein, einen **"Vertrauensanwalt"** zu bestellen. Dabei handelt es sich um einen zwar vom Unternehmen mandatierten und bezahlten Anwalt, der jedoch mit der Untersuchung bzw. den Verfahren nichts zu tun hat, aber besorgten Mitarbeitern vertraulich Ratschläge erteilen und ihre Rechte und Pflichten erörtern kann. Das Unternehmen wird diesen Anwalt zwar zur Geheimhaltung gegenüber dem Unternehmen verpflichten, kann so aber eine Vertrauensperson wählen, von welcher sie annimmt, dass sie zwar die Mitarbeiter richtig beraten, aber nicht unnötig Öl ins Feuer giessen wird.

Unter Umständen ist es sinnvoll eine anwaltliche Vertretung **freiwillig** zuzulassen, um die Atmosphäre zu entspannen, für **gleich lange Spiesse** zu sorgen und damit die Kooperationsbereitschaft bei der Befragung zu erhöhen. Die Erfahrung zeigt auch, dass ein anwesender Anwalt eine Befragung nicht unbedingt einschränkt. Die Aussagen können an Gewicht gewinnen und der Anwalt wird seinen Klienten mitunter sogar zur Aussage ermuntern, wo sein Klient dazu verpflichtet ist. Im Protokoll sollte jedoch festgehalten werden, wenn eine Antwort erst nach Rücksprache mit dem Anwalt erfolgt.

Zieht ein Mitarbeiter einen Anwalt bei, ist darauf zu achten, dass dieser nicht mehrere der von einer Untersuchung betroffenen Personen vertritt. Tut er dies, liegt in aller Regel ein **Interessenkonflikt** vor, auf welchen der Anwalt hinzuweisen ist. In einer solchen Situation kann von der befragten Person verlangt werden, einen anderen Anwalt beizuziehen. Dass sich Anwälte mehrerer betroffener Personen untereinander absprechen, kann hingegen nicht verhindert werden.

Die **Kosten** für eine anwaltliche Vertretung sind durch den Mitarbeiter zu tragen, soweit vertraglich (z.B. in einem Reglement) nichts anderes vorgesehen ist. Der Arbeitgeber hat dann für die Kosten des Rechtsbeistands aufzukommen, wenn ein Mitarbeiter im In- oder Ausland im Rahmen seiner Tätigkeit für das Unternehmen in behördliche Ermittlungen/Verfahren verwickelt wird. Die Kostenübernahme durch den Arbeitgeber ergibt

sich in diesem Fall aus seiner Pflicht, sämtliche durch die Ausführung der Arbeit notwendig entstehenden Auslagen zu ersetzen, d.h. Unkosten zu bezahlen (Art. 327a OR).

Literatur:

Götz Staehelin, Claudia: Unternehmensinterne Untersuchungen, Zürich/Basel/Genf 2019

Rudolph, Roger: Interne Untersuchungen: Spannungsfelder aus arbeitsrechtlicher Sicht, Schweizerische Juristenzeitung (SJZ) 114/2018, 385 ff.

Wantz, Simona/Licci, Sara: Arbeitsvertragliche Rechte und Pflichten bei internen Untersuchungen, Jusletter vom 18. Februar 2019, Rz. 1 ff.

Q33. Worüber muss ein zu befragender Mitarbeiter aufgeklärt werden?

A: Als Ausfluss der **Fürsorgepflicht** des Arbeitgebers ist der zu befragende Mitarbeiter vor der Befragung allenfalls aufzuklären. Dies muss freilich nicht bei jedem Gespräch zur Informationsgewinnung im Rahmen einer internen Untersuchung geschehen, sondern nur bei Befragungen oder anderen Gesprächen, die im Widerspruch zu den persönlichen Interessen des betreffenden Mitarbeiters stehen könnten.

Wer vom unbeteiligten Mitarbeiter in der Buchhaltung wissen will, was die verschiedenen Angaben auf einem Buchhaltungsbeleg bedeuten, wird diesen vorher nicht aufklären müssen. Das wäre unverhältnismässig und würde den Mitarbeiter unnötig verunsichern. Könnte der Mitarbeiter jedoch in ein Fehlverhalten involviert sein oder von einem solchen Kenntnis haben und soll er dazu befragt werden, ist eine Aufklärung angezeigt – und sei es nur, weil es ihm womöglich widerstrebt, Arbeitskollegen anzuschwärzen.

Eine hinreichende und faire Aufklärung kann auch die **Kooperationsbereitschaft** eines Mitarbeiters fördern, da sie hilft, das Gefühl der Machtlosigkeit abzubauen, aber auch an das Pflichtbewusstsein appellieren kann.

Die Aufklärung sollte zu Beginn der Befragung erfolgen und beinhaltet typischerweise (je nach Situation und Stellung des Befragten) einzelne oder alle der nachfolgenden **Elemente**:

Checkliste

- **Vorstellung** der Befragenden.
- Information über **Zweck der Befragung** und ggf. grobe Erläuterung der **Vorwürfe** (strategische Überlegungen sind hierbei zu berücksichtigen).
- Aufklärung über das **konkrete Vorgehen** bei der Befragung, insbesondere darüber, wie sie festgehalten wird; soll die Befragung in Ton oder Video **aufgezeichnet** werden, ist eine **Einwilligung** der befragten Person erforderlich (nicht jedoch bezüglich Notizen oder Wortprotokollen).

- Bei **Rechtsanwälten als Befrager** (im US-Rechtsraum auch als „*Corporate Miranda*"- oder „*Upjohn*"-Warnung bekannt):
  - Aufklärung darüber, dass die Rechtsbeistände des Arbeitgebers ausschliesslich dessen **Interessen** vertreten und nicht jene des Mitarbeiters.
  - Information darüber, dass aufgrund der Teilnahme von Rechtsanwälten der Inhalt der Befragung dem Anwaltsgeheimnis unterliegt, dieser daher vom Befragten vertraulich zu behandeln ist und der Entscheid über den Verzicht auf den Geheimnisschutz beim Arbeitgeber liegt (m.a.W. Aufklärung darüber, dass der Arbeitgeber darüber bestimmt, ob er die Unterlagen an **Strafverfolgungs- bzw. Aufsichtsbehörden** weiterleiten will; für den US-Rechtsraum ist zudem die Pflicht zur Vertraulichkeit wichtig, weil sonst vertreten werden könnte, dass das Unternehmen auf sein → **Legal Privilege** verzichtet hat).
- Hinweis auf die **Treuepflicht** und damit verbunden die **Auskunfts- und Mitteilungspflicht** sowie das Vorliegen einer **Pflichtverletzung** bei Verweigerung der Befragung.
- Hinweis darauf, dass **entlastende Beweismittel** bezeichnet werden können.
- Hinweis auf das **Auskunftsverweigerungsrecht,** falls es sich um private Sachverhalte handelt, die nicht im Zusammenhang mit dem Arbeitsverhältnis stehen; aus taktischen Gründen kann es sinnvoll sein den Mitarbeiter darauf hinzuweisen, dass er sich strafrechtlich nicht selbst belasten muss (→ **Q37**).
- Hinweis darauf, dass das Unternehmen möglicherweise nicht verhindern kann, dass das Ergebnis der Befragung an **Aufsichts- oder Strafverfolgungsbehörden** oder im Rahmen eines Gerichtsverfahrens **herausgegeben werden** muss.
- Hinweis auf **Vertraulichkeit der Befragung** gegenüber Dritten und anderen Mitarbeitern (→ **Q35**).
- Ggf. spezielle Aufklärung, wenn die Befragung virtuell erfolgt (dazu → **Q39**).

Aus taktischen Gründen kann es sich auch empfehlen, auf gewisse Aufklärungen zu verzichten, da die so entstandenen Aussagen für Aufsichts- oder Strafverfolgungsbehörden **schwieriger oder nicht verwertbar** sind (→ **Q37**).

Literatur:

Wantz, Simona/Licci, Sara: Arbeitsvertragliche Rechte und Pflichten bei internen Untersuchungen, Jusletter vom 18. Februar 2019, Rz. 1 ff.

Q34. Müssen wir einem zu befragenden Mitarbeiter vorgängig oder überhaupt Einblick in die Unterlagen gewähren?

A: Nein. Es besteht **keine Pflicht** des Arbeitgebers, dem Mitarbeiter vor der ersten Befragung Einblick in die vorhandenen Unterlagen (Beweismittel etc.) zu gewähren.

Als Ausfluss des **rechtlichen Gehörs** muss der Mitarbeiter aber im Verlaufe der internen Untersuchung mit den belastenden Beweisen konfrontiert werden und dazu Stellung nehmen können. Ähnliches gilt im Strafverfahren: Auch hier ist die Staatsanwaltschaft nicht verpflichtet, dem Beschuldigten vor der ersten Einvernahme Einblick in die Akten zu gewähren. Allerdings kann dieser dort die Aussage verweigern, weil er keiner Pflicht zur strafrechtlichen Selbstbelastung unterliegt, und so eine Einsichtnahme erzwingen, bevor er sich zur Sache äussert.

Weder für die Wahrung des rechtlichen Gehörs noch im Rahmen des datenschutzrechtlichen Auskunftsrechts muss der beschuldigten Person ungehinderter Einblick in alle Unterlagen gewährt werden. Diesem Einblick können berechtigte **Schutzinteressen Dritter** entgegenstehen. Hier ist eine Interessenabwägung erforderlich, welche alle Umstände, wie etwa den Zeitpunkt der Einsicht und das Risiko von Retaliationsmassnahmen berücksichtigt (z.B. wenn es um Aussagen von untergebenen Personen oder Arbeitskollegen geht). Allenfalls kann es sinnvoll sein, betroffene Dritte zu fragen, ob sie Einwände gegen eine Offenlegung haben. Umgekehrt sollte ein Unternehmen seinen Informanten oder befragten Personen nie absolute Vertraulichkeit zusichern; es wird diese nicht unbedingt wahren können – jedenfalls nicht zulasten der Verteidigungsrechte der beschuldigten Person[25].

Der beschuldigte Mitarbeiter muss sich **angemessen gegen Vorwürfe wehren können**, was bedeuten kann, dass er wissen muss, woher oder von wem sie kommen (z.B. ob von einem Widersacher oder von einer neutralen Person). Hier kann eine geschickte Befragung weiterhelfen, ohne dass die Identität eines Dritten offengelegt werden muss, so z.B. die Frage, ob die beschuldigte Person im Unternehmen Feinde hat, die sie möglicherweise unberechtigterweise anschwärzen möchte. Im Sinne einer ergebnisoffenen Untersuchung können entsprechende Auskünfte auch bei der Einordnung von Aussagen Dritter wichtig und hilfreich sein. Soll deren Identität nicht offengelegt werden, so wird vom Arbeitgeber erwartet, dass er deren Vorhaltungen oder Aussagen so **ausführlich zusammenfasst**, dass die beschuldigte Person dazu sinnvoll Stellung nehmen und sich verteidigen kann. Ein Recht zur **Konfrontationseinvernahme** wird normalerweise abgelehnt[26].

25 Entscheid des OGer Zürich vom 27. Oktober 2015, RA150002, E. 8.3.
26 Vgl. Arbeitsgericht Zürich, Entscheide 2017 Nr. 11.

Ist eine Person **keines Fehlverhaltens verdächtigt**, besteht kein Bedarf zur Verteidigung und es muss ihr entsprechend auch kein Einblick in die Unterlagen gegeben werden. Das datenschutzrechtliche Auskunftsrecht bleibt natürlich vorbehalten.

> **Literatur:**
>
> Rudolph, Roger: Interne Untersuchungen: Spannungsfelder aus arbeitsrechtlicher Sicht, Schweizerische Juristenzeitung (SJZ) 114/2018, 385 ff.

Q35. Muss ein befragter Mitarbeiter die Befragung geheim halten?

A: Ja. Die Geheimhaltung einer solchen Befragung liegt im **berechtigten Interesse des Arbeitgebers**, weshalb der Mitarbeiter aufgrund seiner Treuepflicht die Befragung geheim halten muss. Der Mitarbeiter hat zudem, was er während seines Arbeitsverhältnisses an Geschäftsgeheimnissen erfährt, geheim zu halten (Art. 321a Abs. 4 OR). Die Geheimhaltung kann zusätzlich durch eine separat zu unterzeichnende **Geheimhaltungserklärung** abgesichert werden. In einer Untersuchung sollte der Mitarbeiter zur Geheimhaltung ausdrücklich angewiesen werden. Der Arbeitgeber sollte jedoch stets damit rechnen, dass die Geheimhaltung nicht gewahrt wird. Dies kann bedeuten, dass der Arbeitgeber – falls er beabsichtigt mehrere Personen zu befragen – diese Befragungen zeitlich sehr nahe beieinander oder sogar **parallel vornehmen** muss.

Q36. Kann ein befragter Mitarbeiter eine Kopie seines Befragungsprotokolls verlangen?

A: Ja. Gestützt auf das **datenschutzrechtliche Auskunftsrecht**, kann der Mitarbeiter grundsätzlich eine kostenlose Kopie des Befragungsprotokolls verlangen. Die Auskunft kann jedoch aufgeschoben oder verweigert werden, wenn überwiegende eigene Interessen dies gebieten und das Befragungsprotokoll nicht Dritten zugänglich gemacht wird.

Ein solches Interesse kann z.B. während der internen Untersuchung (und einer allfälligen ebenfalls laufenden behördlichen Untersuchung) vorliegen, wenn davon auszugehen ist, dass der Mitarbeiter seine Aussage mit den Aussagen anderer Personen abstimmt, d.h. eine Kollusionsgefahr besteht (ausführlicher zum Auskunftsrecht: → **Q15** und → **Q57**).

Häufig wird eine allenfalls von der beschuldigten Person verlangte Auskunft bis zu dem Zeitpunkt aufgeschoben, in dem dieser **ohnehin Einblick in die Unterlagen** gewährt wird, um ihr eine Stellungnahme im Sinne des rechtlichen Gehörs zu ermöglichen.

Zum **Schutz von Dritten** bzw. zum Schutz von befragten Personen vor dem Einblick durch Dritte vgl. → **Q34**.

> **Literatur:**
>
> Rudolph, Roger: Interne Untersuchungen: Spannungsfelder aus arbeitsrechtlicher Sicht, Schweizerische Juristenzeitung (SJZ) 114/2018, 385 ff.

Q37. Kann ein Mitarbeiter die Aussage verweigern, wenn er sich dadurch selbst belasten würde? Kann sie im Strafverfahren verwertet werden?

A: Im Strafrecht gilt das sog. ***Nemo-tenetur*-Prinzip**, d.h. eine Person kann in einem Strafverfahren die Aussage verweigern, wenn sie sich dadurch selbst belasten würde. Bei einer internen Untersuchung handelt es sich allerdings nicht um ein offizielles Strafverfahren, sondern um ein unternehmensinternes Verfahren.

Das Aussageverweigerungsrecht steht im **Spannungsfeld** zur Auskunftspflicht des Mitarbeiters (dazu → **Q30**). Auf der einen Seite steht das Aussageverweigerungsrecht als Grundprinzip des Strafrechts und auf der anderen Seite die arbeitsrechtlich sanktionierte Aussagepflicht des Mitarbeiters. Das Bundesgericht hat klargestellt, dass das *Nemo-tenetur*-Prinzip lediglich im **Verhältnis zum Staat** zur Anwendung gelangt (BGE 131 IV 36, [43], E. 3.3.1). Bei einer internen Untersuchung stehen sich aber *Private* gegenüber, weshalb der Mitarbeiter die Aussage gestützt auf sein Aussageverweigerungsrecht **nicht verweigern kann**. Der Mitarbeiter hat selbst dann auszusagen, wenn ihn die Aussage selbst belastet. Selbstredend bezieht sich die Aussagepflicht lediglich auf Sachverhalte im Zusammenhang mit dem Arbeitsverhältnis. Der Mitarbeiter kann mithin durchaus seine Aussage verweigern, wenn es um persönliche Lebenssachverhalte geht. Kann er die Aussage nicht verweigern, hat die Aussage wahrheitsgemäss und vollständig zu erfolgen.

In der Praxis sind die rein rechtlichen Grenzen des Aussageverweigerungsrechts häufig von beschränkter Bedeutung – speziell dann, wenn dem Mitarbeiter so oder so Sanktionen drohen, sei es wegen fehlender Kooperation, sei es wegen dem der Untersuchung zugrundeliegenden Fehlverhalten. Für das Unternehmen kann eine fehlende Mitwirkung immerhin insofern von Bedeutung und durchaus von Vorteil sein, als dass sie den Grund für eine Kündigung darstellen kann. Diese kann unter Umständen sogar fristlos erfolgen, auch wenn das Unternehmen eine frühere Gelegenheit zur fristlosen Kündigung bereits verpasst hat. Freilich können Mitarbeiter die Aussage auch ohne ausdrückliche Verweigerung in Form von **Gedächtnislücken** faktisch verweigern.

Eine andere Frage ist, ob die ihn selbst belastende Aussage des Mitarbeiters **in einem Strafverfahren verwertet** werden kann. Dieser Punkt ist ebenso umstritten wie die Voraussetzungen, unter welchen eine solche Verwertung stattfinden kann. Die Frage ist von grosser Praxisrelevanz: Immer mehr Aufsichts- und Strafverfolgungsbehörden gehen dazu über, sich der Erkenntnisse von internen Untersuchungen zu bedienen, weil es ihre eigene Arbeit massiv erleichtern kann. Sie warten in solchen Fällen zu und verlangen nach Abschluss der internen Untersuchung die entsprechenden Unterlagen heraus – durchaus auch gegen den Willen der Unternehmen und ungeachtet des Anwaltsgeheimnisses (dazu → **Q10**). Nach weit verbreiteter Auffassung dürfen in einer internen Untersuchung erhobene Beweise (einschliesslich Aussagen im Rahmen von Befragungen) in einem Strafverfahren dann verwertet werden, wenn

diese unter Einhaltung der Verfahrensgrundsätze des Strafrechts eingeholt wurden. Somit finden selbstbelastende Aussagen ihre Grenzen bei der Verwertbarkeit im Strafverfahren, wenn der Befragte nicht entsprechend aufgeklärt worden ist. So kann es aus **taktischen Gründen sinnvoll** sein, den Mitarbeiter darauf hinzuweisen, dass er sich strafrechtlich nicht selbst belasten muss, falls seine Aussagen in einem Strafverfahren verwendet werden sollen. In der Praxis wird dies häufig getan. Auch das umgekehrte Vorgehen kann je nach Situation angezeigt sein. Zu beachten ist, dass das Bundesgericht diese Problematik tendenziell anders „löst": In einem Entscheid aus dem Jahre 2020[27] sprach es sich *für* die Zulassung eines Befragungsprotokolls eines Arbeitgebers aus, obwohl daraus weder hervorging, dass der Befragte über die Aufzeichnung informiert war, noch dass er sich das Protokoll hätte anschauen können. Gemäss Bundesgericht seien die Umstände der Entstehung des Protokolls im Rahmen der Beweiswürdigung bzw. des Beweiswerts zu berücksichtigen.

Zu beachten ist auch die **Form der Protokollierung**: Eine Aufzeichnung eines Gesprächs (für die vorgängig die Zustimmung des Mitarbeiters einzuholen ist, vgl. Schritt 6 vorne) oder ein wörtliches Protokoll ist einfacher verwertbar als eine Zusammenfassung durch den Befrager, welche immer auch dessen eigene subjektive Wertung und Formulierung der Aussage enthält. Das Unternehmen bzw. ein Befrager sollte also im Vornherein festlegen, ob die Befragung so durchgeführt werden soll, dass sie später strafrechtlich verwertet werden kann.

Ist eine lediglich **zivilrechtliche Verwertung** beabsichtigt (die durchaus auch die Beweisführung in einem Gerichtsverfahren beinhalten kann), sind die Anforderungen an das Verfahren nach herrschender Auffassung weniger hoch.

Literatur:

Graf, Damian K.: Strafprozessuale Verwertbarkeit von Befragungsprotokollen interner Untersuchungen, forumpoenale 1/2016, 39 ff.

Othmar, Strasser: Zur Rechtstellung des vom Whistleblower beschuldigten Arbeitnehmers, in: von Kaenel, Adrian (Hrsg.), Whistleblowing – Multidisziplinäre Aspekte, Bern 2012, 72 ff.

Romerio, Flavio/Bazzani, Claudio/Frei, Daphne: Informationen – Vermittlung, Verwertung und Verbreitung bei komplexen Verfahren / I. – II., in: Romerio, Flavio/Bazzani, Claudio (Hrsg.), Interne und regulatorische Untersuchungen II., Zürich/Basel/Genf 2016

Wantz, Simona/Licci, Sara: Arbeitsvertragliche Rechte und Pflichten bei internen Untersuchungen, Jusletter vom 18. Februar 2019, Rz. 1 ff.

27 Entscheid des BGer 6B_48/2020/6B_49/2020 vom 26. Mai 2020, E. 5.3.

Q38. Dürfen wir einem Mitarbeiter eine Amnestie anbieten, wenn er im Gegenzug kooperiert?

A: Dies ist grundsätzlich möglich, jedenfalls soweit es **zivilrechtliche Ansprüche** des Arbeitgebers gegenüber dem Arbeitnehmer betrifft. Eine Amnestie kann durchaus wirkungsvoll sein, um einen Mitarbeiter dazu zu bewegen, über ein Fehlverhalten auszupacken. Allerdings sind Amnestieversprechen nicht unproblematisch. Sie können betriebsintern zu Repressalien führen (was allerdings auch für eine freiwillige Kooperation zu Lasten anderer Mitarbeiter gilt), vor allem, wenn sie nicht geheim gehalten werden.

Im **strafrechtlichen Bereich** sind die Möglichkeiten des Arbeitgebers beschränkter. Im Falle von Antragsdelikten kann er auf einen Strafantrag verzichten, was den Arbeitnehmer allerdings nur schützt, soweit es keine anderen strafantragsberechtigten Personen gibt. Im Falle von Offizialdelikten kann sich dort, wo ein Strafverfahren auf Anzeige des Arbeitgebers eröffnet wurde, eine Desinteresseerklärung anbieten, die allerdings keinen zuverlässigen Schutz bietet (→ **Q50**). Der Verzicht auf strafrechtliche Schritte oder der Rückzug aus einem Strafverfahren bietet sich vor allem im Falle einer vergleichsweisen Erledigung einer Auseinandersetzung an.

Auch **ausländische Behörden**, die gegen ein Unternehmen ermitteln, können Amnestien kritisch gegenüberstehen, weil sie vom Unternehmen mitunter erwarten werden, dass es gegen die fehlbaren Mitarbeiter vorgeht. Handelt ein Unternehmen mit einer ausländischen Behörde eine vergleichsweise Beilegung einer Untersuchung aus, wird eine solche die fehlbaren Mitarbeiter häufig nicht mitumfassen.

Wird eine Amnestie versprochen, sind die Rahmenbedingungen vorgängig genau zu klären.

> **Literatur:**
>
> Wantz, Simona/Licci, Sara: Arbeitsvertragliche Rechte und Pflichten bei internen Untersuchungen, Jusletter vom 18. Februar 2019, Rz. 1 ff.

Q39. Kann eine Befragung des Mitarbeiters auch virtuell erfolgen? Was muss beachtet werden?

A: Eine virtuelle Mitarbeiterbefragung (z.B. per Teams, Zoom) ist durchaus möglich und deren Vorteil liegt sicherlich in der **Schnelligkeit** und **Flexibilität** begründet. Es gibt aber durchaus **Aspekte** und **Risiken** im Zusammenhang mit einer virtuellen Befragung, die vom Arbeitgeber auch bei Abwägung der Frage, ob eine solche durchgeführt werden soll, zu beachten sind. Aus der Fürsorgepflicht des Arbeitgebers kann sich ein gewisser **Zwang zur virtuellen** Befragung ergeben. Zu denken ist etwa an eine gesundheitlich angeschlagene oder gefährdete Person, der das physische Erscheinen zur Befragung selbst mit Schutzmassnahmen nicht mehr zugemutet werden kann. Auch die Umstände können zur virtuellen Mitarbeiterbefragung zwingen, wenn die

zu befragende Person sich etwa im Ausland befindet und ein Zuwarten nicht möglich oder nicht praktikabel ist.

Bei einer virtuellen Befragung können Vorteile, welche sich aus der **physischen Interaktion** ergeben, verloren gehen. So kann es schwieriger sein, eine angenehme Befragungsatmosphäre zu schaffen, Vertrauen aufzubauen und damit die Kooperationsbereitschaft des Einzelnen zu erhöhen. Ausserdem können wichtige Indizien, wie die Körpersprache einer Person, nicht gleichermassen wahrgenommen werden. Wird auf eine physische Befragung insistiert und diese z.B. mit Masken oder anderen Schutzmassnahmen durchgeführt, können freilich die für einen Befragenden wichtige Eindrücke wie etwa die Mimik verloren gehen. Hingegen kann die physische Distanz dem Befragten auch ein gewisses Sicherheitsgefühl vermitteln, dass ihn eher reden lässt. Die Erfahrung zeigt jedenfalls, dass virtuelle Befragungen verhältnismässig gut funktionieren und der Befragte rasch vergisst, dass er nicht vor Ort ist.

Auch sind die **Tücken der Technik** zu beachten. Nicht immer ist die Verbindung gut, was den Redefluss erheblich stören kann. Auch müssen beide Parteien über die entsprechende Infrastruktur verfügen (Computer, Webcam, Mikrofon).

Ein Risiko besteht ferner darin, dass der befragte Mitarbeiter nicht alleine an der Befragung teilnimmt oder die Vertraulichkeit nicht gewahrt ist. Ob sich noch eine zweite Person im Raum befindet, kann selbst durch das Einschalten der Webcam nicht gänzlich ausgeschlossen werden. Der Mitarbeiter sollte daher aufgefordert werden, zu bestätigen, dass er sich alleine in einem privaten Raum befindet und keine weiteren Personen mithören können. Ausserdem sollte die Befragung über einen **Einwahllink mit einmaligem Passwort** erfolgen, bei dem sichergestellt wird, dass keine unbefugten Personen zusätzlich teilnehmen können. Der „Befragungsraum" ist technisch für den Zuritt Unbefugter zu sperren.

Der zu befragende Mitarbeiter sollte darüber aufgeklärt werden, dass das **heimliche Aufzeichnen** der Befragung untersagt ist. Plant der Arbeitgeber seinerseits eine Aufzeichnung der Befragung, ist die ausdrückliche Erlaubnis des Mitarbeiters einzuholen. Ohnehin zeigen viele Videokonferenzsysteme allen Beteiligten an, wenn die Konferenz aufgezeichnet wird. Zu beachten ist, dass die Aufzeichnungen häufig nicht eine etwaige parallele Kommunikation via Chat erfassen.

Unter Umständen muss der Mitarbeiter bei einer Befragung mit gewissen **Dokumenten/Beweismitteln** konfrontiert werden und dazu Stellung nehmen. Dies kann per Screensharing erfolgen. Der Mitarbeiter sollte vorgängig darüber aufgeklärt werden, dass er die Dokumente weder kopieren, abfotografieren noch auf eine andere Weise einbehalten darf. Technisch kann dies allerdings kaum verhindert werden.

Literatur:

Naber, Sebastian/Ahrens, Tim: Remote Investigations: Die Aufklärung von Compliance-Verstössen im New Normal, Compliance Berater (CB) 2020, 465 ff.

Q40. Worauf kann ich bei der Formulierung meiner Fragen achten?

A: Erfolgreiches, investigatives Befragen ist keine Kunst, sondern vor allem Technik. Sie kann erlernt werden, denn die meisten Grundelemente und Methoden basieren auf **psychologischen Erkenntnissen**, wie wir Menschen in gewissen Situationen reagieren. Diese Verhaltensweisen sind gut bekannt und erprobt. Ihre Anwendung erfordert allerdings viel Übung und vor allem viel Aufmerksamkeit. Denn im Kern geht es darum, das Gegenüber zu beobachten, seine Signale zu deuten und darauf einzugehen. Die erfolgreichsten Befragungen sind oft ruhige, vertrauensvolle Gespräche, ohne Geschrei, ohne böse Worte und ohne unfreundlichen Ton.

Häufig wird empfohlen, eine zu befragende Person zu Beginn einer Befragung **selbst berichten zu lassen** ohne sie zu unterbrechen. Dies kann sinnvoll sein, wird aber dann scheitern, wenn die Person zunächst einmal selbst verstehen will, worum es geht und was von ihr erwartet wird. Möglicherweise ist sie eingeschüchtert oder misstrauisch und wird daher nicht von sich aus reden. Sie werden ihr vorgeben müssen, worüber sie sprechen soll. In solchen Situationen kann es helfen, die zu befragende Person auf ungefährliches, ihr gut vertrautes Terrain zu führen, um für Entspannung zu sorgen – falls Sie dies wollen. In einer Befragung sollten Sie allerdings nicht die Rolle des passiven Beobachters einnehmen und den Gesprächsverlauf dem Zufall überlassen oder von Thema zu Thema hüpfen. Sie sollten das Interview stattdessen **aktiv steuern** und dies nach einem Plan.

Eine der wichtigsten Grundtechniken für solche Befragungen ist eine Art thematisches **"Eintrichtern"** des Befragten: Begonnen wird mit offenen und unverdächtigen Fragen, die den Befragten allerdings immer mehr mit immer stärker fokussierten Fragen auf ein Zielthema hinsteuern. Der Befragte erkennt dies im Idealfall erst, wenn es bereits zu spät ist. Diesen Prozess wiederholen Sie als Befrager mit jedem Thema, das Sie im Interview abdecken wollen. Diese Vorgehensweise macht es für den Befragten sehr viel schwerer, Ihre Fragen oder Ihre Stossrichtung zu antizipieren und somit Ihre Bemühungen zu durchkreuzen. Ausserdem wird diese Technik den Befragten in der Beantwortung der Fragen auch disziplinieren. Dies ist wichtig, da Sie die Kontrolle über das Interview nicht verlieren wollen. Schliesslich sorgt das Eintrichtern auch für eine gewisse thematische Ordnung in der Befragung. Es lässt sich auf diese Weise Thema für Thema abarbeiten und es geht nichts vergessen.

Das Fragenstellen will allerdings gelernt und geübt sein. Insbesondere sollten Sie als Befrager die verschiedenen Fragetechniken bewusst einsetzen – oder auf bestimmte Fragen bewusst verzichten. In allen Fällen gilt: **Je kürzer und einfacher die Frage, desto besser.**

Die drei üblichen Fragetypen in Befragungen sind:

- **Offene Fragen** („Erklären Sie mir, was Sie an diesem Morgen getan haben"). Sie führen zu längeren Antworten, geben der befragten Person mehr Raum – auch abzuweichen und über für Sie irrelevante Dinge zu sprechen (und Sie damit ggf. zwingen,

die befragte Person zu unterbrechen). Die befragte Person wird sich aber in aller Regel wohler fühlen. Mit solchen Fragen sollten Sie beginnen und möglichst lange dabei bleiben. Sie sind insbesondere zu Beginn des „Eintrichterns" wichtig.

- **Die „W"-Fragen** („Wer hat Ihnen die Freigabe erteilt?"). Es sind Fragen nach dem Wer, Wie, Was, Wann, Wieviel, Wie oft oder Warum. Sie werden typischerweise zur Vertiefung einer Antwort auf eine offene Frage eingesetzt. Diese Fragen können Ihnen auch helfen, den Wert der befragten Person als Informationsquelle einzuschätzen.
- **Geschlossene Fragen** („War der Beleg von ihm unterzeichnet?"). Die möglichen Antworten sind vorgegeben (typischerweise „Ja" oder „Nein") und erfordern keine Erläuterung, auch wenn die befragte Person sie Ihnen womöglich trotzdem geben möchte. Solche Fragen kommen in der Regel zum Ende des „Eintrichterns" zum Zuge.

Fragen können auch nach ihrem **Zweck** unterschieden werden. So können sie benutzt werden, um eine Person zum Weiterreden zu ermuntern („Wie ging es weiter?"), um die Richtigkeit einer Aussage zu überprüfen (sie fragen nach nebensächlichen Dingen, die eine Person, welche die Wahrheit sagt, rasch beantworten können müsste, wie z.B. „Welches Sitzungszimmer hatten Sie für dieses Gespräch reserviert?") oder um eine Person zu leiten oder ihr die Antwort zu erleichtern („Ging es dabei um die Lieferung, den Rabatt oder aber etwas anderes?")

Während in einem Kreuzverhör vor Gericht normalerweise nur geschlossene Fragen verwendet werden, sind in internen Untersuchungen offene Fragen die Regel. Ausnahmen gibt es auch hier, etwa, wenn eine zu befragende Person nicht kooperieren will oder **sie offenkundig lügt** und der Lüge – auch gegenüber sich selbst – überführt werden muss, um ein offeneres Gespräch führen zu können.

Seien Sie sich beim Stellen Ihrer Fragen aber auch folgender für interne Untersuchungen heikle oder gar unzulässiger Fragen bewusst:

- **Suggestivfragen** („Ihnen war bewusst, dass Sie damit gegen die Richtlinie verstossen haben?", „Ihr Chef hat Ihnen keine Freigabe erteilt, richtig?"). Sie geben die von Ihnen erwartete Antwort der befragten Person vor. Diese Fragetechnik erzeugt Druck, was etwa bei nicht wahrheitsgemäss antwortenden Personen sinnvoll sein kann. Nutzen Sie sie beispielsweise um sich bisherige Aussagen des Befragten auf diese Weise von ihm bestätigen zu lassen. Aber setzen Sie solche Fragen nicht in zu hoher Dosis ein. Diese Art der Fragestellung kann aggressiv wirken, insbesondere, wenn sie versteckte Vorwürfe birgt.
- **Hypothetische Fragen** („Was werden Sie tun, wenn wir herausfinden, dass der Beleg von Ihnen unterzeichnet worden ist?"). Eine solche Frage führt bei einer zum Sachverhalt befragten Person höchstens zu Spekulationen und in aller Regel zu nichts, was Sie weiterbringt. Sie wollen wissen was war, nicht was sein könnte. Sinn

machen hypothetische Fragen nur bei einem Experten, den Sie in seinem Fachgebiet befragen („Wie wahrscheinlich ist es, dass diese E-Mail gefälscht wurde?"). Dasselbe gilt für Fragen basierend auf Annahmen.

- **Mehrfachfragen** („Wer war an der Sitzung dabei und wie lange? Wer hat den Antrag unterstützt?"). Der Befragte wird in der Regel nur eine der Fragen beantworten und Sie werden die restlichen Fragen erneut stellen müssen. *One fact per question* lautet eine eiserne Regel auch in Kreuzverhören. Sonst gibt es ein Durcheinander.
- **Unklare Fragen** („Haben Sie sich ihr gegenüber korrekt verhalten?"). Kann die Frage unterschiedlich verstanden werden (hier: was „korrekt" bedeutet), ist auch nicht klar, auf welches Verständnis sich die Antwort bezieht. Im besten Fall bemerken Sie den Interpretationsspielraum, im schlimmsten Fall reden Sie aneinander vorbei ohne es zu merken.
- **Irreführende Fragen**, in welchen Sie Fakten behaupten, die nicht zutreffen – sei es aus taktischen Gründen, sei es aus einem Versehen. Das kann eine von Ihnen zitierte angebliche Aussage einer anderen Person sein, ein behauptetes Beweismittel, über das Sie nicht verfügen oder eine rechtliche Qualifikation, die nicht zutreffend ist, aber den Befragten unter Druck setzt. Sie unterminieren damit ihre Glaubwürdigkeit und den Beweiswert der Antwort, den Sie damit allenfalls erzielen.

Achten Sie schliesslich auch darauf, dass vor allem **die befragte Person spricht**, und nicht nur Sie selbst erzählen.

Will die befragte Person gar nicht sprechen, so geben Sie nicht sofort auf. Bleiben Sie hartnäckig und gehen Sie Ihr Beweismaterial durch, legen Sie es der Person vor, stellen Sie Ihre Fragen. Sie sollten es der Person nicht einfach machen, sich vor der Befragung zu drücken. Sie können auf eine gestellte Frage ohne Weiteres auch eine oder zwei Minuten in Stille warten. Anhaltende Stille empfinden viele Befragte in dieser Situation als unangenehm und peinlich und werden sich daher möglicherweise überwinden, doch zu antworten. Darauf können Sie aufbauen, denn beginnt eine Person erst einmal zu sprechen, ist das Eis normalerweise gebrochen. Weigert sie sich standhaft, dann fassen Sie für das Protokoll jeweils zusammen, bei welchen Fragen sich die Person geweigert hat zu antworten.

Handelt es sich um die beschuldigte Person, so erklären sie ihr, dass ihre Befragung ihre (möglicherweise einmalige oder beste) Gelegenheit ist, ihre Sicht der Dinge zu präsentieren und auch **ihre Motivation zu erläutern**. Dieser letzte Punkt ist wichtig, denn auch viele Personen, die bewusst gegen Regeln verstossen haben, legen sich in der Regel eine Begründung bereit, die ihr Verhalten rechtfertigt oder weniger gravierend oder verwerflich erscheinen lässt – und sie haben ein Bedürfnis, darüber zu sprechen (dazu → **Q41**). Geben Sie den Personen diese Chance, und sie werden sie womöglich gerne ergreifen. In der Folge kann dann auch über den Sachverhalt gesprochen werden.

Bei solchen Gesprächen ist es allerdings von entscheidender Bedeutung, dass Sie als Befrager die befragte Person in ihrem Verhalten oder als Mensch **nicht erkennbar werten**. Sie werden das Vertrauen Ihres Gegenübers nicht gewinnen, wenn die Person den Eindruck erhält, dass Sie sie in ihrem Verhalten oder gar als Mensch abwerten oder verurteilen. Bleiben Sie neutral oder zeigen Sie Mitgefühl für eine Not, in welcher sich die befragte Person möglicherweise befand, und es wird Ihnen sehr viel einfacher fallen, in einem Gespräch mit der Person eine Beziehung aufzubauen und so Ihr Ziel zu erreichen.

Literatur:

Pozner, Larry S./Dodd, Roger: Cross Examination: Science and Techniques, Charlottesville, 1993

Wendler, Axel/Hoffmann, Helmut: Technik und Taktik der Befragung, Stuttgart, 2015

Q41. Was sind das für Menschen, die in den Unternehmen gegen Gesetze und andere Regeln verstossen?

A: Einige mögen zunächst an jene intelligenten und charismatischen Mitmenschen denken, die trotz ihrer narzisstischen, vielleicht sogar auch dissozialen Persönlichkeitsstörung gut in die Gesellschaft und das Unternehmen integriert sind, die deswegen als Manager, Verkäufer, Anwälte oder andere Führungspersonen und Geschäftemacher womöglich sogar besonders erfolgreich sind, sich aber **ohne schlechtes Gewissen über Regeln hinwegsetzen**, weil sie denken, diese gelten nur für die anderen. Oder wie es Josef Sachs, der als Begründer der forensischen Psychiatrie in der Schweiz gilt, formulierte: „Narzissten sind mitreissend, neigen aber zu Selbstüberschätzung und Allmachtsfantasien – wenn sie Gesetze übertreten, fühlen sie sich unverletzlich und vor Strafverfolgung gefeit".

Doch in einer internen Untersuchung können Sie auch ganz anderen Typen von Menschen begegnen, die gegen die Regeln verstossen haben. Einige Beispiele aus konkreten Fällen:

- Mitarbeiter, die mit einer kleinen Lüge, **mit einem geringen Fehltritt begonnen** haben, vielleicht geboren aus der Not oder einer Zwangslage, oder aus Neugier. Ihr Fehlverhalten ist dabei nicht aufgefallen, hat sich aber für sie ausgezahlt. Hatten sie zu Beginn noch Angst, entdeckt zu werden und ein schlechtes Gewissen, schwand dieses Gefühl über die Zeit zusehends und sie geraten immer tiefer in die Sache hinein, können nicht mehr zurück, finden sich immer mehr damit ab und werden womöglich in ihrem Verhalten bestärkt. Den einen oder anderen wird es zugleich belasten, mit niemandem offen über die Sache sprechen zu können, und tut dies darum vielleicht in Andeutungen. Kommt es zum Knall und bricht das Kartenhaus zusammen, fällt diesen Personen unter Umständen auch eine Last von den Schultern.

- Mitarbeiter, deren Ansichten oder Verhaltensweisen **nicht in die heutige Zeit passen** und sie sich daher in einer Art und Weise verhalten, die für Ihr Unternehmen nicht akzeptabel ist. Nicht alle werden einsichtig sein und verstehen, dass sie zwar anderer Meinung sein dürfen, sie sich in Ihrem Unternehmen jedoch trotzdem in einer bestimmten Art und Weise zu verhalten haben – wie auch immer dies zu werten ist.
- Mitarbeiter, die **ihre Arbeit gut machen** und womöglich auch die Erwartungen ihrer Vorgesetzten erfüllen wollen, die vielleicht unter beruflichem Druck stehen und sich so zu einem Verhalten hinreissen lassen, dass gegen die Regeln verstösst und möglicherweise sogar strafbar ist. Vielleicht sind diese Personen auch der Ansicht, dass ihr Fehlverhalten nicht so schlimm sein kann, weil „alle es machen" und sie ihre Arbeit sonst nicht korrekt erfüllen können. Im Bereich der Korruption, insbesondere wo es um Schmiergelder geht, werden Sie dieser Auffassung in bestimmten Ländern regelmässig begegnen – und sie ist sehr oft auch gut begründet. So kann es gut sein, dass in einer solchen Konstellation die ausführenden Mitarbeiter für sich selbst keine Vorteile im Blick haben, sondern sogar überzeugt sind, im Interesse des Unternehmens zu handeln, weil ihre Vorgesetzten sie diesbezüglich nicht richtig führen und sogar froh darüber sind, dass sie sich die Hände nicht selbst „schmutzig" machen müssen, aber davon profitieren.
- Mitarbeiter, die als **Hasardeure** unkalkulierbare Risiken eingehen, die beispielsweise primär ihren Abschluss oder ein Geschäft im Auge haben und der Ansicht sind, ein Regelbruch (Bestechung, Manipulation, etc.) kann nicht schaden und wird nicht auffliegen – dies nach dem Motto *"no risk, no fun"*.
- Mitarbeiter, die **aus einer Gefühlslage, Unachtsamkeit oder Fehleinschätzung** handeln, und daran glauben, dass das Verhalten (z.B. eine intime Beziehung) über einen gewissen Zeitraum möglicherweise auch „gut" geht oder „unter dem Radar" bleibt. Aufgrund veränderter Umstände oder einer anderen Entwicklung (z.B. einem Medienbericht, einer Beschwerde) nimmt die Sache aber eine Wendung, die das Unternehmen zum Handeln zwingt. Dem ansonsten möglicherweise tadellosen Mitarbeiter kann Naivität oder ein Fehlurteil vorgeworfen werden, aber nicht den Willen, dem Unternehmen zu schaden.
- Mitarbeiter, die sich vom Arbeitgeber zu Recht oder Unrecht **schlecht behandelt fühlen**, innerlich möglicherweise bereits gekündigt haben und daher auch nicht in einen Gewissens- oder Loyalitätskonflikt geraten, wenn sie gegen die Interessen des Arbeitgebers verstossen, Regeln brechen oder sich von ihm nehmen, was ihnen nach ihrer Ansicht zusteht – dies nach dem Motto der „ausgleichenden Gerechtigkeit" oder „es trifft keinen Falschen". Die gesetzlichen und arbeitsrechtlichen Bestimmungen, gegen die sie dabei verstossen, interessieren solche Mitarbeiter womöglich gar nicht.

Aufgeführt sind nur einige Profile der Persönlichkeiten, die in interne Untersuchungen verwickelt werden, weil sie sich in gewichtiger Weise falsch verhalten haben. Die beispielhafte Aufzählung soll verdeutlichen, dass unterschiedlichste Beweggründe und Anlässe hinter einem Fehlverhalten stehen können. Als untersuchende Person hat es sich bewährt, die **Motive der Personen nicht zu werten**. Ist Ihnen der Auftrag zur Untersuchung eines Sachverhalts aufgetragen, ist es nicht Ihre Aufgabe, über die von Ihnen allenfalls „überführten" Personen zu urteilen. So meint Sachs: „Wer sich während längerer Zeit in illegale Handlungen verstrickt, kann oft nicht mehr aussteigen, ohne sich einem Entdeckungsrisiko auszusetzen. Dann zimmert er die Realität so zurecht, dass er sich in einem günstigen Licht sehen kann. Das nennt man ‚kognitive Verzerrung'." Zeigen Sie Verständnis für eine Person, die sich zwar klar unkorrekt verhalten hat, dies aber aus ihrer Sicht aus vertretbaren Gründen getan hat. So steigt die Wahrscheinlichkeit, einen *Rapport* zu ihr aufzubauen und sie dazu zu bewegen, sich Ihnen in der Sache zu offenbaren. Ihre professionelle Distanz und Objektivität müssen Sie hierzu nicht aufgeben.

So unterschiedlich die Motive solcher Personen sind, so verschieden können auch ihre **Reaktionen auf eine interne Untersuchung** sein. Gewisse Personen werden die Untersuchung als Herausforderung wahrnehmen, andere wiederum werden sie auszusitzen versuchen und darauf hoffen, dass die Bedrohung möglichst rasch wieder verschwindet. Oder sie nehmen sie nicht ernst und sehen in ihr keine Gefahr. Besonderes Augenmerk sollten Sie auf jene richten, denen eine solche Untersuchung den Boden unter den Füssen wegzieht und damit ihre bisher sicher und geordnet erscheinende Welt mit einem Schlag zusammenzustürzen droht. Es wird ihnen plötzlich bewusst, in welcher Situation sie stecken – mit entsprechenden emotionalen Folgen. Verlieren sie ihren Job? Geraten sie gar in ein Strafverfahren? Was, wenn Freunde und Bekannte davon erfahren – von der eigenen Familie ganz zu schweigen? Werden sie je wieder eine Stelle finden? Ist alles, was über all die Jahre aufgebaut wurde, verloren? Weil hier selbst Gedanken an Selbstmord nicht selten sind, sollten Sie auf entsprechende Signale achten und bei Bedarf fachliche Unterstützung beiziehen. Die nüchterne Erkenntnis, dass auch für eine fehlbare Person die Welt mit ihrer Enttarnung nicht „untergeht", hilft ihr in einem solchen emotionalen Zustand leider erfahrungsgemäss oft nicht weiter.

In der Praxis ist immer wieder zu sehen, dass **Abgeltungssysteme** und vergleichbare Mechanismen zur Incentivierung (z.B. Beförderungen) nicht nur das zulässige Verhalten von Arbeitnehmern, sondern auch das Fehlverhalten beeinflussen können. So mag ein an sich redlicher Mitarbeiter für den Abschluss eines besonders grossen Auftrags, der ihm persönlich einen finanziellen Vorteil bringt, eher bereit sein, bezüglich der Einhaltung der Regeln und Vorschriften ein Auge zuzudrücken. Ein anderer wird dafür sogar absichtlich oder eventualvorsätzlich Vorgaben umgehen. Ist ein Abgeltungssystem auf kurzfristige Erfolge ausgerichtet, werden gewisse Mitarbeiter bereit sein, hohe Risiken für das Unternehmen

(und auch für sich) einzugehen, in der Hoffnung oder der Zuversicht, die Sache werde schon nicht „schief gehen". Kommt das Gefühl der Unverletzlichkeit des Narzissten hinzu, ist dies besonders gefährlich. Auch wenn die Mehrheit der Mitarbeiter redlich ist und versucht sein wird, Schaden vom Unternehmen abzuwenden, wird es ab einer bestimmten Betriebsgrösse immer auch Menschen geben, die eine andere Agenda haben. Bekanntgewordene Fälle der internationalen Bankenwelt haben hier schon Erstaunliches offenbart, so etwa Mitarbeiter, die nicht nur im grossen Stil Märkte für entsprechende Gewinne manipulierten, sondern sich auch in geschäftlichen Chats darüber unterhielten, obwohl sie wissen mussten, dass diese aufgezeichnet werden. Doch Vorsicht ist auch im „kleinen Rahmen" geboten, etwa bei *Sales*-Aktionen, in welchen Verkäufern für bestimmte Abschlüsse Prämien versprochen werden: Ist das Verkaufsteam hinreichend gross, werden Personen versucht sein, das System für ihre eigenen Zwecke zu missbrauchen und dabei auch nicht zurückschrecken, Kunden zu täuschen, um sie beispielsweise zu einem Abschluss zu bewegen. Hier ist es nicht nur wichtig, dass Unternehmen Massnahmen treffen, um solche Fälle frühzeitig zu erkennen, sondern auch zu prüfen, ob eine Begrenzung von Incentivierungen angezeigt ist – um die Gelegenheit zu verhindern, die „Diebe macht".

So oder so: Die arbeitsrechtliche Fürsorgepflicht gebietet es, dass Sie auch **mit fehlbaren Personen fair umgehen**. Dies bedeutet nicht, dass Sie in der Sache nicht genau, beharrlich und gründlich ermitteln. Es bedeutet mit der betroffenen Person respektvoll umzugehen und auf ihre berechtigten Bedürfnisse Rücksicht zu nehmen, so gut Sie dies ohne Gefährdung der Untersuchung tun können. Die Erfahrung zeigt etwa, dass für beschuldigte Personen die Ungewissheit, was ihnen genau vorgeworfen wird, was bekannt ist und was in der Sache und mit ihnen weiter geschehen wird, besonders belastend ist. Ungewissheit über den Ausgang einer internen Untersuchung und die Konsequenzen für die betroffene Person liegen zwar in der Natur der Sache, aber klare Informationen zum Verfahren, zum Zeitplan und zu den Zuständigkeiten, aber auch taktisch vertretbare Aussagen zum Sachverhalt, können eine Person wesentlich entlasten. Haben Sie den Eindruck, dass eine Person ihr Fehlverhalten bereut, dann geben Sie ihr die Gelegenheit, darüber zu sprechen. Dies mag die Sache nicht ungeschehen machen und für die Sachverhaltsermittlung nicht relevant sein, kann für die Person aber wichtig sein und dazu führen, dass sie in der Folge wesentlich besser an der Aufklärung des Sachverhalts mitwirkt. Als untersuchende Person sollten Sie sich allerdings davor hüten, aus Mitleid oder anderen Gründen Zusagen zu machen, die Sie nicht einhalten wollen oder können oder Ergebnisse vorwegzunehmen. Auch sollten Sie darauf achten, dass Fairness oder Mitgefühl nicht missbraucht wird, um Sie oder die Untersuchung zu manipulieren oder zu sabotieren. Hier ist viel Menschenkenntnis gefragt. In einer internen Untersuchung müssen die Zügel in Ihrer Hand bleiben.

Während in Organisationen ab einer gewissen Grösse schon statistisch gesehen Personen aller Art und Motivation anzutreffen sind, sind in einem internationalen Umfeld zusätzlich **kulturelle und gesellschaftliche Unterschiede** zu beachten.

So kann das Verständnis für die Sinnhaftigkeit und Wichtigkeit vom in der Schweiz gelebten Begriff der *Compliance* und die bei uns geltenden Regeln in anderen Ländern und Kulturen teils sehr unterschiedlich sein. Die Schweiz lag im *Corruption Perception Index* von Transparency International im Jahre 2020 weltweit auf Platz 3[28]. Es ist einfach, in Ländern wie der Schweiz auf die Einhaltung von Regeln zur Bekämpfung der Bestechung zu pochen. Wer jedoch in Ländern wie Indien (Platz 86), Brasilien (Platz 94) oder Russland (Platz 129) tätig ist, wird von anderen Erfahrungen berichten, was wiederum Auswirkungen darauf hat, wie wahrscheinlich es ist, dass sich die Mitarbeiter in den Niederlassungen eines Konzerns in diesen Ländern ebenfalls an die Vorschriften zur Bekämpfung von Korruption halten. Die Sichtweise derjenigen, die es nicht tun, mag aus unserer Sicht kurzsichtig sein, aber bösgläubig ist sie deswegen nicht zwangsläufig. Das ändert zwar nichts daran, dass ein Unternehmen gegen solches Fehlverhalten vorgeht, aber das Bewusstsein für die Haltung, Position und Alltagserfahrung einer Person kann für eine erfolgreiche Kommunikation mit ihr entscheidend sein.

Das gilt auch für andere kulturelle Unterschiede. Eine interessante Hilfestellung ist die *Cultural Dimensions*-Theorie des niederländischen Psychologen Geert Hofstede, welcher in sechs Faktoren zum Ausdruck bringt, wie sich die Kultur eines Landes auf die Werte seiner Einwohner und damit ihr Verhalten auswirkt[29]. Diese Faktoren können über eine Datenbank im Internet pro Land abgerufen und verglichen werden („*Culture Compass*“)[30]. So zeigt z.B. der Vergleich zwischen der Schweiz und Indien, dass der Wert für den Faktor *“Power Distance“*, welcher vereinfacht gesagt die Akzeptanz von Hierarchien zum Ausdruck bringt, in der Schweiz mit 34 weniger als halb so hoch ist wie in Indien mit 77.

Solche Aussagen sind natürlich zu verallgemeinernd, um sie gültig auf ein einzelnes Individuum zu übertragen. Sie können jedoch in der Kommunikation mit Menschen aus anderen Kulturen helfen und dazu beitragen, ihr Verhalten besser zu verstehen und auf sie einzugehen. Stammt z.B. ein zu befragender Zeuge aus einem Land, das seine Staatsmacht repressiv einsetzt, in welchem Gerichtsverfahren nicht fair sind und in dem seine Bürger bespitzelt werden, wird dieser möglicherweise weniger offen über den Fehltritt eines Arbeitskollegen sprechen als eine Person, die in der Schweiz aufgewachsen ist und davon ausgeht, dass ihm deswegen kein Unrecht widerfahren wird.

28 https://www.transparency.org/en/cpi/2020/index/nzl.
29 https://en.wikipedia.org/wiki/Hofstede%27s_cultural_dimensions_theory.
30 https://www.hofstede-insights.com/product/compare-countries/.

Literatur:

Babiak, Paul/Hare, Robert D.: Snakes in Suits: When Psychopaths Go to Work, New York, 2007

Benecke, Lydia: Sadisten – Tödliche Liebe – Geschichten aus dem wahren Leben, München, 2015

Haller, Reinhard: Die Narzissmusfalle, Anleitung zur Menschen- und Selbstkenntnis, Salzburg, 2019

Gedanken zum Thema.

Eine Befragung fängt für mich schon bei der Begrüssung an, ob an der Rezeption oder der Kaffeemaschine. Das Eis bricht und die Person fühlt sich als Mensch wahrgenommen und respektiert. Das ist die Basis und eine Gelegenheit, etwas über die Person zu erfahren. Natürlich sind eine gute Vorbereitung und die richtigen Fragen wichtig. Aber ebenso höre ich genau zu, nehme Anteil und versuche nicht zu werten. Damit gewinne ich Vertrauen und nicht selten nehmen Befragungen so Wendungen, die ich nicht erwartet habe. Allerdings können dies auch dramatische sein. In den bald 20 Jahren meiner Tätigkeit als Untersuchende versuchte sich bereits zwei Mal eine Person das Leben zu nehmen. Das hat mir deutlich vor Augen geführt, dass auch das Wohlergehen des Gegenübers davon abhängt, dass wir nicht nur auf seine Worte, sondern auch seine anderen Signale achten. Denn es sind alles Menschen, keine Maschinen.

Sandra Middel
Head of Group Compliance
Clariant

7. Überwachungsmassnahmen

Kurz gesagt

- Heimliche Überwachungsmassnahmen sind auch gegenüber Arbeitnehmern möglich, wenn es um ein hinreichend schweres Fehlverhalten geht, ein hinreichender Verdacht besteht und es kein milderes Mittel gibt.
- Wesentlich ist, dass die Massnahmen (z.B. Kameraaufnahmen) zeitlich und sachlich beschränkt sind und nicht das Verhalten des Arbeitnehmers an sich überwachen, sondern ein Fehlverhalten aufgeklärt oder dokumentiert wird.
- Sehen Sie Überwachungsmassnahmen in Ihren Reglementen und Hinweisen in allgemeiner Form vor und dokumentieren Sie den Entscheid zur Durchführung einer Massnahme.

Worum es geht

Überwachungsmassnahmen sind aus rechtlichen Gründen und aus Sicht der Fairness ein heikles Feld, denn eine Überwachung findet in aller Regel heimlich statt. Gemeint sind hier nicht laufende Überwachungsmassnahmen im Alltag (z.B. Internet-Sperren, Filter für Malware, Systeme zur *Data Loss Prevention*, Sicherheitskameras, Torkontrollen), deren Daten in einer internen Untersuchung ausgewertet werden. Vielmehr geht es um Massnahmen, die erst im Laufe einer internen Untersuchung lanciert werden, wie z.B. das Überwachen von Mitarbeitern durch elektronische Massnahmen im Betrieb, die Überwachung der Aktivitäten einer Person im Internet oder die Observierung einer Person durch einen Privatdetektiv.

Worauf zu achten ist

- Für eine heimliche Überwachung sind konkrete Verdachtsmomente auf ein schweres Fehlverhalten erforderlich, nicht bloss die Vermutung, dass da etwas nicht stimmt.
- Es gilt das Verhältnismässigkeitsgebot – jede legale Überwachung ist auf das zu beschränken, was nötig (das mildeste Mittel), geeignet und zumutbar ist.
- Der Privat- und Geheimbereich ist grundsätzlich tabu.

Apropos Tracker

Überwacht werden können natürlich nicht nur Personen, sondern auch Gegenstände (z.B. GPS-Tracker in einem Wertsachenbehälter). Dies ist unproblematisch, solange kein Personenbezug besteht (problematisch: GPS-Überwachung eines Firmenfahrzeugs, das immer von derselben Person benutzt wird).

- Eine Überwachung des Verhaltens von Arbeitnehmern ist höchstens vorübergehend und an bestimmten Stellen erlaubt, d.h. sie muss zeitlich und sachlich beschränkt sein.
- Gut ist, wenn vorgängig auf die grundsätzliche Möglichkeit einer Überwachung hingewiesen worden ist. Auf die konkrete Überwachung muss hingegen nicht spezifisch hingewiesen werden, da sie dadurch typischerweise vereitelt wird.
- Erhoben werden darf nur, was die Eignung des Mitarbeiters betrifft oder für die Durchführung des Arbeitsverhältnisses nötig ist (Arbeitsplatzbezug).
- Von einer Person ohne Einschränkung publizierte Daten (z.B. in öffentlichen Social-Media-Profilen[31]) dürfen grundsätzlich benutzt werden.

Das **Bundesgericht** beschäftigte sich wiederholt mit der Überwachung am Arbeitsplatz. 2009 befand es über eine **heimliche Videoaufnahme** des Kassenbereichs im Hinterzimmer eines Uhren- und Juwelengeschäfts, um Diebstähle einer Mitarbeiterin aufzudecken (BGer 6B_536/2009 vom 12. November 2009). Weil die Videoüberwachung die Angestellten nur „sporadisch und während kurzer Zeit“ aufgezeichnet und „nicht das Verhalten der Arbeitnehmer am Arbeitsplatz über längere Zeit überwacht“ hat, erachtete sie das Bundesgericht nicht als geeignet, die Gesundheit und das Wohlbefinden der Arbeitnehmer zu beeinträchtigen. Das Bundesgericht beurteilt sie deshalb nicht als Verstoss gegen Art. 26 Abs. 1 → **ArgV3**, welcher Verhaltensüberwachungen in solchen Fällen verbietet. Es erachtete die Videoüberwachung im Übrigen auch unter dem Titel des DSG, Art. 28 ZGB, Art. 328 OR und Art. 328b OR für zulässig. Das Bundesgericht bestätigte diesen Entscheid kurz danach im Fall eines Privatdetektivs, der Aufnahmen eines Mitarbeiters erstellte, wobei meist nur seine Hände und ein Kassengerät im Bild waren – es befand, es gehe nicht um Verhaltensüberwachung, sondern dem Schutz vor Diebstählen und Veruntreuung (BGer 9C_785/2010 vom 10. Juni 2011, E. 6.5). Eine vorgängige Mitteilung sei nicht erforderlich (E. 6.7.3). In BGE 138 V 125

Auch die Polizei

… darf einen Arbeitnehmer zwecks Überführung einer Straftat nicht einfach am Arbeitsplatz überwachen, selbst wenn der Arbeitgeber eingewilligt hat. Dies muss auch vom Zwangsmassnahmegericht genehmigt sein (BGE 145 IV 42).

31 Öffentlich ist ein Profil dann, wenn es von einer unbeschränkten Zahl an Personen eingesehen werden kann. Eine Pflicht zur Anmeldung auf der betreffenden Plattform steht dem nicht entgegen.

führte das Bundesgericht ebenfalls aus, dass zwar über eine präventive Videoüberwachung informiert werden muss, sie aber dann nicht nötig ist, wenn es darum geht, ein Fehlverhalten aufzuklären, weil die Information der Massnahme zuwiderlaufen würde. In BGE 139 II 7 musste es über den Einsatz von **Spyware** entscheiden, die gegen einen Mitarbeiter eingesetzt wurde, der im Verdacht stand, seine Arbeitszeit und Bürocomputer für private Angelegenheiten zu nutzen. Die Software fertigte über drei Monate lang regelmässige Screenshots seiner Tätigkeiten an, darunter auch von privaten und streng vertraulichen Angelegenheiten. Dies wurde als verbotene Verhaltensüberwachung und in jedem Fall als unverhältnismässig erachtet. Die **Analyse von Protokollen des Internet-Verkehrs** und des E-Mail-Verkehrs hätte genügt, wo Sperrmassnahmen nicht ihr Ziel erreicht hätten. Mit einer solchen Sperrmassnahme beschäftigte sich das Bundesgericht 2017 in BGE 143 II 443, wo es allerdings um einen öffentlich-rechtlichen Betrieb und eine spezielle gesetzliche Regelung ging, die vor dem Entscheid einer personenbezogenen Auswertung der Internet-Zugriffe eine anonyme Analyse erfordert, bis ein Missbrauch klar feststeht (hier: Pornografie am Arbeitsplatz). Das Obergericht des Kantons Zürich erachtete 2019, die bei einer **routinemässigen Kontrolle eines Geschäftshandys** gefundenen **privaten WhatsApp-Chats** als unzulässiges Beweismittel (für eine fristlose Kündigung wegen Ehrverletzung, Geheimnisverrat, Mobbing), da die Datenbeschaffung weder die Eignung der betroffenen Mitarbeiterin betraf, noch für die Durchführung des Arbeitsverhältnisses (Art. 328b OR) nötig war, da es der Arbeitgeberin nicht um die Prüfung geschäftlicher Kommunikation ging (OGer ZH LA180031-O/U vom 20. März 2019). Offengelassen wurde die Frage, ob die Arbeitgeberin bei konkretem Verdacht hätte prüfen dürfen. In BGE 130 II 435 erlaubte das Bundesgericht 2004 den Einsatz eines **GPS-Lokalisierungssystems** im Firmenwagen eines Wartungstechnikers von Feuerlöschern, weil es dem Unternehmen eine gewisse Kontrolle der Qualität seiner Dienstleistung erlaubte, die wiederum auch im öffentlichen Interesse stand (Vermeidung defekter Feuerlöscher). Wichtig war, dass die Überwachung sich nur auf das Fahrzeug und nicht auf den Mitarbeiter bezog und nicht dauerhaft dessen Verhalten überwachte, sondern nur einen Aspekt, und dies zudem auch nur nachträglich (keine Verfolgung in Echtzeit). Ähnlich argumentierte das Bundesgericht 2011 (BGer 2C_116/2011 vom 29. August 2011) mit Bezug auf ein GPS-Lokalisierungssystem in Taxis, weil es nur die Bewegungen des Taxis registrierte und der Chauffeur das System ausserhalb seines Dienstes abschalten konnte. Auch der **Europäische Gerichtshof für Menschenrechte** (EGMR) beschäftigte sich mit der Überwachung am Arbeitsplatz. 2017 befand er (EGMR 61496/08 vom 5. September 2017), dass Mitarbeiter über die grundsätzliche Möglichkeit einer Überwachung informiert sein müssen (um sich darauf einzustellen), dass Überwachungsergebnisse nur zur

Durchsetzung der Regeln verwendet werden dürfen, dass es eines gewichtigen Grundes für die Überwachung bedarf (konkreter Verdacht, nicht bloss grundsätzliche Gefahr eines Fehlverhaltens) und die Massnahme verhältnismässig sein muss (insbesondere muss das mildeste Mittel gewählt werden).

Wie vorzugehen ist

1. **Sie möchten eine Überwachung durchführen oder Ergebnisse einer Überwachung nutzen.** Überwachungsmassnahmen sind im Schweizer Recht vor allem dann heikel, wenn sie:

   - heimlich erfolgen (Verstoss gegen den Grundsatz der Transparenz im Datenschutz),
   - Arbeitnehmer betreffen (Schutz des Arbeitnehmers im Arbeitsrecht und Datenschutz) oder
   - den Privat- oder Geheimbereich einer Person tangieren (Schutz der Privatsphäre).

   Andere Überwachungsmassnahmen (z.B. die Aufzeichnung einer gut sichtbaren Sicherheitskamera an einem sensiblen Ort) sind weitgehend unproblematisch. Zwar unterliegt auch die Verwendung deren Ergebnisse datenschutzrechtlichen Grenzen (wie dem Grundsatz der Verhältnismässigkeit und Zweckbindung), sobald sie Rückschlüsse auf eine bestimmte Person zulassen. Sie sind aber sehr viel einfacher möglich als in den drei erwähnten Fällen. Zu den rechtlichen Folgen einer unzulässigen Überwachung vgl. → **Q42**.

   Auch die **Sichtung des Inhalts des E-Mail-Postfachs** oder des Notebooks eines Mitarbeiters oder seines Schranks wird umgangssprachlich teils als „Überwachung" verstanden. Das ist hier aber nicht gemeint, denn die Aufzeichnung der Daten erfolgte nicht zu Überwachungszwecken, sondern wird lediglich rückwirkend zur Aufklärung eines Fehlverhaltens ausgewertet. Die eingangs genannten Massnahmen stellen der Natur nach eine Spurensuche dar, wobei auch in der Rechtsprechung nicht klar differenziert wird. Mit Überwachung ist hier die **zielgerichtete, systematische Beobachtung** einer Person durch einen Dritten gemeint. Freilich ist der Datenschutz auch bei der Spurensuche zu beachten. Zur Durchsuchung von Mailboxen → **Q18**.

2. **Haben Sie einen berechtigten Anlass für die Überwachung?** Auf heikle, personenbezogene Überwachungsmassnahmen sollten Sie grundsätzlich nur dann

zurückgreifen oder abstellen, wenn ein konkreter Verdacht besteht, dass ein relevantes Fehlverhalten seitens der Person vorliegt, um die es in der Überwachung geht. Ein blosses Gerücht, ein Bauchgefühl oder die bloss grundsätzliche Wahrscheinlichkeit, dass ein Fehlverhalten vorliegen könnte, rechtfertigt eine Überwachung nicht. Nicht zulässig sind daher z.B. die stichprobenweise Beauftragung eines Privatdetektivs, um mögliche Blaumacher zu überführen, oder die Durchsuchung der E-Mails aller Mitarbeiter nach Lästermails im Sinne einer „Rasterfahndung". Wird ein Mitarbeiter, der angeblich das Bett hüten muss, hingegen von einem Arbeitskollegen im Ausgang angetroffen, genügt dies als Anfangsverdacht. Das mutmassliche Fehlverhalten muss geschäftsbezogen und von gewissem Gewicht sein; Strafbarkeit ist nicht nötig – ein schwerer Verstoss gegen die Treuepflicht genügt.

Quellen?

- Internet-Zugriffslogs
- Videokameras
- Aufzeichnung von Kommunikation
- Datentransfers
- Verbindungsdaten
- Observation
- Observation im Netz
- GPS-Tracker

3. **Haben Sie einen guten Grund für die Überwachung?** Ein Grund kann sein, dass Sie noch einen bestimmten Beweis benötigen. In diesem Falle sollten Sie angeben können, welchen Aspekt Sie mit der Überwachung genau beweisen können möchten. Eine *"Fishing Expedition"*, also eine *unspezifische* Überwachung in der Hoffnung, dass sich vielleicht irgendetwas Belastendes ergibt, wird normalerweise nicht zulässig sein. Steht das Fehlverhalten schon fest, kann es allenfalls erforderlich sein, mittels Überwachungsmassnahmen dessen Ausmass festzustellen oder zu klären, ob es noch andauert, um weitere, beteiligte Personen zu ermitteln. Überwachungsmassnahmen können auch erforderlich sein, um weiteres Fehlverhalten zu verhindern (z.B. den Diebstahl von weiteren Geschäftsgeheimnissen), wenn es aus ermittlungstaktischen Gründen noch nicht möglich ist, den Mitarbeiter freizustellen, zu sperren oder sonst eine für ihn erkennbare Schutzmassnahme zu treffen.

4. **Erscheint die Überwachung wirklich erfolgsversprechend?** Die Eignung einer Datenerhebung für den vorgesehenen Zweck ist Teil des Verhältnismässigkeitsgebots, wie es im Datenschutz und Arbeitsrecht gilt. Sie sollten aufzeigen können, warum Sie eine berechtigte Erwartung haben, dass die ins Auge gefasste Überwachungsmassnahme auch tatsächlich dem Grund für die Überwachung gerecht wird, also z.B. den noch benötigten Beweis liefert. Eine Person zu observieren bringt höchstens dann etwas, wenn aus dem, was zulässigerweise an Informationen in einer Observation gewonnen werden kann, etwas für den Fall abgeleitet werden kann (z.B. nützt eine Observation nichts, wenn sich mit ihr zwar feststellen lässt, welche Menschen die Zielperson in der Öffentlichkeit trifft, nicht aber, wozu

oder was sie mit diesen bespricht, es aber genau darauf ankommt. Geht es hingegen darum, eine Verbindung oder Beziehung zwischen zwei Personen zu belegen, kann das Foto beim gemeinsamen Mittagessen genügen).

Für eine einfache Observation durch einen Privatdetektiv (z.B. für die Klärung der Frage, ob jemand tatsächlich zu Hause bleibt, etwa im Home Office) ist mit Kosten um die CHF 1'750 pro Tag zu rechnen (inklusive Nebenkosten).

5. **Ist die Überwachung die mildeste Massnahme?** Auch dies ist Ausfluss des Verhältnismässigkeitsgebots. Sie müssen zeigen können, dass es keine weniger invasive und die Persönlichkeit der betroffenen Personen weniger tangierende Möglichkeiten gegeben hätte, um an die erforderlichen Nachweise zu gelangen – wie im eingangs zitierten Spyware-Fall: Statt einer Überwachung mittels Spyware hätte die Auswertung der Internet-Zugriffsprotokolle genügt um zu zeigen, dass ein Mitarbeiter während der Arbeitszeit ständig private Webseiten benutzt.

Eine Überwachung kann auch **andere Personen tangieren**. Auch diese sind in ihrer Persönlichkeit und ihrer Privatsphäre geschützt. Sie sollten solchen „Beifang" so weit wie möglich reduzieren.

6. **Ist diese Massnahme für sich gesehen zulässig?** Abgesehen von der datenschutzrechtlichen Zulässigkeit der Erhebung von Personendaten im Rahmen einer Überwachungsmassnahme sollten Sie sich fragen, ob die Massnahme an sich rechtlich verpönt ist. Von einer solchen Massnahme sollten Sie die Finger lassen.

Das Anbringen eines GPS-Trackers an ein öffentlich parkiertes Fahrzeug ist für sich gesehen in der Regel nicht strafbar, aber das **Abhören** fremder Gespräche, das **Aufzeichnen eigener Gespräche** ohne Zustimmung der Beteiligten oder **Aufnahmen des Privat- oder Geheimbereichs** anderer Person sind beispielsweise strafrechtlich sanktioniert[32]. Überreden Sie einen Provider oder sonst jemand dazu, Ihnen geheime Informationen zu verraten, kann dies eine strafbare Anstiftung zum **Geheimnisverrat**[33], ein verbotenes **Auskundschaften** von Geschäftsgeheimnissen[34] oder unerlaubtes → **Beschaffen von Personendaten** sein[35]. Mit der Revision

32 Art. 179bis, Art. 179ter und 179^{quater} StGB.
33 Art. 162 und 321 ff. StGB.
34 Art. 5 → **UWG**.
35 Art. 179^{novies} StGB.

des Datenschutzgesetzes wird der Tatbestand der unbefugten Datenbeschaffung sowie ein allgemeines Berufsgeheimnis geschaffen und auch der **Identitätsmissbrauch** unter Strafe gestellt. Auch das **Eindringen in fremde Computersysteme** ist natürlich verboten[36].

7. **Wurde über die Möglichkeit einer solchen Massnahme informiert oder ist sie intern geregelt?** Ein wichtiges Element zum Schutz betroffener Personen ist Transparenz. Wurden Arbeitnehmer oder andere betroffene Personen darauf hingewiesen, dass sie grundsätzlich in einer bestimmten Weise überwacht werden können, falls sich die Notwendigkeit in einer internen Untersuchung ergeben sollte, ist der Eingriff in die Persönlichkeit durch die Überwachung bereits weniger gewichtig, weil sich die Personen darauf einstellen können. Prüfen Sie, ob Ihre internen Ankündigungen oder Regelungen die von Ihnen ins Auge gefasste Überwachung regeln, erlauben oder ausschliessen. In den meisten Unternehmen ist das höchstens bei der IT- und Internet-Überwachung, allenfalls auch bezüglich von Fahrzeugen und mobilen Geräten der Fall.

   Die Durchführung der hier diskutierten Überwachungen verletzt *per se* die Persönlichkeit einer betroffenen Person, weil sie heimlich erfolgt und somit den **Grundsatz der Transparenz** (Art. 4 Abs. 2, 3 und 4 DSG) verletzt. Sie sind also auf einen → **Rechtfertigungsgrund** angewiesen (Art. 13 Abs. 1 DSG). Je gewichtiger die Verletzung ist, desto schwerer wird Ihnen die Rechtfertigung fallen. Aufnahmen von Dashcams sind aus diesem Grund kaum beweisverwertbar (BGE 146 IV 226). Je besser Sie **vorab über die Möglichkeit der Überwachung informieren**, desto besser sind daher Ihre Chancen, dass die Ergebnisse der Überwachung verwertbar sind.

8. **Kann der Arbeitsvertrags- oder Geschäftsbezug begründet werden?** Sie werden eine Überwachung eines Mitarbeiters nur rechtfertigen können, wenn es um ein für das Unternehmen geschäftlich relevantes Fehlverhalten geht. Was geschäftlich relevant ist, hängt wiederum von der Funktion und Stellung der betroffenen Person ab. Für Arbeitnehmer muss zudem gezeigt werden, dass die Informationen, die Sie mit der Überwachung eines Arbeitnehmers gewinnen wollen, dessen Eignung für das Arbeitsverhältnis betrifft oder für die Durchführung des Arbeitsvertrags erforderlich ist (Art. 328b OR[37]). Letzteres umfasst allerdings auch die Einhaltung

36 Art. 143 f. StGB.

37 Nach der hier vertretenen Ansicht kann eine Verletzung dieses Grundsatzes durch ein überwiegendes Interesse gerechtfertigt werden, doch ist dies umstritten.

von Gesetzen und die dem Arbeitnehmer zulässigerweise auferlegten Verhaltensregeln.

9. **Tangiert die Überwachung den Privat- oder Geheimbereich der Person?** Trotz geschäftlichem Bezug einer Überwachung kann diese den Privat- oder Geheimbereich einer Person tangieren. Steht eine sexuelle Belästigung durch entsprechende Kurzmitteilungen eines Arbeitnehmers im Raum, so mögen diese geschäftlich relevant sein, weil sie im Kontext einer geschäftlichen Beziehung erfolgten, aber privater Natur sind sie trotzdem. Auch der Mitarbeiter, der sich Firmendokumente an seine private E-Mail-Adresse versendet, der die private Mobiltelefonnummer des Mitarbeiters eines Konkurrenten zwecks Absprache von Angebotspreisen anruft oder der in einem halb-öffentlichen Devisenhandels-Chat mit seiner neusten Eroberung prahlt, bringt private Elemente in eine geschäftlich relevante Kommunikation ein. Ist dies der Fall, sind je nach Fall zum Schutz der Privatsphäre der betroffenen Personen besondere Massnahmen zu treffen, wie etwa die Sichtung durch unabhängige Personen (→ **Q19**). Von solchen privaten Aktivitäten im geschäftlichen „Raum" abgesehen, dürfen Überwachungsmassnahmen nicht in den Privat- oder Geheimbereich der Person eindringen. Das gilt auch bei Observationen: Beobachtungen in der Öffentlichkeit (alles, was von öffentlichen Strassen und – mit gewissen Ausnahmen – in für das Publikum öffentlich zugänglichen Gebäuden frei zu sehen oder einzusehen ist) sind im Rahmen der Verhältnismässigkeit (mildestes Mittel) bei begründetem Verdacht (z.B. berechtigte Zweifel an korrektem Verhalten eines Arbeitnehmers) grundsätzlich erlaubt[38]. Normalerweise nicht erlaubt ist es hingegen, sich Zugang zum Privat- oder Geheimbereich einer Person zu verschaffen[39]. Das gilt übrigens auch online, etwa indem sich jemand durch *"social engineering"* Zugang zum privaten Kreis eines Social-Media-Profils verschafft. Private E-Mail-Konten und Computer sind ebenfalls tabu.

Private Konten?

An private Computer, E-Mail- und Cloud-Konten dürfen Sie nicht ran. Es gibt zwei Ausnahmen: Sie haben die Erlaubnis des Inhabers. oder die Staatsanwaltschaft gelangt in einem Strafverfahren an diese Daten und Sie erhalten über Akteneinsicht Zugang dazu. Das dauert aber oft länger, als Sie warten können: → **Q20**.

38 Hier bietet es sich an, sich an die Praxis des Bundesgerichts zur Zulässigkeit der Überwachung von Versicherungsnehmern durch private Versicherer anzulehnen (BGE 136 III 410, E. 4.1; Entscheid BGer 4A_110/2017 vom 27. Juli 2017, E. 5.2).

39 Vgl. hier auch Art. 179^{quater} StGB.

Trägt eine Person ihr Privatleben **von sich aus in die Öffentlichkeit** (z.B. auf einem Social-Media-Profil), so dürfen diese Informationen datenschutzrechtlich in der Regel verwendet werden, solange die Person dem nicht widerspricht (Art. 12 Abs. 3 DSG). Im Falle eines Arbeitnehmers gilt allerdings auch diesbezüglich, dass die Erhebung solcher Informationen nötig sein muss, um die Eignung des Mitarbeiters zu beurteilen oder um den Arbeitsvertrag durchzuführen (Art. 328b OR). Ob überwiegende Interessen eine Verletzung dieses Grundsatzes rechtfertigen können, ist umstritten.

10. **Ist die Überwachung sachlich, örtlich und zeitlich auf das Mindestmass beschränkt?** Aus dem Verhältnismässigkeitsgebot und den arbeitsrechtlichen Vorgaben ergibt sich weiter, dass eine Überwachung weder allgegenwärtig noch andauernd erfolgen darf. Sie müssen begründen und zeigen können, dass die Überwachung in jeder Hinsicht auf das Minimum beschränkt und ggf. auch frühzeitig abgebrochen wurde bzw. wird, wenn die nötigen Beweise vorliegen oder die Überwachung aussichtslos erscheint. Sie müssen und dürfen den Internet-Verkehr einer Person nicht über Monate auswerten, wenn bereits die Daten einer Woche genügen, um den Sachverhalt aufzuklären. Ist Rohmaterial (oder „Ausgangsmaterial“) nicht beweisrelevant, ist es zu löschen, sobald dies feststeht.

11. **Haben Sie den Zugang zu den Ergebnissen beschränkt?** Stellen Sie sicher, dass nur jene Personen Zugang zu den Überwachungsergebnissen erhalten, die diesen unbedingt brauchen. Das beweisrelevante Rohmaterial sollte noch weniger Personen zugänglich sein, muss sicher und nach der Auswertung für keine weiteren Personen zugänglich verwahrt werden[40]. Die ausgewerteten Ergebnisse sind so aufzubereiten, dass die Persönlichkeit und Privatsphäre der betroffenen Personen möglichst gut gewahrt wird, d.h. fremde Personen und private Elemente sind unkenntlich zu machen.

Privacy Filter

Kommen Videokameras am Arbeitsplatz zum Einsatz, so sind sie so auszurichten, dass die Arbeitnehmer normalerweise nicht erfasst werden. Ist das nicht möglich, kann mit sog. Privacy Filtern gearbeitet werden, d.h. Stellen im Bild, welche die Software automatisch abdeckt.

12. **Wie wäre die Reaktion der Belegschaft, Kunden und Öffentlichkeit, wenn sie davon erfährt?** Die rechtlichen Rahmenbedingungen sind das eine; in bestimmten Fällen ist eine Überwachung von Mitarbeitern durchaus zulässig. Sie sollten sich

40 Eine besondere Verschlüsselung wird in einem ordnungsgemäss gesicherten Firmennetzwerk normalerweise genügen. Muss aufgrund der Brisanz der Sache verhindert werden, dass auch die IT-Abteilung zugreifen kann, ist mit einer zusätzlichen Verschlüsselung zu arbeiten.

aber auch die Frage stellen, wie die Belegschaft, die Kunden und die Öffentlichkeit darauf reagieren würden, wenn sie von der Überwachung erfährt. Werden sie die Massnahme als verhältnismässig erachten? Der Reputationsschaden kann wesentlich schwerer wiegen als die rechtlichen Konsequenzen.[41]

13. **Dokumentieren Sie die Antworten auf die obigen Fragen.** Wollen Sie die aus einer Überwachung gewonnenen Erkenntnisse als Beweismittel in einem Verfahren verwenden können, so müssen Sie zeigen, dass Sie sie rechtmässig beschafft haben. Das können Sie nur, wenn Sie zeigen, dass die genannten Voraussetzungen erfüllt waren. Eine Aktennotiz ist schon mehr, als es in manchen Fällen gibt.

14. **Eine Überwachung kann auch entlasten.** Wenn Sie im Rahmen einer Untersuchung eine Überwachung durchführen, so werden Sie dies in Ihrem Bericht offenlegen und begründen müssen. Sie müssen damit rechnen, dass betroffene Personen Einsicht in die Überwachungsergebnisse verlangen. Konnte die Überwachung einen Verdacht nicht erhärten, müssen Sie damit rechnen, dass die verdächtigte Person dies als Entlastungsbeweis verwenden wird – auch wenn Sie der Ansicht sein mögen, dass die Überwachung ergebnislos war und möglicherweise ein anderes Resultat gezeitigt hätte, hätte sie länger angedauert oder wäre sie tiefer gegangen.

41 Vgl. etwa der Fall der Beschattungsaffäre einer Schweizer Grossbank im Jahr 2019/2020 die Beiträge von srf.ch: https://bit.ly/2MsKgYk und https://bit.ly/3o8l3Av.

Do's	Don'ts
• Informieren Sie die Belegschaft über die grundsätzliche Möglichkeit einer Überwachung (z.B. in einer Datenschutzerklärung oder einem Reglement). • Überwachen Sie nur, wenn es keine für die betroffene Person mildere Massnahme gibt, um die nötigen Informationen zu erlangen. • Beschränken Sie eine Überwachung auf das, was wirklich nötig und erfolgsversprechend ist – Sie können sie immer noch ausweiten. • Halten Sie die Ergebnisse einer Überwachung unter Verschluss – Zugang nur für jene, die ihn wirklich brauchen.	• Überwachen Sie eine Person nicht ohne einen konkreten Anfangsverdacht gegen eben diese Person vorweisen zu können. • Überwachen Sie nicht wegen Lappalien. • Setzen Sie keine Spyware oder dergleichen ein. Diese wird (fast) nie zulässig sein. • Keine „*fishing expeditions*"; Sie riskieren ein Beweisverwertungsverbot.
• Eine Überwachung ist eine sehr weitgehende Massnahme. Rechtliche Begründungen zur Durchführung finden sich meistens. Hören Sie aber auch auf Ihr Bauchgefühl: Ist die angedachte Massnahme fair und legitim?	

Wann Sie externe Unterstützung beiziehen sollten

- Wenn eine Überwachung vermutlich den **Privat- oder Geheimbereich** der überwachten oder einer anderen Person tangiert.
- Für **Observationen**.
- Wenn Sie **behördliche Unterstützung** zur Durchführung einer Überwachung benötigen (z.B. Strafverfahren).
- Wenn Sie **unsicher** sind, wie Sie konkret vorgehen sollten, ob eine Überwachung zulässig und wie sie zu begründen oder zu dokumentieren ist.
- Wenn Ihnen Ihr **Bauchgefühl** sagt, dass die Überwachung keine gute Idee ist.

Häufige Fragen und Antworten

Q42. Was sind die rechtlichen Folgen einer unzulässigen Überwachung eines Mitarbeiters?

A: Die unzulässige Überwachung eines Mitarbeiters kann für den Arbeitgeber zahlreiche rechtliche Konsequenzen nach sich ziehen. Zum einen kann rechtswidrig erworbenes Material in einem allfälligen Straf- oder Zivilverfahren als Beweismittel nicht verwertet werden (**Beweisverwertungsverbot**), es sei denn, das Gericht lässt es wegen überwiegendem Interesse an der Wahrheitsfindung ausnahmsweise zu. Wird gestützt auf eine unzulässige Überwachung eine fristlose Kündigung ausgesprochen, kann der betroffene Mitarbeiter sich dementsprechend zur Wehr setzen. So urteilte das Bundesgericht, dass die Ergebnisse einer unzulässigen Überwachung durch eine **Spyware** nicht verwertet werden können und die Grundlage einer in der Folge ausgesprochenen fristlosen Kündigung damit nicht belegbar sei (BGE 139 II 7).

Der Arbeitgeber verletzt durch die unzulässige Überwachung arbeitsvertragliche Pflichten, Persönlichkeitsrechte des Mitarbeiters sowie Bestimmungen des Datenschutzrechts. Bei Vorliegen eines Schadens kann er dafür **schadenersatzpflichtig** werden, wobei sich die Beträge allerdings eher im symbolischen Bereich bewegen.

Möglich sind ebenfalls **aufsichtsrechtliche Konsequenzen**, wenn sich der → **EDÖB** einschaltet, z.B. aufgrund einer Meldung durch den Mitarbeiter über die unzulässige Überwachung. Der EDÖB kann den Sachverhalt weiter abklären und derzeit Empfehlungen abgeben (bzw. sie bei Nichtbefolgung „einklagen“). Künftig wird er selbst Verfügungen betr. unzulässige Datenbearbeitungen erlassen können.

Schliesslich sind auch **strafrechtliche Konsequenzen** aufgrund von strafbaren Handlungen gegen den Geheim- und Privatbereich möglich, vor allem, wenn Gespräche aufgenommen werden oder der Geheim- oder Privatbereich durch Aufnahmegeräte tangiert wird (vgl. insbesondere Art. 179 ff. StGB). Die Observation im öffentlichen Bereich ist jedoch grundsätzlich *strafrechtlich* nicht relevant, auch nicht das Verfolgen eines Fahrzeugs mit einem GPS-Tracker.

Nützliche Links

Für ergänzende Informationen zur Überwachung von Mitarbeitern am Arbeitsplatz haben der EDÖB sowie das SECO Merkblätter publiziert:

- EDÖB: Leitfaden Internet- und E-Mailüberwachung am Arbeitsplatz (Privatwirtschaft), 2013 (Download: www.edoeb.admin.ch > Datenschutz > Dokumentationen > Leitfäden > Internet- und E-Mailüberwachung am Arbeitsplatz)
- SECO: Technische Überwachung am Arbeitsplatz, 2015 (Download: www.seco.admin.ch > Publikationen & Dienstleistungen > Arbeit > Arbeitsbedingungen > Broschüren und Flyer)
- SECO: Checkliste Überwachung der Arbeitnehmenden am Arbeitsplatz (Download: www.seco.admin.ch > Publikationen & Dienstleistungen > Arbeit > Arbeitsbedingungen > Checklisten)

Literatur:

Meier-Gubser, Stefanie: Mitarbeiterüberwachung: Rechte, Pflichten und Verbote, der Treuhandexperte (TREX) 2020, 286 ff.

Wolfer, Simon: Die elektronische Überwachung des Arbeitnehmers im privatrechtlichen Arbeitsrechtsverhältnis, Zürich/Basel/Genf 2008

Wantz, Simona/Licci, Sara: Arbeitsvertragliche Rechte und Pflichten bei internen Untersuchungen, Jusletter vom 18. Februar 2019, Rz. 1 ff.

Q43. Worauf sollten wir bei der Auswahl und Beauftragung einer Detektei für unsere interne Untersuchung achten?

A: In der Schweiz gibt es weit **über 200 Detektivbüros**, wobei die Qualität und Seriosität stark schwankt. Ihr Spektrum an Aufgaben variiert auch stark. Die am häufigsten nachgefragte Leistung ist zweifellos die **Observation**. Aber auch Abklärungen im Bereich *Open-Source Intelligence* („OSINT“[42]) und IT-Forensik werden häufig in Auftrag gegeben.

Folgende Anhaltspunkte können bei der Auswahl einer geeigneten Detektei helfen:

- **Keine Einzelunternehmer (*“Onemanshow“*)**. Dies ist oft ein Merkmal von Ermittlern, welche den Beruf lediglich als zweites Standbein ausüben und kaum über die

42 Die Recherche in offen zugänglichen Quellen wie Internet, Verzeichnisse, Registern, Datenbanken, Medienarchiven.

Workforce verfügen, um umfangreichere und qualitativ anspruchsvollere Ermittlungen durchzuführen und entsprechend taugliche Berichte zu verfassen.

- **Eigene Büroräumlichkeiten (an angemessener Adresse)**. Ein weiterer Hinweis darauf, dass man es mit Profis zu tun hat. Angebote für Treffen in Kaffees oder gar in den Wohnräumlichkeiten des Ermittlers sind meist ein Hinweis auf ungenügende Professionalisierung.
- **Kostenlose Vorermittlungen.** Dies zeugt von Interesse an zielgerichteter Auftragserledigung zugunsten des Auftraggebers. Der Detektei wird der Fall unterbreitet, ihr mit einer Geheimhaltungserklärung allenfalls sogar Zugang zu Unterlagen gewährt, worauf sie einen Vorschlag für eine Vorgehensweise inkl. Kostenvoranschlag macht.
- **Detaillierte Offertstellung.** Dies zeugt davon, dass ein konkreter Plan zur Auftragserledigung vorliegt und Kostenfaktoren nicht einfach aus der Luft gegriffen werden.
- **Ein gewisses Preisniveau** sollte nicht unterschritten werden. *You get what you pay for.*
- **Branchenspezifische Referenzlisten,** d.h. für Anwälte eine Referenzliste, für Unternehmen eine Referenzliste und für Privatkunden eine Referenzliste.
- **Google Bewertungen.** Gute Bewertungen zeugen von kontinuierlicher und zuverlässiger Arbeitsleistung. Sie können allerdings auch manipuliert bzw. gefälscht sein.
- **Berufsbewilligungen vorhanden.** Gemeint ist sowohl eine kantonale wie auch eine eidgenössische Bewilligung, die noch gültig sein muss. Ist dies nicht der Fall, kann dies dazu führen, dass Beweise nicht verwertbar sind.
- **Anzahl der geleiteten Ermittlungen.** Viele Fälle der Ermittlungsleitung zeugen von einer gewissen Erfahrung und Professionalität. Allerdings lassen sich diese Angaben auch schwer prüfen. Referenzlisten sind hier hilfreicher.
- **Juristische Grundausbildung.** Mindestens eines der Geschäftsleitungsmitglieder sollte branchenspezifisch juristisch bewandert sein und die Mitarbeiter sollten darin intern geschult werden.

Leider kein Qualitätsmerkmal ist eine **Verbandsmitgliedschaft**, jedenfalls für sich allein nicht. Es gibt zahlreiche Detektivverbände und der Fokus liegt eher auf Vermarktung der Mitglieder als der Qualitätssicherung. Der Weltverband WAD wird in Fachkreisen am besten bewertet.

In der Auftragserteilung und -abwicklung ist auf folgende Punkte zu achten:

- **Alle fallrelevanten Informationen** seitens des Auftraggebers sollten von Anfang an zur Verfügung gestellt werden. Auch scheinbar unbedeutende Details können Grundlage für eine gelungene Vorgehensweise oder zusätzliche Ermittlungsansätze sein.

- **Ergebnisoffene Herangehensweise.** Oft kommt es vor, dass vorgefasste Vermutungen über einen Sachverhalt im Laufe der Ermittlungen umgestossen werden. Dies kann im ersten Moment kontraintuitiv oder sogar enttäuschend sein. Aber gelingt es, sich auf die veränderte Ausgangslage einzustellen, ergeben sich oft neue Möglichkeiten, die zum eigenen Vorteil genutzt werden können.
- **Resilienz.** Anders als in Film und Fernsehen ist es möglich, dass Ermittlungsansätze ins Leere laufen. Dies sollte nicht als Misserfolg des Projekts gewertet werden, oft kann ein weiterer Versuch den entscheidenden Hinweis liefern.
- **Ständiger Informationsfluss** zwischen Privatdetektei und Auftraggeber, also eine transparente Auftragserledigung.

Bezahlt wird eine Detektei in der Regel **nach Aufwand**, wobei die Preise je nach Erfahrung und Stellung des Mitarbeiters schwanken. Ein Stundenansatz im mittleren Segment liegt bei ca. CHF 150 für reguläre Ermittler, CHF 175 bei technischen Spezialisten und CHF 250 für Geschäftsleitungsmitglieder. Die Zuschläge für Einsätze in der Nacht, an Wochenenden und Feiertagen, betragen im Schnitt 25 Prozent. Hinzu kommen Spesen. Üblich ist die Entrichtung eines Kostenvorschusses. Die Kostenstruktur wird in einem schriftlichen Vertrag detailliert vereinbart.

Das Arbeitsergebnis ist ein in Schriftform verfasster **gerichtsverwertbarer Bericht**, welcher detailliert die durchgeführten Ermittlungen und die jeweiligen Ergebnisse dokumentiert. Im Bericht sind in der Regel auch Fotos, Screenshots und andere Abbildungen enthalten. Je nach Aufgabenstellung gehören auch Videoaufnahmen in Form von gängigen Videodateiformaten dazu. Bei komplexeren Fällen können die Ermittlungsergebnisse zur besseren Veranschaulichung auch in Form von Dateien vorliegen.

Gedanken zum Thema.

Auch wenn dies nicht geplant oder gewünscht wird: Interne Untersuchungen können zu Gerichtsverfahren führen, sei es vor einem Strafgericht oder einem Zivilgericht. Im Gerichtsverfahren kann aber nur auf verwertbare Beweise abgestellt werden. Wer sich dies nicht verbauen will, sollte bei internen Untersuchungen von Anfang prüfen und sicherstellen, dass die erhobenen Beweise auch in einem allfälligen Gerichtsverfahren verwendet werden können. Wenn sich da der Untersuchende als Staatsanwalt und Richter in einem fühlt und obendrein noch die für solche geltenden Verfahrensregeln nicht beachtet, wird es damit schwierig. Das wird leider nicht immer beachtet.

Claudius Gelzer
Gerichtspräsident am Appellationsgericht
des Kantons Basel-Stadt

8. Berichterstattung

Kurz gesagt

- Der Auftrag zur internen Untersuchung hält fest, was als Ergebnis erwartet wird: Nur die Abklärung des Sachverhalts, zusätzlich seine rechtliche Würdigung oder sogar Empfehlungen zum weiteren Vorgehen und etwaiger Abhilfemassnahmen.
- Der Bericht hat zwischen erstellten (und belegbaren) Fakten und lediglich möglichen Szenarien zu unterscheiden, darf letztere mit den nötigen Vorbehalten aber durchaus behandeln, wenn sie auf gewissen Erfahrungswerten basieren.
- Es ist immer damit zu rechnen, dass der Bericht in die Hände von Behörden im In- und Ausland sowie der beschuldigten Person gelangt. Er ist daher entsprechend abzufassen.

Worum es geht

Eine interne Untersuchung resultiert normalerweise in einem entsprechenden Bericht. Im Vordergrund stand dabei bisher die Darstellung des Sachverhalts, nicht dessen rechtliche Einordnung. Diese ist in aller Regel nicht abschliessend möglich, weil ein Sachverhalt selten restlos aufgeklärt werden kann. Noch seltener als eine rechtliche Einordnung des Sachverhalts werden vom Auftraggeber Empfehlungen für etwaige, vom Unternehmen zu treffenden Massnahmen verlangt. Diese werden häufig vom Bericht getrennt einem kleineren Empfängerkreis abgegeben. In Anbetracht der einschränkenden Praxis des Bundesgerichts zum Anwaltsgeheimnis ist allerdings zu erwarten (→ **Q10**), dass interne Untersuchungen von Anwälten wieder verstärkt den Fokus auf die rechtliche Einordnung oder Vorbereitung eines Unternehmens auf etwaige zivil-, aufsichts- oder strafrechtliche Verfahren legen werden.

Worauf zu achten ist

- Ein Untersuchungsbericht ist neutral, objektiv und unabhängig zu verfassen. Dazu gehört auch Entlastendes.
- Er hat sich im Kern bezüglich des Sachverhalts auf Fakten zu beschränken und die Belege sind nachprüfbar anzugeben.
- Thesen, Szenarien und Einschätzungen sind davon abgetrennt möglich, aber sie sind als solche zu bezeichnen, müssen begründet sein und es muss klar sein, von welchen Annahmen und Voraussetzungen sie abhängen.
- Der Bericht ist so abzufassen, dass er Dritten (wie Behörden oder beschuldigten Personen) offengelegt werden kann, ggf. mit Schwärzungen zum Schutz von Quel-

len und Geschäftsgeheimnissen. Gehen Sie trotzdem davon aus, dass er auch im „Klartext“ unerlaubt weitergereicht wird. Sie müssen auch dann dazu stehen können.

- Vor einer finalen Fassung des Berichts ist zu prüfen, ob den betroffenen bzw. beschuldigten Personen (nochmals) die Möglichkeit zur Stellungnahme gegeben werden sollte.
- Der Bericht sollte zwar Klartext sprechen, aber auch bezüglich derjenigen Dinge klar sein, die offen bleiben müssen oder nicht geklärt werden konnten.
- Die rechtliche Würdigung ist vom Sachverhalt klar zu trennen – sie wird subjektiv und oft mit entsprechenden Vorbehalten versehen sein.
- Ein Bericht kann auch gegen das Unternehmen eingesetzt werden, z.B. in den Händen von Zivilklägern oder Aufsichtsbehörden des Unternehmens.
- Für eine Information der Öffentlichkeit bietet sich eine – von den Autoren des Berichts – erstellte Zusammenfassung an.

Der gute Ruf

Ein wesentlicher Grund, warum es gegenüber einer Aufsichtsbehörde oder der Öffentlichkeit genügen kann, einen Fall mit einer internen Untersuchung aufzuarbeiten ist der gute Ruf der Anwälte, die sie durchführen. Es ist daher wichtig, dass sie den Bericht nicht als Vertreter des Klienten verfassen, sondern als unabhängig agierende Dritte. In diesem Zusammenhang ist frühzeitig zu klären, wer Adressat des Berichts ist – das Unternehmen oder die Behörde.

Wie vorzugehen ist

1. **Was ist der Gegenstand der Untersuchung? Worin besteht der Auftrag?** Der Gegenstand der Untersuchung bzw. der Auftrag muss selbstverständlich nicht erst zum Schluss geklärt werden, sondern schon zu Beginn der Untersuchung. Allerdings spielt der Gegenstand beim Verfassen des Berichts eine besondere Rolle: Alles, was nicht zum Gegenstand der Untersuchung gehört, ist grundsätzlich wegzulassen und braucht auch nicht abgeklärt zu werden (was seitens des Auftraggebers durchaus auch beabsichtigt sein kann). Der Gegenstand kann sich während einer Untersuchung freilich auch verändern, etwa wenn Erkenntnisse in eine neue, unerwartete Richtung weisen oder sich zeigt, dass der Fokus der Untersuchung eingeschränkt werden kann. Das Mandat des Unternehmens zur Durchführung der internen Untersuchung sollte schriftlich festgehalten sein.

Nicht immer lässt sich der Gegenstand der Untersuchung kontrollieren. Insbesondere in Befragungen können neue Aspekte auftauchen, welche die Untersuchung beeinflussen oder das Unternehmen ausserhalb der Untersuchung zum Handeln zwingen können. In einer Befragung bringt ein Mitarbeiter z.B. ein anderes, nicht untersuchtes Fehlverhalten ins Gespräch. Entsprechende neue Aspekte können den Sachverhalt in einem völlig anderen Licht erscheinen lassen, etwa weil sie eine beschuldigte Person entlasten. Sie müssen daher ebenfalls untersucht werden. Denkbar sind auch **Zufallsfunde**. Selbst wenn diese im Untersuchungsbericht nicht thematisiert werden müssen, weil sie nichts zur Sache beitragen, werden sie in den Befragungsprotokollen auftauchen und somit *"on record"* sein. Das Unternehmen wird unter Umständen auch solchen nachgehen müssen – wenngleich separat.

2. **Was soll das Ergebnis der Untersuchung umfassen?** Hierbei stehen drei Möglichkeiten zur Auswahl:

   - Im Kern geht es in jeder internen Untersuchung um die **Feststellung des Sachverhalts**. Eine rechtliche Würdigung gehört nicht unbedingt dazu. Trotzdem findet natürlich auch eine Abklärung des Sachverhalts nicht im rechtsleeren Raum statt, sondern wird letztendlich immer in der einen oder anderen Form zur rechtlichen Beurteilung führen. Bloss muss sie nicht Teil der Untersuchung und somit des Berichts sein, sondern kann davon getrennt erfolgen (dazu die Ziff. 3). Aus diesem Grund ist auch die Abklärung eines Sachverhalts nicht ohne Blick auf seine mögliche rechtliche Einordnung möglich: Wer eine sexuelle Belästigung, einen Bestechungsfall oder einen Geheimnisverrat aufklären will, muss wissen, auf welche Sachverhaltselemente es in diesen Fällen ankommt. Sonst kann er nicht die richtigen Fragen stellen bzw. wird er die relevanten Antworten nicht erhalten. Das gilt insbesondere für Befragungen: Unter Umständen besteht für das Stellen der „richtigen" Fragen nur eine Chance.

Entscheidbasis

Gibt ein Beschuldigter ein Fehlverhalten nicht zu, kann er aber auch nicht entlastet werden, liefert eine interne Untersuchung aufgrund ihrer inhärenten Grenzen oft keine restlose Klärung, sondern eine mehr oder weniger aussagekräftige Indizienlage. Für das Management des Unternehmens wird das aber in vielen Fällen genügen, um seine Entscheide zu fällen. Es hat hierzu oft auch viel weniger Zeit als etwa ein Gericht.

- Ist ein Sachverhalt ganz oder teilweise erstellt, so stellt sich für den Auftraggeber natürlich sofort die Frage nach der **rechtlichen Beurteilung des Sachverhalts**. Hat sich der Beschuldigte strafbar gemacht oder hat er „nur" gegen eine interne Regel des Unternehmens verstossen – oder nicht einmal das? Es kann sinnvoll sein, diese Fragen ebenfalls zu beantworten, aber es ist in zweierlei Hinsicht Vorsicht geboten: *Erstens* bedingt jede juristische Beurteilung in der Regel Wertungen. Diese können je nach Person unterschiedlich ausfallen. Am Ende hat jedoch der Richter und nicht der „Ermittler" zu entscheiden. *Zweitens* kann auch eine eingehende Untersuchung oft nicht alle Fragen klären, die für ein komplettes Bild nötig wären. Es fehlt die Zeit, es fehlen Informationen, es fehlen Zwangsmassnahmen, und nicht selten fehlt auch der Wille oder die Erforderlichkeit: Völlige Klarheit ist für das Unternehmen nicht unbedingt immer vorteilhaft und oft auch nicht nötig, sofern klar ist, was *pro futuro* getan werden muss. Die rechtliche Einschätzung ist daher klar vom Sachverhalt zu trennen und mit den nötigen Vorbehalten zu versehen. Sie ist subjektiv, der Sachverhalt objektiv.

- Führt die Untersuchung zu Missständen, so kann sich auch die Frage nach **Massnahmen** aufdrängen, also Empfehlungen an das Unternehmen, wie es weiter zu verfahren hat. Das kann den konkreten Fall betreffen (z.B. welche Sanktionen gegenüber einem fehlbaren Arbeitnehmer auszusprechen sind, ob eine Selbstanzeige bei den Behörden angezeigt ist, ob ein Strafverfahren initiiert werden sollte oder, ob es besser ist, alles unter dem Deckel zu behalten) oder darüber hinaus zu gehen (z.B. welche technischen und organisatorischen Massnahmen zu treffen sind, um solche Vorfälle in Zukunft zu verhindern). In der Fachsprache ist von *"remediation"* die Rede. Selbst wenn keine Behörden im Spiel sind, wird das Unternehmen sich mit den möglichen Massnahmen auseinandersetzen wollen, will es sich doch nicht den Vorwurf einhandeln, nicht angemessen reagiert zu haben.

Zweitnutzung

Bei der Formulierung des Auftrags zur internen Untersuchung sollte das Unternehmen stets damit rechnen, dass es schriftliche Ergebnisse und die ihnen unterliegenden Quellen den Behörden übergeben muss. Haben Behörden sie, können unter Umständen wiederum Dritte (z.B. Zivilkläger) an sie herankommen. Zum Schutz durch das Anwaltsgeheimnis vgl. → **Q10**.

Lässt sich ein Sachverhalt nicht lückenlos aufklären oder bleiben Widersprüche bestehen, kann es nötig sein, in einer Untersuchung mit **Thesen und Szenarien** zu arbeiten, d.h. keine Fakten zu präsentieren, sondern nach der allgemeinen Lebens- und Berufserfahrung besonders wahrscheinliche Fallvarianten. Diese sind nach Möglichkeit im Bericht von den Fakten zu trennen, als Hypothesen zu kennzeichnen und darzulegen, was sie stützt, was gegen sie spricht und welche Voraussetzungen zur Bestätigung ihrer Gültigkeit bisher noch fehlen. Dies ermöglicht es dem Leser, sich ein eigenes Bild zu machen. Erlaubt ist auch die **Würdigung von Beweisen** – sofern sie objektiv, unabhängig und fair erfolgt. Ob eine Aussage glaubwürdig wirkte, kann ihrer Niederschrift nicht unbedingt entnommen werden. Hier sind die persönlichen Eindrücke des Befragers wichtig.

3. **In welcher Form sollen die Untersuchung und ihre Ergebnisse dokumentiert werden?** Üblicherweise werden die Ergebnisse einer internen Untersuchung in Form eines Berichts geliefert, welcher den Sachverhalt mitsamt den wichtigsten Belegen im Detail darstellt. Er führt auch aus, wie vorgegangen wurde, welche Quellen benutzt wurden, wann welche Personen befragt wurde, was analysiert wurde und auch, auf welche Schritte verzichtet wurde und warum (z.B. warum gewisse Quellen oder Datenbestände nicht benutzt wurden, was wichtig sein kann, sollten sie sich im Nachhinein als relevant darstellen). Gewisse Unternehmen haben für die regelmässigeren, kleineren internen Untersuchungen spezielle Formularvorlagen entwickelt, mit welchen sie die Untersuchung und ihre Ergebnisse schematisch dokumentieren.
Damit wird sichergestellt, dass nichts vergessen geht. Wird eine rechtliche Einschätzung verlangt, ist sie häufig ebenfalls Teil des Berichts. Es kann jedoch sinnvoll sein, sie separat zu verfassen, damit der Bericht einfacher mit Dritten geteilt werden kann, so z.B. auch mit den beschuldigten Personen oder Behörden, denen die eigene rechtliche Einschätzung nicht offengelegt werden soll (und grundsätzlich auch nicht muss). Ist der Bericht nicht im Hinblick auf eine Würdigung verfasst, wird es umgekehrt schwieriger, diesen unter Berufung auf ein → **Legal Privilege** den Behörden vorzuenthalten, etwa

Der Bericht

- Executive Summary
- Untersuchungsanlass
- Gegenstand
- Vorgehensweise, inkl. Quellen und worauf verzichtet wurde
- Sachverhalt, z.B. nach Themen oder chronologisch
- Thesen und Szenarien
- Ungeklärte Fragen bzw. Ansätze für weitere Abklärungen
- Stellungnahmen von betroffenen Personen
- Anhänge (wichtige Belege, Protokolle, Analysen etc.)

wenn die Herausgabe angeordnet oder der Bericht beschlagnahmt werden sollte (→ **Q10**). Dasselbe gilt für etwaige empfohlene Massnahmen; sind sie Teil des Berichts, kann dies das Management unter einen Handlungszwang setzen, auch wenn es gewisse Massnahmen aus guten Gründen nicht umsetzen möchte. Die Art und Weise der Präsentation der Untersuchung und ihrer Ergebnisse hat somit auch eine wichtige taktische Komponente. Üblich ist, dass die Personen, welche die Untersuchung durchgeführt haben, die Ergebnisse dem Management auch persönlich präsentieren, mit entsprechenden Ausführungen auf der Tonspur. Dabei kann es sich anbieten, etwa die aufgrund der Ergebnisse einer Untersuchung möglichen Massnahmen (*"Take-away actions"*) mit der Geschäftsleitung oder dem Verwaltungsrat zuerst mündlich zu diskutieren und abzustimmen, bevor sie schriftlich dokumentiert werden. Bei einer verfrühten Dokumentation lässt sich nur noch schwerlich von festgehaltenen Schlüssen abweichen, insbesondere, falls eine Herausgabe der Untersuchungsergebnisse an Behörden im Raum steht. In der Praxis wird diesbezüglich auch gerne mit Entwurfsfassungen von Berichten gearbeitet, wobei es durchaus vorkommen kann, dass ein (nur für ein internes Publikum bestimmter) Bericht nie finalisiert wird. In für das Unternehmen besonders heiklen Fällen kann schliesslich auch erwogen werden, auf einen schriftlichen Bericht vollständig zu verzichten.

Gewisse Unternehmen schützen die Vertraulichkeit eines Berichts dadurch, dass sie ihn sich nicht senden lassen, sondern nur jeweils **bei ihrem Anwalt einsehen**. Inwieweit dies Schutz vor Behördenzugriffen gewährleistet, ist unklar. Grundsätzlich kann eine Behörde jene Unterlagen, die ihr zustehen, auch vom Anwalt herausverlangen.

4. **Soll der Bericht den Beschuldigten vorgelegt werden?** Dies wird in der Praxis unterschiedlich gehandhabt. Oft bleibt der Bericht jedoch unter Verschluss und dem Beschuldigten wird, wenn überhaupt, nur das Protokoll seiner eigenen Aussage vorgelegt. Wird einem Arbeitnehmer ein Fehlverhalten vorgeworfen, so muss er dazu Stellung nehmen können. In der Regel wird er zwar für den Bericht selbst befragt worden sein, aber selten wird zu diesem Zeitpunkt bereits das volle Bild der Sachlage bestehen. So kann es erforderlich werden, ihm auch nach seiner Befragung die Gelegenheit einzuräumen, zu den Ergebnissen Stellung zu nehmen und diese in den Bericht einfliessen zu lassen,

Drittanwalt

Während der eigene Mitarbeiter an ein Berufsgeheimnis zum Schutz der Kunden seines Arbeitgebers gebunden sein mag, ist es sein Anwalt in der Regel nicht. Gibt ein Unternehmen ihm Kundendaten bekannt (z.B. im Rahmen eines Untersuchungsberichts), kann dies eine Verletzung des Berufsgeheimnisses darstellen.

wenn der Bericht Grundlage für einen ihn betreffenden Entscheid darstellt oder in anderer Weise verwendet werden soll bzw. kann (z.B. Weitergabe an eine Behörde). Gegen eine Offenlegung des Berichts können taktische Gründe sprechen, aber auch der Schutz der im Bericht genannten Quellen und der Geschäftsgeheimnisse des Arbeitgebers. Was der Arbeitnehmer während seines Arbeitsverhältnissen an Geschäftsgeheimnissen erfährt, muss dieser zwar geheim halten (Art. 321a Abs. 4 OR). Auch unterliegt er dem Datenschutz. Aber in der Praxis ist auf die Einhaltung dieser Pflichten – gerade in strittigen Verhältnissen – nicht unbedingt Verlass. Komplizierend ist allerdings zu beachten, dass eine betroffene Person auch datenschutzrechtlich Anspruch auf Einsicht in den Bereich bzw. die sie betreffende Teile des Untersuchungsberichts haben kann (Art. 8 DSG). Wie weit sich das diesbezügliche Auskunftsrecht erstreckt (d.h. welche Teile tatsächlich offengelegt werden müssen), ist allerdings umstritten. Immerhin gibt es auch Gründe, die Auskunft aufzuschieben, zu verweigern oder einzuschränken (Art. 9 DSG). Umgekehrt verpflichtet das Datenschutzrecht Sie an sich nicht zur Geheimhaltung eines Berichts.

5. **Soll der Bericht an Behörden weitergegeben werden?** Auch diese Frage wird in der Praxis je nach Fall und Unternehmen unterschiedlich gehandhabt. In gewissen Fällen wird ein Unternehmen alles daran setzen, den Bericht nicht offenlegen zu müssen und ihn im Falle einer Beschlagnahmung siegeln lassen (→ **Q10**). In anderen Konstellationen wird es einen Bericht als Beleg für seine saubere Aufarbeitung eines Compliance-Verstosses verwenden wollen, insbesondere wenn er von einer unabhängigen dritten Stelle verfasst worden ist. Immer wieder haben sich Unternehmen auch dazu entschieden, Untersuchungsberichte in einer Zusammenfassung zu publizieren[43]. Wird ein Bericht einer bestimmten Behörde weitergegeben (z.B. einer Aufsichtsbehörde), muss allerdings damit gerechnet werden, dass diese ihn weiteren Behörden zugänglich macht (auf dem Weg der Amts- oder Rechtshilfe) oder sogar betroffenen Dritten (auf dem Weg des datenschutzrechtlichen Rechts auf Auskunft, des Akteneinsichtsrechts oder des Öffentlichkeitsprinzips). Ob und wie eine Behörde auf die Ergebnisse einer internen Untersuchung in eigenen Verfahren gegen Dritte abstellen darf, ist allerdings umstritten.[44]

Ehrverletzung

Die Autoren eines Untersuchungsberichts zu strafrechtlich relevantem Fehlverhalten können selbst Rechtsrisiken ausgesetzt sein. In Frage kommen insbesondere Ehrverletzungsdelikte und der Tatbestand der falschen Anschuldigung, wenn sie damit rechnen, dass ihr Bericht auch den Behörden zugänglich gemacht werden soll. Dazu → **Q45**.

43 So z.B. im Fall der PostAuto: https://www.post.ch/de/ueber-uns/aktuell/postauto-untersuchung.
44 Vgl. etwa Entscheid des BGer 1B_212/2014 vom 14. Januar 2014 wo die Frage offengelassen wurde.

☝ Normalerweise ist derjenige der **Adressat des Berichts**, der die Untersuchung in Auftrag gegeben hat. Das muss aber nicht immer so sein. Sind Behörden von Anfang an in eine Angelegenheit involviert, ist es auch denkbar, dass sie die Adressaten des Berichts sind und die mit der Untersuchung beauftragte Kanzlei primär ihnen und nicht dem Unternehmen Bericht erstattet, auch wenn das Unternehmen die Ergebnisse erfährt und auch dazu Stellung nehmen kann. Davon abzugrenzen ist der ***"Monitor"***, der insbesondere in US-Verwaltungsverfahren, Straf- oder Bussgeldverfahren auf Verlangen der verfahrensleitenden Behörde bestellt wird und überwachen und darüber berichten soll, ob ein Unternehmen im Nachgang zu einem Compliance-Verstoss die nötigen Massnahmen trifft, um künftige Verstösse zu verhindern. Abzugrenzen ist eine interne Untersuchung auch von **behördlich angeordneten Untersuchungen**, z.B. durch einen Untersuchungsbeauftragten der FINMA (Art. 36 FINMAG) – auch wenn in all diesen Fällen das Unternehmen jeweils die Rechnungen bezahlen muss.

6. **Quellen, Kunden und Geschäftsgeheimnisse sind zu schützen.** Untersuchungsberichte enthalten regelmässig nicht nur unangenehme, sondern auch sonst höchst sensible Informationen aus dem Innern eines Unternehmens. Für eine saubere Aufarbeitung eines Sachverhalts ist es allerdings auch wichtig, dass die Dinge beim Namen genannt werden und die dargelegten Fakten belegt und Schlussfolgerungen nachvollziehbar sind. Ohne die Offenlegung von Quellen und Geheimnissen des eigenen Unternehmens aber auch seiner Kunden und anderen Geschäftspartner geht es nicht. Es sollte jedoch bereits beim Verfassen des Berichts und insbesondere bei der Weitergabe – auch unternehmensintern – darauf geachtet werden, dass diese geschützt bleiben, selbst wenn der Bericht oder Auszüge davon in die Hände von Personen gelangen, die ihn nicht mit der gehörigen Vertraulichkeit behandeln.

☝ Eine beliebte Schutzmassnahme ist die Verwendung von Kürzeln statt Namen und der Einsatz von **Codenamen**, wo es um Namen geht, die besonders zu schützen sind, wie z.B. Kunden, deren Identität und Daten dem Schutz des Berufsgeheimnisses unterstehen und Dritten nicht ohne Weiteres offengelegt werden dürfen. Eine andere Möglichkeit sind klassische **Schwärzungen**. Soll die **Öffentlichkeit** über die Ergebnisse einer Untersuchung informiert werden, bietet sich auch das Erstellen einer **Zusammenfassung** an. Um die Empfänger eines Berichts vor einer Weitergabe abzuschrecken, können die abgegebenen Exemplare zudem **personalisiert**

werden – in erkennbarer oder nicht erkennbarer Form mit unsichtbaren „Wasserzeichen“ (im letzteren Fall sollten die Empfänger auf die Codierung hingewiesen werden, damit sie ihren Effekt haben).

Do’s	Don’ts
• Ein Untersuchungsbericht darf spannend sein, sollte aber nüchtern und faktenbasiert bleiben. Hypothesen dürfen diskutiert werden, soweit sie als solche erkennbar sind. • Wenn Sie einen unabhängigen Dritten mit einer Untersuchung beauftragen, dann lassen Sie ihn auch bestätigen, dass er die Untersuchung so durchführen konnte, wie er wollte und das Unternehmen ihm alle Freiheiten liess. • Die Verfasser sollten im Bericht genannt werden. Für das, was sie schreiben, sollten sie mit ihrem Namen einstehen. • Die wichtigsten Belege gehören in den Bericht, einschliesslich der Befragungsprotokolle. • Schützen Sie Quellen, insbesondere die eigenen Arbeitnehmer. • Seien Sie ausgewogen und fair. Es geht nicht darum, Beweise gegen den Beschuldigten zu suchen, sondern den Sachverhalt aufzuklären.	• Schreiben Sie als Verfasser eines Berichts nichts, was sie gegenüber der beschuldigten Person nicht auch persönlich vertreten könnten. • Vermischen Sie nicht den Sachverhalt und dessen rechtliche Einschätzung (aber arbeiten Sie den Sachverhalt so auf, dass eine rechtliche Einschätzung möglich ist). • Verlassen Sie sich nicht darauf, dass das *Legal Privilege* Sie vor der Preisgabe der Untersuchungsergebnisse schützt. • Verwenden Sie keine fremden Inhalte (z.B. Fotos), für welche Sie nicht über die erforderlichen Rechte verfügen oder zu deren Verwendung Sie sich nicht auf einen hinreichenden Rechtfertigungsgrund stützen können (z.B. Zitatrecht).

Wann Sie externe Unterstützung beiziehen sollten

- Wenn **Behörden** mit im Spiel sind.
- Wenn Sie zeigen möchten, dass eine Untersuchung **von einem unabhängigen Dritten durchgeführt** wurde, der mit seinem guten Ruf dahinter steht.
- Wenn Sie eine **rechtliche Einschätzung** des Sachverhalts benötigen.
- Wenn Sie einen Untersuchungsbericht auf seine **rechtliche Angreifbarkeit** prüfen lassen wollen.
- Wenn Sie **unsicher** sind, wie Sie einen Bericht verfassen sollen.
- Wenn Sie Unterstützung dabei brauchen, **Personendaten und Geschäftsgeheimnisse** vor einer Weitergabe des Berichts oder seiner Beilagen zu schwärzen oder sonst zu schützen und dazu selbst nicht die Mittel haben.

Häufige Fragen und Antworten

Q44. Wann müssen wir einem beschuldigten Mitarbeiter Einsicht in den Untersuchungsbericht gewähren?

A: In einem offiziellen Strafverfahren folgt aus dem Grundsatz des **rechtlichen Gehörs** das Recht auf Akteneinsicht. Bei einer internen Untersuchung gilt, dass der beschuldigten Person die Möglichkeit eingeräumt werden muss, sich zu belastenden Beweisen und zu den Vorwürfen zu äussern. Dies geschieht normalerweise **vor der Erstellung des Berichts** (dazu → **Q34**). Der Arbeitgeber kann daher einen Untersuchungsbericht in der Regel bis zum Abschluss der Untersuchung unter Verschluss halten und selbst dann wird er ihn selten davon betroffenen Personen ohne Schwärzungen (zum Schutz von Mitarbeitern oder Geschäftsgeheimnissen) offenlegen. Einen eigentlichen Anspruch auf Einsicht in den vollen Untersuchungsbericht hat auch der beschuldigte Mitarbeiter normalerweise nicht.

Zu beachten ist, dass jeder betroffenen Person (nicht nur dem beschuldigten Mitarbeiter) das **datenschutzrechtliche Auskunftsrecht** zusteht und sich daraus ebenfalls ein Anspruch auf Einsicht zumindest in Teile des Untersuchungsberichts ableiten lässt. Das Auskunftsrecht will der betroffenen Person ermöglichen, die korrekte Bearbeitung ihrer Personendaten zu kontrollieren, um nötigenfalls eingreifen zu können. Im Falle einer internen Untersuchung steht dabei vor allem die Zulässigkeit der beschafften Beweismittel und die Richtigkeit und Vollständigkeit der personenbezogenen Aussagen im Vordergrund. Zu beachten ist jedoch, dass das Auskunftsrecht sich nur auf Personendaten bezieht, d.h. nicht auf den Bericht als solches. Eine betroffene Person hat somit datenschutzrechtlich Anspruch auf *die sie betreffenden Personendaten* im Bericht, nicht auf den Bericht als solches oder als Ganzes.

In der Praxis bedeutet dies, dass dem Arbeitnehmer der Bericht wenn überhaupt **nur auszugsweise offengelegt** werden muss bzw. jene Teile, die nicht als seine Personendaten gelten, schon von vorneherein nicht offengelegt werden müssen, weil sie nicht dem Auskunftsrecht unterliegen. Alternativ zur Offenlegung eines geschwärzten Berichts ist es auch möglich, die die Person betreffenden Aussagen separat mitzuteilen, denn Anspruch hat sie nicht auf eine Kopie des Berichts, sondern nur auf die darin enthaltenen Personendaten als solches. Wird sie z.B. in einem Befragungsprotokoll erwähnt, kann die fragliche Aussage isoliert mitgeteilt werden. Die **Abgrenzung**, ab wann eine Aussage als Personendatum einer Person gilt, wird freilich nicht immer einfach sein, insbesondere bei der beschuldigten Person.

Steht fest, welche Informationen als Personendaten der um Auskunft ersuchenden Person gelten, muss in einem nächsten Schritt geprüft werden, ob der Auskunft **Gründe zur Verweigerung, Aufschiebung oder Beschränkung** entgegenstehen. Das Gesetz sieht hier mehrere vor, so insbesondere zum Schutz von Dritten (z.B. anderen Mitarbeitern) und zum Schutz der Interessen des Arbeitgebers (z.B. ungestörte Durchführung der Untersuchung, Verhinderung der Kollusion, Wahrung von Geschäftsgeheimnissen). Zum Ganzen: → **Q57**.

Immerhin kann es aus **taktischen Überlegungen** sinnvoll sein, einem beschuldigten Mitarbeiter einen Untersuchungsbericht auch vollständig oder nur mit minimalen Schwärzungen zum Schutz bestimmter Mitarbeiter offenzulegen. Ist die Beweis- und Rechtslage klar zu seinen Ungunsten, wird der Mitarbeiter sich womöglich rechtlich nicht gegen entsprechende Konsequenzen wehren, weil er weiss, was das Unternehmen gegen ihn in der Hand hat (und dies z.B. auch zu weiteren Konsequenzen führen kann). Wird ihm der Untersuchungsbericht offengelegt, wird es ihm auch schwerer fallen zu argumentieren, ihm sei das rechtliche Gehör verweigert worden.

Neben der direkten Offenlegung eines Untersuchungsberichts gegenüber einer betroffenen Person durch das Unternehmen sind auch **indirekte Offenlegungen** zu berücksichtigen. Wird der Untersuchungsbericht einer Behörde eingereicht (freiwillig oder aufgrund einer Pflicht), so können beteiligte Personen unter Umständen auf dem Weg der Akteneinsicht oder des Auskunftsrecht bei diesen Behörden Einsicht in den Bericht erhalten.

Im Hinblick auf eine etwaige Offenlegung ist es auch sinnvoll, beim Verfassen des Untersuchungsberichts klar zwischen erstelltem Sachverhalt, Mutmassungen über mögliche Szenarien und rechtlicher Würdigung zu unterscheiden und ggf. auch **getrennte Berichte** anzufertigen.

Q45. Wann ist ein Untersuchungsbericht ehrverletzend oder sonst strafrechtlich relevant?

A: Die **Ehre** des Einzelnen ist im schweizerischen Recht **strafrechtlich geschützt** (Art. 173 ff. → **StGB**). Geschützt wird unter anderem das berufliche, wirtschaftliche

und gesellschaftliche Ansehen einer Person (BGE 107 II 4, E. 2). Ehrverletzend können Tatsachenbehauptungen, aber auch Werturteile sein.

Im Rahmen interner Untersuchungen ist Vorsicht insbesondere dort geboten, **wo ein strafbares Verhalten im Raum steht**, was naturgemäss häufig der Fall sein wird. Das Risiko einer Ehrverletzung besteht dann, wenn das mutmassliche strafbare Verhalten im Bericht einer bestimmten Person zugeordnet wird. Hierbei wird vorzugsweise mit entsprechenden Vorbehalten gearbeitet und darauf geachtet, was tatsächlich erwiesen ist und was nur vermutet wird. Das gilt auch bei vermeintlich zuverlässigen „Beweismitteln": Der Zeitstempel eines Badge oder eines Logins beweist nicht die Anwesenheit oder die Computernutzung einer Person, sondern die Verwendung ihres Badges oder ihres Zugangscodes.

Auch empfiehlt es sich, auf die strafrechtliche Unschuldsvermutung hinzuweisen und die Stellungnahme der beschuldigten Person in den Bericht einfliessen zu lassen, so dass entsprechende Indizien nicht unwidersprochen wiedergegeben werden. Da im Rahmen einer internen Untersuchung die Möglichkeiten der Beweiserhebung letztlich begrenzt sind, wird ausser im Falle eines entsprechenden Geständnisses die Beweislage selten klar sein. Nicht strafbar ist immerhin derjenige Autor, der beweisen kann, dass seine Behauptung wahr ist oder er **ernsthafte Gründe** hatte, sie in guten Treuen **für wahr zu halten**. Nicht zum Beweis zugelassen wird jedoch derjenige, der ohne begründeten Anlass handelte „vorwiegend in der Absicht … jemandem Übles vorzuwerfen"[45]. Wird eine interne Untersuchung sauber durchgeführt, wird diese Voraussetzung allerdings kaum je erfüllt sein.

Reine Werturteile können ehrverletzend sein, wenn sie unangemessen sind, unsachlich oder **unnötig verletzend**. Ehrverletzend kann es somit ebenfalls sein, einem Arbeitnehmer in einem Bericht die gesamte Fachkompetenz zur Ausübung seines Berufes abzuerkennen und ihn als „inkompetent" zu bezeichnen. Selbstredend können vulgäre, herablassende und beleidigende Ausdrücke (z.B. die Bezeichnung einer Person als Rassist) ehrverletzend sein.

Muss davon ausgegangen werden, dass ein Untersuchungsbericht auch in einem behördlichen Verfahren zum Einsatz kommt, so sind ferner die Tatbestände der **falschen Anschuldigung** (Art. 303 StGB) und der Irreführung der Rechtspflege (Art. 304 StGB) zu beachten. Diese Tatbestände erfordern jedoch ein Handeln wider besseren Wissens oder gar Arglist; die Schwelle ist entsprechend höher als im Falle der Ehrverletzung. Solange kein rechtskräftiges Strafurteil vorliegt, kann im Bericht mit Formulierungen wie „möglicherweise strafbares Verhalten" gearbeitet werden, aber auch andere Redewendungen sind denkbar, welche verdeutlichen, dass die Strafbarkeit einer Person

45 Art. 173 Ziff. 3 StGB.

noch nicht geklärt ist. Der blosse Hinweis auf die **Unschuldsvermutung** bei ansonsten klar „verurteilenden" Aussagen ist hingegen nicht zu empfehlen.

Zu beachten ist, dass die Schwelle zur Annahme einer **zivilrechtlichen Persönlichkeitsverletzung** tiefer liegt als zur Annahme einer strafrechtlichen Ehrverletzung. Erstere kann entsprechend zivilrechtlich verfolgt werden. Dies umfasst auch Berichtigungsansprüche (→ **Q46**).

> **Literatur:**
>
> Aebi-Müller, Regina, Art. 28 N 18 f., in: Handkommentar zum Schweizer Privatrecht, Personen- und Familienrecht – Partnerschaftsgesetz, Art. 1 – 456 ZGB – PartG, 3. Aufl., Zürich 2016

Q46. Kann eine beschuldigte Person die Berichtigung eines Berichts verlangen?

A: Ja, soweit eine Aussage nachweislich falsch ist. Die Richtigkeit von Daten stellt einen datenschutzrechtlichen Grundsatz dar. Stellen, die Personendaten bearbeiten, sind verpflichtet, sich über die Richtigkeit der Daten zu vergewissern. Unrichtige Daten sind zu vernichten oder zu korrigieren (Art. 5 Abs. 1 → **DSG**). Das Datenschutzrecht gewährt einer betroffenen Person ausdrücklich das **Recht zur Berichtigung unrichtiger Daten** (Art. 5 Abs. 2 DSG). Dieses Recht kann von der betroffenen Person jederzeit geltend gemacht werden. Kann die Richtigkeit oder Unrichtigkeit nicht festgestellt werden, kann die betroffene Person einen Bestreitungsvermerk verlangen. Da eine beschuldigte Person in einer internen Untersuchung normalerweise ohnehin Gelegenheit erhält, zum Ergebnis und den einzelnen Vorhaltungen Stellung zu nehmen, und diese Stellungnahme sinnvollerweise Eingang in den Bericht findet, liegt bereits ein solcher Bestreitungsvermerk vor.

Zu beachten ist in allen Fällen, dass sich die Richtigkeit einer Aussage **an ihrem Zweck orientiert**. Macht ein Arbeitskollege der beschuldigten Person eine aus ihrer Sicht falsche Aussage und wird diese im Bericht wiedergegeben, muss sie selbstverständlich nicht korrigiert werden, denn der Bericht gibt die Tatsachen richtig wieder, nämlich die Aussage des Arbeitskollegen, wie er sie vorgenommen hat.

> **Literatur:**
>
> Baeriswyl/Blonski, Art. 5 DSG N 1 ff., in: Baeriswyl, Bruno/Pärli, Kurt (Hrsg.), Kommentar zum Datenschutzgesetz, Bern 2015

Q47. Wie lange dürfen die Unterlagen der internen Untersuchung aufbewahrt werden?

A: Die Grundregel lautet: Solange wie erforderlich. Ausgangspunkt ist die Tatsache, dass Unterlagen einer internen Untersuchung (gesicherte E-Mails und Dokumente,

Befragungsprotokolle, Untersuchungsberichte etc.) in der Regel Personendaten enthalten. Das Unternehmen darf Personendaten nur solange bearbeiten (wozu auch das Aufbewahren zählt), wie dies zur **Erfüllung des Zweckes** zu dem diese erhoben wurden, notwendig ist. Nicht mehr benötigte Daten müssen mit anderen Worten gelöscht werden. Dies ergibt sich aus dem datenschutzrechtlichen Prinzip der **Verhältnismässigkeit** (Art. 4 → **DSG**). Vorbehalten bleiben gesetzliche Aufbewahrungspflichten und andere → **Rechtfertigungsgründe** (Art. 13 DSG), wie z.B. ein überwiegendes privates Interesse (z.B. falls die Löschung mit hohem Aufwand verbunden ist und Massnahmen getroffen sind, eine unrechtmässige Nutzung zu verhindern). Unter die Löschung fällt ebenfalls die **Anonymisierung**.

In der EU haben die **Datenschutzbehörden** teilweise unrealistisch kurze Aufbewahrungsfristen postuliert. So wird vertreten, Personendaten im Zusammenhang mit der Untersuchung eines Verdachts auf ein Fehlverhalten müssten sofort gelöscht (oder anonymisiert) werden, wenn sich ein Hinweis als falsch erweist. Erweist sich ein Hinweis als zutreffend, vertreten EU-Datenschutzbehörden teilweise, dass die Personendaten zwei Monate nach dem Abschluss der Untersuchung zu löschen sind. Sie übersehen dabei freilich, dass selbst im Falle eines Verdachts, der sich nicht erhärten sollte, ein Unternehmen den Nachweis der korrekten Handhabung der Sache erbringen können muss. Zu denken ist etwa an den Mitarbeiter, der sich anlässlich der nächsten Bonusrunde im Jahr darauf beschwert, für seinen Hinweis abgestraft worden zu sein. Ein anderes Beispiel ist die Aufsichtsbehörde, die nach dem Hinweis eines Whistleblowers vom Unternehmen wissen will, ob es bereits früher intern erfolgte Whistleblowing-Meldungen tatsächlich unbeachtet liess. Im Falle von bösgläubigen Anschwärzungen hat möglicherweise der Angeschuldigte selbst ein Interesse an entsprechenden Beweismitteln. Wird ein Fehlverhalten von gewisser Relevanz festgestellt, so wird ein Unternehmen die massgeblichen Erkenntnisse schon alleine seiner Zeugnispflicht wegen in die Personalakte übernehmen wollen und darin nicht nur bis zum Ende des Arbeitsverhältnisses, sondern auch für Jahre darüber hinaus aufbewahren wollen (formal verjährt der Anspruch erst nach zehn Jahren).

In der Praxis muss zwischen den unterschiedlichen Unterlagen und Dokumenten unterschieden werden:

- **Daten unter einem Legal Hold** können freigegeben werden (was u.U. auch zu deren Löschung führt, falls diese einstweilen ausgesetzt worden ist), sobald klar ist, dass nicht nur die Untersuchung abgeschlossen ist, sondern es auch nicht mehr zu damit zusammenhängenden behördlichen Verfahren oder gerichtlichen Auseinandersetzungen kommen wird.
- **Gesammelte Beweismittel**, so namentlich auch die für einen Review aufbereiteten elektronischen Daten, werden normalerweise aus den Review-Systemen entfernt und entweder beim eDiscovery-Provider archiviert oder dem Kunden bzw. seinen

Anwälten zur Aufbewahrung übergeben, so dass ggf. darauf zurückgegriffen werden kann (z.B. auf Festplatten, so dass ein Online-Zugriff nicht mehr möglich ist). Diese werden typischerweise für zehn bis elf Jahre nach Abschluss der internen Untersuchung aufbewahrt (in diesem Zeitraum sind auch seitens des Unternehmens noch Ansprüche gegen die Untersuchungsperson möglich), mindestens aber solange, wie es noch zu behördlichen Verfahren oder gerichtlichen Auseinandersetzungen kommen kann; laufen solche, sollten die Daten nicht vernichtet werden.

- Der **Untersuchungsbericht** wird in der Regel ebenfalls mindestens zehn oder elf Jahre bis nach Abschluss der Untersuchung aufbewahrt, mindestens aber solange, wie es noch zu behördlichen Verfahren oder gerichtlichen Auseinandersetzungen kommen kann (oder solche laufen). Nebst Ansprüchen aus oder aufgrund der internen Untersuchung ist hier auch das Interesse des Unternehmens von Relevanz, den korrekten Umgang mit den der Untersuchung zugrundeliegenden Vorwürfen demonstrieren zu können (sowohl gegenüber in- wie auch ausländischen Behörden). Hier kann eine längere Aufbewahrung (z.B. 15 Jahre) sinnvoll sein.
- **Entwürfe, interne Notizen und Kommunikation** können entsprechend der Regeln für Beweismittel aufbewahrt werden. Eine Pflicht hierzu besteht jedoch in der Regel nicht. Sie können die saubere Durchführung der Untersuchung und korrekte (oder inkorrekte) Mandatserfüllung belegen und somit den berechtigten Interessen des Unternehmens wie auch der Untersuchungsperson dienen.
- **Hinweise von Hinweisgebern** in Fällen, in denen sich ein Verdacht nicht erhärtet hat, können ein bis zwei Jahre aufbewahrt werden (das Interesse der zu Unrecht verdächtigten Person kann auch eine längere Aufbewahrung rechtfertigen, insbesondere, wenn der Verdacht einer bösgläubigen Anschwärzung im Raum steht). Es ist allerdings festzuhalten, dass sich der geäusserte Verdacht *nicht* bestätigt hat. Sind die Hinweise anonym erfolgt und liegen somit keine Personendaten des Hinweisgebers vor, besteht seinerseits datenschutzrechtlich auch kein Löschanspruch.

Werden Unterlagen entsprechend aufbewahrt ist sicherzustellen, dass der **Zugang dazu beschränkt** ist und sie nur für die Zwecke benutzt werden, für welche sie aufbewahrt werden.

Literatur:

Geiser, Thomas: Interne Untersuchungen des Arbeitgebers: Konsequenzen und Schranken, Aktuelle Juristische Praxis (AJP) 2011, 1047 ff.

Rosenthal, David: Löschen und doch nicht löschen, Zeitschrift für Datenrecht und Informationssicherheit (digma) 2019, 190 ff.

Toneatti, Michael: Löschungsanspruch von personenbezogenen Daten des Arbeitnehmers gegenüber der Arbeitgeberin (inklusive Berücksichtigung der EU Datenschutz-Grundverordnung), Zürich/St. Gallen 2019

Gedanken zum Thema.

Die FINMA erwartet von den von ihr beaufsichtigten Finanzinstituten, dass sie mögliche Unregelmässigkeiten abklären. Eine solche interne Untersuchung bietet zwar keine Garantie dafür, dass die FINMA nicht selbst Abklärungen trifft. Garantiert ist aber, dass ohne eine interne Untersuchung die FINMA eine Untersuchung führen wird.

Susan Emmenegger
Direktorin des Instituts für Bankrecht
an der Universität Bern
Verwaltungsrätin der FINMA

9. Weitere Schritte

Kurz gesagt

- Will der Arbeitgeber einem Mitarbeiter fristlos kündigen, muss er rasch handeln. Alternativen wie die sofortige Freistellung sind in der Praxis allerdings oft zielführender und mit weniger Nachteilen behaftet.
- Ein Unternehmen sollte sich von Anfang an Gedanken darüber machen, in welcher Weise welche Behörden in den Fall involviert werden wollen oder sollen – eine strafrechtliche Untersuchung kann z.B. dabei helfen, Ermittlungslücken zu füllen.
- Die interne und externe Kommunikation kann entscheidend dafür sein, ob und wie ein Fehlverhalten der Reputation des Unternehmens schadet und welche Glaubwürdigkeit ihm in der Bekämpfung von Fehlverhalten zukommt.

Worum es geht

Hat eine interne Untersuchung ein Fehlverhalten aufgedeckt, so stellt sich die Frage, welche weiteren rechtlichen und anderen Schritte angesichts der gewonnenen Erkenntnisse zu ergreifen sind. Sie können darauf ausgerichtet sein, weitere Erkenntnisse zu gewinnen, weil eine private interne Untersuchung mit den ihr zur Verfügung stehenden Mitteln nicht weiterkommt. Es kann auch darum gehen, gegen die Verantwortlichen vorzugehen oder Ansprüche Dritter abzuwehren. Zu denken ist auch an das Ergreifen von Massnahmen, um weitere Verstösse dieser Art zu verhindern (*"remediation"*). Unter Umständen muss ein Unternehmen den Vorfall den Behörden melden oder an Betroffene und an die eigene Belegschaft kommunizieren. Schliesslich ist unter Umständen auch Öffentlichkeitsarbeit erforderlich, damit aus einer Krise kein Skandal wird.

Worauf zu achten ist

- In einer internen Untersuchung ist die Beweisführung oft einfacher und flexibler als vor Gericht, aber es kann rechtlich kein Zwang ausgeübt werden.
- Kommt eine interne Untersuchung an ihre Grenzen, kann ein Strafverfahren weitere Erkenntnisse bringen.

Volle Aufklärung

Oft kann eine interne Untersuchung einen Sachverhalt nicht restlos klären. Es stehen ihr keine Zwangsmittel zur Verfügung und oft drängt auch die Zeit. Das schränkt ihren Wert als Entscheidhilfe für das Management aber nicht unbedingt ein. Für das Ergreifen von Massnahmen ist die restlose Aufklärung oft nicht nötig.

- Die Einleitung eines Strafverfahrens nehmen die Medien in einem heissen Fall gerne zur Kenntnis, die Einstellung desselben geht oft unter.
- Manchmal hilft ein „*Shoot first, litigate later*".
- Behördliche und gerichtliche Verfahren brauchen viel Zeit, und die haben nicht alle.
- Aus jeder internen Untersuchung sollte ein Unternehmen seine Lehren ziehen und dies dokumentieren. Mit dem richtigen Umgang lässt sich bereits viel Schaden vermeiden.
- *Shitstorm*? Die Empörung führt zum Skandal, nicht die Schwere des Verstosses.

Wie vorzugehen ist

1. **Disziplinarische Massnahmen gegen Verantwortliche?** Steht ein Fehlverhalten im Betrieb im Raum, sollten Sie sich ohne Verzug überlegen, ob arbeitsrechtliche Sofortmassnahmen erforderlich sind. Zu denken ist primär an eine Verwarnung, eine förmliche Abmahnung, eine Freistellung, eine fristlose oder eine ordentliche Kündigung. Das kann dazu dienen, den betroffenen Arbeitnehmer oder andere Arbeitnehmer zu schützen (auch bezüglich ihrer Persönlichkeit). Solche Massnahmen können zudem verhindern, dass der betroffene Arbeitnehmer die Untersuchung oder das Unternehmen beeinträchtigt (z.B. durch Vernichtung von Beweisen im Unternehmen oder Sabotage). Sie können schliesslich aufgrund der öffentlichen Wirkung erforderlich sein (Signalwirkung: das Unternehmen handelt). Wird ein Mitarbeiter fristlos entlassen, steht er allerdings auch nicht mehr für Befragungen und zur Unterstützung zur Verfügung (auch nicht für ausländische Behörden, die dies u.U. erwarten). In der Praxis wird daher häufig mit einer sofortigen Freistellung gearbeitet. Hat der Mitarbeiter einen Schaden verursacht und ist er daher schadenersatzpflichtig, darf die Schadenersatzforderung unter Umständen mit seiner Lohnforderung verrechnet werden, was eine der fristlosen Kündigung ähnliche Wirkung haben kann. Allerdings wird in einer solchen Situation mitunter der Arbeitnehmer fristlos kündigen. Auch eine Lohnkürzung ist möglich, wenn ein Mitarbeiter seine Pflicht zur weisungskonformen Ausführung der Arbeit verletzt hat. Hat der Arbeitnehmer nur im weiteren Sinne gegen die Treuepflicht oder Weisung verstossen, dürfen ihm nach verbrei-

Nur Verdacht?

Das Kündigungsrecht ist schonend auszuüben. Eine Kündigung ist zwar schon aufgrund eines Verdachts möglich, doch müssen dafür ernsthafte, sorgfältig abgeklärte Anhaltspunkte vorliegen. Eine Kündigung kann auch missbräuchlich sein, wenn sie wegen eines Verstosses gegen eine zu vage formulierte oder unzulässige Weisung erfolgt.

teter Auffassung nur variable Lohnbestandteile gekürzt werden. Wird ein Mitarbeiter freigestellt, ist sicherzustellen, dass seine Fernzugänge zu den Systemen des Unternehmens blockiert werden. Allerdings ist dabei auch seine Persönlichkeit zu schützen, etwa in Bezug auf die (öffentliche) Erläuterung der Gründe für die Freistellung. Besondere Disziplinarmassnahmen wie Geldbussen oder Strafversetzung müssen gesetzlich oder vertraglich vorgesehen sein (z.B. als Konventionalstrafe). Ist ein sofortiges Handeln nicht erforderlich oder angezeigt, kann sich die Frage von disziplinarischen Massnahmen selbstverständlich auch in einem späteren Zeitpunkt stellen. In vielen Fällen wird es für das Unternehmen darum gehen zu zeigen, dass Verstösse nicht toleriert werden und entsprechende Konsequenzen nach sich ziehen. Darum wird in diesen Fällen auch die interne Kommunikation wichtig sein (dazu hinten), wobei wiederum die Persönlichkeit der betroffenen Personen zu schützen ist.

Eine **fristlose Kündigung** ist nur gerechtfertigt, wenn dem Unternehmen die Fortsetzung des Arbeitsverhältnisses nicht mehr zugemutet werden kann (Art. 337 OR). Ursache kann eine schwerwiegende Verfehlung sein (z.B. Straftaten am Arbeitsplatz, konkurrenzierende Tätigkeiten, Verrat von Geschäftsgeheimnissen, Beleidigungen von Vorgesetzten und Kollegen, die mehr als Bagatellen sind), wenn diese objektiv geeignet ist, die für das Arbeitsverhältnis wesentliche Vertrauensgrundlage zu zerstören oder jedenfalls so tiefgehend zu erschüttern, dass dem Arbeitgeber die Fortsetzung des Vertrags nicht mehr zuzumuten ist und die Verfehlung auch tatsächlich zu einer solchen Zerstörung oder Erschütterung des Vertrauens geführt hat. Bei weniger schwerwiegenden Verfehlungen muss vorher eine Abmahnung erfolgt sein. Reagiert der Arbeitgeber nicht sofort, verwirkt er sein Recht auf fristlose Kündigung. Laut Gerichtspraxis hat er zwei bis drei Tage Zeit, sich zu entscheiden; grössere Unternehmen können etwas mehr Zeit in Anspruch nehmen, wenn die zuständigen Organe nicht präsent sind. Akzeptiert wird auch eine vorgängige sorgfältige Abklärung, wenn diese sofort eingeleitet wird. Die mangelnde Kooperation eines Mitarbeiters kann ihrerseits einen Grund für eine fristlose Kündigung darstellen (BGer 8C_626/2020 vom 21. Dezember 2020). Im Falle einer nicht rechtzeitigen oder in der Sache ungerechtfertigten fristlosen Kündigung hat der Arbeitnehmer Anspruch auf seinen Lohn und eine Entschädigung von bis zu sechs Monatslöhnen.

2. **Sofortmassnahmen zur Schadensabwehr?** Je nach Art des Fehlverhaltens wird das Unternehmen nicht bis zum Abschluss der Untersuchung zuwarten können, um den Schaden zu begrenzen oder abzuwehren oder Personen zu schützen (z.B.

von einem allfälligen Mobbing oder einer sexuellen Belästigung betroffene Mitarbeiter). Das kann gerichtliche oder behördliche Massnahmen bedingen (z.B. Verarrestierung von Vermögenswerten, Massnahmen zur Beweissicherung) oder eigene Vorkehrungen (z.B. Kundeninformation, Sicherung von Computersystemen vor weiterem Datenabfluss, Versetzung oder Beurlaubung einer Person). Hier ist es wichtig, dass die Personen, die mit der Untersuchung beauftragt sind, entsprechende Rückmeldungen ins Unternehmen geben, wenn weiterer Schaden befürchtet werden muss. Massnahmen sollten allerdings mit Bedacht getroffen und kommuniziert werden, um weder die Untersuchung zu gefährden, noch zu einer Vorverurteilung zu führen.

3. **Interne Kommunikation?** Auch eine vertraulich geführte interne Untersuchung führt in aller Regel zu Gerede, das wiederum zur Unruhe, Verunsicherung oder auch Gerüchten bezüglich einzelner exponierter Personen führen kann. Hier wird meist unterschieden, ob der Missstand nur einzelne Personen oder im Sinne einer Unternehmenskrise alle betrifft. In letzterem Fall kann ein Unternehmen zeigen, dass es Mitarbeiter ernst nimmt und rasch offen und realistisch informieren, einschliesslich einer Vorgabe, wie sie selbst kommunikativ reagieren sollten. Dies kann je nach Betriebsgrösse dazu beitragen, dass die Angelegenheit auf Social Media und in den Medien thematisiert wird, doch das können Gerüchte auch. Das Unternehmen kann allerdings aufgrund seiner Fürsorgepflicht (Art. 328 OR) und des Datenschutzes nicht frei informieren, sondern muss die in einen Missstand involvierten Arbeitnehmer schützen – auch wenn sie sich falsch verhalten haben. Die interne Information über ein geahndetes Fehlverhalten kann schliesslich auch eine Compliance-Massnahme sein, indem das Unternehmen damit der Belegschaft zeigt, dass es entsprechende Verstösse nicht toleriert, selbst wenn die Folgen auch für das Unternehmen gewichtig sein mögen.

Exempel?

Aus Compliance-Sicht ist es wichtig, dass ein Unternehmen darüber informiert, dass es Fehlverhalten nicht toleriert. Allerdings müssen dabei die involvierten Personen nicht unnötig exponiert werden.

Auch wenn private Befragungen nicht mit solchen durch die Polizei oder Staatsanwaltschaft zu vergleichen sind, können sie **psychologischen Druck** auf die davon betroffenen Personen ausüben. Das kann dazu führen, dass Mitarbeiter, die sonst nichts sagen würden, über ihnen bekannte Missstände sprechen. Es kann allerdings auch das Betriebsklima belasten. Darum ist es wichtig, auch über die Untersuchung transparent und ehrlich zu informieren.

4. **Strafanzeige und Strafanträge?** Liegt ein strafbares Verhalten im Raum – und Ansätze dazu werden findige Juristen in vielen Fällen finden – stellt sich rasch die Frage, ob ein Strafverfahren eingeleitet werden sollte. Gründe kommen dafür einige in Frage: Es kann dazu dienen, gegenüber etwaigen Nachahmern oder der Öffentlichkeit ein Zeichen zu setzen, oder es kann eingesetzt werden, um Vergeltung zu üben. Das Strafverfahren kann weiter benutzt werden, um die davon betroffenen Personen unter Druck zu setzen, sie zu beanspruchen, und allenfalls auch einen Keil zwischen verschiedene Täter treiben. Es kann helfen, an Beweismittel heranzukommen, die einer privaten Untersuchung nicht zugänglich sind (über staatliche Zwangsmassnahmen und Akteneinsicht). Das Strafverfahren kann aber auch dazu dienen, eine Grundlage für spätere zivilrechtliche Forderungen zu schaffen oder eine Einziehung von Vermögenswerten zu bewirken. Ein solches Verfahren kann sich allerdings auch gegen das Unternehmen auswirken (etwa wenn es weitere Verfahren im In- und Ausland auslöst, auch aufsichtsrechtlicher Natur, z.B. wegen mangelnder Compliance). Es birgt zudem ein eigenes Strafbarkeitsrisiko (falsche Anschuldigung, Ehrverletzung). Vor allem aber dauert ein Strafverfahren lange (oft mehrere Jahre) und das Unternehmen kann es nicht kontrollieren (d.h. es hat höchstens die Geschädigtenrechte). Ob und wie ein Strafverfahren vorangeht und geführt wird, hängt massgeblich vom Stil und der Haltung des jeweiligen Staatsanwalts ab – und mitunter von weiteren Umständen wie der Brisanz, Schwere und Komplexität des Falls, der Medien, der politischen Gemengelage und auch von den eigenen Ressourcen und Prioritäten (andere Fälle). Vielen Staatsanwälten gemeinsam ist, dass sie dem Geschädigten oft erst spät Akteneinsicht gewähren, typischerweise erst nach Akteneinsicht durch die Beschuldigten, welche diese wiederum üblicherweise nach der ersten Einvernahme erhalten.

Öffentlichkeit?

Eine Strafanzeige kann aus PR-Sicht für ein Unternehmen wichtig sein, doch viele Staatsanwaltschaften haben keine Freude an solchen Fällen, weil sie sie unter Druck setzen können. Wird kommuniziert, kann es sinnvoll sein, dies vorgängig mit der Pressestelle der Staatsanwaltschaft abzusprechen, da die Medien ohnehin bei ihr nachfragen werden.

Eine **Strafanzeige** bzw. ein **Strafantrag** muss nicht lang sein (insbesondere nicht bezüglich der Ausführungen zum Recht), aber je besser der Fall punkto Fakten bereits aufgearbeitet ist (etwa auf Basis der Ergebnisse einer internen Untersuchung), desto rascher und besser kann auch die Staatsanwaltschaft tätig werden. Unterstützt der Geschädigte ein Strafverfahren wesentlich, kann dafür auch eine Kostengutsprache geltend gemacht werden.

Bei der Redaktion der Eingabe ist darauf zu achten, dass durch unbedachte Aussagen nicht der Tatbestand der falschen Anschuldigung oder der Ehrverletzung erfüllt wird. Dem Verdächtigen wird also nicht „Betrug" sondern „mutmasslicher Betrug" vorgeworfen oder eine andere Formulierung verwendet, welche genügend Spielraum lässt. Kommen neue Beweismittel ans Licht, kann auch ohne Weiteres nachgeliefert werden. Strafanträge unterliegen einer Frist von drei Monaten, beginnend ab dem Zeitpunkt, ab welchem der antragsberechtigten Person der Täter bekannt wird.

5. **Meldung gegenüber Behörden?** Vorfälle, die im Rahmen einer internen Untersuchung aufgearbeitet werden, können Meldepflichten auslösen. Die FINMA erwartet beispielsweise unverzüglich Meldung über Vorkommnisse, die für die Aufsicht von wesentlicher Bedeutung sind (Art. 29 Abs. 2 → **FINMAG**). In gewissen Bereichen hat sie dazu sogar konkrete Vorgaben entwickelt (z.B. Cyberattacken[46], Anfragen ausländischer Behörden[47]). Das revidierte Datenschutzgesetz sieht eine Pflicht zur Meldung von Verletzungen der Datensicherheit gegenüber dem → **EDÖB** vor, wenn von diesen ein hohes Risiko für die betroffene Person ausgeht (Art. 24 Abs. 1 → **revDSG**). Das Aufsichtsrecht in anderen Branchen kann ähnliche Regelungen enthalten. Zu denken ist auch an ausländische Meldepflichten, denen das Unternehmen untersteht. In gewissen Situationen kann es zudem aus taktischen und kommunikativen Gründen sinnvoll sein, einer Behörde auch ohne Pflicht Meldung zu erstatten. Natürlich kann eine Meldung ihrerseits eine Untersuchung und Sanktionen auslösen. Hier kann es sinnvoll sein, die selbst ermittelten Ergebnisse anzubieten.

Vorgelesen

Zivilkläger in den USA verlangen oft alle Unterlagen, welche den Behörden gegeben wurden. Eine Praxislösung: Dokumente werden den Behörden nicht abgegeben, sondern stattdessen vorgelesen bzw. auf deren Systemen eingetippt.

Behördenmeldungen sind in verschiedener Hinsicht problematisch. *Erstens* kann einer Pflicht zur Meldung oder Mitwirkung im Nachgang einer Meldung der Grundsatz des **strafprozessualen Selbstbelastungsprivilegs** (*"nemo tenetur"*) entgegenstehen. Auf diesen Grundsatz können sich auch juristische Personen berufen, doch legt das Bundesgericht ihn diesbezüglich restriktiv aus, etwa um zu verhindern, dass Aufsichts- und Strafbehörden

46 FINMA Aufsichtsmitteilung 5/20.
47 FINMA Rundschreiben 2017/6 (Direktübermittlung).

auf Unterlagen zugreifen können, welche Unternehmen aufgrund verwaltungsrechtlicher Gesetzesvorschriften zu erstellen haben (BGE 142 IV 207, E. 8.3.3). Macht ein Unternehmen Meldung, so sollte es dies grundsätzlich in der Annahme tun, dass die Unterlagen auch in weiteren Verfahren verwendet werden. Allenfalls können das sogar zivilrechtliche Schadenersatzprozesse im Rahmen der Aufarbeitung eines Fehlverhaltens sein. *Zweitens* sollte ein Unternehmen je nach Behörde auch damit rechnen, dass gemeldete Informationen an die Medien gelangen. Gemeint sind nicht Indiskretionen, wie sie überall vorkommen können, sondern Zugriffe über das **Öffentlichkeitsprinzip** (vgl. etwa BVerwG A-4781/2019 vom 17. Juni 2020). Auch hier gilt daher: Informationen an eine Behörde, die dem Öffentlichkeitsprinzip unterliegt, sollten bereits im Hinblick auf eine spätere Offenlegung abgefasst werden. *Drittens* ist in beschränktem Umfang, jedenfalls für involvierte Personen, ein Zugang zu Behördendokumenten auch über das **datenschutzrechtliche Auskunftsrecht** möglich.

6. **Meldung gegenüber Privaten?** Nebst der Behördenmeldung kann ein Unternehmen aus Gesetz oder Vertrag auch verpflichtet sein, private Stellen über einen Vorfall oder ein Fehlverhalten zu informieren. So sehen viele Verträge im Datenbereich heute Meldepflichten bei Verletzungen der Datensicherheit vor; in gewissen Fällen tut dies auch das Gesetz (Art. 24 Art. 3 und 4 revDSG). Kotierte Unternehmen müssen in der Schweiz gemäss Kotierungsreglement der SIX über gesicherte Tatsachen im eigenen Tätigkeitsbereich informieren, die neu und dem Kapitalmarkt nicht bekannt, aber potenziell kursrelevant sind. Als kursrelevant gelten Tatsachen, die geeignet sind, zu einer erheblichen Änderung des Börsenkurses zu führen (→ **Ad-hoc-Bekanntgabepflicht**). Unter gewissen Umständen, die in jedem einzelnen Fall sorgfältig abzuklären sind, kann allerdings während einer gewissen Zeit ein Bekanntgabeaufschub erlaubt sein, sofern strikte Geheimhaltung sichergestellt und Insiderhandel ausgeschlossen werden kann. Zu prüfen ist ferner, ob die externe Revisionsstelle des Unternehmens informiert werden muss, vor allem dann, wenn sich ein Schaden abzeichnet (insbesondere auch dann, wenn Rückstellungen gebildet werden müssen).

Droht ein Missstand zu einer Unternehmenskrise zu werden, sollte das Unternehmen frühzeitig auch eine **freiwillige Kommunikation** mit allfällig betroffenen Drittbetroffenen wie Kunden, Kreditgeber und andere Geschäftspartner erwägen; auf diese Weise könnte es die Kommunikation kontrollieren (agieren statt reagieren). Allerdings darf ein solcher Entscheid erst nach sorgfältiger Prüfung einer allfälligen Ad-hoc-Bekanntgabepflicht getroffen werden.

7. **Selbstanzeige?** Wurde im Rahmen einer internen Untersuchung ein bussenträchtiges Verhalten festgestellt, stellt sich regelmässig die Frage, ob das Unternehmen damit von sich aus auf die zuständigen Behörden zugehen soll, um auf diese Weise einen vollständigen oder teilweisen Sanktionserlass zu erhalten. In der Schweiz ist ein solcher im Kartellrecht sogar ausdrücklich vorgesehen (Art. 49a Abs. 2 → **KG**). Im Falle von Straftaten kann ein mit einer ausländischen Strafbehörde getroffener Vergleich (z.B. ein → **Deferred Prosecution Agreement** u.a. gegen Bezahlung einer Geldsumme) sogar dazu führen, dass es auch im Inland zu keiner Strafverfolgung mehr kommt (Doppelbestrafungsverbot, *"ne bis in idem"*). Allerdings ist jeweils zwischen der Strafverfolgung des Unternehmens und jener von Individuen zu unterscheiden. Insbesondere in den USA erwarten Behörden von Unternehmen regelmässig, dass sie gegen fehlbare Mitarbeiter vorgehen, oder die Behörden tun es selbst[48].

Sammelklagen

Sammelklagen haben in der Schweiz einen schweren Stand. So hat im "Diesel-Skandal" das Bundesgericht im Juli 2020 die Prozessfähigkeit der Stiftung für Konsumentenschutz bei ihrer Schadenersatzklage für rund 6'000 Autobesitzer aufgrund ihres Stiftungszwecks verneint (BGer 4A_43/2020 vom 16. Juli 2020).

8. **Zivilrechtliche Forderungen gegenüber Verantwortlichen?** Die Frage nach zivilrechtlichen Forderungen stellt sich oft erst im Nachgang einer internen Untersuchung. Typischerweise wird eine solche Forderung in der Geltendmachung von Schadenersatz bestehen. Kann oder soll nicht gegen einen Arbeitnehmer vorgegangen werden, so ist auch an ein Vorgehen gegenüber solidarisch haftenden Dritten zu denken (Art. 50/51 OR), auch wenn diese nur untergeordnet mitgewirkt haben. Die Durchsetzung kann gerichtlich erfolgen (was aber ohne Weiteres Jahre beanspruchen kann) oder – wo Gegenforderungen bestehen (z.B. Lohnforderungen eines Arbeitnehmers) – verrechnungsweise. Im Hinblick auf etwaige Schadenersatzforderungen ist es sinnvoll, bereits von Anfang an die Kosten der Untersuchung und durch das Fehlverhalten verursachte Schäden so festzuhalten, dass sie in einem späteren Prozess substanziiert und nachgewiesen werden können.

48 Vgl. hierzu das *„Yates-Memorandum"* des US-Justizministeriums, in welchem es 2015 ein verstärktes Vorgehen gegen fehlbare und verantwortliche Einzelpersonen in den jeweiligen Unternehmen ankündigte (https://www.justice.gov/archives/dag/file/769036/download).

> Die relative **Verjährungfrist** von deliktischen Ansprüchen beträgt seit 2020 normalerweise drei und nicht mehr ein Jahr (Art. 60 Abs. 1 OR). Das erlaubt ein längeres Zuwarten mit zivilrechtlichen Forderungen, etwa um Erkenntnisse aus einem Strafverfahren abzuwarten oder um den Schadensnachweis zu erleichtern.

9. **Abwehr von Ansprüchen und Sanktionen?** Auch dort, wo ein Unternehmen selbst das „Opfer" des Fehlverhaltens eines Mitarbeiters ist, kann ein Compliance-Verstoss zu gewichtigen Folgen auch für das Unternehmen selbst führen. Das gilt insbesondere dann, wenn dem Unternehmen Mängel in der Compliance bzw. → **Corporate Governance** nachgewiesen werden können, es also das Fehlverhalten früher hätte entdecken oder gar verhindern müssen. Kommt es zu einer grösseren Verfehlung in einem Unternehmen, ist es nicht ungewöhnlich, dass dies nebst einer internen Untersuchung auch eine strafrechtliche Untersuchung sowie in regulierten Branchen eine (davon unabhängige) aufsichtsrechtliche Untersuchung und schliesslich auch zivilrechtliche Ansprüche von Geschädigten gegen Unternehmen und verantwortliche Organe zur Folge haben kann. In allen drei Fällen wird erfahrungsgemäss versucht werden, auf die Unterlagen und Erkenntnisse der internen Untersuchung zurückzugreifen, was entsprechend zu berücksichtigen ist.

10. **Compliance-Massnahmen?** Auch wenn entsprechendes von Behörden nicht verlangt wird bzw. mit diesen nicht vereinbart wurde[49], tut ein Unternehmen gut daran, aus jedem untersuchten Vorfall seine Lehren zu ziehen und Massnahmen zu ergreifen, damit sich ein entsprechender Fall möglichst nicht wiederholen kann oder mindestens frühzeitig entdeckt wird. Dies sollte das Unternehmen auch dokumentieren, um die saubere Aufarbeitung von Missständen – sollten sie später trotz allem ans Licht kommen – belegen zu können. Die Aufarbeitung kann einerseits personelle Massnahmen (wie etwa die Sanktionierung fehlbarer Mitarbeiter und interne Bekanntmachung solcher Fälle) und andererseits die Einführung von zukunftsgerichteten technischen und organisatorischen Massnahmen verlangen (wie z.B. weitgehende Kontrollen, neue Weisungen, Schulungen, Systeme zur Früherkennung von Verstössen, Auditprogramme, veränderte Prozesse und Zuständigkeiten, neue Compliance-Stellen).

11. **Anpassung der Geschäftsabschlüsse?** Wird ein Fehlverhalten aufgedeckt, welches im Ergebnis zu einer falschen Darstellung der Finanzlage bzw. zu einer fehlerhaften Rechnungslegung eines Unternehmens geführt hat, kann sich die Frage

49 Vgl. für die Schweiz etwa den Korruptionsfall von ABB (https://resources.news.e.abb.com/attachments/published/13364/en-US/6ED2BF392D88/10-37-US-d.pdf) oder Panalpina (https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2011/02/16/11-04-10panalpina-world-dpa.pdf).

der nachträglichen Anpassung der Geschäftsabschlüsse aufdrängen. Dazu → **Q54**. Vgl. auch die Frage der „internen Verjährung“ eines Fehlverhaltens in → **Q17**. Die Information der externen Revisionsstelle wurde bereits weiter vorne thematisiert.

12. **Öffentlichkeitsarbeit?** Liegt ein möglicher Compliance-Verstoss oder sonstiges Fehlverhalten vor, kann dies insbesondere das Interesse der Öffentlichkeit auf sich ziehen. Es genügt hierzu ein Mitarbeiter oder eine sonst involvierte Person, die etwas auf Social Media postet oder mit Medienvertretern spricht. Nebst der Aufarbeitung des Sachverhalts und den weiteren zu treffenden Massnahmen sollte auch die Öffentlichkeitsarbeit geplant und vorbereitet sein. Das gilt insbesondere dann, wenn der Verstoss das Potenzial hat, zur Krise für das Unternehmen oder gar zum Skandal zu werden. Die Pressestelle muss vorbereitet sein, falls Anfragen kommen. Plant ein Journalist eine Enthüllung, wird er dem Unternehmen nur sehr kurze Zeit für eine Stellungnahme geben. Dabei sollten die Anwälte an der externen Kommunikation zwar mitwirken (damit sie das Unternehmen rechtlich nicht unnötig angreifbar macht), die Bedenkenträger unter ihnen sollten sie aber sicher nicht bestimmen (damit die Kommunikation nicht unglaubwürdig wird, weil aus juristischen Gründen das Offenkundige bestritten wird, oder sie nicht vertrauenswürdig ist, weil geschwiegen wird, obwohl die Öffentlichkeit erwartet, dass das Unternehmen Verantwortung übernimmt). Allerdings sind auch Schnellschüsse zu vermeiden: Ein Unternehmen darf sich zur Abklärung des Sachverhalts Zeit ausbedingen, solange es den Eindruck erweckt, dass es dies auch ernsthaft und schonungslos tun will[50]. Für Empörung sorgen in der Öffentlichkeit vor allem Fälle, in denen das in ein Unternehmen gesetzte Vertrauen von diesem gebrochen wird – auch wenn kein Rechtsverstoss vorliegt. Dem muss in der Kommunikation vorgebeugt werden. Ob offensiv oder defensiv, proaktiv oder reaktiv kommuniziert wird, hängt vom Einzelfall ab. Wie aber Kommunikationsprofis betonen: Es ist nicht möglich, nicht zu kommunizieren.

Skandal?

Was braucht es, damit aus einem Missstand ein Skandal wird? Nicht die juristische Relevanz zählt, sondern für wie empörend der Missstand gehalten wird. Nur etwa 12 Prozent der Skandale im deutschsprachigen Raum betreffen eindeutige Rechtsverstösse (Quelle: Krisennavigator.de).

50 Hier kann es sich lohnen, einen passenden Kommunikationsrhythmus zu etablieren, in welchem sachlich, richtig und ehrlich informiert wird; dies kann Medienschaffende davon abhalten, investigativ zu arbeiten, was meist erfolgreich ist, da sich immer jemand findet, der „plaudert“.

In der Krisenkommunikation spielen neben den traditionellen Medien, welche ein Thema aufgreifen und allenfalls auch ausschlachten, die verschiedenen **Social Media** Plattformen und ihre Benutzer eine ebenso wichtige Rolle. Ein Unternehmen sollte daher mit Kommunikationsprofis zusammenarbeiten, welche auch diese Kanäle kennen. Ein Unternehmen, welches halbwegs in der Öffentlichkeit steht, sollte diese zudem systematisch beobachten, um frühzeitig für die Reputation des Unternehmens gefährliche Entwicklungen erkennen und darauf reagieren zu können. Hier ist ein Grundpfeiler der Krisenkommunikation – die Wahrung der Dialogbereitschaft – besonders wichtig. Auch einzelne Stimmen können zu einem Shitstorm führen.

Do's	Don'ts
• Rechnen Sie bei jeder Eingabe an eine Behörde damit, dass auch andere Zugang zu den Unterlagen erhalten. • Klagen Sie erst dann, wenn Sie Ihren Fall beisammen haben. Der Prozess wird sowieso lange dauern. • Kommunizieren Sie unangenehme Wahrheiten proaktiv, weil Sie dann nicht nur glaubwürdiger sind, sondern die Kommunikation auch besser kontrollieren können. • Für nicht bestreitbare Missstände brauchen Sie in der Krisenkommunikation eine glaubwürdige Erklärung. • Halten Sie sich an die Wahrheit in der Kommunikation, sonst verlieren Sie ihre Glaubwürdigkeit. • Kommunizieren Sie über Missstände klar und anschaulich, denn sonst gehen Behörden, Medien und andere Drittbetroffene automatisch von Schlimmerem aus.	• Zählen Sie nicht darauf, dass ein Strafverfahren kurzfristig Ergebnisse liefert – ausser vielleicht im Falle einer Hausdurchsuchung, Beschlagnahmung oder Festnahme. • Betreiben Sie Öffentlichkeitsarbeit nicht nur mit klassischen Medien, sondern auch auf Social Media. • Vermeiden Sie in der Kommunikation alles, was als „Salamitaktik" wahrgenommen werden könnte. Sonst wird Ihnen nicht vertraut.

Do's	Don'ts
• Wenn Sie der Öffentlichkeit eine unabhängige Aufklärung der Vorkommnisse versprechen, dann setzen Sie hierzu einen tatsächlich unabhängigen Experten ein und nicht Ihnen vertraute Personen oder gar Ihre Hauskanzlei.	

Wann Sie externe Unterstützung beiziehen sollten

- Wenn es um die Durchführung eines **Strafverfahrens** geht.
- Wenn Sie nicht wissen, welche **Meldepflichten** Sie haben oder wenn Sie auf deren Erfüllung nicht vorbereitet sind.
- Wenn Sie eine **Selbstanzeige** einreichen möchten.
- Wenn Sie in ein **Aufsichtsverfahren** geraten bzw. zu geraten drohen.
- Wenn ein **anonymer Behördenkontakt** („*no name*"-Basis) nötig ist.
- Für die Führung von **Zivilprozessen**, wenn Ihre Rechtsabteilung nicht Zeit oder Erfahrung dafür hat.
- Wenn Sie ein professionelles **Compliance-System aufbauen** müssen.
- Für professionelle **Krisenkommunikation**, soweit Sie nicht schon eigene Profis dafür haben.
- Für die Überwachung von **Social-Media-Aktivitäten**.
- Wenn Sie eine unbefangene **Aussensicht** oder Zweitmeinung benötigen.

Häufige Fragen und Antworten

Q48. Welche Rechte hat ein geschädigtes Unternehmen in einem Strafverfahren?

A: Als **geschädigte Person** gilt im Strafverfahren eine Person, welche in ihren Rechten unmittelbar verletzt wurde, z.B. indem sie in ihrem Vermögen geschädigt wurde. Das geschädigte Unternehmen gilt zunächst als **Verfahrensbeteiligter**. Kann das geschädigte Unternehmen glaubhaft machen, dass es durch die behördlichen Verfahrenshandlungen unmittelbar betroffen ist, stehen ihm die zur Wahrung seiner Interessen erforderlichen Verfahrensrechte einer Partei zu. Darunter fallen die aus dem Anspruch auf rechtliches Gehör fliessenden Rechte (siehe unten).

Für das geschädigte Unternehmen besteht die Möglichkeit, sich im Strafverfahren als **Privatklägerschaft** zu konstituieren, womit ihm sämtliche Rechte einer **Partei** im Strafverfahren zukommen. Durch die Einreichung eines Strafantrages (das Strafdelikt ist in diesem Fall nur auf Antrag zu verfolgen) erfolgt die Konstituierung als Privatklägerschaft automatisch (Art. 118 Abs. 2 → **StPO**).

Die **Parteirechte** umfassen mitunter nachfolgende Rechte:

- Recht auf **Akteneinsicht**, sofern keine öffentlichen oder privaten Geheimhaltungsinteressen entgegenstehen;
- Recht auf **Teilnahme an Verfahrenshandlungen** (z.B. Anwesenheitsrecht bei Beweiserhebung durch die Staatsanwaltschaft);
- Recht auf Rechtsbeistand;
- Recht zur Äusserung zur Sache und zum Verfahren;
- Recht zur Stellung von **Beweisanträgen**.

In der Praxis kommt der **Akteneinsicht** besondere Bedeutung zu, da die Strafverfolgungsbehörden Möglichkeiten der Beweiserhebung haben, welche einer privaten Person nicht zugänglich sind. Sie kann z.B. Hausdurchsuchungen durchführen, Dritte (z.B. Cloud-Provider) zur Herausgabe von Unterlagen oder Daten zwingen oder den Fernmeldeverkehr überwachen oder Fernmeldeteilnehmer identifizieren lassen (z.B. Anhand von IP-Adresssen). Über die Akteneinsicht kann das Unternehmen an die Ergebnisse dieser Beweiserhebungen gelangen. Der Staatsanwaltschaft kommt bei dem Entscheid, *wann* dem geschädigten Unternehmen im Laufe des Verfahrens Akteneinsicht gewährt wird, jedoch grosses Ermessen zu. Manche Staatsanwälte werden dem Unternehmen erst dann Einsicht gewähren, wenn die beschuldigte Person selbst Einsicht hat nehmen können. Umgekehrt kann es für das Unternehmen, welches der Staatsanwaltschaft selbst Unterlagen zur Verfügung gestellt hat, von Relevanz sein, wann diese der beschuldigten Person die Unterlagen offenlegt. Vor der ersten einlässlichen Einvernahme der beschuldigten Person muss die Staatsanwaltschaft dies nicht tun und tut dies normalerweise auch nicht, ausser wenn klar ist, dass die beschuldigte Person ansonsten ohnehin von ihrem Aussageverweigerungsrecht Gebrauch machen wird.

Q49. Wie läuft eine Strafuntersuchung normalerweise ab?

A: Zweck der Strafuntersuchung ist die Vornahme (weiterer) Verfahrensschritte, um den Deliktsvorwurf und Sachverhalt in tatsächlicher oder rechtlicher Hinsicht weiter abzuklären. Letztlich dienen die Handlungen im Rahmen der Strafuntersuchung dazu, die notwendige Basis zu schaffen, damit die Staatsanwaltschaft entscheiden kann, ob ein Strafverfahren eingeleitet bzw. ein Strafbefehl erlassen werden soll, oder ob das Verfahren eingestellt wird. Die Leitung der Strafuntersuchung obliegt der zuständigen **Staatsanwaltschaft.**

Eine Strafuntersuchung lässt sich typischerweise in nachfolgende Stadien unterteilen:

- **Entscheid über Eröffnung einer Strafuntersuchung:** Bevor eine Strafuntersuchung durchgeführt wird, entscheidet die Staatsanwaltschaft in einem ersten Schritt, ob eine solche überhaupt eröffnet wird. Wird der Staatsanwaltschaft, gestützt auf die Ergebnisse einer internen Untersuchung, eine **Strafanzeige** zugestellt, wird diese ihre Zuständigkeit eruieren und die Strafanzeige sowie allfällige Akten studieren. Ergibt sich aus der Strafanzeige, dass die Führung eines Strafverfahrens keine Aussicht auf Erfolg hat (weil die Straftat z.B. bereits verjährt ist oder offensichtlich keine Straftatbestände erfüllt sind) wird die Staatsanwaltschaft eine **Nichtanhandnahmeverfügung** erlassen. Das bedeutet, dass sich die Staatsanwaltschaft der Sache nicht annehmen wird. Das Gesetz schreibt vor, dass eine solche Verfügung lediglich zurückhaltend erlassen werden darf. Im Zweifelsfall ist stets eine Untersuchung zu eröffnen (*in dubio pro duriore*).

  Die Staatsanwaltschaft kann in diesem Stadium des Verfahrens weitere Abklärungen vornehmen, um den Tatverdacht zu erhärten. So können vom Unternehmen, welches die Strafanzeige gestellt hat, weitere (ergänzende) Informationen eingefordert werden, indem z.B. verlangt wird, dass weitere Beweise geliefert werden, um die tatbestandsmässige Organstellung einer Person zu untermauern. Die Staatsanwaltschaft hat ferner die Möglichkeit, die Strafanzeige zur weiteren Durchführung **ergänzender Ermittlungen** der Polizei zu übergeben, falls aus der Strafanzeige der Tatverdacht nicht deutlich hervorgeht.

- **Offizielle Eröffnung der Strafuntersuchung:** Besteht ein **hinreichender Tatverdacht**, m.a.W. lassen die Ergebnisse der internen Untersuchung sowie ggf. weitere Abklärungen konkret auf das Vorliegen einer strafrechtlich relevanten Verhaltensweise schliessen, wird die Staatsanwaltschaft die Strafuntersuchung eröffnen. Dies geschieht per offizieller **Eröffnungsverfügung**, in der die beschuldigte Person sowie der Tatvorwurf bezeichnet werden. Die Eröffnungsverfügung ist den beschuldigen Personen nicht zwingend zu eröffnen bzw. zuzustellen, sondern kann auch in Form einer Aktennotiz erfolgen (*ad acta*). Mit Eröffnung der Strafuntersuchung können die involvierten Parteien ihre Rechte vollumfänglich geltend machen.

- **Beweiserhebung:** Die Staatsanwaltschaft erhebt nun jene Beweise, die notwendig sind, um die Strafuntersuchung zu beenden, indem entweder ein Strafverfahren eingeleitet wird, ein Strafbefehl erlassen wird oder das Verfahren eingestellt wird. Die Staatsanwaltschaft kann mitunter Zeugen/Auskunftspersonen zur Einvernahme vorladen, Durchsuchungen anordnen oder Berichte einholen. Der Staatsanwaltschaft steht dabei die Unterstützung der **Polizei** zur Verfügung (z.B. für die Spurensicherung oder IT-Auswertung). Das Verfahren kann auf weitere Beschuldigte sowie Straftatbestände ausgedehnt werden (sog. Verfahrensausdehnung).

- **Beendigung der Untersuchung:** Hat die Staatsanwaltschaft eine Strafuntersuchung offiziell eröffnet, ist diese auch abzuschliessen. Erachtet die Staatsanwalt-

schaft die Strafuntersuchung für vollständig, kann sie die Untersuchung durch **Erhebung einer Anklage** beenden, womit die Prozessherrschaft dem Gericht übertragen wird. Dieses hat sodann über das relevante Verhalten zu urteilen. Die Staatsanwaltschaft kann die Strafuntersuchung ebenfalls per **Strafbefehl** beenden, wenn z.B. ein umfassendes Geständnis vorliegt. Möglich ist, dass die Staatsanwaltschaft im Rahmen der Strafuntersuchung zum Ergebnis kommt, dass kein Straftatbestand erfüllt ist. In diesem Fall wird die Staatsanwaltschaft die Strafuntersuchung per **Einstellungsverfügung** einstellen.

Literatur:

Bürge, Lukas: Polizeiliche Ermittlung und Untersuchung – Charakteristik, Abgrenzungen und Auswirkungen auf Beschuldigtenrechte, Bern 2018

Q50. Kann das Unternehmen ein Strafverfahren beenden, wenn es sich mit der beschuldigten Person geeinigt hat?

A: Dies hängt vom Deliktsvorwurf ab, der im Raum steht, d.h. ob es sich um ein Offizialdelikt (z.B. Betrug, Veruntreuung) oder ein Antragsdelikt (z.B. Hacking, Daten- oder Sachbeschädigung, Verletzung von Geschäftsgeheimnissen) handelt. Im letzteren Falle ist der **Strafantrag** des Geschädigten eine Voraussetzung für das Verfahren. Wird er **zurückgezogen**, fällt auch das Strafverfahren dahin. Bei Offizialdelikten kann das geschädigte Unternehmen eine sog. **Desinteresse-Erklärung** abgeben (d.h. die Erklärung, dass es nicht weiter an einer Strafverfolgung interessiert ist, weil es sich z.B. mit dem Schädiger geeinigt hat). Die Strafbehörden haben bei Offizialdelikten jedoch unabhängig von einer Desinteresse-Erklärung abzuklären, ob in tatsächlicher und rechtlicher Hinsicht eine strafbare Handlung vorliegt (BGer 6B_1200/2016 vom 30. März 2017, E. 1.3 m.w.H.). Sie können ein Verfahren in der Folge aus Opportunitätsgründen einstellen, müssen dies aber nicht. Relevant sind für solche Entscheide die Schwere des Delikts und die Schwierigkeit der Fortführung der Ermittlungen, falls etwa das geschädigte Unternehmen nicht mehr mitwirkt.

Q51. Können wir für unsere Aufwendungen zur internen Untersuchung im Strafverfahren eine Entschädigung verlangen?

A: Grundsätzlich ja. Zunächst besteht die Möglichkeit, die berechtigten Aufwendungen einer internen Untersuchung im Rahmen einer **Schadenersatzforderung** aufgrund eines unerlaubten Verhaltens oder – im Falle einer Verletzung des Arbeitsvertrags – einer Vertragsverletzung geltend zu machen. Dies kann sowohl im Strafverfahren (adhäsionsweise) als auch in einem zivilrechtlichen Forderungsprozess oder – einfacher – durch **Verrechnung etwa mit der Lohnforderung** eines verantwortlichen Mitarbeiters erfolgen (soweit die diesbezüglichen Voraussetzungen erfüllt sind). Vgl. dazu auch → **Q16**.

Art. 433 → **StPO** sieht eine weitere Möglichkeit vor: Danach hat eine Privatklägerin Anspruch auf angemessene **Entschädigung** für notwendige Aufwendungen im Verfahren, wenn sie obsiegt oder wenn der Beschuldigte nach Art. 426 StPO kostenpflichtig ist. Gemäss Art. 426 Abs. 2 StPO können dem Beschuldigten die Verfahrenskosten bei einer Einstellung oder einem Freispruch ganz oder teilweise auferlegt werden, wenn er „rechtswidrig und schuldhaft die Einleitung des Verfahrens bewirkt oder dessen Durchführung erschwert" hat. Eine Entschädigung kann die Privatklägerin insbesondere dann fordern, wenn ihre Abklärungen (namentlich die interne Untersuchung und deren Resultate) **wesentlich zur Abklärung** der mutmasslichen Strafsache und Verurteilung **beigetragen** und somit das Strafverfahren effizienter gemacht haben (mit entsprechend geringer ausfallenden Verfahrenskosten etc.). Die Privatklägerin bei Verurteilung der beschuldigten Person hinsichtlich der Verteidigungskosten im Zusammenhang mit der Strafklage auf den Zivilweg zu verweisen, ist gemäss bundesgerichtlicher Rechtsprechung mit Art. 433 StPO nicht vereinbar (BGer 6B_310/2012 vom 11. Dezember 2012, E. 4.3).

Q52. Kann das Unternehmen für eine Straftat des Mitarbeiters haften?

A: Im schweizerischen Strafrecht können einem Unternehmen Straftaten zugerechnet werden (Art. 102 → **StGB**). Das Unternehmen kann strafrechtlich verantwortlich gemacht werden, wenn aufgrund von Organisationsmängeln im Unternehmen eine verübte Straftat keiner konkreten natürlichen Person zugerechnet werden kann. Das Unternehmen haftet also nicht für die Straftat selbst, sondern subsidiär (d.h. falls keine natürliche Person haftbar gemacht werden kann) für **Mängel in der Organisation.** Das Unternehmen kann in einem solchen Fall mit einer Busse bis zur Höhe von CHF 5 Mio. sanktioniert werden, wobei bei der Bemessung der Busse Aspekte wie die Schwere der Tat, die Schwere des Organisationsmangels, der angerichtete Schaden sowie die wirtschaftliche Leistungsfähigkeit des Unternehmens miteinbezogen werden.

Unabhängig von der Strafbarkeit einer natürlichen Person haftet das Unternehmen für bestimmte Straftaten, wenn es **nicht alle erforderlichen und zumutbaren Vorkehrungen** getroffen hat, um die Straftat zu verhindern. Als Beispiel kann das Unternehmen – neben dem eigentlichen Täter – für Geldwäscherei sowie Bestechungshandlungen haften. Welche Anforderungen an die erforderlichen und zumutbaren Vorkehrungen gestellt werden, definiert sich im Einzelfall. Zumindest bedarf es wohl eines unabhängigen und wirksamen **Compliance Managements**.

Das **Verwaltungsstrafrecht** sieht ebenfalls Situationen vor, in welchen das Unternehmen für Verfehlungen im Betrieb sanktioniert werden kann, wenn der Aufwand zur Ermittlung der verantwortlichen Personen im Hinblick auf die Schwere einer Straftat unverhältnismässig wäre.

Literatur:

Nadelhofer do Canto, Simone: Millionenbusse gegen Alstom-Tochter wegen ungenügender Vorkehrungen gegen Bestechung, Zeitschrift für Gesellschafts- und Kapitalmarktrecht (GesKR) 1/2012, 129 ff.

Schmid, Niklaus: Strafbarkeit des Unternehmens: die prozessuale Seite, Zeitschrift für juristische Weiterbildung und Praxis (recht), 201 ff.

Q53. Welche Einschränkungen müssen wir bei der Kommunikation und Kooperation mit ausländischen Behörden beachten?

A: Unter dem schweizerischen Strafrecht sind **Handlungen für einen fremden Staat** strafbewehrt (Art. 271 → **StGB**). Amtliche Handlungen auf schweizerischem Territorium obliegen den schweizerischen Behörden und dürfen nicht von ausländischen Behörden vorgenommen werden. Gleichzeitig darf auch keine Hilfeleistung zur Vornahme solcher Handlungen geleistet werden. Als amtliche Handlungen gelten z.B. Beweiserhebungen durch ausländische Behörden. Solche Handlungen sind auf dem offiziellen Amts- oder Rechtshilfeweg vorzunehmen. Der Einzelne darf dazu auch keine Hilfeleistungen leisten, indem er z.B. auf Anfrage für ein ausländisches Verfahren in der Schweiz Beweise erhebt und den ausländischen Behörden übermittelt. Darunter fällt auch die Beantwortung von Auskunfts- und Herausgabeersuchen ausländischer Behörden, sofern es sich um Informationen oder Unterlagen handelt, die sich auf schweizerischem Territorium befinden (bei lokalen Servern, aber nicht mehr unbedingt, wenn die Cloud zur Datenablage eingesetzt wird). Das Schweizer Strafrecht ist hier strenger als viele ausländische Rechtsordnungen. Im Fachjargon ist von einer „*blocking statute*" die Rede, weil die Bestimmung den Zugriff ausländischer Behörden auf Unterlagen in der Schweiz blockieren kann.

Eine **Ausnahme** besteht dort, wo ein Unternehmen für ein eigenes Verfahren im Ausland eigene Unterlagen oder Informationen freiwillig herausgeben oder vorlegen will. Damit die Ausnahme greift, dürfen jedoch keine strafrechtlichen oder strafähnlichen Sanktionen im Widerhandlungsfalle angedroht sein. Art. 271 StGB sieht zwar die Möglichkeit von Bewilligungen vor, doch werden diese nur unter sehr restriktiven Bedingungen erteilt, jedenfalls wenn die Herausgabe von Informationen oder Unterlagen auch Dritte (bspw. Mitarbeiter) betreffen kann.

Ferner wird in der Schweiz der **wirtschaftliche Nachrichtendienst** sanktioniert (Art. 273 StGB). Es soll verhindert werden, dass Schweizer Geschäftsgeheimnisse an eine ausländische Behörde weitergegeben werden. Dies schützt also typischerweise die Geschäftsgeheimnisse von Schweizer Geschäftspartnern eines Unternehmens. Im Gegensatz zu Art. 162 StGB, welcher nur in der Schweiz verletzt werden kann, gilt für Art. 273 StGB das Weltrechtsprinzip, d.h. es spielt keine Rolle, wo gehandelt wird. Ähnliches gilt im Bereich des **Berufsgeheimnisses** (z.B. Bankkundengeheimnis). Auch

hier kann die Offenlegung an ausländische Behörden zur Strafbarkeit führen. Sollen in einem ausländischen Behörden- oder Gerichtsverfahren Daten offengelegt werden, kann es daher erforderlich sein, vorgängig entsprechende Schwärzungen vorzunehmen → **SWISS SECRECY & PRIVACY REVIEWS**.

Q54. Wann müssen Fehler in früheren Abschlüssen angepasst werden?

A: Unter den internationalen Rechnungsstandards (IFRS, US-GAAP) sowie unter Swiss GAAP FER sind Fehler in früheren Abschlüssen mittels Anpassung der Vorjahreszahlen in der aktuellen Jahresrechnung zu berücksichtigen und im Anhang zu erläutern (sogenanntes *"Restatement"*). Wesentliche Fehler erfordern eine rückwirkende Anpassung im ersten auf die Entdeckung folgenden Abschluss. Handelsrechtlich ist eine solche rückwirkende Anpassung der Vorjahreszahlen in der aktuellen Jahresrechnung nur zulässig, falls das Fehlverhalten lediglich zu einem wesentlichen Gliederungsfehler in der Jahresrechnung des Vorjahres führte. Rückwirkende Anpassungen des Vorjahres, welche eine Veränderung der Eigenkapitalposition zur Folge hätten, sind hingegen nicht zulässig, sondern über die Erfolgsrechnung des laufenden Jahres vorzunehmen. Diese Buchungen sind ebenfalls im handelsrechtlichen Abschluss im Anhang zu erläutern. In Ausnahmefällen können schwerwiegende Fehler in den Werten des Vorjahres ein Zurückziehen der Vorjahresrechnung durch den Verwaltungsrat notwendig machen, welche nach Korrektur, ggf. neu geprüft, dem zuständigen Organ erneut vorgelegt wird. Die Rechtsfolgen der ursprünglichen Genehmigung des zuständigen Organs sind dabei zu beachten. [Stand April 2021]

Literatur:

Buchmann René, Praxisänderungen im neuen HWP „Buchführung und Rechnungslegung", ST 10/14 S. 880 ff., 880.

Gedanken zum Thema.

Strafuntersuchungen und interne Untersuchungen haben oft ganz unterschiedliche Ziele. Bei ersteren geht es um öffentliche Anklagen, letztere sollen dagegen oft einfach Unternehmen helfen, zu verstehen, ob etwas und – wenn ja, warum etwas – schiefgelaufen ist, um die nötigen Korrekturen vorzunehmen. Leider ist aber eine unheillige, mitunter auch unfreiwillige «Public-Private-Partnership» nicht ausgeschlossen. Die Staatsanwaltschaft muss von Amtes wegen alle bedeutenden Tatsachen abklären. Da liegt es nicht fern, sich auch an den Erkenntnissen einer internen Untersuchung bedienen zu wollen. Die Rechte der betroffenen Personen, inklusive der Unternehmen, werden dann aufs Spiel gesetzt. Unsere Strafprozessordnung ist darauf nicht vorbereitet, das sieht man auch an der Rechtsprechung zur Geltung des Anwaltsgeheimnisses. Deshalb müssen interne Untersuchungen so aufgegleist werden, dass die Rechte der Einzelnen gewahrt bleiben. Man sollte etwa befragte Personen mindestens warnen und ihnen keine Geheimhaltungsversprechen machen, die man – wenn es hart auf hart kommt – vielleicht gar nicht halten kann.

Sabine Gless
Professorin für Strafrecht und Strafprozessrecht
Universität Basel

10. Werkzeuge für eDiscovery

Kurz gesagt

- Findet ein Review statt, werden normalerweise alle Daten (E-Mails, Dokumente, etc.) in ein separates sog. Review-System geladen, in welchem diese von mehreren Personen gleichzeitig gesichtet und klassifiziert werden können; bei einem Review können das ohne Weiteres 100‘000 und mehr Dokumente sein.
- Um die Menge der manuell zu sichtenden Daten zu reduzieren, stehen heute zahlreiche verschiedene Werkzeuge und Such-, Deduplizier- und Filtermethoden bereit, mit denen nicht mehr nur nach Texten, sondern auch nach Mustern gesucht werden kann („künstliche Intelligenz“).
- Während die Verarbeitung von E-Mails und Dokumenten heute kein Problem ist, ist die Übernahme von Daten aus neuen Datenquellen wie Chats, Videokonferenzen oder *Cloud-Tools* noch eine Herausforderung und nicht überall vollständig möglich.

Worum es geht

Müssen grosse Mengen an elektronischen Daten aus Unternehmen für interne Untersuchungen oder andere Vorhaben (z.B. Zivilprozesse, Auskunftsersuchen, Behördenanfragen) verarbeitet werden, braucht es dafür spezielle Werkzeuge. Mit ihnen können die Daten gesammelt, konvertiert, lesbar gemacht, aufbereitet, analysiert, gesichtet und „produziert“ werden, d.h. für die Übergabe an Dritte hergerichtet werden. Der Markt für solche „eDiscovery“-Tools ist inzwischen auch für Experten nur noch schwer überschaubar. Wer sich mit dem Thema beschäftigt, muss zwar nicht jedes Werkzeug kennen, aber sollte mit den wichtigsten Einsatzmöglichkeiten vertraut sein.

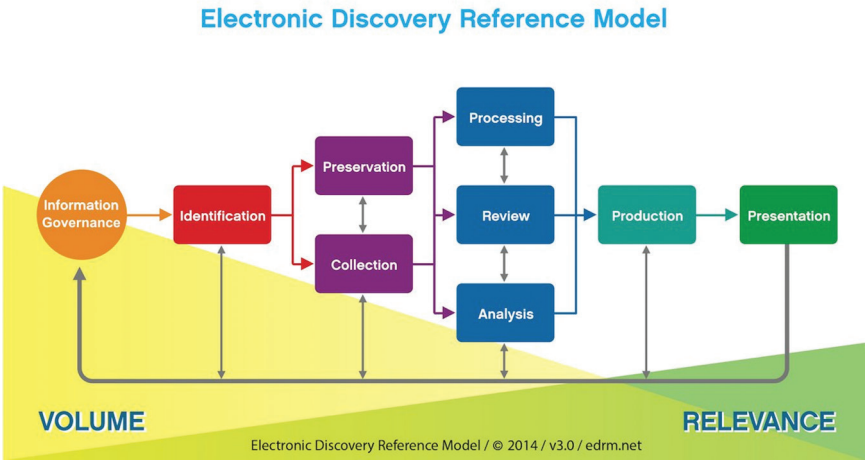
Worauf zu achten ist

- Jedes Tool hat seine eigenen Schwerpunkte und Stärken. Es gibt kein Werkzeug, das alles optimal abdeckt. Darum werden *Tools* oft kombiniert.
- Der Markt ist stark umkämpft und die Anbieter versprechen dabei regelmässig das Blaue vom Himmel, vor allem in Bezug auf den Einsatz von „künstlicher Intelligenz“.
- Normalerweise kaufen Unternehmen die Software nicht, sondern mieten sie als Service im Bedarfsfall.

eDiscovery?

Unter eDiscovery versteht man die Identifikation, die Sicherung, das Einsammeln, die Verarbeitung, die Sichtung, die Analyse und die Produktion elektronisch gespeicherter Informationen (*“electronically stored information”*, ESI) für die Zwecke der sog. Discovery-Phase im Rahmen eines Common-Law-Zivilprozesses.

- Insbesondere Analyse-Werkzeuge brauchen viel Erfahrung in der Handhabung; die relevanten Dokumente finden sich auch mit den besten *Tools* nicht von allein.



International hat sich das ***"Electronic Discovery Reference Model"*** (**EDRM**) zur Illustration der verschiedenen Phasen einer eDiscovery durchgesetzt: In einer ersten Phase werden die relevanten Daten identifiziert, dann gesichert (*"Preservation"*) und eingesammelt (*"Collection"*), in der nötigen Form aufbereitet (*"Processing"*), gesichtet (*"Review"*) und analysiert und schliesslich wieder ausgegeben (*"Production"*) und präsentiert (*"Presentation"*).

Wie vorzugehen ist

1. **Legal Hold Management.** In grösseren Unternehmen wird heute Software eingesetzt, um *Legal Holds* (d.h. angeordnete Vernichtungsstopps) zu verteilen, zu dokumentieren und zu verwalten. Zum Thema *Legal Hold* vgl. → **DIE RICHTIGE VORBEREITUNG** und → **ERSTE SCHRITTE**.

2. **Forensische Datensicherung.** Bevor Daten ausgewertet werden können, müssen sie gesichert werden. Je nach Quelle ist dafür unterschiedliche Software und teils auch Hardware erforderlich. Die Datensicherung wird deshalb als „forensisch" bezeichnet, weil sie Beweiszwecken dient. Sie muss so durchgeführt werden, dass die Daten durch die Sicherung nicht bewusst oder unbewusst verändert werden (Beweisintegrität)[51]. Dies muss auch entsprechend dokumentiert wer-

51 Ein hierbei wichtiges Verfahren ist der Einsatz von → **Hash-Werten**.

den. Im Einzelfall muss beurteilt werden, ob nur bestimmte Daten eines Geräts gesichert werden sollen (z.B. den Inhalt eines Verzeichnisses) oder das Gerät mit seinen Inhalten integral gesichert wird (d.h. erst später bestimmt wird, welche Daten weiterverarbeitet werden). In der Praxis wird für letzteres spezielle Software benutzt. Grössere Unternehmen, die regelmässig (z.B. für US-Zivilprozesse) in ihrem Betrieb Daten forensisch sichern müssen, setzen gerne auch Software ein, mit welcher sie über ihr internes Netzwerk von zentraler Stelle aus die verschiedenen relevanten Datenquellen sichern können (vgl. auch nächster Punkt).

Gelöschte Daten

Wo Daten nicht in der Cloud oder einem virtuellen System sondern auf einem herkömmlichen Datenträger gespeichert werden (z.B. Notebook, USB-Stick), kann es im Einzelfall auch möglich sein, mit der passenden Software auf gelöschte Daten zurückzugreifen. Zur Relevanz: → **Q56**.

Die umfassendste Sicherung eines Geräts ist die sog. **Spiegelung**. Es wird ein 1:1-Abbild der gesamten Datenträger („*Image*“) erstellt. Diese Methode wird gerne bei Notebooks und anderen mobilen Geräten benutzt. Eine Spiegelung benötigt i.d.R. kein Login, d.h. der Benutzername und das Passwort des Benutzers müssen nicht bekannt sein. Allerdings kann die Spiegelung erschwert werden oder nutzlos sein, wenn der **Datenträger verschlüsselt** ist. Verschlüsselt ein Unternehmen seine Notebooks, wird es daher gut beraten sein, hierfür einen Zweit- oder Generalschlüssel zu haben, um auch ohne Benutzer-Login an die Daten zu gelangen. Bei persönlichen Mobilgeräten (z.B. Mobiltelefonen) muss jedoch in der Regel der **Entsperr-Code** bekannt sein, da die Geräte ansonsten über Sicherheitslücken gehackt werden müssen, damit auf die Daten zugegriffen werden kann. Das ist nicht in jedem Fall möglich.

3. **eDiscovery-Schnittstellen.** Wenn neue Software angeschafft oder abonniert[52] wird, sollte darauf geachtet werden, dass diese über Schnittstellen für eDiscovery verfügt, so dass forensische Datensicherungen einfach möglich sind. Wer beispielsweise seinen E-Mailserver von Microsoft in der Cloud betreiben lässt, kann von Microsoft einen „Compliance“-Zugang erhalten, mit dem Postfächer einzelner Benutzer gesperrt werden können (sodass keine Löschungen mehr möglich sind) und mit dem Daten sich so herunterladen lassen, dass sie für Reviews einfach weiterverarbeitet werden können.

52 Software-as-a-Service, also Software, die in der Cloud betrieben und als Dienstleistung angeboten wird.

4. **Extrahieren, Konvertieren und Aufbereiten.** Liegen gesicherte Daten vor, müssen sie je nach Format mit spezieller Software vorverarbeitet werden. Liegt beispielsweise ein *Image* der Festplatte eines Notebooks vor, muss dieses *Image* zuerst auf einem Computer mit einer Spezialsoftware so bereitgestellt (*"gemountet"*) werden, dass der Benutzer die einzelnen Verzeichnisse und sonstigen Inhalte anschauen kann. Dort können dann die gewünschten Daten extrahiert und separat abgespeichert werden. In anderen Fällen müssen Daten von *Backup-Tapes* extrahiert werden oder es liegen Dateien nur in proprietären Datenformaten vor, welche die Software, mit welcher der Review durchgeführt werden soll, nicht oder nicht hinreichend „versteht". Zwar gibt es wohl für fast jedes Datenformat irgendeine Lösung, wie die Daten für einen Review aufbereitet werden können, doch braucht jeder dieser Schritte zur Extraktion, Konvertierung oder Aufbereitung viel Zeit (oft viele Stunden) und die Zwischenergebnisse müssen jeweils gesondert gespeichert werden, damit jeder Schritt dokumentiert werden kann.

Geld sparen

Gewisse Review-Systeme kosten pro Gigabyte an gespeicherten oder verarbeiteten Daten. Da kann es bei grossen Datenbeständen sinnvoll sein, diese mit einer günstigeren Software vorab aufzubereiten (z.B. zu konsolidieren oder zeitlich einzuschränken). Allerdings können dadurch auch gewisse Informationen verloren gehen.

Haben Mitarbeiter für ihre Kommunikation **"sichere" Messenger-Systeme** eingesetzt, welche Mitteilungen *"End-to-End"* verschlüsseln (z.B. WhatsApp, Threema) und verfügt das Unternehmen über keinen Zugang zu den Schlüsseln, so wird es ihm in der Regel nicht möglich sein, ohne Mitwirkung der Inhaber der betreffenden Endgeräte an die betreffende Kommunikation zu gelangen. Ihre Verwendung sollte daher für geschäftliche Zwecke untersagt werden. Allerdings wird das fehlbare Mitarbeiter nicht davon abhalten, sie für ihre Zwecke trotzdem zu verwenden. In rechtlicher Hinsicht ist es unter Umständen denkbar, die Mitarbeiter gerichtlich unter Androhung einer Ungehorsamsstrafe nach Art. 292 StGB zur Offenlegung zu zwingen, soweit klare Hinweise bestehen, dass die Kommunikationsdienste für geschäftliche Zwecke benutzt wurden.

5. **Scannen.** Nicht jede relevante Information liegt bereits in elektronischer Form vor. Unter Umständen müssen Papierdokumente sogar ordnerweise verarbeitet werden. Hierfür muss auf Scanner zurückgegriffen werden. Dies ist und bleibt letztlich Handarbeit, auch wenn es Softwarelösungen gibt, mit denen der Prozess

etwas besser koordiniert und verwaltet werden kann. Wichtig ist es, sich zu überlegen, ob Ordner am Stück oder in einzelnen Dateien gescannt werden und wie die Dateien zu bezeichnen sind. Prüfen Sie, ob eine gleichzeitige Texterkennung den Prozess verlangsamt (das sollte bei modernen Geräten nicht mehr der Fall sein). So oder so kann sie später noch hinzugefügt werden.

Wer bei einem Überraschungsbesuch auf grössere Mengen an Papierdokumenten stösst, wird diese typischerweise mitnehmen müssen. Wenn aber die Personen vor Ort die Unterlagen **für das Tagesgeschäft noch benötigen**, kann dies logistische Probleme verursachen. Sie können nur mit einem Kopierer vor Ort oder einem relativ teuren Einsatz von externen Kopierteams gelöst werden, so dass die Ordner rasch retourniert werden können. Solche Teams müssen aber i.d.R. vorgängig organisiert werden.

6. **Texterkennung und Indexierung.** Alle Review-Systeme arbeiten letztlich mit Text, d.h. sie müssen in der Lage sein, den in einem Dokument enthaltenen Text zu lesen. Da dies nicht bei jedem Dokument gegeben ist (z.B. gewisse PDFs, Bilder), verfügen heutige Review-Systeme über die Möglichkeit, Text zu erkennen und die Dokumente so „durchsuchbar" zu machen (*"Optical Character Recognition"*, OCR). Das ist heute eigentlich keine komplizierte Sache mehr, ist aber nicht absolut zuverlässig (ein Teil der Texte wird nicht oder nicht richtig erkannt und ist damit über Suchbegriffe nicht auffindbar) und benötigt Zeit. Sind grosse Datenbestände in ein Review-System einzulesen, können daher viele Stunden vergehen, bis die Dokumente für den Review bereit sind. Ein weiterer solcher Prozess ist die Indexierung, bei welcher die in den Dokumenten vorkommenden Begriffe so in einer Datenbank abgelegt werden, dass die Dokumente später über Suchbegriffe und weitere Kennungen rasch gefunden werden können.

7. **Transkription.** Gerade dort, wo im Tagesgeschäft mit Audioaufzeichnungen gearbeitet wird (*Call-Center, Trading-Floors*), kann eine Untersuchung es erfordern, dass auch solche einem Review unterzogen werden. Hier gibt es zwei Möglichkeiten: Entweder werden die Aufzeichnungen angehört, oder es wird zuerst manuell oder automatisch ein Transkript erstellt, das dann gesichtet wird– allenfalls auch auf bestimmte Stichwörter hin.

8. **Review-Software.** Sie ist das Herzstück eines jeden Reviews: Es ist die Software, in welche alle zu sichtenden Inhalte „geladen" werden und mit welcher diese dann analysiert, durchsucht, gesichtet, codiert, geschwärzt und auch produziert werden können. Die meisten Unternehmen betreiben sie nicht selbst, sondern beziehen sie als Dienstleistung bei einem eDiscovery-Provider, der sie in seinem eigenen Rechenzentrum oder in der Cloud betreibt. Sind die Daten für einen Review

aufbereitet, können sich die Benutzer via Internet einloggen (entweder über einen Browser oder über eine Terminal-Session, z.B. mittels Citrix) und dort auf alle oder alle ihnen zugewiesene Anwendungen und Daten zugreifen, diese ansehen und entsprechend bearbeiten. Jede Review-Software hat andere Schwergewichte und Stärken. So gibt es Lösungen, die sich äusserst vielfältig konfigurieren und mit allerlei Zusatzmodulen ergänzen lassen, dafür aber Provider-seitig in der Handhabung eher komplex sind. Andere Lösungen bieten nicht sehr viel Flexibilität und Funktionalität, sind aber besonders einfach zu bedienen. Gewisse Lösungen eignen sich sehr für die Sichtung von Daten, andere sind besser, wenn es um die Schwärzung von Dokumenten geht. Auch bezüglich der Analyse- und Suchmöglichkeiten unterscheiden sie sich. Nachfolgend sind einige der typischen Funktionalitäten aufgeführt, die je nach Anbieter und Lösung angeboten werden.

Native Files

Normalerweise wird jedes Dokument mit Hilfe des in der Review-Software integrierten Betrachterprogramms angezeigt, da dies am effizientesten ist. Wo diese Darstellung nicht genügt oder nicht richtig funktioniert (z.B. bei Excel-Tabellen), können die Dokumente i.d.R. auch im Original gesichtet werden (d.h. die Software startet z.B. Excel und zeigt die Tabelle an).

Um die Menge an Dokumenten zu reduzieren, wird meist eine → **Deduplizierung**, ein → **E-Mail-Threading** und ein → **DeNISTing** durchgeführt. Die ersten beiden Techniken eliminieren Duplikate (so dass z.B. E-Mails, die in mehreren Mailboxen und Mail-Ketten zugleich auftauchen, nur ein Mal erscheinen). Bei letzterer Technik werden Dateien, die für den Review höchstwahrscheinlich nicht relevant sind (z.B. Software- und Systemdateien) entfernt.

9. ***Boolean Search / Text Search*.** Dies ist die wichtigste Methode, um in Dokumenten nach bestimmten Suchbegriffen zu suchen. Im Kern geht es um eine simple Textsuche (d.h. ein Text wird nach dem Vorkommen eines Suchbegriffs abgesucht; ist der Begriff enthalten, gilt das Dokument als Treffer), bei welcher mehrere Suchbegriffe gleichzeitig zum Einsatz kommen. Diese werden mittels sogenannter „booleschen" Operatoren verknüpft. Die bekanntesten sind „*AND*", „*OR*" und „*NOT*". So können komplexere Suchabfragen formuliert werden (z.B. bedeutet „schmieren AND einkäufer", dass ein Dokument nur dann als Treffer gilt, wenn beide Worte vorkommen). In der Praxis kommen noch diverse weitere Operatoren und Möglichkeiten hinzu, Suchaufträge zu formulieren. So z.B. der Stern als „Wildcard", der für beliebige Zeichenfolgen stehen kann (z.B. findet „schmier*" sowohl „schmiert"

wie auch „schmieren“) oder ein Operator, um maximale Wortabstände auszudrücken (z.B. muss bei „schmieren W/5 einkäufer“ das eine Wort im Text innerhalb von fünf Wörtern im Text vorkommen, damit das Dokument als Treffer gilt).[53] Je nach Review-System ist die Schreib- und Funktionsweise wie auch die Auswahl an solchen Operatoren und Spezialzeichen unterschiedlich[54]; in der Praxis ist häufig auch einfach von *“Text Search“* die Rede. Die Formulierung solcher Suchabfragen erscheint auf den ersten Blick als eine einfache Aufgabe, erfordert aber sehr viel Erfahrung, wenn Suchläufe möglichst wenig *“false positives“* erzeugen sollen, d.h. möglichst wenige Treffer, die nicht das enthalten, was gesucht wird. Das ist wichtig, weil die Suchläufe normalerweise dazu dienen, den Kreis derjenigen Dokumente zu limitieren, die manuell gesichtet werden müssen. Je präziser die Suchabfragen sind, desto weniger muss gesichtet werden und desto rascher und günstiger kommt der Review zum Ergebnis. Zugleich sollen auch die *“false negatives“*, d.h. Dokumente, die eigentlich relevant sind, aber durch die Maschen schlüpfen, so gering wie möglich gehalten werden.

Optimieren

In der Praxis bringt ein Suchlauf nie auf Anhieb das ideale Ergebnis. Er muss in mehrfachen Suchläufen optimiert werden. Dabei können *Search Term Reports* helfen: Das Review-System zeigt an, welche Wortvarianten in welcher Häufigkeit mit bestimmten Suchläufen gefunden werden.

Haben die einen Fall betreuenden Anwälte wenig Erfahrung, ist oft die Ansicht zu beobachten, es würde genügen, dem eDiscovery-Provider eine **Liste mit einigen möglichen Suchbegriffen** zu geben, damit er danach die Texte absucht (z.B. „Korruption“, „Schmiergeld“, „Bestechung“, „bestechen“ etc. im Falle einer Korruptionsuntersuchung). Sie sind dann überrascht, wenn entweder sehr viele Treffer oder kaum Treffer kommen. Die Entwicklung von guten Suchaufträgen braucht nicht nur viel Übung und gute Kenntnis der Operatoren und Spezialzeichen, die das jeweilige Review-System unterstützt, sondern auch Zeit. Das kann ohne Weiteres Stunden dauern. Zudem sollten Suchaufträge auch im Laufe des Reviews konstant optimiert werden, wenn Feedbacks aus dem Review z.B. zeigen, dass bestimmte Kategorien von *false positives* besonders häufig vorkommen. Die Investitionen in das Ausarbeiten guter Suchaufträge lohnen sich. Auch Systeme mit „künstlicher Intelligenz“ machen das nicht überflüssig. Sie springen auf andere Dinge an.

53 Sie gelten genau genommen nicht mehr als Boolesche Operatoren.
54 Hier ein Beispiel der bekannten Lösung „Relativity“: https://help.relativity.com/10.3/Content/Relativity/dtSearch/Using_dtSearch_syntax_options.htm.

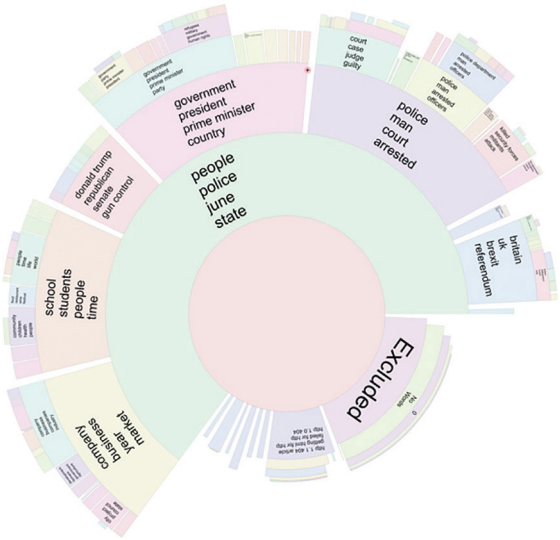
10. ***Metadata Search*.** Im Rahmen einer *Metadata Search* wird nicht nach dem Inhalt von Dokumenten, sondern nach bestimmten Randdaten eines Dokuments gesucht, also seinen „Metadaten". Bei einer E-Mail sind es z.B. der Sender, die Empfänger, die Übermittlungszeiten, die Grösse, die Zahl und Art der Anhänge und weitere Angaben. So kann es in einer Untersuchung wegen Geheimnisverrat z.B. Sinn machen, nur jene E-Mails herauszusuchen, die sich ein Mitarbeiter an seine eigene private oder generell an externe E-Mail-Adressen gesandt hat, oder die Anhänge enthalten. In einem guten Review-System können die Treffer z.B. auch nach bestimmten Metadaten gefiltert werden.

11. *Concept Search***.** Eine *boolean search* kommt dort an ihre Grenzen, wo bestimmte Wörter unterschiedliche Bedeutungen haben, wo sie falsch oder unterschiedlich geschrieben werden, oder wo für dieselbe Aussage eine andere Formulierung verwendet wird. Um dieses Problem zu lösen, wurde die *"concept search"*-Methode entwickelt, bei welcher der Computer auf Basis von Berechnungen versucht, den Kontext und die semantische Bedeutung der Begriffe in den durchsuchten Dokumenten zu verstehen. Zwar gibt es Review-Systeme, bei denen eine *concept search* auf Basis eines Suchbegriffs bzw. einem ganzen Satz durchgeführt wird. Häufiger sind aber andere Anwendungsfälle. Das Review-System kann z.B. beauftragt werden, alle ihm vorliegenden Dokumente zu analysieren und jeweils jene Dokumente in einem Cluster zusammenzufassen, die am wahrscheinlichsten dasselbe Thema betreffen, weil sie ähnliche formulierte und aufgebaute Texte enthalten, auch wenn die Wörter unterschiedlich sind. Wird dies mit der E-Mailbox eines Juristen gemacht, gibt es vielleicht einen Cluster zu einer bestimmten Vertragsverhandlung, einen Cluster mit E-Mails zu Lunchverabredungen, einen Cluster zu Spesenabrechnungen etc. Diese Methode kann benutzt werden, um bestimmte Dokumentengruppen zu priorisieren oder gezielter zu durchsuchen (siehe auch Schritt 13). Eine andere Anwendung ist die Suche ähnlicher Dokumente: Wurde ein relevantes Dokument gefunden, kann das Review-System gebeten werden, Dokumente mit mutmasslich ähnlichem Inhalt zu finden.

12. **Kommunikationsanalyse.** Es handelt sich um eine besondere Darstellungsform der Metadaten von E-Mails oder anderer Kommunikation. Der Computer analysiert z.B. anhand der Inhalte diverser E-Mailboxen, wer mit wem wie häufig und wann kommuniziert hat und stellt dies grafisch dar. Auf diese Weise kann es einfacher sein, das Kommunikationsverhalten einer bestimmten Person zu verstehen und z.B. festzustellen, ob es bestimmte, bisher nicht bekannte Personen gibt, mit welchen sich eine Zielperson besonders oft ausgetauscht hat.

Kommunikationsanalyse von "Relativity".

13. ***Cluster Wheel.*** Eine beliebte Darstellungsform für das Ergebnis einer *concept search*: Im Kreis werden alle *Cluster* als Flächen angeordnet, an denen dann jeweils die Untercluster hängen. Jeder *Cluster* wird mit einigen mutmasslich typischen Begriffen bezeichnet, so dass der Benutzer erkennen kann, worum es in den Dokumenten geht. Es ist dies im Prinzip eine interaktive Benutzerschnittstelle, mit welcher der Benutzer im „Universum" der durchsuchten Dokumente in den diversen Clustern virtuell herumwühlen kann. Klickt er auf einen *Cluster*, wird das „Rad" neu aufgebaut und die im Cluster enthaltenen Untercluster dargestellt. So kann er immer weiter in den *Cluster* vordringen. Das eignet sich für die manuelle Suche.



Cluster Wheel von „Brainspace".

14. ***Predictive Coding.*** Es handelt sich im weitesten Sinn um eine weitere Verwendungsform von *concept searches* und anderen Funktionen zur Mustererkennung und anderen Formen der Analyse von Dokumenten, die vor allem bei sehr grossen Datenmengen zum Einsatz kommt. Hierbei werden zunächst eine überschaubare Menge an Dokumenten der Gesamtpopulation manuell gesichtet und wie gewünscht klassifiziert. Anhand dieses Beispielsets an relevanten Dokumenten beurteilt der Computer dann die restlichen Dokumente der Gesamtpopulation, d.h. er wird gebeten, die Klassifizierung des Beispielsets in derselben Art und Weise auf die restlichen Dokumente anzuwenden oder eine Klassifizierung zumindest vorzuschlagen, um einen Review zu beschleunigen. Die Grösse und Qualität des Beispielsets bestimmt also nebst der Qualität des verwendeten Systems die Qualität des Ergebnisses. Die Technik ist zwar naturgemäss nicht hundertprozentig zuverlässig, weil lediglich mit Wahrscheinlichkeiten und Mustern gearbeitet wird – der Computer versteht die Inhalte ja nicht –, aber die Methode ist insbesondere in den USA (wo in Zivilprozessen regelmässig sehr grosse Mengen an Daten geliefert werden müssen) zwischenzeitlich als Alternative zu vollständig manuellen Reviews akzeptiert. Das hat insbesondere auch damit zu tun, dass bei grossen Datenmengen die Reviews bei manueller Sichtung sonst nie fertig würden. Bei weniger grossen Datenmengen (unter 10'000 zu sichtende Dokumente) oder bei stark unterschiedlichen Datenquellen (z.B. bei unterschiedlichen Sprachen oder bei gemischten Daten aus Buchhaltungssystemen, Kommunikation und Verträgen)

ist der Nutzen von *predictive coding* beschränkt. Immerhin kann die Technik benutzt werden, um Dokumente für einen Review zu priorisieren oder zu gruppieren.

> Eine moderne Form von *predictive coding* ist das *continuous active learning*. Dabei wird das Review-System nicht an einem Set von manuell gesichteten Dokumenten trainiert, sondern das System „lernt" laufend dazu, indem es die Codierungen der Reviewer beobachtet und auswertet. Die Erkenntnisse daraus werden benutzt, um die Reihenfolge der zu sichtenden Daten dynamisch so anzupassen, dass die potenziell besonders relevanten Dokumente priorisiert angezeigt werden. Dies hat zur Folge, dass die Relevanz der Dokumente im Review laufend abnimmt und der Review mit der Zeit womöglich vorzeitig beendet werden kann.

15. ***Redaction-Tools.*** Müssen Dokumente gegenüber Dritten offengelegt werden, besteht regelmässig das Bedürfnis, gewisse Dokumente teilweise zu schwärzen (z.B. Geschäftsgeheimnisse oder private Daten, → **SWISS SECRECY & PRIVACY REVIEWS**). Auch hierfür gibt es inzwischen Spezialsoftware, auch wenn viele Review-Systeme ebenfalls über entsprechende Werkzeuge verfügen. Spezialsoftware kann nötig und sinnvoll sein, wenn es um Spezialformate geht (z.B. Excel[55]). Eine gute Software für Schwärzungen (*redactions*) zeichnet sich dadurch aus, dass sie den Schwärzungsprozess sehr effizient unterstützen. Schwärzungen brauchen mehr Zeit als reine Reviews, weshalb der Zeit- und Kostendruck oft noch höher ist. Eine gute Software muss nicht einfach nur das „Malen" von schwarzen Kästchen erlauben, sondern diverse weitere Funktionen aufweisen, wie z.B. unterschiedliche Selektionswerkzeuge (Textstellen, Bereiche), die Möglichkeit für Qualitätskontrollen nach dem Vier-Augen-Prinzip (z.B. semitransparente Schwärzung, damit die zweite Person noch sehen kann, was sich unter der vorgeschlagenen Schwärzung befindet, bevor sie final angewandt wird) oder die Möglichkeit zur Beschriftung von Schwärzungen. Auch automatische Schwärzungen werden immer besser, wobei sie die Handarbeit bisher höchstens dort ersetzen können, wo es um die Schwärzung syntaktisch normierter Inhalte geht, d.h. Inhalte, die in ihrem Erscheinungsbild formelhaft umschrieben werden können, wie z.B. Kreditkartennummern oder Bankkontonummern, die immer gleich aufgebaut sind (sog. *regular expressions* oder → **RegEx**).

55 Ein Demovideo zur Software „Blackout": https://www.youtube.com/watch?v=lbIVUCyMFVE.

> *Redactions* sind nicht nur in Dokumenten möglich, sondern auch bei **Ton- und Videoinhalten**, nur sind es dort natürlich keine Schwärzungen im wortwörtlichen Sinn. Wird z.B. das Fehlverhalten von Börsenhändlern untersucht, kann es erforderlich sein, in den aufgezeichneten Handelsgesprächen genannte Kundennamen unkenntlich zu machen. Hierzu gibt es besondere *Tools*, die mit den entsprechenden Multimedia-Formaten umgehen können. Da häufig parallel Transkripte verwendet werden, ist auf eine Synchronisation der *redactions* zu achten.

16. **Linguistische Analyse.** Gewisse Anbieter werben damit, dass ihre Werkzeuge eine linguistische Analyse vornehmen. Damit ist entweder eine automatisierte *concept search* oder eine manuelle Variante davon gemeint. Bei letzterer analysiert ein Linguistik-Spezialist relevante Dokumente und baut gestützt darauf entsprechende Suchaufträge auf.

> Ein Schweizer Unternehmen (OrphAnalytics SA) hat eine Technologie entwickelt, mit welcher sich die **Autorenschaft anonymer Textdokumente** aufgrund deren Stilmusters angeblich automatisiert nachweisen lässt.

17. **Maschinelle Übersetzungen.** Sie erlauben es den Reviewern, fremdsprachige Dokumente zumindest ansatzweise zu verstehen. Die Qualität ist sehr unterschiedlich (und oft nicht so gut wie etwa bei DeepL). Bei relevanten Dokumenten sollte mit einer „menschlichen" Übersetzung durch eine mit dem Fall vertraute Person gearbeitet werden, da es auf Nuancen ankommen kann, die der Computer nicht erfasst.

18. **Produktionsformate.** Je nach Fall müssen die in einem Review-System als relevant ermittelten oder geschwärzten Dokumente wieder aus dem System extrahiert werden, damit sie Dritten (Behörden, Gegenparteien etc.) zur weiteren Verwendung übergeben werden können. In der Fachsprache ist von „Produktion" die Rede (*production*). Dokumente können in unterschiedlichstem Format „produziert" werden. Am gängigsten sind:

    - **TIFF:** Die Dokumente werden in ein Bild umgewandelt und als Bilddatei im gleichnamigen Format geliefert. Dies erfordert sehr viel Speicherplatz und alle Metadaten gehen verloren, weshalb sie als separate Tabelle mitgeliefert werden. Der Vorteil dieser Lösung ist die hohe Qualität der Ab-

Bates-Stamp

So heissen in den USA die Nummern (z.B. R0031087), die auf jede Seite in der Fuss- oder Kopfzeile eines in einem offiziellen Verfahren produzierten Dokumentes aufgedruckt wird. Sie dienen der Referenzierung.

bildungen und dass die Seite immer gleich dargestellt wird, egal mit welchem Viewer oder auf welchem System sie angeschaut wird. Dies ist beim PDF-Format nicht zwingend der Fall. Allenfalls wird eine Textdatei mitgeliefert, die den reinen Text des Dokuments enthält, damit nach Stichworten gesucht werden kann. Das TIFF-Format wird oft in US-amerikanischen Verfahren angefordert, weil die dafür eingesetzten speziellen Review-Systeme auch bei grossen Datenmengen damit problemlos umgehen können.

- **PDF:** Die Dokumente werden im PDF-Format geliefert. Es ist das bei informellen Produktionen am häufigsten verwendete Format, weil die Dateien leicht zu handhaben und verhältnismässig klein sind. Das PDF kann „durchsuchbar" erzeugt werden. Der Nachteil dieser Variante ist, dass die meisten Metadaten verloren gehen, sofern sie nicht mit einer Spezialsoftware eincodiert werden.
- **Native:** Die Dokumente werden im ursprünglichen Format geliefert, d.h. als Datei im Dateiformat von Word, Excel, Outlook etc. Der Vorteil dieser Variante ist, dass alle Metadaten erhalten bleiben. Allerdings sind hier Schwärzungen nicht möglich bzw. nur dann, wenn in die Dokumente selbst eingegriffen wird, wobei Schwärzungen dann i.d.R. nicht unbedingt als solche sichtbar sind. Im Falle von proprietären Datenquellen (z.B. Chats) kann sich die Verwendung eines standardisierten Formats (wie z.B. XML) anbieten – vor allem dann, wenn bereits die Extraktion der Daten aus dem Ursprungssystem nur mit Klimmzügen möglich ist und auch kein anerkanntes Format wie „docx" oder PDF existiert.

Verschachtelt

Bei Native-Dateien muss beachtet werden, dass sich in solchen Dokumenten ihrerseits weitere Dokumente "verstecken" können (z.B. eine Excel-Tabelle oder ein PDF innerhalb einer Word-Datei).

Excel-Dateien werden oft unabhängig vom gewählten Produktionsformat als Native produziert, da sie ab einer gewissen Grösse nicht sauber in ein PDF oder Bild umgewandelt werden können (die Tabellen sind aufgebrochen und auf zahlreiche Seiten verteilt und damit nicht mehr vernünftig lesbar).

- **Sonderformat:** Wenn Dokumente vom Empfänger gleich wieder in ein Review-System importiert werden sollen, was häufig der Fall ist, kann es auch sinnvoll sein, sie gleich im Format des Review-Systems zu exportieren. Das hat den Vorteil, dass alle Metadaten erhalten bleiben und keine aufwändige Konvertierung nötig ist. Wird ein solches Sonderformat verwendet, können auch Klassifizierungen (*Tags*, Kommentare etc.) mitgeliefert werden, was bei den anderen Formaten nicht vorgesehen ist.

Für jede Produktion muss entschieden werden, ob und welche Metadaten der einzelnen Dokumente mitgeliefert werden. Der Empfänger wird normalerweise soviele **Metadaten** wie möglich mitgeliefert haben wollen, da sie wertvolle Informationen (z.B. das Erstellungsdatum eines Dokuments oder die Bezeichnung des Autors) enthalten und für das Durchsuchen und Analysieren der Dokumente wichtig sein können. Falls PDF- oder TIFF-Dateien geliefert werden, können alle oder gewisse Metadaten in einer separaten Datei mitgeliefert werden. Ferner muss bei **E-Mails** darauf geachtet werden, dass diese jeweils mit ihren **Anhängen** zusammen geliefert werden (die Rede ist von einer „Familie"), damit der Kontext erhalten bleibt. Irrelevante Anhänge können nötigenfalls durch ein sog. *Slipsheet* ersetzt werden.

Falls Schwärzungen vorgenommen wurden, muss sehr genau darauf geachtet werden, dass die geschwärzten Texte bzw. Dokumentenstellen nicht über die Metadaten, Textdateien oder Native-Dateien **versehentlich ungeschwärzt** geliefert werden. Es nutzt nichts, den Namen des Empfängers einer E-Mail im Bild oder im PDF der E-Mail zu schwärzen, wenn der Name des Empfängers in den Metadaten weiterhin enthalten ist oder die E-Mail als Native-Datei geliefert wird (wo der Name ebenfalls enthalten sein wird). Entweder werden in diesen Fällen keine Metadaten und Native-Dateien geliefert, oder es werden die Metadaten geliefert, aber geschwärzt bzw. editiert. Auch sollte ein geschwärztes Dokument nach der Bereitstellung zur Produktion nochmals von neuem durch die **Texterkennung** laufen, da ansonsten die geschwärzten Stellen in der zum Bild zugehörigen Textinformation nach wie vorenthalten sein können.

19. **Sonderformate.** In vielen Reviews machen „ganz normale" E-Mails und weitere Dokumente (*loose files*) in klassischen Textformaten wie Word-, PDF- und Powerpoint-Dokumente die Mehrheit der zu sichtenden oder schwärzenden Dokumente aus. Mit ihnen kommen die Review-Systeme gut zurecht. Mit anderen Kategorien von Dokumenten kommen sie teils nicht wirklich zurecht, weshalb in diesen Fällen Zusatzprogramme nötig werden können. So gibt es Spezialsoftware zum Schwärzen von grossen Excel-Dokumenten (ohne solche Software müssen sie jeweils im Native-Format bearbeitet werden, was sich nicht ohne Weiteres nachverfolgen lässt und daher suboptimal ist). Spezialprogramme können sich auch für den Review oder die „Schwärzung" von Audiodaten (z.B. Telefonaufzeichnungen) und Videos aufdrängen. Mit Chats kommen viele Review-Lösungen ebenfalls nicht ohne Weiteres zurecht, so dass sich hier ein Markt an Spezialtools entwickelt hat. Hinzugekommen ist seit der Corona-Pandemie auch der Bedarf an der Auswertung von Inhalten von Videokonferenz- und Teamkollaborationswerkzeugen wie etwa „Microsoft Teams". Die Schwierigkeit bei diesen neuen Datenquellen liegt darin, dass die Betreiber der Lösungen oft noch nicht in der Lage sind, alle von den Benutzern generierten Daten auch entsprechend zu archivieren und im Fall der Fälle bereitzustellen. Die Review-

Lösungen wiederum haben Mühe, die Inhalte aus diesen neuen Datenquellen so darzustellen, wie sie ursprünglich dargestellt waren. Fehlen dabei Elemente, kann das natürlich auch inhaltlich sinnentstellend sein. Es ist daher sehr wichtig, dass mit den beigezogenen eDiscovery-Spezialisten genau abgeklärt wird, was fehlt oder anders dargestellt werden muss. Die Frage der korrekten Darstellung stellt sich natürlich auch, wenn die Daten später in einem Verfahren weiter verwendet und zu diesem Zweck herausgegeben werden sollen oder müssen.

Bei **Microsoft Teams** sind z.B. Mitteilungen in privaten Kanälen, Audioaufzeichnungen und Reaktionen anderer (wie z.B. Likes) nicht für ein eDiscovery verfügbar. Werden die Daten eines *Custodians* abgerufen, sind seine privaten Kanäle nicht automatisch erfasst, sondern müssen separat abgerufen werden. Werden Mitteilungen innerhalb von Teams korrigiert, wird über die eDiscovery-Funktion nur die letzte Fassung gesichert. Whiteboard-Inhalte werden überhaupt nicht gesichert. Obwohl davon auszugehen ist, dass sich diese Dinge in naher Zukunft wieder ändern werden, muss weiterhin damit gerechnet werden, dass bei neuen Funktionen in einer solchen, sich so dynamisch entwickelnden Umgebung, anfallende Daten sich eine gewisse Zeit lang nicht ohne Zusatzaufwand korrekt sichern und auswerten lassen.

20. **Dokumentenlieferung.** Liegen die Dokumente als „Produktionsdatei“ vor, muss diese dem Empfänger übermittelt werden. Hier gibt es in der Praxis grundsätzlich zwei Möglichkeiten: Sie werden über sichere Server zum Download bereitgehalten oder sie werden auf verschlüsselten Datenträgern gespeichert und per Kurier versendet. Das Passwort bzw. der Schlüssel zur Entschlüsselung sollte über einen separaten Kommunikationsweg (z.B. SMS) an den Empfänger übermittelt werden. Ausgedruckt werden Dokumente in der Regel nicht mehr. Eine Lieferung kann durchaus einen Tag beanspruchen. Es ist somit genügend Zeit einzuberechnen.

Do’s	Don’ts
• Nehmen Sie sich Zeit für das Kennenlernen der von Ihnen benutzten eDiscovery-Werkzeuge. Wichtiger als die Wahl des besten *Tools* ist die Beherrschung des gewählten *Tools*. • Machen Sie sich mit dem Angebot an *Tools* Ihres Providers vertraut,	• Betreiben Sie eDiscovery-Lösungen nicht selbst. Die Technik erfordert Erfahrung und entwickelt sich ständig weiter. Der Wettbewerb sorgt für gute Preise. • Vertrauen Sie nicht darauf, dass „künstliche Intelligenz“ Ihre Arbeit macht. Sie kann Sie höchstens

Do's	Don'ts
damit Sie wissen, welche *Tools* für Ihren Fall wirklich sinnvoll sind, Sie aber zugleich jede Unterstützung in Anspruch nehmen, die Ihr Provider bietet. • Achten Sie auf die Performance Ihrer Review-Lösung: Reviews sind mitunter Fliessbandarbeit. Wird von Seite zu Seite gesprungen, muss das „ruckzuck" gehen, da sonst während des Reviews zu viel Zeit verloren geht. • Rechnen Sie genügend Zeit für die Aufbereitung von Dokumenten ein. Liegen die Daten vor, kann in aller Regel nicht gleich losgelegt werden. Die Aufbereitung kann einen Tag oder mehr beanspruchen.	unterstützen. Finden müssen Sie relevante Dokumente primär selbst. • Vermeiden Sie bei der Beschaffung von Dokumenten Formate, welche der Provider vorgängig konvertieren muss, bevor er sie verarbeiten kann. Das Konvertieren von Daten ist zwar meist möglich, kostet aber Zeit und Geld.

Wann Sie externe Unterstützung beiziehen sollten

- Wenn Ihnen die **Expertise oder die Ressourcen** für den Betrieb eines eigenen eDiscovery-Systems fehlen.
- Wenn Sie anlässlich der **Beschaffung einer neuen Informatiklösung** sicher sein wollen, dass sie eDiscovery-tauglich ist
- Wenn Sie nicht wissen, wie Sie in einem konkreten Fall **an die nötigen Daten herankommen**.
- Falls Sie es mit **vielen Daten** zu tun haben.
- Falls es wichtig ist, dass Dokumente **gerichtsverwertbar sichergestellt** werden.
- Falls Sie nach **gelöschten Dokumenten** suchen wollen.
- Wenn Sie nicht wissen, welche **Hilfsmittel für die Suche nach relevanten Dokumenten** für Ihren Fall am besten passen.
- Wenn Sie Mühe haben, **passende Suchaufträge** zu formulieren.
- Wenn Sie **unsicher** sind (z.B. ob es nicht noch andere Methoden gibt, Ihre Dokumente zu analysieren).

Häufige Fragen und Antworten

Q55. Wir verwenden Microsoft 365. Wie einfach ist das Übernehmen von Dokumenten in ein Review-System?

A: Das ist nicht sehr schwierig. Voraussetzung ist aber, dass das Unternehmen einen passenden Lizenzplan verwendet (z.B. E3 oder höher). Ist dies der Fall, kann den für eDiscovery zuständigen Personen (z.B. Mitarbeitern der IT oder des Compliance-Teams, ggf. auch der eDiscovery-Provider) im System von Microsoft die entsprechenden Berechtigungen zugewiesen werden. Sie müssen dazu in die von Microsoft vordefinierte Berechtigungsgruppe der „eDiscovery Manager" aufgenommen werden. Diese Gruppe kennt zwei Subgruppen: Den „eDiscovery Manager", der die von ihm selbst angelegten sowie die ihm zugewiesenen eDiscovery-Fälle verwalten kann, und den „eDiscovery Administrator", der auf alle Fälle zugreifen und deren Daten auch exportieren kann.

Folgende **Datenquellen** können derzeit innerhalb von Microsoft 365 gesichert und über den eDiscovery Manager bezogen werden: Exchange (Postfächer, öffentliche Ordner), SharePoint Online, OneDrive for Business, Microsoft 365-Gruppen, Skype for Business, Teams (Chats, Kanäle), Yammer (öffentliche und private Chats).

Kommt es zu einem konkreten Fall, muss zunächst ein entsprechendes Falldossier im System angelegt werden. Diesem können bei Bedarf mehrere eDiscovery Manager zugeteilt werden.

In einem nächsten Schritt kann ein „eDiscovery Hold" aktiviert werden, d.h. in den ausgewählten Exchange-Mailboxen, OneDrive-Konten und E-Mailboxen und Sites, die mit Teams und Office 365 verknüpft sind, können keine Daten mehr gelöscht werden. Es sind dabei auch selektive *Holds* möglich, d.h. ein *Hold*, der nur die Ergebnisse einer Suchabfrage betrifft.

Danach können Suchabfragen – etwa in allen E-Mails einer bestimmten Mailbox in einer bestimmten Zeitspanne – durchgeführt werden. Das System zeigt an, wieviele Daten mit der Suchabfrage erfasst werden.

Schliesslich kann im System der Export der über die Suchabfragen gefundenen Daten ausgelöst werden. In einem ersten Schritt werden diese Daten in einen speziellen Speicherbereich in der Microsoft-Cloud exportiert. Von dort können sie dann mit einem speziellen Programm auf den lokalen Computer heruntergeladen werden. Darin sind auch entsprechende Protokolle enthalten (was exportiert wurde und ob Fehler aufgetreten sind).

Zu beachten ist allerdings, dass bei Microsoft wie auch bei vielen anderen Cloud-Providern die eDiscovery-Möglichkeiten heute noch beschränkt sind. Über die erwähnten Schnittstellen stehen insbesondere nicht alle Daten aller Dienste zur Verfügung oder

die Interaktionen werden nicht so lückenlos protokolliert, wie dies bei E-Mails der Fall ist. Dies betrifft insbesondere neue Kommunikationskanäle wie Videokonferenzen oder Chats und Apps etwa für Umfragen, zur Aufgabenplanung oder *Whiteboards*. Hier können nur Screenshots weiterhelfen. Zu unterscheiden ist auch zwischen Inhalten und Metadaten.

Q56. Welche Relevanz haben gelöschte Dokumente?

A: Die Relevanz gelöschter Dokumente hängt sehr stark vom Untersuchungsgegenstand ab.

In internen Untersuchungen wird auf den Systemen häufig nicht spezifisch nach gelöschten Dateien gesucht. Jedoch werden etwaige, vom Benutzer zwar gelöschte, im E-Mail-System aber noch vorhandene Mails regelmässig in Reviews mit einbezogen. Sie können wertvolle Hinweise liefern, wie etwa ein angefangener, dann aber gelöschter Entwurf einer E-Mail, der sonst dementsprechend nirgends auftaucht. So wissen viele Benutzer nicht, dass der elektronische „Papierkorb" in ihrem E-Mail-Postfach je nach Standardeinstellung des Unternehmens nie von selbst geleert wird und sich darin auch nach Jahren noch gelöschte E-Mails befinden können. Doch auch vermeintlich gelöschte (weil im Postfach für den Benutzer nicht mehr sichtbare) E-Mails werden z.B. auf „Microsoft 365" je nach Konfiguration noch während 30 Tagen aufbewahrt und stehen für eine eDiscovery zur Verfügung.

In anderen Fällen kann die Suche nach gelöschten Dokumenten ein guter Startpunkt für eine interne Untersuchung sein, etwa wenn es darum geht, ob Kundendaten wegkopiert worden sind oder Dokumente gefälscht wurden. Die Wiederherstellung gelöschter Dokumente kann auch frühere Versionen von Dokumenten aufzeigen.

Wiederhergestellte temporäre Dateien des Betriebssystems oder von Anwendungen wiederum können relevante Hinweise auf das Vorgehen eines Täters geben, so etwa wenn es um den Nachweis geht, dass eine Zielperson einen Drohbrief geschrieben hat, obwohl er nie abgespeichert wurde. So erstellt z.B. Word laufend Zwischenspeicherungen von den gerade bearbeiteten Dokumenten, die für den normalen Benutzer nicht ersichtlich sind, aber mit forensischen Methoden aufgespürt werden können. Mit ihnen kann dann gezeigt werden, dass ein bestimmtes Schreiben auf einem bestimmten Computer bearbeitet worden sein muss.

Gedanken zum Thema.

Trotz Fortschritten beim *Technology Assisted Review* zeigt sich, dass künstliche Intelligenz noch nicht in der Lage ist, manuelle Reviews vollständig zu ersetzen. Wenn es aber um die Unterstützung solcher enorm kostspieligen Reviews geht, gibt es unglaubliche Fortschritte. Zum Glück gilt im *eDiscovery*-Prozess, auch bei Reviews, das Verhältnismässigkeitsprinzip, welches keine Perfektion verlangt und somit insbesondere bei grossen Datenmengen eine gewisse Fehlertoleranz anerkennt. Wir dürfen gespannt sein, wie sich die technischen Entwicklungen auf den gesamten Reviewprozess auswirken werden – und ob sich die in gewissen Rechtsordnungen wie England abzeichnende Entwicklung durchsetzt, im *eDisclosure* mehr auf Qualität statt Quantität zu achten. Der *Scope* von Herausgabebegehren wird da frühzeitig immer mehr hinterfragt. Oder anders formuliert: Weniger kann durchaus mehr sein.

Alain Pfäffli
Senior Discovery Manager
Novartis

11. DSAR-Reviews

Kurz gesagt

- Jeder darf Auskunft über seine Personendaten verlangen und oft muss sie gewährt werden.
- Je nach anwendbarem Recht bleiben Geschäftsgeheimnisse, Inhalte betreffend die interne Meinungsbildung oder andere Personen betreffende Daten geschützt.
- Wenn ein Auskunftsersuchen sehr viele Daten betrifft (z.B. alle eine bestimmte Person und ein bestimmtes Thema betreffenden E-Mails) kann dies einen systematischen Review dieser Dokumente erfordern.

Worum es geht

Auskunftsersuchen können jedes Unternehmen treffen. Das europäische Datenschutzrecht gibt jeder Person das Recht, Auskunft darüber zu verlangen, welche Personendaten über sie bearbeitet werden. Sie hat einen Anspruch auf eine Kopie dieser Personendaten. Unternehmen können diese Auskunft je nach nationalem Recht aus unterschiedlichen Gründen verweigern und müssen dies sogar, wenn sonst Daten Dritter unberechtigt offengelegt würden. Die meisten Auskunftsersuchen lassen sich einfach beantworten. Insbesondere in Streitfällen werden Auskunftsersuchen aber mitunter benutzt, um an interne Informationen von Unternehmen heranzukommen (wie z.B. interne E-Mails), die ein Unternehmen nicht ohne weiteres herausgeben will oder darf. Dies wiederum bedingt, dass die Informationen vorgängig geprüft und ggf. geschwärzt werden. Bei grösseren Datenmengen sind die meisten Unternehmen nicht dafür eingerichtet.

Worauf zu achten ist

- Auskunftsersuchen müssen innert 30 Tagen beantwortet werden; die Frist kann verlängert werden.
- Jede natürliche Person hat Anspruch auf Auskunft; sie braucht keinen Grund und keine Kundenbeziehung.
- Eine unvollständige oder unkorrekte Beantwortung von Auskunftsersuchen kann gebüsst werden.

Know-how

- Im angelsächsischen Raum werden Auskunftsersuchen als *"Data Subject Access Requests"* oder kurz DSARs bezeichnet.
- Das Datenschutzrecht kennt neben dem klassischen Auskunftsrecht auch noch den Anspruch auf "Datenportabilität", d.h. es können zuvor einem Dienstleister übergebene oder von diesem über den Benutzer gesammelte Daten zwecks Weiterverwendung herausverlangt werden.

- Auskunft ist nur über Personendaten zu erteilen, nicht über Dokumente, in denen sie vorkommen; es kann aber einfacher sein, die ganzen Dokumente herauszugeben.
- Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, also z.B. auch E-Mails, in denen eine bestimmte Person als solche erkennbar vorkommt.
- Unternehmen dürfen je nach anwendbarem Recht eine Auskunft einschränken, aufschieben, verweigern oder von einer geringen Gebühr abhängig machen.
- Kommen in den Personendaten auch andere Personen erkennbar vor, muss geprüft werden, ob deren Angaben zu schwärzen oder anderweitig zu schützen sind.

Das Auskunftsrecht ist insbesondere in der Schweiz in den vergangenen Jahren regelmässig für die Zwecke der vorprozessualen Beweisbeschaffung missbraucht worden. Das revidierte Datenschutzgesetz (ab 2022) soll dem stärker als bisher einen Riegel vorschieben, indem klargestellt wird, dass nur Daten als solche herausverlangt werden können (nicht Dokumente) und missbräuchliche Auskunftsersuchen einfacher zurückgewiesen werden können. Es ist in der Schweiz allerdings nicht strafbar, eine Auskunft zu verweigern, d.h. Unternehmen können vergleichsweise risikofrei eine restriktive Auskunftspolitik verfolgen.

Wie vorzugehen ist

1. **Prüfen Sie die Identität des Gesuchstellers.** Ist er durch einen Anwalt vertreten, lassen Sie sich eine entsprechende Vollmacht zeigen.
2. **Versuchen Sie zu verstehen, welche Daten er sehen möchte.** In den meisten Fällen will ein Gesuchsteller nicht „alles" sehen und selbst dann hat er normalerweise eine Vorstellung davon, was er vom Unternehmen genau sehen möchte.
3. **Finden Sie heraus, wer innerhalb Ihres Unternehmens Daten über den Gesuchsteller hat.** Das ist manchmal schwieriger als es erscheint. Von einem Arbeitnehmer bearbeitet ein Arbeitgeber nicht nur das Personaldossier, sondern auch Daten in E-Mail-Postfächern zahlreicher Personen, in Zugangskontrollsystemen, in der Buchhaltung, in Arbeitsdokumenten, auf der Website, im Adressverzeichnis usw.

Es ist üblich und erlaubt, dem Gesuchsteller zunächst nur jene Daten zu liefern, die Personen wie er typischerweise haben wollen bzw. ihn interessieren, also im Falle eines Arbeitnehmers das Personaldossier, nicht aber weitere Angaben, auch wenn er „alle" Daten verlangt hat. Dem Gesuchsteller sollte dann mitgeteilt werden, spezifischer auszuführen, was ihn zusätzlich interessiert, falls ihm die erste Antwort nicht genügt.

4. **Prüfen Sie, welche dieser Daten vom Auskunftsersuchen erfasst sind und lassen Sie sie Ihnen liefern.** Das kann eine gewisse Zeit dauern und Sie werden den Personen erfahrungsgemäss enge Fristen setzen müssen. Falls Sie sehen, dass die Zeit nicht reichen wird (auch für die nachfolgenden Schritte), teilen Sie dies dem Gesuchsteller mit und sagen Sie ihm, wie lange sich die Antwort verzögert. Diese Antwort sollte er spätestens 30 Tage nach seinem Gesuch erhalten.

5. **Ermitteln Sie die relevanten Personendaten.** Geht es um ein Personaldossier, so sind alle darin enthaltenen Informationen relevant. Geht es hingegen um E-Mails, so müssen Sie die relevanten E-Mails aus den diversen, in Frage kommenden Postfächern erst herausfiltern. Sie können den Inhaber des Postfachs bitten, dies zu tun, aber diese Methode ist erfahrungsgemäss zu umständlich und unter Umständen auch nicht zuverlässig. Für diese Aufgabe können stattdessen → **WERKZEUGE FÜR EDISCOVERY** und → **DOKUMENTEN-REVIEWS** sinnvoll sein.

6. **Prüfen Sie die herauszugebenen Daten auf heikle Inhalte.** Solche heiklen Inhalte können Geschäftsgeheimnisse, andere interne Informationen, Daten Dritter, kompromittierende Informationen etc. sein. Sie müssen nicht alles liefern, sondern es gibt je nach anwendbarem Recht unterschiedliche Möglichkeiten, gewisse Personendaten nicht herauszugeben oder die Herausgabe aufzuschieben. Sind darin Daten von Dritten (einschliesslich anderer Arbeitnehmer) enthalten, so sind Sie sogar verpflichtet zu prüfen, ob diese Dritten geschützt werden müssen. Denn: Mit den von Ihnen herausgegebenen Daten kann der Gesuchsteller in den Grenzen des Rechts tun und lassen, was er will. Auch für diese Aufgabe können → **WERKZEUGE FÜR EDISCOVERY** und → **DOKUMENTEN-REVIEWS** sinnvoll sein. Zur Durchführung eines Reviews im Hinblick auf datenschutzrechtlich heikle Inhalte oder Geschäftsgeheimnisse siehe → **SWISS SECRECY & PRIVACY REVIEWS**.

Hilfsmittel

Wenn Sie in Postfächern oder anderen grossen Datenmengen nach Daten über Gesuchsteller suchen, eine Vielzahl von Do-kumenten aussortieren oder schwärzen müssen, so sollten Sie dafür spezielle Systeme einsetzen. Diese können fallweise gebucht werden. Dazu → **DOKUMENTEN-REVIEWS** und → **WERKZEUGE FÜR EDISCOVERY**.

Die Löschung der Daten, um einer Auskunft zu entgehen, ist nach herrschender Auffassung unter der DSGVO nicht erlaubt. Etwas weniger klar ist die Situation unter dem DSG.

7. **Beinhalten die herauszugebenen Daten heikle Daten, so legen Sie Ihre Strategie dazu fest.** Diese Strategie kann darin bestehen, dass Sie die Auskunft verweigern oder hinausschieben (Beispiel: Ein Arbeitnehmer will Einblick in die Unterlagen einer laufenden internen Untersuchung; gefährdet dies die Ermittlung, kann die Auskunft aufgeschoben werden). Eine andere, häufiger anzutreffende Strategie ist die Einschränkung der Auskunft, indem die Personendaten entweder so dargestellt werden, dass sie keine heiklen Informationen mehr enthalten. Oder die heiklen Informationen werden geschwärzt, falls Sie nicht nur Daten, sondern Dokumente (z.B. E-Mails, Protokolle) herausgeben. Auch für diese Aufgabe können → **WERKZEUGE FÜR EDISCOVERY** und → **DOKUMENTEN-REVIEWS** sinnvoll sein. Zur Durchführung eines Reviews im Hinblick auf datenschutzrechtlich heikle Inhalte oder Geschäftsgeheimnisse siehe → **SWISS SECRECY & PRIVACY REVIEWS**.

   Wenn Sie **Schwärzungen** vornehmen, sollten Sie erwägen, die Schwärzungen mit einem Erklärungscode zu versehen (z.B. „Geschäftsgeheimnis", „Drittperson", „interne Meinungsbildung"), damit die betroffene Person jeweils weiss, warum eine bestimmte Stelle schwarz ist. Das Datenschutzrecht verlangt normalerweise, dass Einschränkungen einzeln begründet werden.

8. **Erteilen Sie auch die weiteren Auskünfte, die der Gesuchsteller verlangen kann.** Nebst seinen Daten kann ein Gesuchsteller auch noch weitere Angaben verlangen (z.B. die verfügbaren Angaben zur Herkunft von Daten).

9. **Haben Sie Auskunft erteilt, so sollten Sie diese dokumentieren, einschliesslich der Original-Quellen.** Sie dürfen diese Daten auch dann aufbewahren, wenn der Auskunftsersuchende die Löschung verlangt, jedenfalls solange Sie sie für Beweiszwecke brauchen, d.h. es also noch zum Streit über die erteilte Auskunft kommen kann.

Do's	Don'ts
• Dokumentieren Sie die Prüfung der Identität, aber beschränken Sie sich darauf, was wirklich nötig ist. • Dokumentieren Sie Ihre Suche nach passenden Daten zur Beantwortung des Auskunftsgesuchs, damit Sie bei etwaigen Vorwürfen beweisen können, was Sie getan haben.	• Verwenden Sie für Schwärzungen keine Programme, bei denen Sie nicht sicher sind, dass sich die Schwärzungen nicht wieder entfernen lassen. • Geben Sie keine Vollständigkeitserklärungen ab, auch wenn diese verlangt werden.

Do's	Don'ts
• Erklären Sie dem Gesuchsteller, was Sie getan haben, um an seine Daten heranzukommen. • Geben Sie ihm auch Antwort, wenn Sie nichts finden. • Ergänzen Sie die Auskunft mit den nach dem jeweiligen Recht erforderlichen Pflichtinformationen (z.B. zu den Rechten des Gesuchstellers). • Falls Sie einen externen Dienstleister einsetzen, um Dokumente zu sichten oder zu schwärzen, sollte das benutzte Protokoll hinreichend detailliert sein, um eine einheitliche Sichtung bzw. Schwärzung zu gewährleisten.	• Geben Sie keine ganzen Dokumente heraus, ausser, dies ist im konkreten Fall einfacher oder unproblematisch. • Geben Sie keine falschen Auskünfte; das kann Sie teuer zu stehen kommen.

Wann Sie externe Unterstützung beiziehen sollten

- Falls das Auskunftsgesuch im Zusammenhang mit einem laufenden oder drohenden **Rechtsstreit** erfolgt und Sie mit solchen Konstellationen keine Erfahrung haben.
- Falls es gilt, Daten aus einer **grösseren Menge an Dokumenten** oder anderen Inhalten herauszusuchen, sie zu sichten oder sie zu schwärzen, sofern Sie nicht selbst über geeignete eDiscovery-Werkzeuge verfügen.
- Falls Sie eine **Auskunft verweigern** oder einschränken möchten, aber nicht sicher sind, ob und auf welcher Grundlage Sie dies tun dürfen.
- Falls Sie mit einer besonders **hohen Zahl** von Auskunftsersuchen konfrontiert sind, die Sie mit Ihren internen Ressourcen nicht mehr bewältigen können.

Häufige Fragen und Antworten

Q57. Welche Möglichkeiten haben wir nach Schweizer Recht, um ein Auskunftsersuchen zurückzuweisen oder einzuschränken?

A: Das datenschutzrechtliche Auskunftsrecht gilt **nicht absolut**. Dem Unternehmen stehen Möglichkeiten zu, sich gegen ein Auskunftsersuchen zu wehren. Einem Auskunfts-

ersuchen können **gesetzliche Geheimhaltungsbestimmungen**, **überwiegende Interessen Dritter** oder auch überwiegende **private Interessen** entgegengehalten werden. Soweit solche Gründe vorliegen, kann das Unternehmen die Auskunft **einschränken** (z.B. durch Anonymisierungen, Abdeckungen, Freigaben nach Unterzeichnung einer Geheimhaltungserklärung), die **Auskunft zeitlich aufschieben** oder sie **ganz verweigern.** In jedem Fall hat das Unternehmen eine **Einzelfallabwägung** zwischen den unterschiedlichen Interessen vorzunehmen, um zu entscheiden, ob eine Einschränkung angezeigt ist. Sie müssen grundsätzlich auch einzelfallweise (d.h. pro Einschränkung, Schwärzung etc.) begründet werden, jedenfalls wenn es zum Rechtsstreit kommt.

Eine Einschränkung des Auskunftsersuchens kann in einem **formellen Gesetz** vorgesehen sein. So sieht das Geldwäschereigesetz vor, dass der Finanzintermediär Betroffene oder Dritte nicht über Meldungen an die Meldestelle für Geldwäscherei informieren darf. Ferner können das **Amtsgeheimnis, Berufs- oder Bankgeheimnis** die Auskunft beschränken. Allerdings kann sich nur der Geheimnisträger, nicht der Geheimnisherr, darauf berufen. So kann sich unter diesem Titel etwa nur der Anwalt und nicht dessen Klient auf das Anwaltsgeheimnis berufen. Will das Unternehmen sich auf Geheimhaltungsinteresse berufen, so muss es dies im Rahmen eines überwiegenden privaten Interesses tun.

Es gibt Fälle, in denen durch das Auskunftsersuchen gleichzeitig **Personendaten Dritter** bekanntgegeben werden würden. Als Beispiel kann ein Vorfall mehrere Personen betreffen, welche in derselben Textstelle in der Akte genannt werden. Die Textstelle enthält dann Personendaten mehrerer Personen. Erfasst ein Auskunftsersuchen Daten Dritter kann die Auskunft nicht automatisch verweigert werden. Vielmehr hat wiederum eine Abwägung der Interessen stattzufinden. Unter Umständen kann auch eine Schwärzung der betroffenen Stellen ausreichen, um die Persönlichkeit der Drittperson zu schützen. Umgekehrt wird eine Schwärzung schwieriger zu begründen sein, wenn die betroffene Person den Inhalt der Information bereits kennt (allerdings kann der Schutz trotzdem eine Schwärzung erfordern, weil die Herausgabe in ungeschwärzter Form den Missbrauch der Information erleichtern kann).

Schliesslich können auch **private Interessen des Inhabers** der Personendaten dem Auskunftsersuchen entgegengehalten werden. Die Verweigerung der Herausgabe der Personendaten gestützt auf Eigeninteressen ist allerdings nur möglich, wenn die Personendaten Dritten (z.B. dem Marketingunternehmen) nicht bekanntgegeben werden. Beispiele für private Interessen sind der Schutz von Geschäftsgeheimnissen, die Geheimhaltung der internen Meinungsbildung zu bestimmten Themen oder das Interesse, eine interne Untersuchung ohne Gefahr der Vereitelung durchführen zu können. Die Auskunft kann in diesen Fällen nicht per se verweigert werden. Es ist wiederum eine Interessenabwägung erforderlich. Auch wirtschaftliche Gründe können angeführt werden, z.B. der hohe Aufwand der Aufbereitung der Auskunft.

Kommt es zu einer Interessenabwägung, wird das **Interesse des Auskunftssuchenden** relevant. Mit anderen Worten wird dieser sein Interesse in diesen Fällen offenlegen

müssen, obwohl das Auskunftsrecht an sich unbegründet geltend gemacht werden kann. Hierbei ist auch die Art der Einschränkung zu berücksichtigen: Wird die Auskunft generell verweigert oder z.B. lediglich bis zum Ende einer internen Untersuchung aufgeschoben? Wird dem Auskunftsersuchenden zwar Einblick gewährt, aber keine Kopie herausgegeben? Ein klassischer Verweigerungsgrund betrifft Korrespondenz oder sonstige Unterlagen, die der Auskunftssuchende bereits hat: Sein Informationsinteresse wird in solchen Fällen meist geringer sein als das Interesse des Unternehmens, den Rechercheaufwand nicht tätigen zu müssen.

Generell muss sich das Unternehmen kein **rechtsmissbräuchliches Auskunftsersuchen** gefallen lassen, wenn dieses etwa lediglich als Schikane dient. Allerdings sind die Hürden aufgrund der Gerichtspraxis so hoch gesteckt, dass ein Rechtsmissbrauch nur schwer nachweisbar ist. Insbesondere verlangen die Gerichte heute nicht, dass ein Auskunftsersuchen primär der Durchsetzung des Datenschutzes dient; der Datenschutz darf gemäss Gerichtspraxis faktisch auch nur als Vorwand vorgebracht werden. Unter dem revidierten Datenschutzgesetz wird dem voraussichtlich ein Riegel vorgeschoben: Dient ein Auskunftssuchen einem datenschutzfremden Zweck (z.B. der Beweisbeschaffung für ein datenschutzfremdes Gerichtsverfahren), wird die Auskunft verweigert werden können.

Das Unternehmen kann, falls die Frist von 30 Tagen nicht eingehalten werden kann – unter Information an den Gesuchsteller – die **Frist** für Erteilung der Auskunft erstrecken (Art. 1 Abs. 4 VDSG). Schliesslich kann das Unternehmen die Auskunft verweigern, falls es **Anspruch auf eine Kostenbeteiligung** (→ **Q59**) hat und der Gesuchsteller diese Beteiligung verweigert.

Die falsche oder unvollständige Auskunft ist in der Schweiz zwar **bussenbewehrt** (Art. 34 DSG), doch besteht keine Pflicht zur Vollständigkeitserklärung. Ein Unternehmen tut somit gut daran, keine Erklärung abzugeben, dass die Auskunft vollständig erteilt worden ist. Stattdessen sollte es nur erklären, aus welchen Quellen es welche Personendaten offenlegt. Die unberechtigte Verweigerung einer Auskunft ist nicht bussenbewehrt, da der Auskunftssuchende in diesen Fällen die Möglichkeit hat, sie auf dem Weg des Zivilrechts durchzusetzen.

> **Literatur:**
>
> Rosenthal/Jöhri, Art. 9 N 1 ff., in: Rosenthal, David/Jöhri, Yvonne (Hrsg.), Handkommentar zum Datenschutzgesetz, Zürich/Basel/Genf 2008
>
> Rosenthal, David: Das neue Datenschutzgesetz, in: Jusletter 16. November 2020

Q58. Was muss von der Auskunft erfasst werden und in welcher Form ist die Auskunft zu erteilen?

A: Das auskunftspflichtige Unternehmen hat dem Gesuchsteller grundsätzlich **sämtliche** über ihn vorhandene **Daten** mitzuteilen und zwar unabhängig von der Form

der Aufzeichnung (Text, Bild, Ton) und der Speicherform (zur Einschränkung der Auskunftspflicht: → **Q57**) Die Auskunft muss auch die verfügbaren Informationen über die **Herkunft der Daten** enthalten.

Die Auskunft hat in der Regel **schriftlich** und in **verständlicher Form** zu erfolgen und zwar in Form eines Ausdrucks oder einer Fotokopie. Die Auskunftserteilung kann elektronisch stattfinden, wenn dies durch das Unternehmen ausdrücklich vorgesehen ist und geeignete Massnahmen getroffen wurden, damit der Gesuchsteller korrekt identifiziert werden kann; dies dient dem Schutz vor unberechtigtem Zugriff Dritter. Möglich ist auch die Einsichtnahme an Ort und Stelle, wenn das Unternehmen und der Auskunftssuchende damit einverstanden sind. Schliesslich kann die Auskunft auch mündlich erteilt werden, wenn der Gesuchsteller dem zugestimmt hat und korrekt identifiziert worden ist.

> **Literatur:**
>
> Rudin, Beat, Art. 8 N 1 ff., in: Baeriswyl, Bruno/Pärli, Kurt (Hrsg.), Stämpflis Handkommentar, Bern 2015

Q59. Kann ich die Kosten für ein Auskunftsersuchen auf den Gesuchsteller abwälzen?

A: Die Bearbeitung eines Auskunftsersuchens ist mit **Kosten** verbunden. Grundsätzlich ist die Auskunft **kostenlos** zu erteilen. In nachfolgenden Fällen können die Kosten durch das auskunftspflichtige Unternehmen ausnahmsweise auf den Gesuchsteller abgewälzt werden (Art. 2 VDSG):

- **Erneute Auskunftserteilung:** Eine Kostenbeteiligung des Gesuchstellers kann verlangt werden, wenn dieser in den **zwölf Monaten** vor dem Gesuch die gewünschten Auskünfte bereits erhalten hat und **kein schutzwürdiges Interesse** an einer erneuten Auskunftserteilung nachweisen kann. Ein schutzwürdiges Interesse liegt z.B. vor, wenn die Personendaten ohne Mitteilung verändert wurden.
- **Aufwandentschädigung:** Hat das Unternehmen einen **besonders grossen Aufwand** im Zusammenhang mit der Bearbeitung des Auskunftsersuchens, kann ebenfalls eine Kostenbeteiligung legitim sein (z.B. ausserordentlich grosse Mengen an Daten).

Die Kostenbeteiligung ist betragsmässig auf **CHF 300** beschränkt. Der Gesuchsteller ist vor Erteilung der Auskunft auf die Kostenbeteiligung **hinzuweisen**.

> **Literatur:**
>
> Rudin, Beat, Art. 8 N 1 ff., in: Baeriswyl, Bruno/Pärli, Kurt (Hrsg.), Stämpflis Handkommentar, Bern 2015

Gedanken zum Thema.

Ab einer bestimmten Grösse muss jedes Unternehmen damit rechnen, dass es früher oder später mit einer internen oder behördlichen Untersuchung konfrontiert wird. Hat es sich nicht frühzeitig auf die dabei unvermeidbare *eDiscovery* vorbereitet, hat es einen strategischen Nachteil und zahlt für die dann erforderliche Feuerwehrübung einen hohen Preis. In unseren Diskussionen sehen wir, dass der erhöhte Zeitbedarf die Unternehmen dabei oft stärker trifft als zusätzliche Ausgaben. Darum diskutieren wir die Prozesse zur Datenbeschaffung und Aufbereitung auch immer wieder.

Christian Zeunert
Präsident
Cross-border eDiscovery & Investigations Association (CeDIV)

12. Data Breach Reviews

Kurz gesagt

- Werden Ihnen Daten in grösserer Zahl gestohlen, müssen Sie rasch in der Lage sein einzuschätzen, wie heikel die betroffenen Datenbestände sind und welche Dritten (Kunden, Mitarbeiter) davon betroffen sind.
- Dies können Sie mit einem entsprechenden Review dieser Daten feststellen, sofern Sie noch über eine Kopie des mutmasslich betroffenen Datenbestands verfügen. Dies ermöglicht es Ihnen auch, betroffenen Dritten genauere Auskunft über den Inhalt der Daten zu geben.
- Die besondere Herausforderung ist neben der Zeit und dem Geld, die ein solcher Review kostet, die korrekte Instruktion der Reviewer: Sie kennen die Dokumente nicht, müssen sie aber hinsichtlich ihrer Sensibilität klassifizieren.

Worum es geht

Immer wieder sind Unternehmen damit konfrontiert, dass Daten aus dem Unternehmen in die falschen Hände gelangen, sei es durch einen Cyberangriff von aussen (Hacker, Ransomware etc.), sei es durch untreue Mitarbeiter (z.B. Diebstahl von Kundendaten, um diese zu verkaufen) oder sei es durch fahrlässiges Verhalten (z.B. Verlust eines Datenträgers). In solchen Fällen kann es erforderlich sein, dass ein Unternehmen rasch feststellen kann, welche Daten von einer solchen Verletzung der Datensicherheit (Englisch: → **Data Breach**) betroffen sind. Sind die Daten zahlreich, ist hierzu in der Regel ein sog. *Data Breach Review* erforderlich.

Worauf zu achten ist

- Wer herausfinden will, welche Daten verloren gegangen sind, muss diese zuerst in verwertbarer Form sichern. In der Praxis stellt dies oftmals die grösste Hürde dar: Das Unternehmen weiss, dass Daten abfliessen konnten, weiss aber nicht, welche abgeflossen sind. In diesen Fällen verlangt das Datenschutzrecht normalerweise, dass vom schlimmsten realistischen Fall ausgegangen wird.
- Es kann hilfreich sein, vorab ein *Monitoring* oder *Logging* zu implementieren, welches kontinuierlich die Zugriffe auf Daten aufzeichnet; dies kann im Falle eines *Data Breaches* wertvolle Angaben liefern.
- Wenn Daten im Zusammenhang mit einem *Data Breach* beurteilt werden müssen, geht es darum festzustellen, welchen Schaden das haben kann. Das Datenschutzrecht schützt nur natürliche Personen. In der Praxis wird ein Unternehmen hingegen

auch wissen wollen, inwiefern seine Unternehmenskunden und andere Geschäftspartner oder eigene Geschäftsgeheimnisse betroffen sind.

- Es muss in der Regel sehr schnell agiert werden. Das EU-Datenschutzrecht verlangt eine Meldung an die Aufsichtsbehörde teilweise innert 72 Stunden. Diese wird wissen wollen, welche Daten betroffen sind. Sind hingegen keine Daten natürlicher Personen betroffen, sondern „nur" Geschäftsgeheimnisse, kann unter Umständen mehr Zeit bleiben.
- Sind von einem *Data Breach* Daten Dritter betroffen, werden diese wissen wollen, ob und mit welchen Daten sie tangiert sind. Das Unternehmen selbst wird ihnen die Daten oft nicht vorlegen können, da sich darin eigene Geschäftsgeheimnisse oder Daten Dritter befinden können. In diesen Fällen muss das Unternehmen die Daten selbst sichten und im Falle einer Herausgabe vorgängig schwärzen.

Meldepflichten bei Verletzungen der Datensicherheit sieht nicht nur das Datenschutzrecht vor. Auch die **Aufsichtsbehörden** (z.B. FINMA) erwarten bei gewichtigen Vorfällen in der Regel eine Information (z.B. Art. 29 FINMAG). Kann der Vorfall Auswirkungen auf den Börsenkurs einer Gesellschaft haben, so kann eine Pflicht zur **"ad hoc"-Information** bestehen. Viele B2B-Verträge, in deren Rahmen einem Unternehmen Daten anvertraut werden, sehen heute ebenfalls eine **Meldepflicht gegenüber dem Vertragspartner** vor. In all diesen Fällen muss in der Regel rasch festgestellt werden, worum es geht.

Wie vorzugehen ist

1. **Sichern Sie die Daten.** Falls die Daten noch vorliegen, so lassen Sie eine weitere Kopie anfertigen. Falls nicht klar ist, welche Daten abhanden gekommen sind, sollten Sie auf der Basis einer Hypothese arbeiten, falls ansonsten keine Aussage über die abhanden gekommenen Daten möglich ist. Fehlen die Daten, können Daten auf *Backups* Hinweise auf die abhanden gekommenen Daten liefern.
2. **Prüfen Sie eine automatisierte Auswertung der Daten.** Handelt es sich um *strukturierte Daten* (z.B. Datenbankeinträge), lassen sich diese möglicherweise mit Hilfe eines Datenbankspezialisten automatisiert auswerten, soweit dazu nicht die bereits bestehenden IT-Anwendungen benutzt werden können. Handelt es sich um *unstrukturierte Daten* (z.B. E-Mails, Dokumente), so kann eine automatisierte Auswertung in der Regel nur Angaben über den Dateityp bzw. die Anwendung liefern, es sei denn, das Unternehmen hat die Daten mit weiteren Angaben (Metadaten) versehen.

Mit einer automatisierten Auswertung lässt sich in aller Regel auch feststellen, ob die Daten bereits verschlüsselt waren, als sie abhanden gekommen sind, d.h. auch in den Händen eines unbefugten Dritten nicht im Klartext zugänglich sind. Damit wäre Ihr Problem möglicherweise mindestens halbwegs gelöst.

3. **Prüfen Sie, ob ein manueller Review der Daten sinnvoll ist.** Fragen Sie sich, ob nur mit einer manuellen Sichtung vernünftige Angaben darüber möglich sind, welche natürlichen Personen und Unternehmen vom *Data Breach* in relevanter Weise betroffen sind, und in welcher Weise. Je nach Situation kann es sich anbieten, nur einen Teil der Daten zu sichten, um einen ersten Eindruck zu gewinnen und danach zu entscheiden, ob die Sichtung fortgeführt werden soll, da diese viel Zeit und Geld kosten kann.

4. **Falls ein Review durchgeführt werden soll, organisieren Sie diesen.** Hierzu wird in der Regel ein Team und der Einsatz von entsprechenden Review-Systemen benötigt (→ **WERKZEUGE FÜR EDISCOVERY**), damit die Daten von mehreren Personen gleichzeitig und systematisch gesichtet und codiert werden können. Siehe dazu auch → **DOKUMENTEN-REVIEWS**.

5. **Definieren Sie die Kriterien für das → Tagging.** Anders als in anderen Reviews muss bei einem *Data Breach* Review jedes Dokument gesichtet und vollständig bewertet werden. Dies macht einen solchen Review tendenziell aufwändiger. Umso wichtiger ist es, dass Ihr Team von Anfang genau weiss, nach welchen Kriterien es jedes Dokument klassifizieren soll[56] und wie bei jedem Dokument die Namen der betroffenen Dritten festgehalten werden sollen. Dabei ist zu beachten, dass ein Dokument sowohl bezüglich eigener heikler Informationen wie auch bezüglich heikler Information von Dritten codiert werden sollte. Letzteres kann wichtig sein um das Schadenspotenzial des *Data Breach* und die betroffenen Dritten zu ermitteln, während ersteres für eine allfällige spätere Herausgabe der Dokumente und die Einschätzung des eigenen Geheimnisverlusts bedeutend ist.

> **Challenge**
>
> Welche Angaben sind wirklich heikel? Wann ist ein Geschäftsgeheimnis altershalber nicht mehr relevant? Ein Review-Team ist auf praxisnahe Beispiele angewiesen.

6. **Verfolgen Sie den Review laufend, um nötigenfalls korrigierend eingreifen zu können.** Korrekturen werden erfahrungsgemäss immer nötig sein, aber sie sind

56 Beispielsweise „Eigene Geschäftsgeheimnisse“, „Daten über Mitarbeiter“, „öffentliches Dokument“, „Geschäftsgeheimnis von Kunden“, allenfalls mit Abstufungen.

so frühzeitig wie möglich vorzunehmen, da sie jeweils immer nur für die Zukunft durchgeführt werden können.

Ist das *Tagging* geschickt gemacht, kann das Unternehmen anhand vom Review-System generierter Berichte sehr gut feststellen, wieviele heikle Dokumente welcher Natur bereits gefunden wurden.

7. **Prüfen Sie, ob gewisse Dokumente automatisiert codiert werden können.** Je nach Art der Daten können die verwendeten Review-Systeme anhand der bereits gesichteten und klassifizierten Dokumente weitere Dokumente ermitteln, die vergleichbar sind und diese automatisch klassifizieren. Das funktioniert für vorliegende Zwecke erfahrungsgemäss zwar nur für praktisch identische Dokumente zuverlässig, kann jedoch einiges an Aufwand ersparen.

Auch wenn die Review-Systeme Dokumente nicht unbedingt automatisch klassifizieren können, so sind Sie möglicherweise in der Lage, mutmasslich besonders heikle Dokumente anhand bisheriger Klassifizierungen in der Warteschlange nach vorne zu schieben. So kommen Sie unter Umständen rascher zu wichtigen Ergebnissen.

8. **Herausgabe relevanter Dokumente.** Verlangen die betroffenen Dritten Einsicht in die abhanden gekommenen Dokumente und ist das Unternehmen bereit, sie zu gewähren, können sie bei entsprechend geschickt gewählten Klassifizierungen automatisch selektiert und exportiert werden. Sind darin eigene Geschäftsgeheimnisse oder Angaben Dritter enthalten, sind diese allerdings vorgängig ggf. zu schwärzen. Auch hierfür können die Review-Systeme eingesetzt werden. Vgl. dazu → **SWISS SECRECY & PRIVACY REVIEWS** und → **WERKZEUGE FÜR EDISCOVERY**.

Do's	Don'ts
• Klassifizieren Sie Dokumente nicht nur nach betroffenen Dritten, sondern auch danach, wie heikel sie für das eigene Unternehmen sind. • Stellen Sie sicher, dass die Namen der betroffenen Dritten sowohl bei den Dokumenten als auch separat erfasst werden, damit Sie immer wissen, um wen es sich handelt.	• Erwarten Sie keine schnellen Ergebnisse. Ein Review braucht erfahrungsgemäss eine gewisse Zeit um auf „Touren" zu kommen und dauert meist länger als zunächst gedacht. • Vermeiden Sie zu komplizierte oder umfangreiche Tagging-Strukturen. Je mehr ein *Reviewer*

Do's	Don'ts
• Stellen Sie dem Review-Team Personen aus den betroffenen Geschäftsbereichen zur Verfügung, die Fragen zu den Dokumenten beantworten können. Es ist wichtig, dass das Review-Team ein Verständnis dafür entwickelt, was es sichtet. • Falls Sie Schwärzungen vornehmen, stellen Sie sicher, dass diese sich nicht wieder entfernen lassen	klassifizieren muss, desto mehr Fehler unterlaufen ihm und desto mehr Zeit braucht er pro Dokument. • Vermeiden Sie schwammige Instruktionen, da sie dazu führen, dass die einzelnen Reviewer sie unterschiedlich auslegen. Damit leidet die Konsistenz des Reviews.

Wann Sie externe Unterstützung beiziehen sollten

- Falls Sie **mehr als nur einige hundert Dokumente** gesichtet haben müssen.
- Falls Sie über **keine internen Ressourcen** zur Durchführung der Sichtung oder Schwärzung verfügen oder die Mitarbeiter **jeweils nur für kurze Zeit zur Verfügung** stehen (sie werden nicht effizient arbeiten, da sie nie lange genug an der Arbeit sind).
- Falls Sie Dokumente nach mehr als nur einigen wenigen alternativen Kriterien aussortieren müssen; nur professionelle Review-Systeme bieten die **Möglichkeit des *Taggings***.
- Falls die Sichtung aufgrund der **Vertraulichkeit** der Angelegenheit nicht intern erledigt werden kann.
- Falls die Sichtung aufgrund der **erforderlichen Unabhängigkeit** nicht durch eigene Leute erledigt werden kann (und damit den betroffenen Dritten kommuniziert werden kann, dass Spezialisten damit beauftragt worden sind).

Häufige Fragen und Antworten

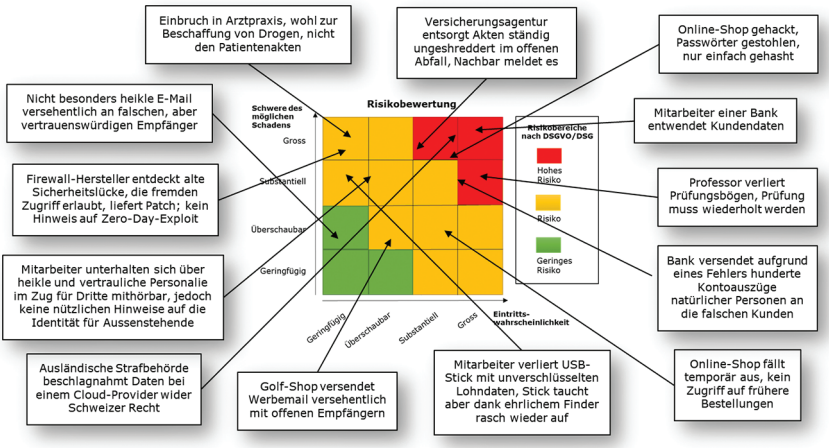
Q60. Welche gesetzlichen Meldepflichten bestehen für das Unternehmen bei einem *Data Breach* in der Schweiz?

A: Derzeit sieht das schweizerische Datenschutzrecht **keine Meldepflicht** bei einem *Data Breach* vor, jedenfalls nicht ausdrücklich. Aus den allgemeinen Grundsätzen des Datenschutzes kann sich jedoch eine Pflicht zur Schadensminderung ergeben, was wiederum erfordern kann, dass betroffene Personen oder ggf. Dritte informiert werden,

soweit dies erforderlich ist, damit diese Gegenmassnahmen ergreifen können (z.B. Sperrung von Kreditkarten oder Nutzerkonten).

Mit dem **revidierten Datenschutzgesetz**, das voraussichtlich 2022 in Kraft treten wird, wird jedoch eine Meldepflicht auch in der Schweiz eingeführt. Sie ist allerdings etwas weniger streng als jene in der EU-Datenschutz-Grundverordnung (DSGVO) und zudem nicht bussenbewehrt. Während im EWR jede Verletzung der Datensicherheit, die zu einem Risiko für betroffene Personen führt, den Aufsichtsbehörden gemeldet werden muss, wird das in der Schweiz nur für Verletzungen gelten, die ein **hohes Risiko von Nachteilen** für die betroffenen Personen mit sich bringen. Das Schweizer Recht kennt auch keine 72-Stunden-Frist, sondern verlangt, dass unverzüglich gemeldet werden muss. Das erlaubt, die für eine sinnvolle Meldung erforderlichen Informationen erst zusammenzutragen.

Die folgende Grafik gibt Hinweise auf die Einschätzung des Risikos unter der DSGVO und dem revidierten Datenschutzgesetz:



Die betroffenen Personen müssen informiert werden, sobald dies **zu ihrem Schutz erforderlich** ist, also wenn sie etwas tun können, um sich besser auf die Folgen der Verletzung der Datensicherheit vorzubereiten oder Schaden zu minimieren.

Literatur:

Rosenthal, David: Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, Rz. 160 ff.

Q61. Muss betroffenen Dritten Einblick in die abhanden gekommenen Daten gewährt werden?

A: Ein solcher Anspruch kann sich aus **vertragsrechtlicher Sicht** ergeben, soweit die Einsichtnahme erforderlich ist, damit die betroffene Person oder das betroffene Unternehmen ihren bzw. seinen Schaden mindern kann. Ein Anspruch auf Einsichtnahme kann sich zudem aus Treu und Glauben ergeben. Dies wird dort, wo mutmasslich sensible Daten betroffen sind und keine eigenen, überwiegenden Interessen (z.B. Geheimhaltungsinteressen) entgegenstehen, häufig gegeben sein.

Im Falle einer betroffenen natürlichen Person (und bis zur Revision des Datenschutzgesetzes) wird sich ein solches Einsichtsrecht mindestens teilweise auch **aus dem Auskunftsrecht ableiten** lassen. Allerdings sieht dieses keinen Auskunftsanspruch bezüglich der Verletzung der Datensicherheit vor, sondern nur bezüglich der vom Unternehmen bearbeiteten Daten. Welche davon tatsächlich von der Verletzung der Datensicherheit betroffen sind und welche nicht, muss das Unternehmen im Rahmen der Auskunftspflicht unter dem bisherigen Recht nicht offenlegen.

Unter dem revidierten Datenschutzgesetz ist die Auskunftspflicht weiter gefasst. Das Auskunftsrecht kann über die **Generalklausel** auch solche weitergehenden Informationen abdecken. Auch aus der Pflicht zur Information der betroffenen Personen können unter Umständen sekundäre Informationspflichten abgeleitet werden, soweit solche Informationen nötig sind, damit sich die betroffenen Personen vor Schaden schützen können.

Gedanken zum Thema.

Ein *Data Breach* kann leider jedem widerfahren. Wie gut man ihn meistert und wie weit man den Schaden minimieren kann, hängt von verschiedenen Faktoren ab. Es braucht einen definierten Prozess mit einem Team aus Spezialisten. Die dringendste Massnahme ist natürlich, das Leck so schnell wie möglich zu schliessen. Auch Kommunikationsmassnahmen sind wichtig und sollten frühzeitig vorbereitet sein. Vor allem aber muss das ganze Ausmass der Verletzung der Datensicherheit analysiert werden. Welche und wie viele Daten sind betroffen? Welche Personen sind vom *Data Breach* tangiert und welche Risiken sind für sie entstanden? Wie können diese Risiken minimiert werden? Das ist aber oft leichter gesagt als getan – und nicht selten der aufwändigste und schwierigste Teil.

Nicolas Passadelis
Head of Data Governance
Swisscom

13. Vertragsreviews

Kurz gesagt

- Elektronische Vertragsreviews bieten sich vor allem dort an, wo Sie eine grosse Zahl von Verträgen prüfen müssen und Ihnen diese als elektronische Dateien zur Verfügung stehen (d.h. nicht bloss in einem virtuellen *Data Room*).
- Mit halbautomatischen Reviews können Sie eine Software-Lösung Verträge auf standardisierte Inhalte (z.B. Klauseln zu bestimmten Themen) prüfen lassen (Mustererkennung). Sie müssen die Software dazu vorher aber anhand genügender Beispiele trainieren.
- Der Markt für Software für Vertragsreviews boomt derzeit – und die Hersteller versprechen oft das Blaue vom Himmel.

Worum es geht

Vorliegend geht es um die Sichtung einer grösseren Zahl von Verträgen, so z.B. im Rahmen einer *Due Diligence*, der Durchführung einer M&A-Transaktion oder einem Streitfall. Auch im Falle einer Rechtsfortentwicklung kann es erforderlich sein[57], eine grössere Anzahl von Verträgen auf bestimmte Inhalte hin zu prüfen und anzupassen. Erfolgten solche Reviews früher ausschliesslich manuell, existieren heute hierzu verschiedene Softwarelösungen, die einen solchen Review teilweise automatisieren und damit unterstützen können. Im Rahmen des Reviews geht es primär darum, Verträge im Hinblick auf bestimmte Inhalte zu identifizieren, diese zu extrahieren (z.B. nach involvierten Parteien) oder sie zu klassifizieren (z.B. nach Vertragstypen, bestimmten Klauseln oder Regelungen) und sie zu bewerten (z.B. mittels einer Risikoeinschätzung) oder sonst zu bearbeiten (z.B. mittels Durchführung einer Vertragsanpassung).

Worauf zu achten ist

- Computergestützte Vertragsreviews lohnen sich erst ab einer grösseren Zahl von Dokumenten (ab einigen Hundert).
- Für automatisierte Reviews braucht es noch mehr Dokumente (1‘000 oder mehr), damit sie Sinn machen, weil die Systeme zuvor trainiert werden müssen; das erfordert Spezialwissen.
- Computer können Verträge und ihre Klauseln inhaltlich nicht bewerten, sondern höchstens nach bestimmten Kriterien klassifizieren oder bestimmte, standardisierte Inhalte extrahieren.

- Der Markt für Lösungen für computergestützte Vertragsreviews ist unübersichtlich; wer sich hier etablieren wird, ist noch unklar. Oft wird mehr versprochen, als eingehalten werden kann.
- Ohne Handarbeit geht es nach wie vor nicht.
- Die Schwärzung von Verträgen lässt sich nur beschränkt automatisieren (→ **SWISS SECRECY & PRIVACY REVIEWS**).

Im Rahmen von Lösungen für Vertragsreviews ist meist von „künstlicher Intelligenz" (KI) und „maschinellem Lernen" oder „*Deep Learning*" die Rede. Gemeint sind damit in aller Regel **Verfahren zur Mustererkennung**. Es ist nicht so, dass die Systeme die ihnen gefütterten Verträge inhaltlich verstehen, sondern sie suchen normalerweise nur, aber immerhin nach Klauseln, deren Text ähnliche Muster (Wörter bzw. Wortkombinationen, Satzstellung etc.) aufweisen wie jene Klauseln, die ihnen zu einem bestimmten Klauseltyp (z.B. Geheimhaltungsklausel, Haftungsbegrenzung etc.) im Rahmen des Trainings vorgelegt worden sind. Vgl. hierzu die → **Concept Search** in → **WERKZEUGE FÜR EDISCOVERY**. Dem Training kommt somit eine entscheidende Bedeutung zu.

Wie vorzugehen ist

1. **Beschaffen Sie die Verträge in elektronischer Form.** Damit Sie einen Review durchführen können, müssen die Verträge elektronisch vorliegen, d.h. mindestens als Scan. Die Texterkennung, d.h. die Umwandlung in maschinenlesbaren Text, kann in der Regel von entsprechenden Computerprogrammen besorgt werden (dazu → **WERKZEUGE FÜR EDISCOVERY**). Sind die Dokumente von schlechter Qualität, kann die Präzision der Texterkennung allerdings leiden. Das schränkt wiederum die Einsatzmöglichkeiten automatisierter Vertragsreviews ein. Dasselbe gilt bei Dokumenten mit Tabellen und Grafiken.

   Sollten Sie über ein **elektronisches Vertragsmanagement** verfügen, ist es denkbar, dass Sie aus diesem nicht nur die Verträge, sondern auch entsprechende Metadaten exportieren können (z.B. Namen der Vertragsparteien, weitere Eckdaten). Prüfen Sie, ob und in welcher Form das Review-System diese Daten übernehmen kann. In den meisten Fällen wird die Weiterverarbeitung dieser Metadaten freilich nicht möglich sein, d.h. die Angaben gehen verloren

2. **Formulieren Sie das Ziel des Reviews.** Was soll der Review bewerkstelligen? Geht es darum, sich einen Überblick über den Inhalt einer Serie von Verträgen (z.B. in einem *Data Room*) zu verschaffen, wobei die Verträge ihrerseits sehr unterschiedli-

cher Natur sind? Oder geht es darum, eine Serie von Verträgen daraufhin zu prüfen, ob sie eine bestimmte Regelung enthalten (z.B. mit welchen Kunden ein Unternehmen Vertragsstrafen vereinbart hat, oder das Verbot des Beizugs Dritter)? Vielleicht soll der Review aber auch dazu dienen, den Regelungsgehalt der einzelnen Verträge zu einem bestimmten Thema zu klassifizieren? Ist Ihnen bereits gedient, wenn Sie die vorhandenen Verträge nach Typen aufteilen können (Mietverträge, Finanzierungsverträge, Lizenzverträge, Einkaufsverträge etc.)? Soll eine Liste der Vertragsparteien erstellt werden oder aber eine Liste mit einer kurzen Zusammenfassung und Kommentierung jedes Vertrags? Das Ziel des Reviews wird Ihnen und einem etwaigen Spezialisten helfen, das richtige Werkzeug für den Review zu ermitteln.

3. **Legen Sie fest, welche Angaben zu jedem Vertrag im Rahmen des Reviews zur weiteren Verarbeitung erfasst werden sollen.** Je nachdem, wie Sie den Vertragsreview weiterverarbeiten wollen, benötigen Sie pro Vertrag mehr als nur die Angaben, welche Art von Klausel, Regelung etc. er beinhaltet, sondern es sind auch Angaben zum Vertrag selbst erforderlich. In jedem Fall sind diese Anforderungen frühzeitig festzulegen, damit die Reviewer oder Programmierer der Review-Systeme entsprechend instruiert werden können.

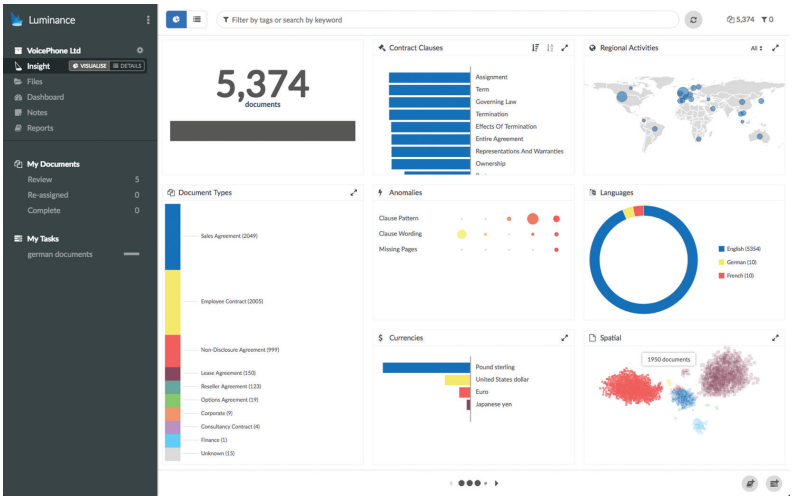
Systeme für **automatisierte Vertragsreviews** kommentieren Verträge nicht, sondern können sie nach formalen Kriterien einteilen und Inhalte mit bestimmten Charakteristika extrahieren, so z.B. Vertragstyp, Vertragssprache, Parteien, Regelungen zu einem bestimmten Thema (z.B. Vertragsstrafen, Kündigungsregeln, Kontrollwechselklauseln, Geheimhaltungspflichten) oder formalisierte Inhalte (z.B. Höhe eines Haftungsbetrags).

4. **Strukturieren Sie den Review.** Haben Sie viele Verträge (Hunderte oder Tausende), ist es aus Gründen der Effizienz wichtig, deren Review systematisch zu strukturieren. So kann es sinnvoll sein, dass ein erstes Team die Verträge grob aussortiert, während weitere Teams unterschiedliche Typen von Verträgen analysieren (und dies entsprechend effizient durchführen können, weil sie immer mit demselben Vertragstyp arbeiten). Ist eine Beurteilung von einzelnen Klauseln erforderlich, kann es sinnvoll sein, mit Reviewern für unterschiedliche Schwierigkeitsgrade zu arbeiten, d.h. Verträge mit unklaren Regelungen werden zur Klassifizierung frühzeitig an erfahrenere Team-Mitglieder eskaliert.

5. **Wählen Sie das Review-System aus.** So oder so werden Sie sich für den Review normalerweise an einen Provider halten, der Ihnen das System für den Review bereitstellt. Die Wahl dieses Dienstleisters setzt allerdings voraus, dass Sie sich bereits eine Vorstellung darüber gemacht haben, welche Art Review-System Sie verwenden möchten. Während die „Big Four" in der Regel alle Arten von Review-Systemen anbieten, hat sich im Markt, nebst den auf klassisches eDiscovery ausgerichteten

Providern, eine neue Garde von Anbietern von speziell für Vertragsreviews entwickelte Lösungen herausgebildet. Die Wahl des Anbieters entscheidet faktisch über die Art von Review-System, das zum Einsatz kommt. Darum sollten Sie sich darüber Gedanken machen, welchen Typ von Review-System Sie einsetzen wollen:

- **Systeme für Vertragsreviews (z.B. Kira, Luminance):** Sie sind speziell auf die Sichtung und Analyse von Verträgen ausgerichtet. Ein Vertrag wird von diesen Systemen nicht nur als Gesamt-Dokument eingelesen und verarbeitet, sondern in seine Teile (d.h. die einzelnen Klauseln) aufgebrochen und entsprechend analysiert. Auf diese Weise können auch einzelne Klauseln kommentiert und klassifiziert werden. Dies erfordert allerdings mehr Übung in der Handhabung und setzt voraus, dass die Verträge in entsprechender technischer Qualität vorliegen. Diese Systeme bieten die automatisierte Analyse von Verträgen an, was sich in der Regel erst ab einer hohen Zahl von Dokumenten lohnt (1'000 oder mehr), weil die Systeme über gewisse Grundfähigkeiten hinaus entsprechend programmiert und trainiert werden müssen. Sich selbst trainieren können sie nur soweit es darum geht, Anomalien in bestehenden Datensätzen aufzuspüren. Die automatische Analyse kann benutzt werden, um bestimmte Standardinformationen aus einem Vertrag zu extrahieren (z.B. Parteibezeichnungen) oder Verträge auf bestimmte inhaltliche Muster hin zu durchsuchen (z.B. bestimmte Regelungstypen oder -themen). Der richtige Umgang mit solchen Systemen erfordert Expertise.



Auswertung in „Luminance" (Quelle: www.luminance.com)

- **Klassische Review-Systeme (z.B. Relativity):** Diese Systeme bieten keine speziell auf Verträge ausgerichteten Funktionen, sind aber für den Reviewer

entsprechend einfacher zu bedienen und bieten mehr Flexibilität in der Anpassung auf Kundenbedürfnisse. Das Angebot an Providern ist zudem grösser und ihr Einsatz oft auch deutlich günstiger, weil keine besondere Programmierung und kein Training der Systeme nötig ist. Dem Reviewer wird jeweils das gesamte Dokument angezeigt, er kann darin blättern und er kann es als Ganzes klassifizieren, Kommentare erfassen und Lesezeichen setzen. Zwar verfügen auch die klassischen Review-Systeme über Funktionen, mit denen Muster erkannt werden können („*Predictive Coding*“) oder mit denen nach Formulierungen zu bestimmten Themen gesucht werden kann („*Concept Search*“). Auch können sehr ähnliche Dokumente (z.B. Mietverträge, in denen jeweils nur die Parteien andere sind) gruppenweise verarbeitet werden. Aber diese Systeme sind nicht speziell auf den Review von Verträgen ausgerichtet und differenzieren daher insbesondere nicht nach Vertragsklauseln.

In der Praxis sind auch Kombinationen denkbar, doch üblicherweise macht es aus Gründen der Effizienz (und aufgrund von Datenverlusten an den Schnittstellen) keinen Sinn, zuerst das eine System für die Analyse von Dokumenten zu benutzen, um sie dann für einen Review in ein anderes System zu laden, weil dieses in der Handhabung für die Reviewer etwas einfacher ist.

6. **Führen Sie den Review durch.** Es gelten hier die allgemeinen Grundsätze für → **DOKUMENTEN-REVIEWS**, etwa zur Instruktion und Überwachung der Reviewer und laufenden Anpassungen. Kommt eine automatisierte Analyse von Verträgen zum Einsatz, wird der Review typischerweise in drei Phasen unterteilt sein:

   - **Programmierung und Training:** Das Review-System wird von Experten für die Analyse vorbereitet. Dies umfasst insbesondere auch das Trainieren der Mustererkennungseinheit anhand von möglichst vielen Beispielen. Diese müssen normalerweise Sie selbst liefern. Das kann wiederum einen vorgängigen Review einer Serie von Verträgen erforderlich machen.

   - **Automatisierte Analyse der Verträge:** Ist das Review-System programmiert und trainiert, wird es mit den zu untersuchenden Verträgen gefüttert. Diese werden in der Folge analysiert. Rechnen Sie nicht damit, dass diese Analyse auf Anhieb gute Ergebnisse liefert. Es können durchaus mehrere Durchgänge nötig sein, bis das System optimal eingestellt ist. Auch dies erfordert den Einsatz von Experten, was kostenmässig zu berücksichtigen ist.

   - **Manueller Review der Verträge:** Nur in wenigen Fällen ist es mit der automatisierten Analyse getan. Sie mag dort genügen, wo das Unternehmen lediglich grobe Statistiken benötigt oder bestimmte, klar ermittelbare Informationen (z.B. die Namen der Vertragsparteien oder die Aufstellung der Vertragstypen und Sprachen). Ist eine inhaltliche Beurteilung der Verträge erforderlich, geht dies nicht ohne Handarbeit. Immerhin vereinfachen die spezialisierten Systeme für Ver-

tragsreviews diese Arbeit dahingehend, dass sie die Reviewer jeweils direkt zu den von ihnen als relevant ermittelten Stellen in den Verträgen führen können.

Zu berücksichtigen sind nicht nur *„false positives“*, d.h. Klauseln, welche das System fälschlicherweise als relevant erkannt hat. Im Rahmen der **Qualitätssicherung** ist auch zu prüfen, ob es in relevanter Zahl zu *„false negatives“* kommt, d.h. Vertragsklauseln, die zwar relevant sind, aber vom System nicht identifiziert werden.

7. **Exportieren Sie die Ergebnisse.** Überlegen Sie sich frühzeitig, wie Ihnen das Ergebnis des Reviews zur Verfügung stehen soll. Review-Systeme können eingelesene Dokumente als PDFs, als Bilddateien oder in ihrem nativen Format exportieren. Die *Taggings* und Kommentare können sie in separaten Dateien bereitstellen. Überlegen Sie sich frühzeitig, wo und wie Sie diese Informationen weiter verarbeiten wollen und ob die Exportformate (insbesondere auch der Metadaten) von den Systemen unterstützt werden, mit welchen Sie weiterarbeiten wollen.

Do’s	Don’ts
• Wählen Sie ein Review-System erst dann aus, wenn Sie genau wissen, was Sie mit dem Review erreichen wollen und Sie somit prüfen können, ob das System für Ihren Fall überhaupt Sinn macht. • Setzen Sie automatisierte Reviews erst ab einer grösseren Zahl von Verträgen ein (mindestens 1‘000). • Wie in jedem Review sollten Sie auch für Vertragsreviews eine Qualitätskontrolle vorsehen, auch wenn der Review automatisiert erfolgt. • Achten Sie auf die Sprache der Verträge. Mustererkennungen sind sprachabhängig.	• Verlassen Sie sich nicht blind auf einen automatisierten oder menschlichen Review. Beide können zu Fehlern führen, die Sie berücksichtigen müssen. • Vermeiden Sie bei der Instruktion Ihrer Reviewer soweit wie möglich, dass diese Vertragsklauseln werten müssen, es sei denn, sie haben hierfür klare, enggesteckte Vorgaben oder die Reviewer sind sehr erfahren.

Wann Sie externe Unterstützung beiziehen sollten

- Für den **Einsatz eines Review-Systems**, weil die meisten Firmen diese Art von Systemen nicht selbst betreiben, sondern als Dienstleistung beziehen.
- Falls Sie über **keine internen Ressourcen** zur Durchführung des Reviews verfügen und zum Beispiel günstige Reviewer benötigen.
- Falls Sie neben Ihrem Review-Provider eine unabhängige Stelle **für die Qualitätssicherung** benötigen.
- Falls Sie **alternative Mustertexte** für das Training eines automatisierten Systems benötigen.
- Falls Sie sich **unsicher** sind (z.B. welches Review-System für Ihren konkreten Fall wirklich sinnvoll ist).

Häufige Fragen und Antworten

Q62. Lassen sich die Systeme für Vertragsreviews auch für eine klassische *Due Diligence* in einer M&A Transaktion einsetzen?

A: Nur beschränkt, jedenfalls auf Seiten des Käufers. Das liegt daran, dass in einer klassischen M&A-Transaktion der Käufer heute zwar Zugang zu einem elektronischen Datenraum erhält, die Daten kann er allerdings nicht aus diesem Datenraum herausnehmen und der Verkäufer wird sie ihm in aller Regel auch nicht aushändigen wollen. Er kann sie somit auch nicht in sein System für den Vertragsreview einlesen.

Gedanken zum Thema.

Die Einhaltung der einschlägigen datenschutzrechtlichen Vorschriften und Massgaben ist eigentlich selbstverständlich – stellt einen in der Praxis aber immer wieder auf die Probe. Verschaffen Sie sich daher frühzeitig einen Überblick über die für Ihre konkrete Untersuchung tatsächlich und auch potenziell relevanten Jurisdiktionen sowie die einschlägigen Gesetze und Vorschriften. Denn die rechtlichen und tatsächlichen Fragen sind mannigfaltig – muss ich etwa im Rahmen einer internen Untersuchung in der Schweiz die DSGVO beachten? Wo sind die Daten gespeichert? Wo sind die betroffenen Mitarbeiter angestellt oder wem «gehören» die Kundendaten? Wohin sollen die Untersuchungsergebnisse übermittelt werden? Werden für das Reporting personenbezogene Daten benötigt? Setzen Sie sich also möglichst zu Beginn einer Untersuchung mit Ihrer IT an einen Tisch – es wird sich lohnen.

Philipp Becker
Senior Legal Counsel Litigation and Investigations
Zurich Insurance

14. Swiss Secrecy & Privacy Reviews

Kurz gesagt

- Wenn Sie Anwälten, Behörden, Providern oder Parteien im Zusammenhang mit einem ausländischen Verfahren Unterlagen von sich aus der Schweiz übergeben wollen, prüfen Sie vorher nicht nur den Datenschutz (private/sensible Inhalte), sondern auch Ihre eigenen Geheimhaltungspflichten gegenüber Dritten.
- Stehen solche Inhalte zur Diskussion, können Sie im schlimmsten Fall gezwungen sein, vorgängig alle Unterlagen zu sichten und die heikelsten Inhalte zu schwärzen. Das kostet Zeit und Geld, was einzuplanen ist.
- Gefährlich ist vor allem die Verletzung von Berufs- und Geschäftsgeheimnissen, da dies zur persönlichen Strafbarkeit führen kann. Im Bereich des Datenschutzes gibt es etwas mehr Spielraum.

Worum es geht

Wenn Unternehmen im Rahmen eines ausländischen Rechtsstreits, eines ausländischen Behördenverfahrens oder in anderem Zusammenhang nicht-öffentliche Daten und Dokumente herausgeben müssen, wirft dies Fragen des Datenschutzes, des Arbeitsrechts und des Schutzes von Geschäftsgeheimnissen Dritter auf. In letzterem Falle geht es um Informationen, die Kunden und andere Geschäftspartner dem Unternehmen anvertraut haben und deren Vertraulichkeit das Unternehmen daher zu bewahren hat. Die Offenlegung in einem Rechtsstreit (welcher nicht diese Kunden oder Partner betrifft) kann nicht nur Geheimhaltungsvereinbarungen verletzen, sondern auch strafrechtliche Folgen für das Unternehmen haben (Art. 162 StGB, Art. 273 StGB, Bestimmungen zum Berufsgeheimnis). Dies kann es erforderlich machen, die betreffenden Informationen vor einer Offenlegung zu finden und zu schwärzen. Der Datenschutz und das Arbeitsrecht wiederum können es erforderlich machen, dass besonders sensible Inhalte von Mitarbeitern oder anderen Personen (z.B. Angaben zur Gesundheit, private Inhalte) ausgesondert oder – gerade wenn es um Mitarbeiterdaten geht – komplett anonymisiert werden müssen, weil eine Offenlegung negative Folgen für diese haben könnte und der Arbeitgeber sie vor solchen zu bewahren hat.

Was für das Schweizer Recht gilt, kann in ähnlichem Umfang auch für andere europäische Rechtsordnungen gelten. Das ist speziell zu beachten, wenn Daten von Personen aus anderen europäischen Ländern bearbeitet werden (z.B. Postfachinhalte von Mitarbeitern aus ausländischen Gesellschaften). Die **EU-Datenschutz-Grundverordnung** (DSGVO) stellt ähnliche Anforderungen an den

Schutz von Mitarbeitern und weiteren Personen wie das Schweizer Datenschutz- und Arbeitsrecht. Im Geheimnisschutz geht das Schweizer Recht jedoch erfahrungsgemäss weiter als viele ausländische Rechtsordnungen, da die Schweiz den Verrat von Geschäftsgeheimnis strafrechtlich sanktioniert.

Worauf zu achten ist

- Vor einer Schwärzung sollte genau analysiert werden, welche Schwärzungen wirklich nötig sind und wo mit anderen Mitteln ein Schutz der betroffenen Personen erreicht werden kann.
- Es ist leider noch nicht möglich, private Daten oder Geschäftsgeheimnisse zuverlässig automatisch aufzuspüren und schon gar nicht, sie automatisch zu schwärzen; es braucht also Handarbeit.
- Es gibt jedoch gute Hilfsmittel, mit welchen sich die Kosten für einen *Swiss Secrecy & Privacy Review* deutlich senken lassen.
- Die Qualität und Effizienz eines *Secrecy Reviews* hängt primär von der Kenntnis des eigenen Geschäfts ab, insbesondere dem Wissen, über welche Geschäftsgeheimnisse das Unternehmen verfügt.
- Ob ein *Swiss Secrecy & Privacy Review* in der Schweiz stattfinden muss, hängt wiederum von den Umständen ab; allenfalls kann er mit einem Review in der Sache kombiniert werden, was Kosten sparen kann.
- Die Review-Vorgaben sind zu dokumentieren, damit im Falle von Fehlern (die immer vorkommen) die eigene Sorgfalt belegt werden kann.

Wie vorzugehen ist

1. **Müssen Mitarbeiterdaten anonymisiert werden?** Die Frage hängt primär davon ab, wo und wem Dokumente offengelegt werden sollen – und welches potenzielle Ungemach damit für die betroffenen Mitarbeiter verbunden sein kann. Der Arbeitgeber muss sich nicht nur an den Datenschutz halten (was u.a. bedeutet, dass so wenig Personendaten wie nötig offenzulegen sind), sondern hat auch eine arbeitsrechtliche Fürsorgepflicht gegenüber dem Mitarbeiter, d.h. er muss ihn schützen. Drei typische Konstellationen:
   - **Ausländischer Zivilprozess** (z.B. *pre-trial discovery*): Hier können Mitarbeiternamen in aller Regel offengelegt werden, jedenfalls wenn es im Streit nur um Ansprüche gegen das Unternehmen geht und die Mitarbeiter zwar allenfalls als Zeugen in Frage kommen, aber letztlich jeweils nur in ihrer Eigenschaft als Arbeitnehmer.

Auch wenn Mitarbeiterdaten nicht geschwärzt werden, so können sie trotzdem nicht schutzlos offengelegt werden, jedenfalls wenn im betreffenden Land kein gesetzlicher Datenschutz besteht. Bei Zivilverfahren in den USA hat sich die Praxis eingebürgert, dass mit der Gegenseite im Rahmen einer *pre-trial discovery* ein sog. *Protective Order* vereinbart wird, der auch Personendaten erfasst (normalerweise dient er nur dem Schutz von Geschäftsgeheimnissen). Er verpflichtet die Gegenseite, die erhaltenen Daten vertraulich zu behandeln und für keinen anderen Zweck zu verwenden. Der Vertrag wird vom Gericht zusätzlich verfügt.

- **Ausländisches Straf- oder Administrativverfahren:** Untersucht eine ausländische Behörde das Fehlverhalten eines Unternehmens und kann dies negative Folgen für Mitarbeiter haben (z.B. straf- oder aufsichtsrechtlicher Natur), so werden diese üblicherweise zunächst anonymisiert, um den Gang der Dinge abzuwarten. Eine Offenlegung ist nicht per se ausgeschlossen, aber es muss – vereinfacht gesagt – zuerst klar sein, dass sie nicht die Falschen trifft. Stellt sich heraus, dass ein Mitarbeiter z.B. in einer Betrugs-, Kartell- oder Korruptionsuntersuchung massiv gegen seine Pflichten als Arbeitnehmer verstossen hat, kann dies eine Offenlegung durch den Arbeitgeber rechtfertigen.
- **Datenschutzrechtliches Auskunftsbegehren**: Ist ein Unternehmen nach Datenschutzrecht zur Auskunft verpflichtet, so bedeutet dies nicht, dass alle die anfragende Person betreffende Daten herausgegeben werden dürfen. Betreffen sie zugleich Drittpersonen (wozu auch Mitarbeiter zählen), so muss geprüft werden, ob diese überwiegende Interessen an der Geheimhaltung haben, in welchem Fall ihre Personendaten zu schwärzen bzw. anonymisieren sind.

2. **Kommen sensible Personendaten vor, die geschwärzt werden müssen?** Selbst wenn die Identität von Mitarbeitern nicht geschwärzt wird, kann es erforderlich sein, bestimmte sensible Personendaten zu schwärzen. Das gilt selbst dann, wenn grundsätzlich nur Dokumente herausgegeben werden, die für den konkreten Fall relevant sind. Eine Schwärzung drängt sich insbesondere auf für:

   - Private, nicht öffentliche Daten einer Person
   - Gesundheitsdaten einer Person
   - Vertrauliche HR-Daten einer Person, inklusive Daten über strafrechtliche oder administrative Sanktionen und Verfolgungen

   soweit sie für den konkreten Fall nicht von Relevanz sind. So kann der Inhalt einer Mitarbeiterbeurteilung für eine behördliche Untersuchung von Bedeutung sein. Der auch in geschäftlicher Kommunikation übliche *Smalltalk* muss hingegen nicht

geschwärzt werden, auch nicht jene privaten Äusserungen, welche die betroffene Person bewusst vor einem nicht kontrollierbaren Publikum macht.

3. **Sind Berufsgeheimnisse oder Geschäftsgeheimnisse Dritter zu schützen?** Eine solche Pflicht zum Schutz von Geschäftsgeheimnissen Dritter kann sich entweder aus Vertrag (Geheimhaltungsklausel, *Non-Disclosure-Agreement [NDA]*) oder aus Gesetz (Berufsgeheimnis) ergeben. Ob der Pflicht einer Offenlegung bestimmter Dokumente im konkreten Fall etwas entgegensteht, muss in der Regel durch Auslegung ermittelt werden, d.h. es muss geklärt werden, ob der Geheimnisherr davon ausging, dass seine Geschäftsgeheimnisse z.B. Eingang in ein ausländisches Verfahren des Unternehmens finden können. Die Erfahrung zeigt leider, dass die Situation oft nicht völlig klar ist.
Hinzu kommt, dass die in der Schweiz zahlreichen Strafnormen zur Durchsetzung von Geheimhaltungspflichten, teilweise sehr vage formuliert sind (vgl. z.B. Art. 273 StGB). Werden Daten unzulässigerweise offengelegt, kann dies strafrechtliche Konsequenzen für die betreffenden Entscheidungsträger haben. Sie haben daher ein persönliches Interesse daran, dass das Geschäftsgeheimnis eines Geschäftspartners im Zweifel geschwärzt wird. Im Falle des Bankkundengeheimnisses kann bereits die fahrlässige Verletzung strafrechtlich geahndet werden.

Art. 273 StGB

Das Besondere an Art. 273 StGB (wirtschaftlicher Nachrichtendienst) ist, dass die Norm nicht einzelne Geheimnisherren, sondern die Schweizer Wirtschaft schützen will. Sie sanktioniert bereits das Zugänglichmachen (keine Kenntnisnahme erforderlich), greift nur, wenn Zugriffe aus dem Ausland möglich sind, kann nicht immer mit einem *Waiver* "erledigt" werden und gilt anders als sonst im StGB üblich weltweit. Die Norm kann greifen, selbst wenn kein NDA besteht.

4. **Genügend Zeit sicherstellen.** Ein *Swiss Secrecy & Privacy Review* kann je nach der Anzahl der Dokumente viel Zeit beanspruchen (d.h. Wochen oder sogar Monate). Dies ist im Verfahren, für welchen der Review durchgeführt werden soll, angemessen zu berücksichtigen. Nicht immer ist dies selbstverständlich: Ist ein Schweizer Unternehmen in den USA in einen Prozess involviert, in welchem ein *pre-trial discovery* durchgeführt wird, so gehen US-Anwälte in der Regel nicht davon aus, dass alle Dokumente noch auf Geschäftsgeheimnisse Dritter oder private Daten gesichtet werden müssen, weil dies nach US-Recht schlicht nicht er-

Zeit gewinnen

Eine Möglichkeit, in einem ausländischen Verfahren Zeit zu gewinnen ist eine sog. *Rolling Production*. Dabei werden Dokumente nach und nach geliefert, d.h. der Empfänger muss nicht bis zum Abschluss mit seiner Sichtung der Unterlagen warten.

forderlich ist. Lässt sich ein Unternehmen in einem solchen Verfahren selbst von US-Anwälten vertreten, werden diese in Unkenntnis der Sitten und Vorgaben in Europa möglicherweise eine Dokumentenlieferung zusichern, die das Unternehmen nicht einhalten kann. Ähnliches gilt für Verfahren vor ausländischen Behörden. Das Unternehmen tut daher gut daran, dass mindestens im Sinne eines Erwartungsmanagements rechtzeitig ein realistischer und nicht zu ehrgeiziger Zeitplan vorgesehen wird, welcher auch die Möglichkeit unerwarteter Verzögerungen (die es meistens gibt) vorsieht.

5. **Können die Schwärzungen mit einem anderen Review kombiniert werden?** Dies ist nur teilweise in sinnvoller Weise möglich. Hierbei sind speziell zwei Faktoren zu berücksichtigen:

   - **Komplexität des Reviews:** Auf den ersten Blick kann es effizient erscheinen, die Reviewer, welche die Dokumente ohnehin anschauen müssen, gleich auch noch zu bitten, etwaige Geschäftsgeheimnisse Dritter zu schwärzen sowie private und weitere sensible Daten. Die Erfahrung zeigt jedoch, dass dies häufig ein Trugschluss ist: Je mehr einem Reviewer aufgetragen wird, desto langsamer wird er und desto häufiger kommt es zu Fehlern. Ein Reviewer geht an ein Dokument, das er auf sensible Inhalte und Geschäftsgeheimnisse hin prüfen muss, gedanklich auch anders heran als ein solches, dass er z.B. nach Fallbezug und Relevanz beurteilen muss.

   - **Arbeitsweise der Reviewer:** Reviewer ist nicht gleich Reviewer. Insbesondere von einem Reviewer in einem *Secrecy Review* wird viel Mitdenken und Ermessen gefordert, da jedenfalls zu Beginn eines solchen Reviews oftmals leider keine sehr präzisen Vorgaben für den Reviewer formuliert werden können. Damit kommen viele Profi-Review-Teams erfahrungsgemäss schwer zurecht, da sie es gewohnt sind, mit sehr genauen Instruktionen zu arbeiten, die möglichst kein Ermessen darüber zulassen, was zu schwärzen ist und was nicht.

   
   Um die Qualitätssicherung und Einhaltung des Schweizer Rechts sicherzustellen, sollte ein *Swiss Secrecy & Privacy Review* normalerweise unter der Anleitung und Aufsicht von **Schweizer Anwälten** oder Juristen stattfinden. Dies schliesst den Einsatz auch ausländischer Review-Teams (ggf. sogar vor Ort in der Schweiz) nicht aus.

6. **Muss der Review in der Schweiz stattfinden?** Diese Frage kann aus dem soeben erwähnten Grund relevant sein, denn wenn der Review nicht in der Schweiz stattfinden muss, kann allenfalls auf günstigere Reviewer im Ausland zurückgegriffen werden oder der Review kann mit einem anderen Review, der allenfalls schon im Ausland stattfindet, kombiniert werden. Der Datenschutz erfordert norma-

lerweise nicht zwingend einen Review in der Schweiz. Im Kern geht es vor allem um das Risiko eines Zugriffs ausländischer Behörden, die im Falle eines Reviews (und damit Datenzugangs) im Ausland nicht mehr abgewehrt werden können. Werden also US-Anwälten die Daten übergeben und erhält ihr Klient eine Herausgabeanordnung eines ausländischen Gerichts oder Behörde, werden diese die Daten typischerweise auch gegen den Willen des Klienten herausgeben – auch ohne vorherige Schwärzung derjenigen Daten, die einer ausländischen Behörde nicht zugänglich gemacht werden dürfen. Das wiederum kann zur Strafbarkeit von Personen in der Schweiz führen, sei es aufgrund der Verletzung des Berufsgeheimnisses oder eines Geschäftsgeheimnisses. Daher kann eine vorherige Schwärzung der Dokumente in der Schweiz angezeigt sein. Im Bereich von Bankkundendaten (*Client Identifying Data*, CID) ist es beispielsweise Standard, dass solche Reviews in der Schweiz durchgeführt werden, d.h. keine CID die Schweiz ungeschwärzt verlassen dürfen, sofern kein *Waiver* vorliegt.

> In gewissen Fällen gibt es auch Zwischenlösungen, so namentlich das *Hosting* der Daten auf einem Server in der Schweiz und unter Kontrolle des Unternehmens in der Schweiz, während die **Anwälte aus dem Ausland nur Fernzugriff** erhalten. Dieser kann ihnen bei Bedarf auch entzogen werden. Eine Beschlagnahmung der Unterlagen ist mit dieser Lösung nur beschränkt möglich. Allerdings ist darauf zu achten, dass die Download-Funktion für Anwälte im Ausland deaktiviert wird.

7. **In welcher Reihenfolge muss der Review stattfinden?** Diese Frage mag auf den ersten Blick banal erscheinen, hat aber erhebliche Kostenfolgen, falls nebst dem *Swiss Secrecy & Privacy Review* auch ein Review zur Selektion von herauszugebenden Dokumenten erfolgen muss. Kann der Review zur Selektion *als erstes* durchgeführt werden, reduziert sich die Zahl der ggf. zu schwärzenden Dokumente massiv, und damit auch die Kosten der Übung. Muss der *Swiss Secrecy & Privacy Review* aus den vorne erwähnten Gründen jedoch in der Schweiz stattfinden, der Review zur Selektion im Ausland, kann dies zu einem Zielkonflikt führt, weil dann zuerst alle, also auch die irrelevanten Dokumente gesichtet werden müssen bevor sie dem ausländischen Review-Team zur Selektion übergeben werden dürfen.

8. **Wie können Berufs- und Geschäftsgeheimnisse Dritter identifiziert werden?** Die Antwort auf die Frage ist entscheidend für die Formulierung des *Redaction Protocols*, das zur Instruktion der *Secrecy Reviewer* dient. Diesbezüglich muss unterschieden werden zwischen:

   - **Berufsgeheimnissen:** Hier wird normalerweise die Schwärzung aller Hinweise auf die Identität der Klienten verlangt, einschliesslich indirekter Hinweise (z.B. über Namen von Mitarbeitern oder beigezogener Berater oder Identifikatoren

wie etwa Bankkontonummern oder anderer nicht nur intern verwendeter Kennnummern).

- **Geschäftsgeheimnissen:** Die Rechtslage erfordert normalerweise nicht, dass jede geheime Information über einen Dritten geschwärzt wird, sondern nur besonders sensible Inhalte. Die Differenzierung ist wichtig, da sonst zu viele Stellen geschwärzt werden. Auch ist eine Abgrenzung zwischen für den Fall relevanten und nicht relevanten Inhalten vorzunehmen. Schliesslich hängt die Pflicht zur Schwärzung auch davon ab, was mit den betroffenen Dritten vereinbart worden ist. Die Formulierung der Regeln, nach welchen geschwärzt werden muss, ist daher nicht abstrakt möglich, sondern ist in der Regel sehr fallspezifisch.

Legal Privilege

Auch in den USA gibt es eine Art *Secrecy Review*, der vor jeder Herausgabe stattfindet: Es werden jene Dokumente herausgenommen oder geschwärzt, die Anwaltsgeheimnisse enthalten. Dieser *Privilege Review* findet jeweils am Ende durch US-Anwälte statt.

In der Praxis zeigt sich, dass die richtigen Personen im Unternehmen meist wissen, zu **welchen Dritten** relevante Geschäftsgeheimnisse in den Unterlagen auftauchen können. Diese Namen können benutzt werden, um entsprechende Dokumente zu finden und wiederum die Instruktionen zur Schwärzung präziser auszuarbeiten. Auch während des Reviews werden in aller Regel Namen, Projektbezeichnungen, etc. auftauchen, die sodann mit dem Unternehmen rasch auf ihre Relevanz abgeklärt werden sollten. Je nach Ergebnis müssen die Instruktionen in der Folge angepasst werden.

9. **Wie können private und andere sensible Daten identifiziert werden?** Die Identifizierung privater Inhalte ist in der Regel sehr viel einfacher als von Geschäftsgeheimnissen, da sie kategoriell vergleichsweise klar umschrieben werden können. Im Einzelfall muss darüber befunden werden, ob beispielweise private Kontaktdaten von Mitarbeitern tatsächlich auch immer geschwärzt werden, oder eine Offenlegung hingenommen wird. Zu berücksichtigen ist auch, dass private Daten, welche die

Im Zweifel …

… schwärzen. So werden Reviewer üblicherweise instruiert, um das Risiko von unerlaubten Offenlegungen zu senken und den Review nicht aufzuhalten. In der Praxis besteht oft keine Zeit, einen Zweifelsfall genau abzuklären. Hier gilt: Es ist einfacher, eine zu weitgehende Schwärzung später anzupassen als umgekehrt.

Mitarbeiter selbst für ein breiteres Publikum offenlegen, nicht zu schwärzen sind (z.B. CVs im Zusammenhang mit Publikations- und Vortragstätigkeiten).

10. **Festlegung der Qualitätskontrolle.** Es geht hier primär um die Frage, von wie vielen Personen ein Dokument angeschaut wird. Das hat direkte Auswirkungen auf den Geld- und Zeitbedarf für einen Review. Im Bereich des Berufsgeheimnisses hat sich das Vier-Augen-Prinzip eingebürgert: Jedes Dokument wird in einem ersten Durchgang geprüft und geschwärzt (1st Level). Anschliessend schaut sich eine andere Person das Dokument und die Schwärzung an, bevor das Dokument finalisiert wird (2nd Level). Für die Schwärzung von privaten und sensiblen Daten wird häufig nur ein vollständiger Durchgang vorgenommen. Die Qualitätskontrolle erfolgt stichprobenweise an einem Sample (Beispiel: Alle geschwärzten Dokumente, in jedem Fall aber 20 Prozent aller Dokumente, zufällig ausgewählt). In der Praxis als sinnvoll erwiesen hat es sich zudem, dass in der Anfangsphase (z.B. die ersten 2‘000 Dokumente) ein Team jedes Dokument zwei Mal anschaut (d.h. jeweils zwei verschiedene Reviewer). Dies führt zu einer steileren Lernkurve der Reviewer und zeigt relativ rasch auf, wo die Anweisungen ggf. justiert werden müssen oder wo sonst Probleme bestehen.

In jedem Review – auch wenn es um Schwärzungen geht – **werden Fehler gemacht**, d.h. es werden zu viele bzw. zu wenig Inhalte geschwärzt. Das gilt selbst dann, wenn nach dem Vier-Augen-Prinzip verfahren wird. Das Recht verlangt keine Fehlerlosigkeit. Wesentlich ist in der Praxis, dass sorgfältige, dem Risiko angemessene Anstrengungen demonstriert werden können. Welche Fehlerrate noch zulässig ist, darüber gibt es jedoch keine Aussagen und auch so gut wie keine Statistiken[58]. Rechtlich besonders heikel sind vor allem Fälle, in denen zu wenig geschwärzt wird. In einem Schweizer Fall, wo es um die Schwärzung von Daten über Bankkunden und Mitarbeiterdaten ging, die nach dem Vier-Augen-Prinzip von Schweizer Juristen durchgeführt wurde, wurden in einer ersten Serie bei 10‘000 Seiten im Rahmen einer Nachprüfung 21 Fehler ermittelt (wobei 20 davon Mitarbeiterdaten betrafen (meist Vornamen, oft in langen Dokumenten oder an Randstellen) und einer betraf einen Bankkunden (ein Teil einer Kontonummer wurde nicht geschwärzt). In einer zweiten Serie kam es bei 2‘800 Seiten zu 12 Fehlern; der Zeitdruck war hier erheblich höher, was zu einer Verdoppelung der Fehlerrate führte. In besonders heiklen Fällen sollte sogar das Sechs-Augen-Prinzip erwogen werden.

58 Ein Fall aus den USA, wo bei Sozialversicherungsnummern eine Fehlerrate von 3% ermittelt wurde: https://bit.ly/3u9Xl9G.

11. **Können zu schwärzende Inhalte automatisch identifiziert werden?** *Swiss Secrecy & Privacy Reviews* sind kostspielig, weshalb ein grosses Interesse daran besteht, sie möglichst effizient auszugestalten. Gespart werden kann einerseits im Rahmen der Qualitätskontrolle (allerdings mit entsprechenden Risiken), andererseits durch eine Automatisierung des Prozesses. Leider ist letzteres in der Praxis nur bis zu einem gewissen Grad möglich. Versprechungen von Service- und *Tool*-Providern, sie könnten private Daten oder Geschäftsgeheimnisse automatisch identifizieren oder sogar schwärzen, sollte grundsätzlich *kein Glaube* geschenkt werden. Automatisch identifizieren und schwärzen können diese Anbieter nur in ihrer Erscheinung präzise definierte Inhalte (z.B. Sozialversicherungsnummern, Kreditkartennummern, IBAN-Nummern, E-Mail-Adressen, vorgegebene Begriffe wie Namen). Dies ist in einem *Swiss Secrecy & Privacy Review* aber nur sehr beschränkt nützlich, weil sie wesentlich breiter sind und auch die indirekte Identifikationen einer Person oder eines Unternehmens abgedeckt sein muss.

> **Stichproben**
>
> Schweizer Banken unterscheiden normalerweise zwischen Schweizer Daten und internationalen Daten. Bankgeheimnisgeschützte Angaben sollten in letzteren Daten an sich nicht vorkommen, tun es aber versehentlich trotzdem immer wieder. Hier hat sich der Einsatz von Stichprobenkontrollen mit Suchbegriffen eingebürgert.

> Sinnvoll kann es sein, **Such- und Filtertechniken** einzusetzen, um den Kreis der zu prüfenden Dokumente einzuschränken. So haben Tests mit geschickt gewählten Suchbegriffen gezeigt, dass sich aus der Gesamtmenge der Dokumente jener Teil der Dokumente aussortieren lässt, der mit hoher Wahrscheinlichkeit keine relevanten Inhalte enthält (und daher gar nicht oder nur von einer statt zwei Personen geprüft werden muss). In den Tests konnte die Population zu prüfender Dokumente halbiert werden. Das Verfahren funktionierte für die Erkennung von privaten und sonstigen sensiblen Inhalten auch fallunabhängig vergleichsweise gut. Im Bereich von Geschäftsgeheimnissen war eine Programmierung für den konkreten Fall erforderlich.

12. **Verfassen eines *„Redaction Protocol“*.** Sind die Eckwerte des *Swiss Secrecy & Privacy Review* festgelegt, müssen diese zu Papier gebracht werden. Das geschieht durch das Verfassen eines entsprechenden → **Redaction Protocol**. Es dient einerseits dem Review-Team (und eDiscovery-Provider, welcher das System betreibt) als Anleitung und Grundlage für die Arbeit, und dokumentiert andererseits für Dritte, was geschwärzt wurde und wie vorgegangen worden ist. Werden einer Behörde nur geschwärzte Unterlagen vorgelegt, wird sie in der Regel wissen wollen, nach welchen Regeln die

Schwärzungen vorgenommen wurden. In diesen Fällen ist es auch wichtig, dass der Review durch einen Dritten durchgeführt wird, da diesem in der Regel mehr Vertrauen geschenkt wird als dem Unternehmen selbst. Im *Redaction Protocol* wird nicht nur geregelt, welche Inhalte zu schwärzen sind (und welche nicht), sondern auch, wie dies praktischerweise geschieht (z.B. in Bezug auf die Qualitätskontrolle).

Bei **Schwärzungen** stellt sich immer die Frage, ob sie **speziell bezeichnet** werden müssen. Technisch ist das überhaupt kein Problem: Jedes schwarze „Kästchen" kann mit einem Text (*Label*) versehen werden. Die Bezeichnung ist vor allem eine Frage des Aufwands, weil dieser deutlich steigt, wenn zusätzlich beschriftet werden muss. Hierbei ist auch zu unterscheiden zwischen einer generischen Bezeichnung (z.B. „P" für Privat, „B" für Business Secret, „CID" für Bankkundendaten) oder ob weitergehende Bezeichnungen nötig sind (z.B. „Client 1", „Employee 3"), weil sonst der Leser des Dokuments seinen Inhalt nicht mehr versteht.

13. **Instruktion der Reviewer.** Eine Instruktion der Reviewer erfolgt wie bei anderen → **DOKUMENTEN-REVIEWS** ebenfalls. Im Unterschied zu Reviews, die relevante Inhalte aufspüren sollen, fokussieren sich in einem *Swiss Secrecy & Privacy Review* die Reviewer aber auf völlig andere Dinge. Das Anbringen von Schwärzungen benötigt zudem wesentlich mehr Zeit als die blosse Sichtung und das *Tagging* eines Dokuments. Werden Geschäftsgeheimnisse gesucht, sollte mit den Reviewern erörtert werden, wie neue Erkenntnisse (z.B. Namen betroffener Drittunternehmen) möglichst rasch zentral abgeklärt und ausgewertet werden können. Besondere Instruktionen können auch für Sonderformate nötig werden, die besondere Techniken für das Schwärzen erforderlich machen, wie z.B. Excel-Tabellen, Audiodokumente oder Chats.

14. **Durchführung des Reviews.** Die Durchführung eines *Swiss Secrecy & Privacy Reviews* ähnelt ebenfalls sehr den herkömmlichen → **DOKUMENTEN-REVIEWS**. So ist es auch hier wichtig, dass sich die Reviewer gegenseitig austauschen können. Hinzu kommt, dass insbesondere bei Geschäftsgeheimnissen bestimmte Dokumente immer wieder zurückgestellt werden müssen, weil das Unternehmen zuerst abklären muss, ob z.B. die Dokumente eines bestimmten Projekts oder Kunden im konkreten Fall offengelegt werden dürfen oder nicht. Müssen in einem Review Schwärzungen vorgenommen werden, braucht dies auch viel mehr Zeit. Während in einem „normalen" Review ein guter Reviewer im Schnitt 400 Dokumente pro Tag (8h)

Metadaten

Nicht zu vergessen sind in einem Review auch Metadaten von Dokumenten, da auch sie sensible Angaben enthalten können. Aus technischen Gründen müssen sie oft separat behandelt werden.

sichten kann, kann die Zahl auf 150 Dokumente pro Tag sinken, wenn auch geschwärzt werden muss. Dies ist nur ein grober Erfahrungswert, denn wenn beispielsweise nur nach privaten Inhalten gesucht werden muss und solche kaum vorkommen, kann ein Review auch sehr schnell gehen, da die meisten Dokumente sofort als rein geschäftlich eingestuft werden können und der Reviewer mit diesen keine Zeit verliert.

15. **Justierung des Reviews.** Auch ein *Swiss Secrecy & Privacy Review* muss erfahrungsgemäss laufend nachjustiert werden. Darum wird das *Redaction Protocol* typischerweise auch laufend angepasst. In der Regel kommen im Laufe eines Reviews zusätzliche Regeln und Anwendungsfälle hinzu, denen die Reviewer im Laufe des Reviews begegnet sind und welche die Review-Leitung zusammen mit dem Unternehmen geklärt hat. Heikel sind jene Fälle, in denen eine Vorgabe im Laufe eines Reviews strenger formuliert wird, d.h. mehr geschwärzt werden muss als ursprünglich vorgesehen. Hier muss das Unternehmen entscheiden, ob ein Teil des Reviews im schlimmsten Fall wiederholt wird (um die strengeren Anforderungen auf bereits gesichtete Dokumente anzuwenden), ob etwaige frühere Vorkommen bestimmter Inhalte gezielt durch ein separates Team gesucht werden oder ob nichts getan wird. Dies sind jeweils Risikoentscheide, da jedes Zurückkommen auf bereits gesichtete Dokumente zwar technisch möglich, aber sehr aufwändig ist.

Das ***Redaction Protocol*** sollte als wichtigstes Arbeitsdokument laufend nachgeführt werden. Da es nicht nur ein wichtiges Instrument der Reviewer ist, sondern auch ihre Arbeit dokumentiert und sie damit nachvollziehbar macht (was rechtlich wichtig sein kann), sollten darin auch alle Erkenntnisse aus dem Review aufgenommen werden, z.B. die Namen der Unternehmen und Projekte, die geschwärzt werden müssen, welche Fehler typischerweise vorkommen und wie sie vermieden werden können und wie mit Grenzfällen umzugehen ist. Allerdings ist darauf zu achten, dass das *Redaction Protocol* selbst ebenfalls geheime Informationen enthalten kann und daher unter Umständen **nicht ungeschwärzt herausgegeben** werden darf.

16. **Produktion.** Mit der Produktion ist die Aufbereitung der geschwärzten Unterlagen zur Herausgabe gemeint. Dies ist ein vor allem technischer Vorgang. Es muss sichergestellt werden, dass die Schwärzungsmarkierungen auch tatsächlich so angebracht werden, dass der abgedeckte Inhalt technisch nicht rekonstruiert werden kann. Dies sollte ein eDiscovery-Provider an sich im Griff haben. Zu achten ist insbesondere darauf, dass die entsprechenden Dokumente nur als Bild- oder PDF-Datei geliefert werden, nicht jedoch in ihrem ursprünglichen Format (*native*), weil dort die ungeschwärzten Inhalte nach wie vor enthalten sind. Auch etwaige OCR-Dateien sind entweder nicht mitzuliefern oder neu zu erstellen – unter Auslassung der geschwärzten Stellen. Dasselbe gilt für die Metadaten, die von den Reviewern

normalerweise nicht selbst geschwärzt werden können, sondern erst im Rahmen der Produktion geschwärzt, bearbeitet oder ganz weggelassen werden müssen. Das ist technisch in der Regel kein Problem, aber es darf nicht vergessen gehen.

Do's	Don'ts
• Bedingen Sie sich für einen *Swiss Secrecy & Privacy Review* genügend Zeit aus. Das gilt insbesondere in ausländischen Behörden und Gerichtsverfahren. Eine *"rolling production"* kann hier eine Lösung sein. • Überlegen Sie sich schon vor dem Review, von welchen Kunden und Geschäftspartnern heikle Informationen enthalten sein könnten, denn wenn der Review erst einmal läuft, können Kurskorrekturen sehr teuer und zeitraubend werden, weil der Review teilweise wiederholt werden muss. • Führen Sie jeden *Swiss Secrecy & Privacy Review* mindestens zu Beginn nach dem Vier-Augen-Prinzip durch, damit das Reviewer-Team ein „Gefühl" für die Dokumente und die Aufgabe bekommt. • Führen Sie das *Redaction Protocol* laufend nach. Es ist ein wichtiges Arbeitsinstrument für die Reviewer und belegt für später, was Sie getan haben, damit dies Behörden und andere Beteiligte nachvollziehen können. Jeder, das Ergebnis beeinflussende Schritt sollte darin dokumentiert sein.	• Übergeben Sie keine Daten an Anwälte oder andere Stellen im Ausland bevor Sie nicht geklärt haben, ob damit gegen Schweizer Geheimhaltungspflichten verstossen wird – dafür können Sie persönlich strafbar gemacht werden. • Vertrauen Sie nicht darauf, dass Schwärzungen automatisiert möglich sind. Die Anbieter übertreiben diesbezüglich mit ihren Versprechungen gerne. • Vergessen Sie nicht die Schwärzung auch der Metadaten der Dokumente, da auch diese sensible Inhalte enthalten können. • Geben Sie das *Redaction Protocol* nicht heraus, bevor Sie es nicht auf geheime Informationen (z.B. geheime Angaben über Projekte oder Geschäftspartner) hin geprüft haben. • Entfernen Sie das Review-Projekt nicht zu früh aus dem System des eDiscovery-Providers, da sie es ggf. brauchen, um bei Beanstandungen die vorgenommenen Schwärzungen zu verifizieren.

Wann Sie externe Unterstützung beiziehen sollten

- Falls Sie einer ausländischen Partei oder **Behörde gegenüber belegen** müssen, dass ein *Swiss Secrecy & Privacy Review* **überhaupt nötig** ist.

- Falls Sie einen **datenschutzkonformen *Protective Order*** mit US-Anwälten verhandeln müssen und Sie damit keine Erfahrung haben.
- Für den **Einsatz eines Review-Systems**, weil die meisten Firmen diese Art von Systemen nicht selbst betreiben, sondern als Dienstleistung beziehen.
- Falls Sie über **keine internen Ressourcen** zur Durchführung des Reviews verfügen und zum Beispiel günstige Reviewer benötigen.
- Falls Sie neben Ihrem Review-Provider eine unabhängige Stelle **für die Qualitätssicherung** benötigen.
- Für das Verfassen eines ***Redaction Protocols***, falls Sie so etwas noch nie gemacht haben.
- Falls Sie sich **unsicher** sind (z.B. ob bestimmte Inhalte im konkreten Fall offengelegt werden dürfen oder nicht).

Häufige Fragen und Antworten

Q63. Kümmert es US-Behörden und -Gerichte überhaupt, ob das Schweizer Recht eingehalten wird?

A: Ja, das tut es erfahrungsgemäss schon, soweit sie überzeugt sind, dass die Verletzung Schweizer Rechts **nicht nur Vorwand** für die Nichtlieferung von Dokumenten ist und dies tatsächlich rechtliche Konsequenzen für die betroffenen Unternehmen oder Entscheidungsträger haben kann, insbesondere strafrechtlicher Natur. Es liegt am Unternehmen, die Notwendigkeit von Schwärzungen (und eines angepassten *Protective Order*) mit dem nötigen Nachdruck darzulegen, nötigenfalls auch mit einem entsprechenden **Kurzgutachten eines Rechtsexperten**.

Das Unternehmen muss jedoch damit rechnen, dass es einige Gegenwehr geben kann, weil es zunächst immer unter Verdacht stehen wird, dass die Schwärzungen in Tat und Wahrheit der Verschleierung in der Sache dient und nicht dem legitimen Schutz von Drittrechten. Auch die durch einen *Swiss Secrecy & Privacy Review* verursachte **Verzögerung** wird regelmässig für Unmut sorgen.

Q64. Wie wird in der Praxis mit dem Problem zu weitgehender Schwärzungen umgegangen?

A: Sie kommen naturgemäss immer vor, da regelmässig mit der Grundanweisung gearbeitet wird, dass im Zweifel zu viel als zu wenig geschwärzt werden soll. Auch aus Zeitgründen werden Reviewer häufig jeweils ganze Absätze schwärzen statt zu versuchen, nur einzelne Satzteile abzudecken. In der Praxis ist diese Konsequenz **weitgehend akzeptiert**, aber das Unternehmen muss damit rechnen, dass die Gegenseite im Falle von wichtigen Dokumenten bestimmte Schwärzungen anzweifeln und eine erneute Prüfung der Notwendigkeit verlangen wird. Dank den modernen Review-Systemen ist dies auch sehr leicht zu bewerk-

stelligen. Stellt sich heraus, dass eine Schwärzung zu weit ging, erfolgt **eine *de-redaction***, d.h. die Schwärzung wird aufgehoben und das betreffende Dokument erneut produziert.

Q65. Wir sind aufgefordert, einer Schweizer Behörde Unterlagen mit Angaben zu unseren Mitarbeitern und Kunden zu liefern. Müssen wir hier auch Schwärzungen vornehmen?

A: Nein, normalerweise nicht, jedenfalls wenn die Behörde die Herausgabe der Unterlagen befielt (d.h. im Rahmen einer Editionsanweisung). Die Unterlagen sind herauszugeben, wie sie sind, d.h. ohne Schwärzungen – jedenfalls soweit kein Zeugnisverweigerungsrecht besteht (z.B. im Falle von Anwaltskorrespondenz).

Trotzdem kann die Vornahme von Schwärzungen angezeigt sein, wenn die Unterlagen sensible Inhalte enthalten, die **für das jeweilige Verfahren nicht relevant** sind. Daran wird sich die auffordernde Behörde in der Regel auch nicht stören, wenn ihr dies entsprechend mitgeteilt wird. Dies kann auch ihre eigene Arbeit erleichtern, wenn dadurch die Offenlegung gegenüber Dritten z.B. im Rahmen einer **Akteneinsicht** vereinfacht wird (sie muss sich dann ggf. nicht mehr selbst um die Wahrung von Geschäftsgeheimnissen kümmern). Insbesondere in der Praxis der Amtshilfe hat sich gezeigt, dass Schweizer Behörden selbst mitunter zu wenig unternehmen, um betroffene Personen zu schützen, obwohl sie dazu an sich gesetzlich verpflichtet wären. Teilweise werden die Unternehmen kurzerhand aufgefordert, selbst (und vor allem auf eigene Kosten) für die nötigen **Schwärzungen der Personendaten ihrer Mitarbeiter** oder anderen betroffenen, aber nicht relevanten Personen zu sorgen.

> **Literatur:**
>
> Opel, Andrea: Schutz von Bankmitarbeiterdaten in Amtshilfeverfahren, in: Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht (SZW) 2020, S. 593 ff.
>
> Opel, Andrea: Lieferung von Bankmitarbeiterdaten an ausländische Steuerbehörden – wenn Amtshilfe ausartet, Beiträge zur Schweizerischen Bankrechtstagung, in: Emmenegger, Susan (Hrsg.), Banken und Datenschutz, Basel 2019, S. 77 ff.

Q66. Müssen wir unsere Mitarbeiter oder Kunden informieren, wenn wir geschwärzte Unterlagen liefern?

A: Aus rechtlicher Sicht ist dies grundsätzlich **nicht erforderlich**, jedenfalls solange die betroffenen Personen nicht identifiziert werden können. Es liegen dann keine Personendaten mehr vor, weshalb auch der Datenschutz nicht mehr greift. Es ist jedoch zu beachten, dass die Bearbeitung der Personendaten **im Rahmen des Reviews** bereits eine Informationspflicht auslösen kann. Immerhin erhalten auch hierbei Dritte (das Review-Team) möglicherweise Einblick in private oder sonst persönliche Daten von Mitarbeitern, auch wenn dies letztlich zu ihrem Schutz erfolgt.

Gedanken zum Thema.

Wenn ein Unternehmen – wie zum Beispiel eine Bank – unter Druck ausländischer Behörden gerät, gilt es sehr sorgfältig den Schutz der Mitarbeiterinnen und Mitarbeiter zu beachten. Die Fürsorgepflicht des Arbeitgebers gegenüber den Mitarbeitenden hat in solchen Situationen eine besondere Bedeutung, vor allem wenn durch die Herausgabe von Daten für die Mitarbeitenden im Ausland die Gefahr einer Strafverfolgung oder von Administrativ-massnahmen besteht. Gegenüber den exponierten Mitarbeitenden muss das Unternehmen in einer solchen Situation nicht nur vollständig transparent sein, sondern ihnen auch das Recht geben, die Herausgabe ihrer Personendaten zu verweigern. Will es das nicht, muss es die Daten eben schwärzen.

Michael von Felten
Präsident Schweizerischer Bankpersonalverband

15. Organisationen

Kurz gesagt

- In der Schweiz gibt es mehrere Organisationen, in welchen sich Vertreter von Unternehmen über ihre Erfahrungen im Bereich interne Untersuchungen und eDiscovery austauschen.
- Schwergewichtig sprechen sie Fachpersonen im Bereich Compliance an. Es gibt jedoch auch einen international tätigen Verein spezifisch für den Bereich eDiscovery und internationale Untersuchungen.
- Die Weitergabe von Know-how erfolgt vor allem im Rahmen von Veranstaltungen für die Mitglieder.

Worum es geht

Das Instrument der internen Untersuchung ist bisher nur ansatzweise wissenschaftlich aufgearbeitet worden. Auch die gerichtliche Beurteilung hält sich in Grenzen. Entwickelt wird das Gebiet vor allem durch die praktische Umsetzung im Unternehmensalltag und der Erfahrung, welche die beteiligten Stellen – Kanzleien, Berater, Provider, Behörden – dabei machen. Umso wichtiger ist es für Unternehmen ein Gefühl dafür zu bekommen, wie andere die Herausforderungen interner Untersuchungen handhaben und zu verstehen, was in diesem Bereich eine „gute Praxis" ist. Diese können neben erfahrenen Beratern vor allem Fachorganisationen liefern, in welchen sich Fachkreise über die hier relevanten Themen austauschen.

Worauf zu achten ist

- **Cross-border eDiscovery, Privacy & Investigations Association** (**CeDIV**):* Ein 2015 in der Schweiz von UBS, Novartis, Holcim, Zürich Versicherungen und SwissRe gegründeter Verein, der sich dem nationalen und internationalen Erfahrungsaustausch zu eDiscovery und internen Untersuchungen verschrieben hat, mit besonderem Fokus auf grenzüberschreitende Sachverhalte. Er bietet regelmässig Veranstaltungen zum Thema an, an welchem ein geführter Wissensaustausch erfolgt. *Infos: www.cediv.org*
- **Swiss Association of Compliance Officers** (**SACO**): Ein 1998 gegründeter Fachverein für Compliance-Verantwortliche aus der Finanzindustrie der Schweiz und des Fürstentums Liechtenstein, jedoch keine Berater. Der Fachverein organisiert in der Regel zwei Mal jährlich einen vorwiegend seinen Mitgliedern vorbehaltener Weiterbildungsanlass. Die Mitglieder treffen sich ferner vier bis sechs Mal im Jahr in kleinen Gruppen (*"Baskets"*) zum Erfahrungsaustausch. *Infos: www.complianceofficers.ch*

- **Ethics and Compliance Switzerland** (**ECS**): Ein 2014 in der Schweiz gegründeter Verein von Ethik- und Compliance-Officern, der diese Themengebiete in Schweizer Betrieben der privaten und der öffentlichen Hand fördern will. Seine Mitglieder umfassen einerseits über ein Dutzend Unternehmen und den Nachrichtendienst des Bundes sowie Individualmitglieder. Diese treffen sich regelmässig für interne Weiterbildungsanlässe und zum Austausch über *Best Practices* im Bereich Ethik und Compliance. Hierzu hat ECS acht Arbeitsgruppen, die teilweise auch eigene Papiere publizieren. Die Anlässe sind für Mitglieder kostenlos; Interessenten können einmalig an einem Anlass teilnehmen. *Infos: www.ethics-compliance.ch*
- **SwissHoldings**, der Verband der multinationalen Industrie- und Dienstleistungskonzerne: Mitgliedsfirmen sind rund 60 multinationale Dienstleistungs- und Industriekonzerne der Schweiz (Mitglieder: *www.swissholdings.ch/mitglieder*). Der Verband engagiert sich für optimale Rahmenbedingungen für die multinationalen Konzerne mit Sitz in der Schweiz und organisiert Referate und fachliche Diskussionen für und unter den Mitgliedfirmen zu für diese relevanten Themen. Der Verband ist in Fachgruppen und Arbeitsgruppen organisiert. Im vorliegenden Zusammenhang im Vordergrund stehen die Compliance-Gruppe sowie die Datenschutz-Gruppe, in welchen (je nach Thematik der Gruppe) die Compliance-verantwortlichen Personen, General Counsel, Legal Counsel und Datenschutz-verantwortlichen Personen der Mitgliedfirmen vertreten sind. *Infos: www.swissholdings.ch*
- **Verein Unternehmens-Datenschutz** (**VUD**):* Ein 2006 in der Schweiz gegründeter Verein von Unternehmensdatenschützern vieler KMUs und grossen internationalen Schweizer Unternehmen, in welchem sich diese hinter geschlossenen Türen über die praktische Umsetzung des Datenschutzes in der Schweiz austauschen. *Infos: www.vud.ch*

* Offenlegung: David Rosenthal ist Sekretär beider Organisationen.

16. Glossar

Das nachstehende Glossar bietet einen Überblick über wesentliche Begrifflichkeiten, auf die im Text nicht oder nicht überall näher eingegangen wird und dient dadurch dem besseren Verständnis. Die Begriffe sind im Text in der Regel bei erstmaligem Vorkommen im jeweiligen Bereich → **hervorgehoben**:

Ad-hoc-Bekanntgabepflicht	Die Ad-hoc-Bekanntgabepflicht schreibt börsenkotierten Unternehmen die Veröffentlichung neuer und dem Kapitalmarkt unbekannter, aber potenziell kursrelevanter Tatsachen vor. Das Unternehmen hat, sobald die kursrelevante Tatsache in ihren Grundzügen bekannt ist, sofort die Öffentlichkeit zu informieren. Ein Aufschub der Meldung kann möglich sein, wenn die kursrelevante Tatsache auf einem Plan oder einem Entschluss des Unternehmens beruht und die strikte Geheimhaltung während des Bekanntgabeaufschubs gewährleistet und der Insiderhandel ausgeschlossen werden kann.
ADV	→ **Auftragsbearbeitungsvertrag**
ArGV 3	Verordnung 3 zum Arbeitsgesetz (Gesundheitsschutz) vom 18. August 1993 (SR 822.113)
Audit Committee	Zu Deutsch „Prüfungsausschuss". Unter schweizerischem Recht kann der Verwaltungsrat einer Aktiengesellschaft ein Audit Committee als neutrale Instanz zur Kontrolle der internen Revision (internes Kontrollsystem) und der externen Revision (Revisionsstelle) schaffen. Dieses setzt sich in der Regel aus nicht-exekutiven und unabhängigen Mitgliedern des Verwaltungsrates zusammen. Die Mehrheit der Mitglieder des Audit Committee ist idealerweise im Finanz- und Rechnungswesen erfahren. Eine eigentliche Pflicht zur Schaffung eines Audit Committee besteht nicht, jedoch empfiehlt der *Swiss Code of Best Practice* unter dem Gesichtspunkt der → **Corporate Governance** gerade für Publikumsgesellschaften die Einrichtung eines Audit Committee. Dadurch kann bei bedeutsamen Publikumsgesellschaften das Vertrauen in das Unternehmen geweckt werden.
Auftragsbearbeiter	Die natürliche oder juristische Person/Behörde/Agentur oder andere Stelle, die Personendaten im Auftrag eines → **Verantwortlichen** bearbeitet (d.h. unter der Autorität eines Verantwortlichen handelt und den Interessen des Verantwortlichen dient). Ein Auftragsbearbeiter kann ein externer Dienstleister

	sein (z.B. ein Cloud-Anbieter, ein Anbieter von Gehaltsabrechnungen usw.), aber ebenso ein anderes Konzernunternehmen (z.B. ein Konzernunternehmen, welches das HR- oder → **CRM-System** des Konzerns betreibt). Einen Auftragsbearbeiter zu beauftragen bedeutet im Wesentlichen, Teile einer eigenen Bearbeitungstätigkeit an den Auftragsbearbeiter auszulagern (oder zu delegieren). Dies ist grundsätzlich ohne Einholung einer Einwilligung der betroffenen Person zulässig, muss aber unter Einhaltung bestimmter Anforderungen erfolgen, zu denen gemäss revidiertem Datenschutzgesetz auch das Vorhandensein eines ordnungsgemässen → **Auftragsbearbeitungsvertrages** sein wird. Der Verantwortliche bleibt für die Handlungen und Unterlassungen des Auftragsbearbeiters verantwortlich, aber auch der Auftragsbearbeiter ist verantwortlich (z.B. für mangelnde Datensicherheit), insbesondere, wenn er die Anweisungen des Verantwortlichen nicht befolgt. Im Falle der Nichteinhaltung können Verantwortliche und Auftragsbearbeiter mit Geldbussen belegt werden.
Auftragsbearbeitungsvertrag (ADV)	Ein verbindlicher Vertrag zwischen einem → **Verantwortlichen** und einem → **Auftragsbearbeiter** über die Bearbeitung von Personendaten, die der Verantwortliche an den Auftragsbearbeiter delegiert hat. Unter dem revidierten DSG müssen Verantwortliche schriftliche ADVs mit allen Parteien haben, die als Datenbearbeiter in ihrem Namen handeln (z.B. Cloud-Service, Gehaltsabrechnungsdienst, etc.). Sie müssen bestimmten gesetzlichen Anforderungen genügen. Unter der → **DSGVO** bestehen vergleichbare Voraussetzungen.
Auskunftsrecht	Der datenschutzrechtliche Anspruch einer → **betroffenen Person**, Einblick (und eine Kopie) ihrer → **Personendaten** zu verlangen, um auf diese Weise feststellen zu können, ob ihre Personendaten rechtmässig bearbeitet werden. Nebst den Personendaten können noch eine Reihe weiterer Angaben verlangt werden. Das Datenschutzgesetz sieht allerdings auch Möglichkeiten zur Einschränkung des Auskunftsrechts vor. Vgl. dazu → **Q57** und → **DSAR-REVIEWS**.
Bearbeiten (von Personendaten)	Bezeichnet jeden Vorgang, der mit → **Personendaten** durchgeführt wird (z.B. Erheben, Erfassen, Ordnen, Strukturieren, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreiten oder sonstiges Zugänglichmachen, Abgleichen oder Zusammenführen,

	Einschränken, Löschen oder Vernichten). Auch das blosse Aufbewahren von Personendaten, ohne sie zu „nutzen", ist also eine Bearbeitung und unterliegt damit grundsätzlich dem Datenschutzrecht. Die Bearbeitung bezieht sich auf jeden einzelnen Vorgang mit Personendaten. Um eine Menge von Bearbeitungsvorgängen zu bezeichnen, die alle zusammengehören, weil sie demselben Zweck dienen, wird oft der Begriff „Bearbeitungstätigkeit" verwendet. Das Gesetz verpflichtet Verantwortliche und Auftragsbearbeiter dazu, eine Übersicht über ihre Datenbearbeitungstätigkeiten zu erstellen.
Beschaffung (von Personendaten)	Ist oft der erste Schritt in der Datenbearbeitung. Zum Zeitpunkt der Erhebung oder Beschaffung von Personendaten muss der Verantwortliche die betroffene Person über die Erhebung und Verwendung ihrer Personendaten informieren. Dies vorausgeschickt, dürfen Personendaten nur für festgelegte, eindeutige und rechtmässige Zwecke erhoben werden. Wenn Personendaten zur Erfüllung dieses Zwecks nicht mehr erforderlich sind, müssen sie vom Verantwortlichen gelöscht werden. Der Begriff „Beschaffung" umfasst nur Fälle, in denen der Verantwortliche Personendaten in geplanter Weise erhebt, d.h. wenn eine bestimmte Absicht besteht, Personendaten zu erheben. Er umfasst nicht die Fälle, in denen der Verantwortliche Personaldaten zufällig erhält.
Besonders schützenswerte Personendaten	Dabei handelt es um bestimmte Kategorien von Personendaten, die datenschutzrechtlich mit erhöhtem Schutz zu behandeln sind, weil sie jeweils als besonders schützenswert gelten (sprich: das DSG sieht für diese Daten zusätzliche Regeln vor). Gesundheitsdaten sind ein Beispiel für solche Daten. Darunter fallen ebenso Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten. Ferner Daten über die Intimsphäre oder die Rassenzugehörigkeit, über Massnahmen der sozialen Hilfe. Auch werden mit dem Begriff Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen erfasst. Im Gegensatz dazu fallen Finanzdaten nicht in diese besonderen Kategorien, da die Definition dessen, was „sensibel" ist, abschliessend ist (dies bedeutet jedoch nicht, dass solche anderen „nicht-sensiblen" Daten mit weniger Sorgfalt behandelt werden können: Unter einem risikobasierten Ansatz müssen sie dennoch im Hinblick auf ihre Sensibilität behandelt werden). Die Weitergabe solcher Daten

	an einen anderen Verantwortlichen bedarf einer ausreichenden Rechtfertigung. Unter der DSGVO ist bei dieser Art von Daten von „besonderen Kategorien" von Personendaten die Rede; die Definition ist unter der DSGVO eine ganz leicht andere.
Betroffene Person	Die Bezeichnung derjenigen Person, auf die sich Personendaten beziehen, d.h. die identifizierbar in einem Dokument oder in Daten vorkommt, und die im Datenschutzrecht geschützt wird. Im geltenden Datenschutzgesetz kann dies eine natürliche wie auch eine juristische Person sein. Im revidierten Datenschutzgesetz sind nur noch natürliche Personen geschützt (z.B. Mitarbeiter, Mitarbeiter von anderen Unternehmen).
BGFA	Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte vom 23. Juni 2000 (SR 935.61)
Boolean Search	Eine Methode, um in Dokumenten nach einer Kombination von Suchbegriffen zu suchen, wobei die Suchbegriffe in einer bestimmten Logik miteinander verknüpft sind. Diese wird durch die Verwendung von Operatoren wie *„AND"*, *„OR"* oder *„NOT"* gebildet. So können komplexere Suchabfragen formuliert werden als bloss mit einzelnen Worten oder Sätzen. Der Suchbegriff „Sonne *AND* Schnee" findet z.B. nur Texte, in denen beide Wörter vorkommen. Jedes → **Review-System** unterstützt die *Boolean Search*. Mehr dazu: → **WERKZEUGE FÜR EDISCOVERY**.
Bring-Your-Own-Device (BYOD)	Bedeutet „Bringen Sie Ihr eigenes Gerät". Darunter verstanden wird die geschäftliche Nutzung eines privaten Gerätes (Laptop, Smartphone, Tablet, etc.), welches vom Mitarbeiter mit eigenen Mitteln erworben wurde. Das Gerät steht im Eigentum des Mitarbeiters, wird von ihm administriert und organisiert, ist jedoch in das System und die Infrastruktur des Arbeitgebers eingebunden (z.B. geschäftliche E-Mails auf dem privaten Handy).
BYOD	→ **Bring-Your-Own-Device**
Code of Conduct	Unternehmensinternes Regelwerk, welches die Verhaltensgrundsätze, Pflichten und Wertvorstellungen des Unternehmens definiert. Der *Code of Conduct* definiert in zentraler Weise die Unternehmenskultur. Durch Integration in den Arbeitsvertrag kann der *Code of Conduct* rechtsverbindlich das erwartete Verhalten des Mitarbeiters vorschreiben. Dies geschieht oft in sehr allgemeiner Weise und wird in der Folge durch spezifischere Weisungen ausgeführt.

Coding Panel	Der Teil der Benutzerschnittstelle eines → **Review-Systems**, in welchem der Reviewer auswählen kann, welche → **Tags** er für ein Dokument setzt und wo er etwaige Kommentare verfassen kann. Über die Definition des *Coding-Panels* wird im Ergebnis definiert, welche Möglichkeiten zur Klassifizierung (→ **Tagging**) der Reviewer hat.
Compliance	Compliance bedeutet Regeltreue bzw. Regelkonformität. Darunter wird die Einhaltung von unternehmensexternen Vorgaben (Gesetze, Selbstregulierungen, Standesregeln) sowie unternehmensinternen Vorgaben (interne Weisungen und Richtlinien) verstanden.
Concept Search	Eine Alternative zur → **Boolean Search**, um Dokumente zu finden, in welcher mutmasslich bestimmte Themen behandelt werden. Der Computer findet dabei Dokumente, die über ähnliche Wörter und Kombinationen derselbigen verfügen wie das Musterdokument, das als Ausgangspunkt dient. Den Inhalt der Dokumente versteht der Computer allerdings nicht. Ein modernes → **Review-System** sollte die *Concept Search* kennen. Mehr dazu: → **WERKZEUGE FÜR EDISCOVERY**.
Corporate Governance	Unter *Corporate Governance* in einem engeren Sinne werden die Grundsätze zum Schutz von Unternehmenseigentümern, in der Regel der Aktionäre, verstanden. Darunter fallen die Grundsätze der Transparenz in der Rechnungslegung, sowie der Kontrolle der Unternehmensführung im Hinblick auf eine ausgewogene Gewaltenteilung (*"checks and balances"*). In einem weiteren Sinne wird *Corporate Governance* als sämtliche Regelungen und Grundsätze eines Unternehmens verstanden, welche alle Anspruchsgruppen (z.B. Arbeitnehmer, Kunden, etc.) umfasst. Unter eine gute *Corporate Governance* fallen mitunter auch eine funktionierende Compliance sowie ein gut ausgestaltetes internes Kontrollsystem (IKS). Der *Swiss Code of Best Practice for Corporate Governance* (2002) der economiesuisse beinhaltet nicht verbindliche Empfehlungen für Unternehmen zur Ausgestaltung ihrer *Corporate Governance* und kann unter folgendem Link kostenfrei heruntergeladen werden: https://www.economiesuisse.ch/de/publikationen/swiss-code-best-practice-corporate-governance

CRM-System	Die Abkürzung steht für *„Client-Relationship-Management"*-System. Mithilfe eines CRM-Systems werden in einem Unternehmen Kundendaten im Hinblick auf Verkaufs- und Marketingaktivitäten gesammelt und verwaltet. Ein bekannter Anbieter solcher Lösungen ist Salesforce.com.
Custodian	So wird diejenige Person bezeichnet, die eine für die Untersuchung relevante Datenquelle hat, also der Inhaber eines E-Mail-Postfachs oder der Mitarbeiter, der bestimmte Unterlagen auf seinem Notebook oder in seinem Büroschrank hat. Die deutsche Übersetzung „Verwahrer" wird kaum gebraucht.
Data Breach	Zu Deutsch „Verletzung der Datensicherheit". Ungeplanter Datensicherheitsvorfall, der zu einer Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität von Personendaten führt (z.B. eine Datenbank mit Personaldaten wird gehackt, eine E-Mail mit Personendaten wird an den falschen Empfänger gesendet, Personendaten gehen durch eine technische Störung verloren und können nicht wiederhergestellt werden usw.). Mit dem revidierten Datenschutzgesetz werden in der Schweiz Meldepflichten im Zusammenhang mit solchen Vorfällen eingeführt: bei einem „hohen Risiko" negativer Folgen für Betroffene (d.h. konkrete, nicht theoretische Gefahr) hat eine Meldung an den EDÖB zu erfolgen. Ist es zum Schutz der betroffenen Person notwendig (z.B. zur Änderung des Passwortes) wird auch diese informiert werden müssen. Vgl. dazu → **DATA BREACH REVIEWS**. Auftragsbearbeiter müssen einen *Data Breach* an den Verantwortlichen melden, unabhängig von dem Risiko, das durch den *Data Breach* verursacht wurde. Die DSGVO kennt bereits seit 2018 ähnliche Meldepflichten.
Datenexport	Der Begriff umfasst jede Bekanntgabe von Personendaten an einen Empfänger in einem anderen Land. Dabei ist es unerheblich, ob die Daten an den Empfänger im Ausland übermittelt werden oder lediglich ein Fernzugriff erfolgt. Es ist auch nicht relevant, ob der Empfänger innerhalb der gleichen juristischen Person oder bei einem Dritten ist. Die Mitnahme von Personendaten auf eine Reise ins Ausland fällt nicht unter den Begriff, solange sie nicht mit jemandem im Ausland geteilt werden. Auch die Veröffentlichung von Personendaten auf einer Website gilt nicht als Export. Die grenzüberschreitende Übermittlung von Daten (z.B. Versenden einer E-Mail mit Personendaten an einen Empfänger im Ausland, Gewährung des Zugangs zu einem

	Server mit Personendaten usw.) in Länder mit angemessenem Datenschutz (alle Länder in Europa sowie einige weitere, nicht aber die USA) bedarf keiner besonderen Massnahmen. Werden Daten in ein Land exportiert, für das kein angemessenes Datenschutzniveau besteht, verpflichtet das DSG den Exporteur, entweder Massnahmen zu ergreifen, die sicherstellen, dass die Personendaten geschützt bleiben (z.B. Unterzeichnung der → **Standardvertragsklauseln** durch beide Vertragsparteien), oder eine ausreichende Rechtfertigung für den Export ohne solche Garantien zu haben (z.B. ein ausländisches Gerichtsverfahren oder die Einwilligung der betroffenen Person).
Datensammlung	Bezeichnet einen Bestand von Personendaten. Dieser Bestand bezieht sich auf eine Mehrzahl von Personen und ist so aufgebaut, dass die betroffenen Personen erschliessbar sind (d.h. es kann ohne unverhältnismässigem Aufwand herausgefunden werden, ob eine Person in der Datensammlung verzeichnet ist). Die für einen Review gesammelten E-Mails und sonstigen Dokumente stellen regelmässig eine Datensammlung dar.
Datenschutzgesetz	Ein Schweizer Gesetz, das sich mit dem Datenschutz befasst und dabei ähnliche Grundsätze wie die DSGVO anwendet, und das – im Prinzip – für jede Bearbeitung von Personendaten in der Schweiz oder mit einem Schweizer Bezug (z.B. eine in der Schweiz betroffene Person) gilt. Es deckt sowohl den privaten als auch den öffentlichen Sektor (des Bundes) ab. Das revidierte DSG (revDSG) wird voraussichtlich im Jahr 2022 in Kraft treten.
Deduplizierung	Ein Vorgang, bei welchem ein → **Review-System** alle identischen Dokumente konsolidiert, so dass sie nur noch ein Mal im System vorkommen. Das bringt für einen Review einen erheblichen Effizienzgewinn mit sich: Werden die Postfächer von drei Personen gesammelt, die miteinander gemailt haben, so wird das E-Mail das A and B und C gesendet hat, zwar drei Mal ins System eingelesen (nämlich aus dem Postfach von A, B und C), muss aber nur ein Mal angeschaut werden. Mehr dazu: → **WERKZEUGE FÜR EDISCOVERY**.
Deferred Prosecution Agreement (DPA)	Darunter zu verstehen ist eine Vereinbarung zwischen Strafverfolgungsbehörden und einer tatverdächtigen Person bzw. einem Unternehmen über den Aufschub einer Anklageerhebung bis zur Erfüllung von definierten Auflagen. Solche DPAs sind in zahlreichen Rechtsordnungen vorgesehen (z.B. USA,

	Grossbritannien, Frankreich, Kanada, Japan). Die Auflagen beinhalten häufig die Zahlung einer bestimmten Summe und die Vornahme von Massnahmen, mit welchen eine Wiederholung der zur Diskussion stehenden Delikte verhindert werden soll. In der Praxis ist es eine Art Vergleich des jeweiligen Unternehmens mit der Strafverfolgungsbehörde, um eine Anklage und Verurteilung jedenfalls des Unternehmens (nicht aber der Mitarbeiter) zu verhindern.
DeNISTing	Ein Vorgang, bei welchem ein → **Review-System** alle Dateien aussortiert, die höchstwahrscheinlich keinen Beweiswert haben, weil es sich z.B. um bekannte Softwareprogramme oder Teile davon handelt. Der Begriff leitet sich aus „NIST" ab, was für *National Institute of Standards and Technology* steht. Es handelt sich hierbei um eine US-Behörde welche mehrmals jährlich eine Datenbank mit den entsprechenden Signaturen publiziert (https://bit.ly/2QbgJEK). Etwas weniger hochstehende Systeme sortieren mutmasslich irrelevante Dateien anhand des Dateityps aus (z.B. „.exe", „.com", „.dll"). Mehr dazu: → **WERKZEUGE FÜR EDISCOVERY**.
DPA	→ **Deferred Prosecution Agreement** oder → **Auftragsbearbeitungsvertrag** (Data Processing Agreement)
DSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992 (SR 235.1)
DSGVO	→ **EU-Datenschutz-Grundverordnung**
Due Diligence	Unter Due Diligence wird eine „gründliche Prüfung" verstanden. Eine Due Diligence wird als Beispiel durchgeführt bevor eine Geschäftsbeziehung mit einem potenziellen Geschäftspartner eingegangen wird. Die Gegenseite wird „durchleuchtet".
eDiscovery	Der Begriff meint das Identifizieren, Einsammeln, Aufbereiten und Bereitstellen von elektronischen Unterlagen und anderen Daten zwecks Übergabe an einen Dritten im Rahmen eines Rechtsverfahrens. Der Dritte kann eine Gegenpartei, aber auch eine Behörde sein, die für eine Untersuchung Unterlagen eines Unternehmens haben möchte. Der Begriff hat seinen Ursprung in den USA, wo *„Discovery"* eine vorprozessuale Phase in einem Zivilrechtsstreit beschreibt, in welcher die Parteien mögliche Beweismittel zum Prozessthema austauschen. Der Begriff wird heute sehr breit verstanden und wird heute auch verwendet,

	wenn es um das Zusammentragen von elektronischen Unterlagen und Daten für eine rein interne Untersuchung geht. Es kommen hierzu regelmässig unterschiedlichste → **WERKZEUGE FÜR EDISCOVERY** zum Einsatz.
EDÖB	Der EDÖB ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB). Ihm kommen im Bereich des Datenschutzes unterschiedliche Aufgaben zu, z.B. die Beaufsichtigung der Datenbearbeitung von Unternehmen und privaten Personen sowie der Bundesverwaltung und bundesnahen Betriebe (SBB, Post, Swisscom). Der EDÖB sensibilisiert und informiert die Öffentlichkeit im Zusammenhang mit dem Datenschutz, führt aber auch Abklärungen bei Hinweisen auf einen Verstoss gegen das DSG durch. In der Schweiz hat er keine Kompetenz zum Ausfällen von Sanktionen, auch nicht unter dem revidierten Datenschutzgesetz. Er wird unter diesem allerdings gegen nach seiner Ansicht unzulässige Datenbearbeitungen vorgehen können.
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)	→ **EDÖB**
E-Mail-Threading	Ein Vorgang, bei welchem ein → **Review-System** die E-Mails ein- und desselben Diskussionsverlaufs (“*Thread*“) konsolidiert darstellt. Dabei werden die in den E-Mail-Ketten redundanten Wiederholungen bzw. Wiedergaben früherer E-Mails entfernt und so die sichtende Textmenge deutlich reduziert. Mehr dazu: → **WERKZEUGE FÜR EDISCOVERY**.
ERP-System	Die Abkürzung steht für *„Enterprise-Ressource-Planing“*-System. Mithilfe eines ERP-Systems werden unternehmerische Ressourcen wie Kapital, Personal, Betriebsmittel, Material und IT für das Unternehmen bedarfsgerecht verwaltet, geplant und gesteuert. Bekannte Anbieter solcher Lösungen sind SAP, Oracle, Sage und Microsoft.
EU-Datenschutz-Grundverordnung (DSGVO)	Eine EU-Verordnung, die die Regeln für die Bearbeitung von Personendaten durch die meisten privaten und öffentlichen Datenbearbeiter in der EU/EWR vereinheitlicht. Als Verordnung gilt sie automatisch und einheitlich für alle EWR-Mitgliedstaaten. Sie kann auch für Verantwortliche und Auftragsbearbeiter

	ausserhalb des EWR gelten (extraterritoriale Anwendbarkeit), wenn Datensubjekte innerhalb des EWR mittels entsprechender technischer Werkzeuge in ihrem Verhalten beobachtet werden oder wenn Produkte oder Dienstleistungen aktiv an Betroffene im EWR angeboten werden (B2C, nicht B2B). Die blosse Erreichbarkeit einer Website aus dem EWR reicht nicht aus, damit die DSGVO Anwendung findet, ebensowenig die blosse Beschäftigung von Mitarbeitern aus dem EWR durch ein Unternehmen in der Schweiz. Die DSGVO sieht bestimmte Grundsätze für die Bearbeitung von Personendaten, Rechte für betroffene Personen und eine Reihe von Governance-Vorschriften vor. Ein Verstoss gegen die DSGVO kann zu hohen Bussgeldern für Unternehmen führen. Sie wird von Aufsichtsbehörden in jedem EWR-Mitgliedsstaat durchgesetzt. Der Text ist hier zu finden: https://dsgvo-gesetz.de/
EuGH	Das höchste Gericht der EU in Fragen des EU-Rechts. Zusammen mit dem Gericht der Europäischen Union bildet er das Gerichtssystem der Europäischen Union. Der EuGH hat die Aufgabe, das EU-Recht auszulegen und seine einheitliche Anwendung in allen EU-Mitgliedstaaten zu gewährleisten. Er entscheidet über Vorabentscheidungsanträge, Nichtigkeitsklagen und Rechtsmittel der nationalen Gerichte. Das heisst, der EuGH entscheidet nicht über nationale Fälle, Allerdings können nationale Gerichte dem EuGH Fragen des EU-Rechts vorlegen. Der EuGH ist für Datenschutzfragen wichtig, weil er bereits eine Reihe von Präzedenzfällen zur Auslegung des EU-Datenschutzrechts geschaffen hat (z.B. Schrems II).
False Positive	Gemeint ist ein falscher Treffer, d.h. ein System oder Vorgang liefert ein Resultat, das aber nicht dem entspricht, was gesucht wird.
Familie	Im Kontext eines → **Reviews** sind damit (in der jeweiligen Datenquelle) zusammengehörende Dokumente gemeint, also z.B. eine E-Mail mit den darin enthaltenen Beilagen, oder ein Dokument und die darin eingebetteten Objekte. Je nach Art der Dokumente kann es sinnvoll sein, Familien vom → **Review-System** während des Reviews zusammenzuhalten.
FINMAG	Bundesgesetz über die Eidgenössische Finanzmarktaufsicht vom 22. Juni 2007 (SR 956.1)

Forensic Accountant	Darunter wird ein Spezialist verstanden, dessen Spezialgebiet es ist, Fehlverhalten in der Buchhaltung sowie in der Finanzberichterstattung von Unternehmen zu erkennen und aufzudecken. Der Einsatz eines *Forensic Accountant* ist bei Finanzdelikten sinnvoll.
Gemeinsame Verantwortliche	Zwei oder mehr Unternehmen (oder andere Stellen), die arbeitsteilig oder zusammen die Zwecke und Mittel ein- und derselben Datenbearbeitungsaktivität festlegen. Unter dem Begriff „Mittel" sind die wesentlichen Aspekte der Bearbeitungstätigkeit zu verstehen, d.h. woher die Daten erhoben werden, welche Kategorien von Personendaten verwendet werden, wo sie bearbeitet werden, was mit den Daten geschehen soll, wie lange sie aufbewahrt werden usw. Gemeinsame Verantwortliche (auch *Joint Controller* genannt) müssen unter der DSGVO eine Vereinbarung abschliessen und festlegen, wer welche Verantwortlichkeitsverpflichtung nach der DSGVO wahrnimmt (Art. 26 DSGVO). Unabhängig von diesen Vereinbarungen bleibt jeder gemeinsame Verantwortliche für die Einhaltung aller Pflichten der Datenbearbeitung verantwortlich und kann daher bei Nichteinhaltung verklagt oder mit einer Geldstrafe belegt werden. Die Identifizierung von gemeinsamen Verantwortlichen ist in der Praxis oft schwierig und viele Konstellationen sind nicht ganz klar.
Gleichstellungsgesetz	Bundesgesetz über die Gleichstellung von Frau und Mann vom 24. März 1995 (SR 151.1)
Grundsätze der Datenbearbeitung	Es handelt sich dabei um die „Grundregeln" des Datenschutzes, welche sich auch als die „Kernprinzipien" des Datenschutzes bezeichnen lassen. Sie legen fest, wie Personendaten bearbeitet werden dürfen. Im schweizerischen Datenschutz gelten als Grundregeln der Datenbearbeitung die Rechtmässigkeit, der Grundsatz von Treu und Glauben, das Transparenzgebot, die Zweckbindung, die Verhältnismässigkeit, die Datenrichtigkeit und die Wahrung der Datensicherheit. In der Praxis wird das Prinzip der Transparenz in der Regel durch eine Datenschutzerklärung sichergestellt. Kann einer der Grundsätze der Datenbearbeitung nicht eingehalten werden (z.B. heimliche Überwachung), so ist hierfür ein → **Rechtfertigungsgrund** erforderlich. Die DSGVO kennt vergleichbare Grundsätze, allerdings erfordert sie immer eine Rechtfertigung (unter der DSGVO ist von „Rechtsgrund" die Rede).

Hash-Wert	Der Hash-Wert ist das Ergebnis eines „*Hashings*“ oder einer Hash-Funktion, d.h. die Umwandlung einer Zeichenfolge in einen normalerweise viel kürzeren Wert fester Länge. Die Umwandlung basiert auf einem mathematischen Algorithmus und zwar so, dass jede unterschiedliche Zeichenfolge statisch gesehen zu einem unterschiedlichen Hash-Wert führt. Wird der Hash-Wert einer ganzen Datei berechnet, kann dieser als eine Art digitaler Fingerabdruck der Datei verwendet werden. Wird nur ein Zeichen oder Bit der Datei verändert, ändert sich auch ihr Hash-Wert. Im Falle einer forensischen Datensicherung kann durch die gespeicherten Hash-Werte der gesicherten Dateien nachgewiesen werden, dass die in der Spiegelung enthaltenen Dateien gegenüber den Dateien im Original nicht verändert worden sind.
Interne Untersuchung	Systematische, vertiefte Ermittlung und Beurteilung der Fakten bezüglich eines Fehlverhaltens (Verstoss gegen interne Regeln, öffentlich-rechtliche Bestimmungen oder Strafnormen), dass durch das Unternehmen selbst durchgeführt wird, im Gegensatz zu einer behördlichen Untersuchung. Mit der internen Untersuchung betraut werden können interne Funktionen (z.B. Compliance), aber auch unabhängige Externe (z.B. eine Anwaltskanzlei).
Investigation Hold	→ **Legal Hold**
Joint Controller	→ **Gemeinsame Verantwortliche**
KG	Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen vom 6. Oktober 1995 (SR 251)
Legal Hold	Darunter wird der Vorgang bezeichnet, mit welchem eine Organisation, welche sich mit einem Rechtsstreit oder behördlichen Verfahren konfrontiert sieht, sicherstellt, dass keine potenziell relevanten Unterlagen und Daten mehr vernichtet werden. In gewissen Rechtsordnungen (z.B. den USA) ist ein *Legal Hold* in gewissen Konstellationen vorgeschrieben und gängige Praxis, in der Schweiz nicht. Zeichnet sich der Bedarf für eine interne Untersuchung ab, gehört die Verhängung eines *Legal Hold* zu den ersten Massnahmen, die getroffen werden müssen (so u.a. mit der Versendung einer → **Legal Hold Notice**). Bei internen Untersuchungen ist Teils auch von *„Investigation Hold“* die Rede, um zu verdeutlichen, dass der Vernichtungsstopp nicht aufgrund einer Rechtspflicht erfolgt. Mehr dazu: → **ERSTE SCHRITTE**.

Legal Hold Notice	Es handelt sich dabei um die Anweisung einer Organisation an seine Mitarbeiter (und ggf. Provider) im Rahmen eines → **Legal Hold**, wonach keine für einen Fall potenziell relevanten Unterlagen und Daten mehr vernichtet werden dürfen. Daten sind zu sichern und Löschroutinen zu stoppen. Die *Legal Hold Notice* kann auch für Datenschutzhinweise benutzt werden. Mehr dazu: → **ERSTE SCHRITTE**.
Legal Privilege	Das Recht einer Person, ihren Austausch mit ihrem Anwalt und dessen Arbeitsprodukte in behördlichen oder gerichtlichen Verfahren nicht offenlegen zu müssen bzw., dass diese nicht beschlagnahmt werden dürfen. Das *Legal Privilege* ist in den unterschiedlichen Rechtsordnungen unterschiedlich ausgestaltet. In der Schweiz können sich z.B. nur Klienten von Anwälten nach → **BGFA** darauf berufen, in den USA schützt das *Legal Privilege* auch den Rechtsrat von Unternehmensjuristen. In der Praxis ist oft vom „Anwaltsgeheimnis" die Rede, was etwas ungenau ist, weil dieses nur die Pflicht des Anwalts beinhaltet, die ihm zugekommenen Informationen geheim zu halten (ihm allerdings auch ein Zeugnisverweigerungsrecht gibt). Mehr: → **Q10**.
Metadaten	Gemeint sind Randdaten, im Gegensatz zu Inhaltsdaten. Sie kommen überall vor, wo Dokumente und andere Inhalte elektronisch verarbeitet werden. Bei einer E-Mail sind es z.B. der Sender, die Empfänger, die Übermittlungszeiten, die Grösse, die Zahl und Art der Anhänge und weitere Angaben. Bei einem Dokument kann es der Erstellungszeitpunkt oder Autor sein.
Near Duplicates	Damit sind die in einem → **Review-System** gespeicherten Dokumente gemeint, die „fast gleich" bzw. ähnlich sind wie das Dokument, welches ein Benutzer gerade bearbeitet. Sind in einem Review-System 200 Kundenverträge enthalten, die ausser dem Namen des Kunden identisch sind, dann zählen sie als Near Duplicates: Das System führt sie als separate Dokumente auf, aber sie können trotzdem als Gruppe behandelt (z.B. gemeinsam klassifiziert) werden, was Zeit spart. Identische Dokumente wird ein Review-System hingegen normalerweise konsolidieren, d.h. nur als ein einziges Dokument darstellen (→ **DeDuplizierung**).
OCR	Die Technik der automatisierten Texterkennung (*Optical Character Recognition*): Das Abbild eines Textes (z.B. ein Foto oder Scan) wird analysiert, um es in ein Textdokument zu überführen, dass nach Wörtern durchsucht oder bearbeitet werden kann. Ein → **Review-System** verfügt über entsprechenden Funktionen. Mehr dazu: → **WERKZEUGE FÜR EDISCOVERY**.

OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Obligationenrecht) vom 30. März 1911 (SR 220)
Personendaten	Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Dabei ist es unerheblich, ob die betroffene Person direkt (z.B. über einen Namen, eine eindeutige Kennung, eine E-Mail-Adresse) oder indirekt (durch Verknüpfung mit Informationen aus anderen Quellen, z.B. einer Suche im Internet, in einer Unternehmensdatenbank, in einem öffentlichen Register) identifiziert werden kann. Nur falls die Informationen irreversibel anonymisiert wurden, handelt es sich nicht mehr um Personendaten. Wenn sie verschlüsselt oder anderweitig pseudonymisiert sind, sind sie für diejenigen, die keinen Zugang zum Schlüssel haben, um den Vorgang rückgängig zu machen, keine Personendaten mehr, für diejenigen, die den Schlüssel haben, bleiben die Informationen jedoch Personendaten. Grundsätzlich unterliegt jede Bearbeitung von Personendaten dem Datenschutzrecht. Dabei macht es keinen Unterschied, ob die Personendaten geschäftsbezogen (z.B. die geschäftlichen E-Mails eines Mitarbeiters) oder privat sind.
Persönlichkeitsprofil	Ein im Datenschutzgesetz definierter Begriff, der jede Zusammenstellung von Daten meint, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt. Ein Personaldossier stellt in der Regel ein Persönlichkeitsprofil dar. Der Begriff wird im revidierten Datenschutzgesetz abgeschafft und durch *„Profiling“* ersetzt, was allerdings nicht dasselbe meint, sondern eine automatisierte Bewertung bestimmter Aspekte einer Person.
Predictive Coding	Im weitesten Sinn eine Verwendungsform einer → **Concept search**, bei welcher ein → **Review-System** in einem ersten Schritt einen Mustersatz an Dokumenten und deren (von menschlichen Reviewern) angebrachten → **Tags** analysiert, um danach weitere vergleichbare Dokumente dementsprechend selbst zu klassifizieren. Damit ist es im besten Fall nicht mehr nötig, dass diese weiteren Dokumente von Menschen gesichtet und entsprechend kodiert werden müssen. Es ist mit anderen Worten eine Form der automatisierten Kodierung von Dokumenten basierend auf Verfahren der Mustererkennung. Entsprechende Verfahren wurden entwickelt, um die Kosten

	für Reviews zu senken und bestenfalls die Qualität zu steigern. Sie zahlen sich allerdings erst bei sehr grossen Volumen aus. Mehr dazu: → **WERKZEUGE FÜR EDISCOVERY**.
Pre-trial discovery	Gemeint ist der vorprozessuale Austausch von Beweismitteln zwischen Parteien eines zivilrechtlichen Streits im *Common Law*. Er soll der jeweils anderen Seite ermöglichen, an Beweismittel zu gelangen (Dokumente, Befragungen etc.). Normalerweise erfolgt der Austausch freiwillig, indem in sog. *meet and confer*-Sitzungen vereinbart wird, welche Kategorien von Unterlagen und Daten bis wann in welcher Form ausgetauscht werden. Auf diese Weise können sehr grosse Mengen an Dokumenten zusammenkommen. Weigert sich eine Partei, bestimmte Unterlagen zu liefern, muss der Richter darüber entscheiden.
Rechtfertigungsgrund	Unter dem schweizerischen Datenschutzrecht bedarf die → **Bearbeitung** von → **Personendaten** nicht per se eines Rechtfertigungsgrundes (im Gegensatz dazu muss unter der DSGVO stets ein Rechtfertigungsgrund vorliegen). Dieses Grundprinzip wird auch unter dem revidiertem DSG bestehen bleiben. Eine Rechtfertigung bedarf es lediglich, wenn gegen die → **Grundsätze der Datenbearbeitung** verstossen wird, eine Person der Bearbeitung widerspricht oder wenn → **besonders schützenswerte Personendaten** (oder ein → **Persönlichkeitsprofil**) mit einem anderen Verantwortlichen geteilt werden. Mögliche Rechtfertigungsgründe sind die Einwilligung der betroffenen Person, das Vorliegen eines überwiegenden, privaten oder öffentlichen Interesses sowie das Vorliegen einer gesetzlichen Grundlage.
Redaction Protocol	Das Dokument, welches die Vorgehensweise bei der → **Schwärzung** von Dokumenten im Rahmen eines Reviews festhält. Es protokolliert allerdings nicht die einzelnen Schwärzungen, sondern hält aber immerhin die Regeln fest, nach welchen geschwärzt wird. Ein solches Dokument muss z.B. im Rahmen von → **SWISS SECRECY & PRIVACY REVIEWS** erstellt werden.
Redactions	Der englische Begriff für → **Schwärzungen**.
RegEx	Die Abkürzung steht für *Regular Expression* oder „regulärer Ausdruck“ und kann im vorliegenden Kontext mit „Suchmusterbegriff“ umschrieben werden. Es ist ein Suchbegriff für eine Such- oder Filterfunktion (z.B. eines → **Review-Systems**), der jedoch nicht nur ein einzelnes, ganz bestimmtes Wort findet, sondern eine Vielzahl von Ausdrücken, die der Regel entsprechen, die im Suchmusterbegriff definiert ist. Eine besonders

	einfache Form ist der Stern: Der Suchbegriff „Sonne*“ findet alles Begriffe, die mit „Sonne“ anfangen, also „Sonne“ ebenso wie „Sonnenuntergang“. Komplexe RegEx können so formuliert werden, dass mit ihnen z.B. beliebige Kreditkarten- oder Bankkonto-Nummern gefunden werden können, sofern sie dem im RegEx festgehaltenen Suchmuster entsprechen.
revDSG	Die Abkürzung steht für das revidierte schweizerische Datenschutzgesetz, welches voraussichtlich 2022 in Kraft treten wird.
Review	Die übliche Bezeichnung für das Verfahren einer systematischen Sichtung von Unterlagen (z.B. E-Mails einer Person) oder Daten durch meist mehrere Personen (Reviewer) unter Einsatz einer speziellen IT-Lösung (sog. → **Review-System**). Mehr dazu: → **DOKUMENTEN-REVIEWS**, → **WERKZEUGE FÜR EDISCOVERY**. Reviews können nicht nur für interne Untersuchungen, sondern auch für andere Zwecke eingesetzt werden: → **DSAR-REVIEWS**, → **DATA BREACH REVIEWS**, → **VERTRAGS-REVIEWS**, → **SWISS SECRECY & PRIVACY REVIEWS**.
Review-System	Die IT-Lösung (lokal installiert oder von einem Provider betrieben, wahlweise auch in der Cloud), mit welcher grosse Mengen an Dokumenten zwecks eDiscovery verarbeitet und insbesondere gesichtet und kodiert werden können. Mehr dazu → **WERKZEUGE FÜR EDISCOVERY**.
Schwärzungen	Der Begriff meint das Abdecken von Stellen in einem Dokument, welche der Empfänger nicht sehen soll. Die Abdeckung erfolgt durch eine schwarze (oder andersfarbige) Fläche, so dass der Empfänger im Sinne der Transparenz sieht, dass an dieser Stelle etwas abgedeckt ist, aber eben nicht was. Auf Englisch ist von *“Redactions“* die Rede, wobei der Begriff nicht nur klassische Schwärzungen umfasst, sondern auch das Ersetzen von Inhalten durch einen Platzhalter wie z.B. „[Client1]“ oder „[redacted]“, wo Schwärzungen im engeren Wortsinn nicht möglich oder praktikabel sind.
Server Logs	Ein „*Log*“ ist eine Protokolldatei. Server Logs bezeichnen automatisch generierte Protokolle über die Aktivitäten, welche über einen Server ausgeführt werden.
Sexuelle Belästigung	Unter sexuelle Belästigung fällt sämtliches belästigendes Verhalten sexueller Natur sowie sämtliches auf die Geschlechtszugehörigkeit beruhendes Verhalten, welches zu einer Beeinträchtigung der Würde von Frauen und Männern führt. Eine sexuelle Belästigung kann in einer Vielzahl von Formen erfolgen (z.B.

	durch sexistische Witze, Gesten, unerwünschten Annäherungen etc.). Die rechtliche Relevanz hängt von der Ausprägung ab. Der Begriff der strafrechtlich relevanten sexuellen Belästigung ist mitunter enger gefasst als das Verhalten, das ein Arbeitgeber am Arbeitsplatz untersagt.
Standard-vertragsklauseln	Eine Reihe von standardisierten Vertragsvorlagen, die von der Europäischen Kommission im Rahmen des EU-Datenschutzrechts genehmigt wurden. Die Standardvertragsklauseln, auf die am häufigsten Bezug genommen wird, befassen sich mit dem Export von Personendaten. Sie zielen darauf ab, (durch eine vertragliche Verpflichtung) sicherzustellen, dass ein Empfänger von Personendaten in einem Land ohne angemessenes Datenschutzniveau dennoch die Grundprinzipien des Datenschutzes einhalten wird. Nach der DSGVO ist dies die einfachste und am häufigsten verwendete „Schutzmassnahme" für den Export von Personendaten in Länder ausserhalb des EWR, die kein angemessenes Datenschutzniveau bieten und daher von der Europäischen Kommission nicht auf die „*Whitelist*" gesetzt wurden. Unter der DSGVO sind die Standardvertragsklauseln für Datenexporte unverändert zu verwenden, wobei in den Anhängen der Umfang des Datenexports und je nach Szenario die zu treffenden technischen und organisatorischen Massnahmen der Datensicherheit zu beschreiben sind. In der „Schrems II"-Entscheidung des → **EuGH** aus dem Jahr 2020 wurde festgestellt, dass Standardvertragsklauseln für den Export in Länder ohne Angemessenheitsstatus unter Umständen nicht mehr ausreichend sind. Es ist daher erforderlich, dass zusätzlich zur Vereinbarung der Standardvertragsklauseln eine Risikobewertung für den rechtmässigen Zugang zum Ausland vorgenommen wird. Die Europäische Kommission will 2021 neue Versionen der Standardvertragsklauseln veröffentlichen, die innerhalb von zwölf Monaten umgesetzt werden müssen. Die Standardvertragsklauseln für Exporte wurden zuletzt im Jahr 2004 bzw. 2010 aktualisiert und werden sehr häufig verwendet. Auch wenn sie kompliziert und streng sind, werden sie allgemein akzeptiert. Beachten Sie, dass die Europäische Kommission voraussichtlich auch Standardvertragsklauseln für Auftragsbearbeitungsverträge veröffentlichen wird; sie werden aller Voraussicht nach nicht verbindlich sein. Die Standardvertragsklauseln für Exporte sind auch unter dem Schweizer Datenschutzgesetz anerkannt.

StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0)
StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007 (SR 312.0)
Strukturierte Daten	Gemeint sind Daten, deren Aussagen in einzelne, definierte Kategorien von Informationen aufgeteilt und entsprechend abgelegt wurden. Beispiel: Die Anschrift einer Person wird aufgeteilt in Anrede, Name, Vorname, Adresse, Postleitzahl und Ort. Werden die Daten so in einer Datenbank abgelegt, kann z.B. einfach nach Ort sortiert werden. Das Gegenstück sind unstrukturierte Daten (z.B. der Inhalt von E-Mails oder Berichten).
Tagging	Vorgang während → **DOKUMENTEN-REVIEWS**, bei welchem die Reviewer die einzelnen, von ihnen gesichteten Dokumente mittels einer entsprechenden Funktion des → **Review-Systems** kodieren bzw. klassifizieren, d.h. mit einem oder mehreren elektronischen Etiketten, Markierungen oder „Reiter" versehen, auch → **Tags** genannt (z.B. „Relevant", „Nicht relevant", „privater Inhalt", „technisches Problem", „Zurückgestellt"). Die möglichen Etiketten können individuell pro Review programmiert werden. Möglich ist auch das Erfassen von Kommentaren.
Tags	Das Ergebnis des → **Taggings**, d.h. die elektronischen Etiketten, mit denen die Reviewer jedes von ihnen gesichtete Dokument versehen haben. Im → **Review-System** können daraufhin alle Dokumente nach ihren jeweiligen Tages abgerufen und gefiltert werden.
TAR	→ **Technology Assisted Review**
Technology Assisted Review	Ein Sammelbegriff für verschiedene Methoden, mit denen ein → **Review** halb- oder ganz automatisiert oder sonst effektiver oder effizienter gestaltet werden kann. → **Predictive Coding** ist ein typisches Beispiel. Mehr: → **WERKZEUGE FÜR EDISCOVERY**.
Thread	Im Kontext eines → **Reviews** ist damit ein Strang von E-Mails oder anderer Kommunikation gemeint (d.h. das initiale E-Mail und alle Antworten darauf). Ein → **Review-System** kann *Threads* im Rahmen eines Reviews zusammenhalten, damit der *Thread* vom selben Reviewer in globo beurteilt werden kann (was einen Effizienzgewinn ergibt).
Unterauftragsbearbeiter	Arbeitet für den → **Auftragsbearbeiter** und übernimmt in deren Auftrag einen Teil der Bearbeitung.

UWG	Bundesgesetz gegen den unlauteren Wettbewerb vom 19. Dezember 1986 (SR 241)
VDSG	Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (SR 235.11)
Verantwortlicher	Ist die natürliche oder juristische Person oder sonstige Stelle, die entscheidet, warum (zu welchem Zweck) und wie (mit welchen Mitteln) Personendaten bearbeitet werden. Unter „Mitteln" sind die wesentlichen Aspekte der Bearbeitungstätigkeit zu verstehen, d.h. woher die Daten stammen, welche Kategorien von Personendaten verwendet werden sollen, wo die Daten bearbeitet werden sollen, was mit den Daten geschehen soll, wie lange sie aufbewahrt werden sollen usw. Die Entscheidungen können vom Verantwortlichen allein oder zusammen mit anderen Verantwortlichen getroffen werden (wobei diese folglich zu → **gemeinsamen Verantwortlichen** werden). Der Verantwortliche ist für die Datenbearbeitung in Übereinstimmung mit den einschlägigen Datenschutzgesetzen verantwortlich. Ein Verantwortlicher kann die Daten selbst bearbeiten oder mit einem Dritten zusammenarbeiten, der als → **Auftragsbearbeiter** bezeichnet wird.
Verletzung der Datensicherheit	→ **Data Breach**
Whistleblowing	Unter Whistleblowing wird die Offenlegung von illegalen, unmoralischen oder illegitimen Praktiken oder Missständen (in) einer Organisation an eine geeignete Stelle verstanden. Die Offenlegung hat zwingend durch einen (aktuellen oder ehemaligen) Insider zu erfolgen, der aufgrund seiner Stellung Zugang zu Insiderinformationen hat. Die Offenlegung erfolgt an eine von der Organisation betriebene Stelle (z.B. → **Whistleblowing-Hotline**) oder auch an Dritte (z.B. Behörden, Medien), wenn diese nach Ansicht des Whistleblowers in der Lage sind, geeignete Massnahmen zu treffen. Ein Whistleblowing kann zu einer internen Untersuchung, aber auch zu einer behördlichen Untersuchung oder zu Presseberichten führen. Die Bezeichnung kommt von *"to blow the whistle"* („verpfeifen"); der Hinweisgeber wird als „Whistleblower" bezeichnet.

Whistleblowing-Hotline	Die Rede ist auch von „Meldestellen“ für Hinweisgeber. Eine von einer Organisation betriebene interne Stelle, an welche sich Insider wenden können, wenn sie im Rahmen eines → **Whistleblowings** ohne Einhaltung des Dienstweges über einen von ihnen vermuteten oder konkreten Missstand innerhalb der Organisation berichten möchten, damit der Vorwurf untersucht wird. Eine solche Meldung kann anonym oder unter Namensnennung erfolgen. Der Kanal ist nicht zwingend das Telefon; Meldungen können auch via Internet, E-Mail, Brief, Apps, persönlich oder anders erfolgen. Immer mehr Unternehmen richten eine solche Meldestelle ein (→ **Q5**); in der EU wird sie für viele Unternehmen sogar Pflicht (→ **Q8**).

Gibt es weitere **Begriffe oder Abkürzungen**, die Sie vorschlagen würden, in diese Tabelle aufzunehmen? Bitte senden Sie uns Ihren Vorschlag an drosenthal@vischer.com.

Schlussgedanken zum Thema.

In einer internen Untersuchung kommt oft nicht nur die beschuldigte Person in eine unangenehme Lage, sondern ebenso ihre Arbeitskollegen, das Linien-Management, das Unternehmen und nicht zuletzt auch Sie selbst als die Person, die alles aufklären muss. Doch auch wenn es heftiger als sonst «schüttelt», geht deswegen nicht die Welt unter, erfahrungsgemäss auch nicht für die Person, um die sich alles dreht.

Christoph Jörg
Senior Compliance Manager
BKW

17. Literatur

ALLGEMEINE LITERATUR

Arbeitsrecht

Geiser, Thomas/Müller, Roland/Kurt, Pärli: Arbeitsrecht in der Schweiz, Bern 2019

Kuoni, Anina: Arbeitsrecht, Zürich/Basel/Genf 2020

Pärli, Kurt: Fachhandbuch Arbeitsrecht – Expertenwissen für die Praxis, Zürich/Basel/Genf 2018

Portmann, Wolfgang/von Kaenel, Adrian: Fachhandbuch Arbeitsrecht – Expertenwissen für die Praxis, Zürich/Basel/Genf 2018

Streiff, Ullin/von Kaenel, Adrian/Rudolph, Roger (Hrsg.): Arbeitsvertrag – Praxiskommentar zu Art. 319 – 362 OR, 7. Aufl., Zürich/Basel/Genf 2012

Datenschutz

Bosse, Christian K./Dietrich, Aljoscha/Kelbert, Patricia/Küchler, Hagen/Schmitt, Hartmut/Tolsdorf, Jan/Wessner, Andreas: Beschäftigtendatenschutz – Rechtliche Anforderungen und Technische Lösungskonzepte, in: IT-Jusletter vom 28. Februar 2020, Rz. 1 ff.

Domenig, Benjamin/Mitscherlich, Christian: Datenschutzrecht für Schweizer Unternehmen, Bern 2019

Fasnacht, Tobias: Die Einwilligung im Datenschutzrecht – Vorgaben einer völker- und verfassungsrechtlich konformen Ausgestaltung der datenschutzrechtlichen Einwilligung im schweizerischen Recht, Zürich/Basel/Genf 2017

Keller, Claudia: Datenschutz, Zürich/Basel/Genf 2019

Passadeli, Nicolas/Rosenthal, David/Thür, Hanspeter (Hrsg.): Datenschutzrecht, Beraten in Privatwirtschaft und öffentlicher Verwaltung, Handbücher für die Anwaltspraxis, Basel 2015

Rosenthal, David: Das neue Datenschutzgesetz, in: Jusletter vom 16. November 2020, Rz. 1 ff.

Rosenthal, David: Löschen und doch nicht löschen, in: Zeitschrift für Datenrecht und Informationssicherheit (digma) Heft 4, Dezember 2019, 190 ff.

Rosenthal, David/Jöhri, Yvonne: Handkommentar zum Datenschutzgesetz, Zürich/Basel/Genf 2008

Vasella, David: Widersprüche im Datenschutzrecht, in: Zeitschrift für Datenrecht und Informationssicherheit (digma) Heft 4, Dezember 2020, 174 ff.

Interne Untersuchungen

Götz Staehelin, Claudia: Unternehmensinterne Untersuchungen, Zürich/Basel/Genf 2019

Lengauer, Daniel/Ruckstuhl, Lea: Compliance, Zürich/Basel/Genf 2017

Mráz, Michael: Kuckuseier im Strafprozess «Interne Untersuchungen», in: forumpoenale Sonderheft 1/2020, 170 ff.

Romerio, Flavio/Bazzani, Claudio: Interne und regulatorische Untersuchungen, Zürich 2015

Strafrecht

Bürge, Lukas: Polizeiliche Ermittlung und Untersuchung – Charakteristik, Abgrenzungen und Auswirkungen auf Beschuldigtenrechte, Bern 2018

Kunz, Peter V.: Wirtschaftsstrafrecht, Bern 2019

Schmid, Niklaus/Jositsch, Daniel: Handbuch des schweizerischen Strafprozessrechts, Zürich/St. Gallen 2017

Weilenmann, Reto: Drittgeschädigte Personen im Strafverfahren unter besonderer Berücksichtigung des Privatklage-, Aushändigungs- und Zuwendungsanspruchs, Zürich/Basel/Genf 2020

■ SPEZIALLITERATUR

Anwaltsgeheimnis und interne Untersuchung

Huber, Roman: Interne Untersuchungen und Anwaltsgeheimnis, in: Gesellschafts- und Kapitalmarktrecht (GesKR) 2019, 65 ff.

Wohlers, Wolfgang/Lynn, Veronica: Das Anwaltsgeheimnis bei internen Untersuchungen, in: Zeitschrift für juristische Weiterbildung und Praxis (recht) 2018, 9 ff.

Amtshilfe und Schutz von Mitarbeiterdaten

Opel, Andrea: Schutz von Bankmitarbeiterdaten in Amtshilfeverfahren, in: Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht (SZW) 2020, 593 ff.

Opel, Andrea: Lieferung von Bankmitarbeiterdaten an ausländische Steuerbehörden – wenn Amtshilfe ausartet, Beiträge zur Schweizerischen Bankrechtstagung, in: Emmenegger, Susan (Hrsg.), Banken und Datenschutz, Basel 2019, 77 ff.

Befragungen/Mitarbeiterrechte

Müller, Roland/Schuchter, Alexander: Untersuchungen mit und ohne behördliche oder gerichtliche Anordnungen, Grenzen zwischen Informationsbeschaffung und Privatsphäre, in: Jusletter vom 12. April 2021, Rz. 1 ff.

Pozner, Larry S./Dodd, Roger: Cross Examination: Science and Techniques, Charlottesville, 1993

Rudolph, Roger: Das Recht des Arbeitnehmers auf Einsicht in sein Personaldossier, in: Allgemeine Juristische Praxis (AJP) 2014, 1672 ff.

Rudolph, Roger: Interne Untersuchungen: Spannungsfelder aus arbeitsrechtlicher Sicht, in: Schweizerische Juristenzeitung (SJZ) 114/2018, 385 ff.

Schmid, Niklaus: Strafbarkeit des Unternehmens: die prozessuale Seite, in: Zeitschrift für juristische Weiterbildung und Praxis (recht), 201 ff.

Toneatti, Michael: Löschungsanspruch von personenbezogenen Daten des Arbeitnehmers gegenüber der Arbeitgeberin (inklusive Berücksichtigung der EU Datenschutz-Grundverordnung), Zürich/St. Gallen 2019

Wantz, Simona/Licci, Sara: Arbeitsvertragliche Rechte und Pflichten bei internen Untersuchungen, in: Jusletter vom 18. Februar 2019, Rz. 1 ff.

Wendler, Axel/Hoffmann, Helmut: Technik und Taktik der Befragung, Stuttgart, 2015

Bring Your Own Device (BYOD)

Beranek Zanon, Nicole: Bring your own device (BYOD) aus rechtlicher Sicht, in: IT Jusletter vom 2. September 2012, Rz. 1 ff.

Birkhäuser, Nicolas/Hadorn, marcel: BYOD – Bring Your Own Device, in: Schweizerische Juristenzeitung (SJZ) 109/2013, 201 ff.

Wildhaber, Isabelle/Hänsenberger, Silvio: Bring Your Own Device (BYOD), in: Zeitschrift für Arbeitsrecht und Arbeitslosenversicherung (ARV) 2016, 151 ff.

Covid-19

Blesi, Alfred/Hirsiger, René/Pietruszak, Thomas, Arbeitsrecht, in: COVID-19, Ein Panorama der Rechtsfragen zur Corona-Krise, Basel 2020, 39 ff.

Cirigliano, Luca/ Niemeyer, Jens, Homeoffice: rechtliche Regelungen sowie Mustervertrag für die Praxis, in: Jusletter vom 30. November 2020, Rz. 1 ff.

Geiser, Thomas/Müller, Roland/Pärli, Kurt: Klärung arbeitsrechtlicher Fragen im Zusammenhang mit dem Coronavirus, in: Jusletter vom 23. März 2020, Rz. 1 ff.

Naber, Sebastian/Ahrens, Tim: Remote Investigations: Die Aufklärung von Compliance-Verstössen im New Normal, Compliance Berater (CB) 2020, 465 ff.

Steiger-Sackmann, Sabine: Arbeitsrechtlicher Reformbedarf für Homeoffice-Arbeit, Zeitschrift für Arbeitsrecht und Arbeitslosenversicherung (ARV) 2020, 300 ff.

eDiscovery

Rosenthal, David/Zeunert, Christian: E-discovery and data protection: Challenges and solutions for multinational companies, in: Jusletter IT 6. Juni 2012

Rosenthal, David: Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in: Jusletter vom 17. Juni 2019, Rz. 1 ff.

Weber, Rolf H./Thouvenin, Florent: Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich/Basel/Genf 2014

Forensische Techniken

Jackmuth, Hans-Willi/de Lamboy, Christian/Zawilla, Peter: Fraud Management in Kreditinstituten, Praktiken, Verhinderung, Aufdeckung, Frankfurt a.M. 2013

Kosten interne Untersuchung

Borle, Markus: Vorprozessuale Anwaltskosten – es führt kein Weg an der Substanziierung vorbei, in: Haftung und Versicherung (HAVE) 2012, 3 ff.

Jenne, Moritz/Schubert, Andreas: Kosten für interne Ermittlungen sind bei Compliance-Verstössen auch von Arbeitnehmern zu ersetzen, in: Compliance Berater (CB) 2020, 487 ff.

Psychologie

Babiak, Paul/Hare, Robert D.: Snakes in Suits: When Psychopaths Go to Work, New York, 2007

Benecke, Lydia: Sadisten – Tödliche Liebe – Geschichten aus dem wahren Leben, München, 2015

Haller, Reinhard: Die Narzissmusfalle, Anleitung zur Menschen- und Selbstkennnis, Salzburg, 2019

Sexuelle Belästigung (#MeToo)

Geiser, Thomas: Rechtsfragen der sexuellen Belästigung und des Mobbings, in: Zeitschrift des bernischen Juristenvereins (ZBJV) 137/2001, 429 ff.

Götz Staehelin, Claudia/Huber, Melanie: Pflichten der Arbeitgeberin in der #MeToo-Ära, in: Recht relevant. für Compliance Officers (RR-COMP), 5 ff.

Götz Staehelin, Claudia/Huber, Melanie: Arbeitsrechtlicher Reformbedarf für Homeoffice-Arbeit, in: Recht relevant. für Compliance Officers (RR-COMP), 300 ff.

Hafner, Peter: Auswertung der E-Mails von Arbeitnehmern, in: Aktuelle Juristische Praxis (AJP) 2018, 1327 ff.

Vögeli Galli, Nicole: Sexuelle Belästigung am Arbeitsplatz – die Rechtsprechung im Spannungsfeld der involvierten Interessen, in: Mitteilung des Instituts für Schweizerisches Arbeitsrecht (ArbR) 2009, 33 ff.

Strafbarkeit des Unternehmens

Arzt, Gunther: Unternehmensstrafbarkeit – Fernwirkungen im materiellen Strafrecht (Fährlässigkeit, Begünstigung, Urkundendelikte, Geschäftsbesorgung), in: Zeitschrift für juristische Weiterbildung und Praxis (recht) 2004, 213 ff.

Heiniger, Matthias: Der Konzern im Unternehmensstrafrecht gemäss Art. 102 StGB, Bern 2011

Nadelhofer do Canto, Simone: Millionenbusse gegen Alstom-Tochter wegen ungenügender Vorkehrungen gegen Bestechung, in: Gesellschafts- und Kapitalmarktrecht (GesKR) 2012, 129 ff.

Pflaum, Sonja: Die Erledigung von Strafverfahren gegen Unternehmen durch Wiedergutmachung, in: Gesellschafts- und Kapitalmarktrecht (GesKR) 2019, 118 ff.

Untersuchungsergebnisse

Graf, Damian K.: Strafprozessuale Verwertbarkeit von Befragungsprotokollen interner Untersuchungen, in: forumpoenale 1/2016, 39 ff.

Graf, Damian K.: Beschlagnahmefähigkeit von Befragungsprotokollen und Ermittlungserzeugnissen interner Untersuchungen, in: forumpoenale 6/2015, 345 ff.

Fritsche, Claudia M./Studer, Nadine: Arbeitsprodukte interner Untersuchungen, in: Aktuelle Juristische Praxis (AJP) 2018, 168 ff.

Mühlemann, David: Fairness und Verwertbarkeit unternehmensinterner Untersuchungen, in: Aktuelle Juristische Praxis (AJP) 2018, 468 ff.

Wohlers, Wolfgang: Beweisverwertungsverbote nach privater Beweiserlangung – wann bzw. unter welchen Voraussetzungen dürfen rechtswidrig durch Private erlangte Beweismittel im Strafverfahren verwertet werden?, in: forumpoenale Sonderheft 1/2020, 198 ff.

Überwachungsmassnahmen

Backhaus Nils: Kontextsensitive Assistenzsysteme und Überwachung am Arbeitsplatz: Ein meta-analytisches Review zur Auswirkung elektronischer Überwachung auf Beschäftigte, in: Zeitschrift für Arbeitswissenschaft, 73(1), 2019, 2 ff.

Geiser, Thomas: Überwachungen am Arbeitsplatz, in: Zeitschrift für Datenrecht und Informationssicherheit (digma) 2015, 50 ff.

Götz, Staehelin Claudia/Bertschi, Manuel: Grenzen der Mitarbeiterüberwachung, in: Recht relevant. für Verwaltungsräte (RR-VR) 3/2020, 5 ff.

Meier-Gubser, Stefanie: Mitarbeiterüberwachung: Rechte, Pflichten und Verbote, in: Der Treuhandexperte (TREX), 286 ff.

Wildhaber, Isabelle/Hänsenberger, Silvio: Internet am Arbeitsplatz, in: Zeitschrift des bernischen Juristenvereins (ZBJV) 152/2016, 307 ff.

Whistleblowing

Erlenbach, Kimberly: Die Regelungen der EU-Hinweisgeberrichtlinie und ihre Auswirkungen auf deutsche Unternehmen, Compliance Berater (CB) 2020, 284 ff.

Hahn, Anne-Catherine: Die neue EU Whistleblower-Richtlinie – Handlungsbedarf für Schweizer Unternehmen? Recht relevant. für Compliance Officers (RR-COMP), 1/2020, 2 ff.

Jungo, Nicole: Whistleblowing – Lage in der Schweiz, in: Zeitschrift für juristische Weiterbildung (recht) 2012, 65 ff.

Licci, Sara: Codes of Conduct im Arbeitsverhältnis mit besonderem Blick auf das Whistleblowing, in: Aktuelle Juristische Praxis (AJP) 2015, 1168 ff.

Rieder, Stefan: Whistleblowing als interne Risikokommunikation, Zürich/St. Gallen 2013

von Kaenel, Adrian (Hrsg.): Whistleblowing – Multidisziplinäre Aspekte, Bern 2012

Zimmermann, Anita/Pärli, Kurt: Whistleblowing und Datenschutz, in: Zeitschrift für Datenrecht und Informationssicherheit (digma) 2016, 18 ff.

In eigener Sache:

Das Investigations & eDiscovery Team von VISCHER

- Teamleiter: David Rosenthal

Unsere Experten:

- Arbeitsrecht: Marc Ph. Prinz
- Strafrecht: Jonas D. Gassmann, Michael H.P. Pfeifer
- Steuerrecht, Sozialversicherungsrecht: Christoph Niederer, Nadia Tarolli Schmidt
- Kartellrecht: Klaus Neff
- Corporate: Felix W. Egli, Benedict F. Christ, Roland M. Müller, Maxime Chollet
- Finanzmarktrecht: Jana Essebier, Adrian Dörig, Markus Guggenbühl
- Gesundheits- und Spitalrecht: Michael Waldner, Andreas C. Albrecht
- Life Sciences: Stefan Kohler, Christian Wyss
- Medien- und Telekommunikationsrecht: Rolf Auf der Maur
- Insolvenzrecht: Markus Guggenbühl, David Jenny, Jana Essebier
- Arrestrecht: Felix C. Meier-Dieterle
- Public Sector, Verwaltungsverfahren: Stefan Rechsteiner
- Litigation & Arbitration: Thomas Weibel, Christian Oetiker, Daniele Favalli, Gérald Virieux, Felix C. Meier-Dieterle
- Internationale Rechtshilfe: Mladen Stojiljkovic, Thomas Weibel, Christian Oetiker
- Associates, Junior Associates: Samira Studer, Tabea Steiger, Anela Lucic, Dorothée Krapf, Seraina Gubler, Dan Pruschy, Marisa Di Francesco, Livia Camenisch
- Projektmitarbeiter

Wir arbeiten mit führenden eDiscovery-Dienstleistern und Spezialisten zusammen.

VISCHER – als schlagkräftiges und innovatives Schweizer Anwaltsunternehmen unterstützen wir unsere Klienten in rechtlichen, steuerlichen und regulatorischen Belangen effizient und lösungsorientiert. Unsere Rechtsanwälte, Steuerexperten und Notare aus allen wirtschaftsrechtlichen Fachgebieten sind unter Führung erfahrener Partner in über 25 Spezialistenteams organisiert. Dies ermöglicht uns eine effiziente und stets auf die Bedürfnisse des individuellen Projekts zugeschnittene Mandatsführung.

Anwaltsrecht • Arbeitsrecht • Banken- und Finanzmarktrecht • Berufliche Vorsorge, Sozialversicherungsrecht • China Desk • Data & Privacy • Energie • Gesellschafts- und Handelsrecht • Gesundheitswesen • Immaterialgüterrecht • Immigration • Immobilien • Informations- und Kommunikationsrecht • Internationale Rechtshilfe • Investigations & eDiscovery • Kartell- und Wettbewerbsrecht • Life Sciences, Pharma, Biotechnologie • Medien und Unterhaltung • Mergers & Acquisitions • Notariat • Private Equity & Venture Capital • Privatkunden • Prozessführung und Schiedsgerichtsbarkeit • Public Sector und Regulatory • Restrukturierung und Insolvenz • Sportrecht • Startup Desk • Steuern • Transport/Luftfahrt • Wirtschaftsstrafrecht

Für ein gedrucktes Exemplar wenden Sie sich bitte an Ihren VISCHER-Kontakt oder bestellen Sie es sich hier: weblaw.ch/shop

Eine Fassung zum Download ist auf www.vischer.com/investigations und www.rosenthal.ch verfügbar. Für Spezialfassungen (z.B. mit eigenem Logo und eigenen Kontaktangaben) bitte den Autor kontaktieren (drosenthal@vischer.com).

Mailingliste für Updates: www.vischer.com/investigations

EDITIONS WEBLAW