www.jusletter.ch

David Rosenthal

Die Tücken spontaner Datenschutzbeurteilungen und was sich dagegen tun lässt

Die Einschätzung des Risikos einer Datenbearbeitung für die betroffenen Personen ist für die rechtliche Beurteilung der Datenbearbeitung wesentlich. Bei potenziell heiklen Datenbearbeitungen schreibt das neue Datenschutzgesetz sogar vor, dass sie dokumentiert werden muss. In der Praxis werden sie oft schnell und spontan gefällt. Doch wie zuverlässig sind solche Beurteilungen? Ein Experiment zeigt welche enorme Bandbreite intuitive Entscheide in diesem Bereich aufweisen können – und wie wichtig daher Massnahmen zur Sicherung der Beurteilungsqualität sind. Diese gibt es und sollten praktiziert werden – auch von Aufsichtsbehörden und Gerichten. Aus dem Experiment gefolgert werden kann aber auch, dass es die eine «richtige» Beurteilung eines Risikos einer Bearbeitung schlicht nicht gibt.

Beitragsart: Beiträge
Rechtsgebiete: Datenschutz, Europäisches Wirtschaftsrecht

Zitiervorschlag: David Rosenthal, Die Tücken spontaner Datenschutzbeurteilungen und was sich dagegen tun lässt, in: Jusletter 28. Februar 2022

ISSN 1424-7410, jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

[1] Seit rund zehn Jahren gibt es den Begriff des «gefühlten» Datenschutzes.[1] Und mindestens hinter vorgehaltener Hand ist in Datenschutzkreisen ebenso klar, dass selbst die Profis in der Wirtschaft, den Behörden und den Gerichten die ihnen vorgelegten Fälle oft zunächst aus dem «Bauch» entscheiden und erst hinterher begründen, warum eine bestimmte Datenbearbeitung so nicht geht oder es gewisse weitere Massnahmen braucht.[2] Diese Vorgehensweise ist nicht auf Datenschutzbeurteilungen beschränkt und sie ist nicht ungewöhnlich. Schon in den 90er-Jahren zeigte der US-Moralpsychologe Jonathan D. Haidt auf, dass wir uns überall dort, wo es um die Frage des *Richtig* und *Falsch* geht, zunächst spontan und daher intuitiv entscheiden und wir erst danach nach Gründen suchen, um unser ursprüngliches Bauchgefühl zu rechtfertigen.[3] Wir liegen nicht gerne falsch.

[2] Das Bauchgefühl ist im Datenschutz daher von zentraler Bedeutung, selbst wenn wir uns im Rahmen einer Fallbeurteilung nicht zu einem spontanen Urteil hinreissen lassen, sondern methodisch vorgehen, um uns nicht auf unsere Intuition verlassen zu müssen oder in die Irre leiten zu lassen. Einige Hinweise, wie das möglich ist, finden sich im hinteren Teil dieses Beitrags.

[3] Doch wie fallen spontane Einschätzung von Datenschutzfällen in der Praxis überhaupt aus? Wie einheitlich sind diese Urteile? Gibt es den *einen* gefühlten Datenschutz? Finden sich für klassische Fallkonstellationen Mehrheiten? Auf diese Frage gibt es bisher kaum Antworten. Um solche zu finden, hat der Verein Unternehmens-Datenschutz (**VUD**)[4] im Sommer 2021 ein Experiment im Kreise seiner Mitglieder durchgeführt. Der 2006 gegründete Verein ist ein Zusammenschluss der Unternehmensdatenschützer vieler KMUs und grosser internationaler Schweizer Unternehmen.[5] Er dient der selbständigen und unabhängigen Meinungsbildung im Bereich Datenschutz und führt dazu regelmässige interne Veranstaltungen durch; öffentlich tritt er kaum

1 Vgl. David Rosenthal, Das Bauchgefühl im Datenschutz, in: Datenschutz-Forum Schweiz (Hrsg.), Von der Lochkarte zum Mobile Computing – 20 Jahre Datenschutz in der Schweiz, Zürich 2012 (https://bit.ly/3kdPnJN, alle Websites zuletzt besucht am 20. Februar 2022).

2 Ebd.

3 Vgl. Matthew Liao, S.M. Liao, Bias and Reasoning: Haidt's Theory of Moral Judgment, London 2011, pp. 108–127; Jonathan Haidt, The emotional dog and its rational tail: A social intuitionist approach to moral judgment, Psychological Review, 4 (108): 814–34, 2001.

4 http://www.vud.ch.

5 Vgl. die Website mit der Mitgliederliste auf http://www.vud.ch.

auf (dieser Beitrag widerspiegelt auch nur die persönlichen Ansichten des Autors, nicht notwendigerweise jene der Mitglieder des VUD).

[4] Das Experiment fokussierte sich auf die Frage nach dem Risiko einer Datenbearbeitung für die davon betroffenen Personen. Sie stellt sich in der Praxis bei jeder neuen Datenbearbeitung, dies nebst der Prüfung der Einhaltung bestimmter Grundsätze[6] und formeller Vorgaben.[7] Es geht nicht um das Risiko der Datenbearbeitung für das Unternehmen, sondern für diejenigen Personen, über die Daten bearbeitet werden sollen. Welche Nachteile kann eine Datenbearbeitung für einen Mitarbeiter haben, über welchen der Arbeitgeber Daten erhebt? Wie kann es einem Konsumenten schaden, wenn ein Online-Händler die Kaufinteressen seiner Kunden auswertet? Inwiefern gefährdet das Tracking eines grossen Online-Konzerns die Interessen eines davon erfassten Internet-Nutzers?

1. Die Bedeutung des «Risikos» im Datenschutz

[5] Diese Frage nach dem Risiko für die betroffenen Personen ist im Datenschutz zentral. Sowohl das Schweizer Datenschutzgesetz (**DSG**) als auch die EU-Datenschutz-Grundverordnung (**DSGVO**) verfolgen einen *risikobasierten Ansatz*: Die zum Schutz der Daten bzw. der Persönlichkeit der betroffenen Personen zu treffenden Massnahmen sind am Risiko für die betroffenen Personen auszurichten. Kann mit bestimmten Daten mehr «Unfug» zum Nachteil der betroffenen Personen als mit anderen angestellt werden, sind tiefgreifendere oder wirksamere Schutzmassnahmen nötig, als wenn es um weniger sensible Daten oder Datenbearbeitungen geht.

[6] Dementsprechend viele Bestimmungen des Datenschutzrechts stellen daher direkt auf das mit einer Datenbearbeitung oder Verletzung der Datensicherheit für die betroffene Person verbundene Risiko ab. Im revidierten DSG sind es zum Beispiel der Begriff des Profilings mit hohem Risiko,[8] die für das «Privacy by Design» zu treffenden Massnahmen,[9] die Massnahmen der Datensicherheit,[10] die Ausnahme von der Pflicht zum Führen eines Verzeichnisses der Datenbearbeitungen,[11] die Pflicht zur Bestellung einer Vertretung für ausländische Verantwortliche,[12] die Datenschutz-Folgenabschätzung und damit verbundene Pflicht zur Konsultation des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (**EDÖB**) in bestimmten Fällen,[13] die Pflicht zur Meldung von Verletzungen der Datensicherheit[14] und indirekt auch Bestimmungen wie den Grundsatz der Verhältnismässigkeit,[15] der Transparenz,[16] die Standards einer gültigen Einwilli-

6 Rechtmässigkeit, Transparenz, Zweckbindung, Verhältnismässigkeit, Richtigkeit, Datensicherheit, Treu und Glauben (Art. 4 DSG, Art. 6 revDSG).

7 Beispielsweise im Falle von Auftragsbearbeitungen oder einer Bekanntgabe von Personendaten ins Ausland.

8 Art. 5 Bst. g revDSG.

9 Art. 7 Abs. 2 revDSG.

10 Art. 8 Abs. 1 revDSG.

11 Art. 12 Abs. 5 revDSG.

12 Art. 14 revDSG.

13 Art. 22 revDSG.

14 Art. 24 revDSG.

15 Art. 6 Abs. 2 revDSG.

16 Art. 6 Abs. 2 und 3 revDSG.

gung[17] und die Möglichkeit einer Rechtfertigung gestützt auf ein überwiegendes privates oder öffentliches Interesse, weil hierbei die Risiken für die Betroffenen abgewogen werden müssen[18]. Die Regelungen in der DSGVO stützen sich in analoger Weise auf das Risiko einer Datenbearbeitung oder das Risiko einer Verletzung der Datensicherheit für die betroffene Person. Mit anderen Worten: Fast alles im Datenschutz hängt vom Risiko ab.

[7] Bezeichnenderweise wird weder in der DSGVO noch im revidierten DSG näher definiert, was mit einem «Risiko» für die betroffene Person genau gemeint ist. Das DSG spricht vom Risiko für die «Persönlichkeit» oder (im Falle der Bearbeitung durch Bundesorgane) die «Grundrechte» der betroffenen Person. In der DSGVO ist vom Risiko «für die Rechte und Freiheiten natürlicher Personen» die Rede. Was dies in der Praxis genau heisst, wird selbst in der wissenschaftlichen Literatur kaum systematisch dargelegt; auch die Datenschutzbehörden äussern sich dazu kaum.[19] Der in verschiedenen Artikeln des DSG und der DSGVO verwendete Begriff des «hohen» Risikos wird in den Erlassen ebenfalls nicht näher definiert, abgesehen von einzelnen Artikeln, in welchen, wie beispielsweise für die Datenschutz-Folgenabschätzung, festgehalten wird, welche Situationen als Fälle von möglicherweise hohem Risiko zu behandeln sind. In der Praxis wird denn auch, wenn überhaupt, mit beispielhaften Aufzählungen gearbeitet und der Begriff des Risikos als unbeabsichtigten Nachteil oder negative Folge für die betroffene Person verstanden.[20]

2. Was meinen wir mit «Risiko»?

[8] In der Praxis zielt die Frage nach dem Risiko für die betroffene Person für die Zwecke einer Datenschutz-Folgenabschätzung somit auf die möglichen negativen Folgen ab, die eine Datenbearbeitung oder Verletzung der Datensicherheit für diese haben kann. Diese negativen Folgen können beliebiger Art sein (z.B. Rufschädigung, Blossstellung, Jobverlust, wirtschaftliche Einbussen, Gefühl der Angst oder unheimlichen Erfahrung, Diskriminierung, körperliche Folgen), doch müssen sie – aus Sicht der Datenbearbeitung – unerwünscht, d.h. nicht angestrebt sein. Zielt eine Datenbearbeitung auf die Verhaftung eines Straftäters, so ist es erwünscht, dass er festgenommen wird; die Festnahme ist nicht das Risiko, sondern der Zweck der Bearbeitung. Nicht erwünscht ist, dass die *falsche* Person festgenommen wird. Zu beurteilen ist demnach nur das Risiko aus der Warte der falsch verdächtigten Person. Datenschutzrechtlich sind selbstverständlich auch «erwünschte» oder beabsichtigte negative Auswirkungen auf eine betroffene Person zu berücksichtigen; sie können sich beispielsweise bei der Prüfung der Verhältnismässigkeit als unzulässig erweisen. Dem Begriff des «Risikos» ist es jedoch begriffsimmanent, dass er Folgen bemessen will, die eine Datenbearbeitung – zu Recht oder zu Unrecht – nicht bewirken will. Ihm steht die «Chance» gegenüber, d.h. die Wahrscheinlichkeit, dass die Datenbearbeitung das von ihr angestrebte Ziel vollumfänglich erreicht. Beide Begriffe sind wertneutral, d.h. sie sagen nichts darüber aus, ob eine negative Folge, sei es als Risiko oder Chance, gerechtfertigt ist. Klar ist im-

17 Art. 6 Abs. 6 und 7 revDSG.

18 Art. 31 revDSG.

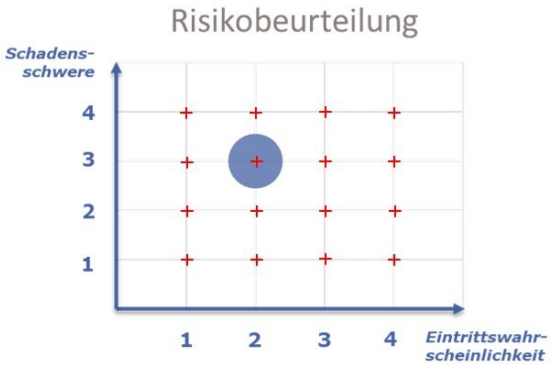
19 Eine der ganz wenigen Ausnahmen ist die jüngst veröffentlichte Liste der Beispiele zur Beurteilung von Verletzungen der Datensicherheit des Europäischen Datenschutz-Ausschusses (EDSA): Guidelines 01/2021 on Examples regarding Personal Data Breach Notification vom 14. Dezember 2021 (Version 2.0), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en.

20 Vgl. etwa David Rosenthal, Das neue Datenschutz-Gesetz, in: Jusletter 16. November 2020, Rz. 162.

merhin, dass negative Folgen, die nicht angestrebt werden, zu vermeiden sind. Darum sind sie es, die im Rahmen einer Datenschutz-Folgenabschätzung zu prüfen sind, weil diese dazu dienen, sie zu minimieren. Es sollte auch beachtet werden, dass die Frage, was eine «negative» Auswirkung bzw. ein «Nachteil» ist (ob von der Datenbearbeitung bzw. dem Verantwortlichen angestrebt oder nicht), immer von der Warte der betroffenen Person und nicht des Verantwortlichen beantwortet wird. Das gilt auch für die Frage, wie gewichtig der Nachteil ist. Er wird in der Risikobeurteilung im Rahmen der Schwere des möglichen Schadens ausgedrückt (siehe sogleich).

[9] Wird eine Risikobeurteilung hingegen zwecks Beurteilung der Meldepflicht einer Verletzung der Datensicherheit vorgenommen, ist der Blickwinkel wiederum ein etwas anderer: Negative Folgen sind hier nicht erwünscht, doch liegt der Fokus «nur» auf jenen Nachteilen, die mutmassliche Folge der zur Diskussion stehenden Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit der Personendaten sind.

[10] Nachteile (sog. *Harms*) können durch verschiedenste Gründe verursacht werden, so z.B. Missbräuche durch interne und externe Stellen, Ausfälle von Systemen, Fehlfunktionen, Verwechslungen oder Ungenauigkeiten. Es sind dies Bedrohungen bzw. Gefahren (sog. *Threats*). Threats können sich wiederum dort verwirklichen (d.h. zu den Nachteilen für die betroffenen Personen führen, den *Harms*), wo eine Datenbearbeitung ungeachtet aller Massnahmen noch Schutzlücken oder -schwächen aufweist, z.B. weil Verwechslungen nicht erkannt werden, Ausfälle nicht überbrückt oder unbefugte interne oder externe Zugriffe nicht verhindert werden können (Verwundbarkeiten, sog. *Vulnerabilities*). Der Begriff des Risikos (*Risk*) greift dies auf und sagt aus, wie wahrscheinlich welcher Schaden in Anbetracht der bestehenden Bedrohungen und Verwundbarkeiten ist. Dargestellt wird ein «Risiko» in der Wissenschaft und Praxis üblicherweise als das Ergebnis der Schwere des möglichen Schadens (*severity*) multipliziert mit dessen Eintrittswahrscheinlichkeit (*probability*). Dies lässt sich mit einer entsprechenden Matrix darstellen:



[11] Die Scheibe stellt das im konkreten Fall gewählte Risiko dar. Das Risiko liegt in diesem Fall numerisch bei 6 auf einer Skala von 1 bis 16, hier bei 6. Es kann eine feinere Aufteilung verwendet werden, aber es hat sich in der Praxis bewährt, mit Skalen mit geraden Zahlen zu arbeiten, um der unbewussten Tendenz menschlicher Beurteiler zur Mitte entgegenzuwirken; so muss entschieden werden, ob es über oder unter der Mitte liegt.

3. Das Experiment: Spontane Risikobeurteilung

[12] Das Experiment wurde in Form einer Befragung an einem Workshop des VUD im Sommer 2021 durchgeführt, an welcher etwas über 50 Vertreter der Mitgliedsunternehmen teilnahmen. Bei diesen Vertretern handelt es sich jeweils um jene Personen, die in den Unternehmen für den Datenschutz zuständig sind. Die sind es mehr oder weniger gewohnt, die Datenschutzkonformität von Datenbearbeitungen der Unternehmen zu beurteilen und die nötigen Massnahmen vorzuschlagen.

[13] Dieser Gruppe wurde über ein Dutzend Fälle aus dem Alltag eines Datenschutzbeauftragten eines Schweizer Unternehmens vorgelegt, in denen für die korrekte Anwendung des DSG oder der DSGVO die Frage des Risikos der Datenbearbeitung für die betroffenen Personen beurteilt werden muss. Es wurden einfache Fälle ausgewählt, welche zwar unterschiedliche Nachteile nach sich ziehen können, aber bezüglich des *falltypischen* Risikos eindimensional waren. Nur dieses Risiko war zu bewerten. Allgemeine Risiken der Datensicherheit waren nicht zu berücksichtigen (d.h. es war von einer bestmöglichen Datensicherheit auszugehen), ebenso nicht sonstige generische Risiken, wie sie bei jeder Datenbearbeitung bestehen können (d.h. es war über die Fallbeschreibung hinaus von einer ansonsten bestmöglichen Ausgestaltung in punkto Datenschutz auszugehen); die Praxiserfahrung zeigt, dass es selbst für Fachleute schwierig ist, die risikomindernde Wirkung bereits ergriffener Massnahmen bei der Risikoeinschätzung wegzudenken, auch wenn Datenschutz-Folgenabschätzungen häufig eine Unterscheidung zwischen Brutto- und Nettorisiko verlangen. Darum wurde darauf verzichtet.

[14] Jeder Fall wurde dem Publikum vom Moderator (dem Autor dieses Beitrags) kurz vorgestellt; es kannte die Fälle somit nicht und konnte sich auf diese auch nicht vorbereiten. Die Teilnehmer wurden daraufhin gebeten, sich den Fall kurz zu überlegen und im Anschluss über ein Online-Tool sowohl die Schwere des möglichen Schadens für die betroffene Person als auch dessen Eintrittswahrscheinlichkeit jeweils auf einer Skala von 1 bis 4 zu beurteilen. Die Skala wurde bewusst nicht in Worten umschrieben. Da nur jeweils eine Bewertung pro Fall abzugeben war, sollte das *gewichtigste* falltypische Risiko berücksichtigt werden. Ferner wurde jeder Teilnehmer aufgefordert anzugeben, an welche Art von typischen Schäden er oder sie denkt. Es wurde jeweils gewartet, bis jeweils ca. 45 oder mehr Antworten vorlagen. Das dauerte jeweils einige Minuten.

[15] Den Teilnehmern wurde bewusst nicht die Möglichkeit gegeben, methodisch vorzugehen, die Fälle zu diskutieren oder sich etwas aufzuschreiben. Auch Hilfsmittel wie Checklisten standen ihnen nicht zur Verfügung. Sie konnten über den Fall etwas nachdenken, mussten sich aber dennoch mehr oder weniger spontan entscheiden. Sie waren auf sich alleine gestellt, konnten sich also nicht an anderen orientieren oder sich beeinflussen lassen; sie mussten mit anderen Worten mehr oder weniger intuitiv gestützt auf ihre berufliche Erfahrung urteilen. Die Fälle waren bewusst nicht kompliziert, sondern Alltagssituation aus dem Datenschutz nachempfunden. Die Ergebnisse wurden erst am Ende gezeigt; die Erhebung erfolgte anonym und das Geschlecht oder andere Kriterien (z.B. Branche oder Grösse des Unternehmens) wurden nicht erfasst.

[16] Einzig beim ersten Fall erläuterte der Moderator anhand einer *eigenen* möglichen Antwort die Funktionsweise der Erhebung. Um zu prüfen, wie sehr diese Vorgabe das Publikum unbewusst in eine Richtung beeinflusste (sog. *Priming*), wurde derselbe Fall (Nr. 1) den Teilnehmern am Ende der Erhebung mit anderer Formulierung nochmals zur Beurteilung vorgelegt (Nr. 13).

4. Eine Datenbearbeitung, unterschiedlich beurteilt

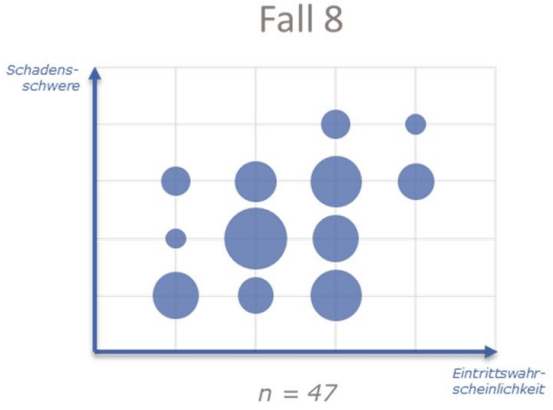
[17] Die Ergebnisse der Umfrage mit der jeweiligen Fallkonstellation und der Beurteilung des Risikos und der typischen Schäden für jeden der 15 Fälle finden sich im Anhang. Für jeden Fall wurde ausgewertet, für welches Risiko wieviele Personen stimmten und dies grafisch mittels unterschiedlich grosser Scheiben dargestellt. Es wurde dabei differenziert, wie ein bestimmter Risikowert zustande kam (2 x 3 v. 3 x 2). Verwendet wurde dabei die obige Risikomatrix. Die Grösse der Scheiben zeigt den Anteil an Stimmen, nicht den absoluten Wert; die absoluten Werte sind im Anhang aufgeführt.

[18] Ein erstes Ergebnis der Umfrage ist, dass sich die Gruppe mit Ausnahme von zwei Fällen nie wirklich einig war, wie das falltypische Risiko für die betroffenen Personen spontan einzuschätzen ist. Die spontanen Antworten zeigten praktisch immer eine signifikante Streuung: Die Einschätzungen verteilten sich auf jeweils mehr als die Hälfte der 16 möglichen Risikokombinationen, oft sogar auf mehr als drei Viertel. Bei den zwei erwähnten Ausnahmen (Nr. 3.1 und 5) waren sich jeweils nicht ganz die Hälfte der Befragten einig, wie der Fall einzustufen ist, was sich im ersten Fall dadurch erklären lässt, da es sich um eine offenkundig harmlose, relativ alltägliche Datenbearbeitung handelte, während dies der zweite Fall jedenfalls auf den ersten Blick nicht ist – es ging um die Überwachung von Arbeitnehmern (dazu hinten). Etliche, teils deutliche «Abweichler» gab es allerdings auch hier. In allen anderen Fällen lag die Einigkeit bei maximal einem Drittel der Teilnehmer, oft tiefer; nur die grobe Tendenz war jeweils klar – ist es ein eher heikler oder weniger heikler Fall. Es deutet also alles darauf hin, dass es beim Bauchgefühl im Datenschutz selbst im Kreis von Personen, die beruflich damit zu tun haben, keine Einheit, ja nicht einmal Mehrheiten gibt.

[19] Vorgelegt wurde den Teilnehmern beispielsweise folgender Fall (Nr. 8):

> «*Eine Beraterfirma will ein Computerprogramm verwenden, das von jeder Stellenbewerbung eines Beraters einen Erfolgsscore aufgrund seines bisherigen Werdegangs und seiner Noten berechnet. Der Score basiert auf den bisherigen Erfahrungen des Unternehmens mit vergangenen Einstellungen. Der Score dient nur der Information des Hiring-Partners. Es wird niemand automatisch aussortiert.*»

[20] Das Risiko von unerwünschten falltypischen Nachteilen für Stellenbewerber wurde spontan wie folgt eingeschätzt:



[21] Zwar nahmen nur (aber immerhin) 3 der 47 befragten Personen an, dass die beschriebene Datenbearbeitung Schäden der schwersten Kategorie verursachen kann. Auch ging kaum jemand davon aus, dass Schäden mit höchster Wahrscheinlichkeit zu erwarten sind. Bezüglich der Schwere der möglichen unerwünschten negativen Folgen waren sich die Teilnehmer aber nicht einig: 15 gaben Stufe 3 von 4 an, weitere 15 plädierten für Stufe 2 von 4 und 14 beurteilten die Schadensschwere mit einer 1, also der tiefen Kategorie. Immerhin zeigt die Befragung, dass über die gesamte Gruppe betrachtet, bei diesem Fall maximal von einem mittleren Risiko auszugehen ist.

[22] Als für diesen Fall typische Schäden gaben die Befragten in qualitativer Hinsicht «Diskriminierung», «Nichtberücksichtigung», «Aussortierung», «Absage», «wirtschaftliche Nachteile», «schwierige Stellensuche», «keinen», «Vermögensschaden», «Unzulässiges Profiling», «Stelle nicht erhalten», «non-hiring», «Nichteinstellung» und «negative Vorselektion» an. Die Antworten vermitteln eine weitere Erkenntnis: Wird nach den Risiken einer Datenbearbeitung gefragt, werden selbst Personen, die beruflich mit dem Datenschutz zu tun haben, spontan an sehr unterschiedliche Schäden oder relevante negativen Folgen einer Datenbearbeitung denken. Hingegen wurden rein unternehmensspezifische Risiken nur selten genannt; das zeigt, dass es sich bei den Befragten um Fachleute handelt, die (richtigerweise) zwischen Folgen für die betroffene Person und das Unternehmen differenzieren. Umso wertvoller sind ihre Risikobeurteilungen.

[23] Es fällt auch auf, dass teilweise nicht zwischen dem, was vorstehend als erwünschte und unerwünschte Folgen differenziert wird. Dies ist aus Sicht des Datenschutzes zwar erforderlich, nicht unproblematisch, denn es erfordert wiederum eine Bewertung und bringt damit einen weiteren subjektiven Faktor ins Spiel. Im Fallbeispiel ist die Selektion der Bewerber ein erwünschtes Ziel, d.h. es liegt in der Natur der Sache, dass bestimmte Bewerber aussortiert werden, da nur eine Person eingestellt werden kann. Unerwünscht ist hingegen nach herrschender Auffassung eine Diskriminierung von Bewerbern, d.h. das Treffen ungerechtfertigter Unterscheidungen zwischen den einzelnen Bewerber. Die Antworten lassen darauf schliessen, dass spontan getroffene Risikobeurteilungen auch dadurch beeinflusst werden, dass nicht zwischen relevanten und nicht relevanten Risiken unterschieden wird. Diese Differenzierung ist für die Qualität der Entscheide jedoch zentral.

[24] Trotz der Bandbreite der spontanen Antworten über das falltypische Schadenspotenzial für eine betroffene Person und die Eintrittswahrscheinlichkeit dieses Schadens, gibt die Beurteilung der Fälle «aus dem Bauch» interessante Einblicke:

- Selbst wo Unbefugte durch Hacking an sensible Personendaten (z.B. zur Gesundheit) gelangen und klar ist, dass sie diese irgendwie verwerten möchten, wird dies nicht als sehr hohes Risiko für die einzelnen Betroffenen erachtet (Fall Nr. 1 und 13).
- Die Weitergabe von Kundendaten im Rahmen einer M&A-Transaktion halten viele spontan für unkritisch (Nr. 2).
- Im Betrieb versteckt genutzte Kameras werden hingegen selbst dann als hohes Risiko betrachtet, wenn sie sehr gezielt, zeitlich und personell begrenzt zur Überführung eines erwiesenermassen aktiven Diebs benutzt werden (Nr. 4). Anders das systematische Tracking von Firmenfahrzeugen: wird es deshalb als unproblematisch betrachtet, weil die Benutzer es im Falle von Privatfahrten ausschalten können (Nr. 5)?
- Ein rein firmeninterner und zeitlicher Data Breach von Kader-Lohndaten wird von manchen immerhin als mittelschweres Risiko eingestuft, auch wenn es keine Hinweise auf einen Zugriff durch unberechtigte Personen gibt (Nr. 6).

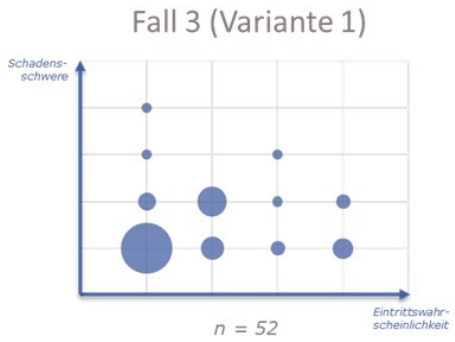
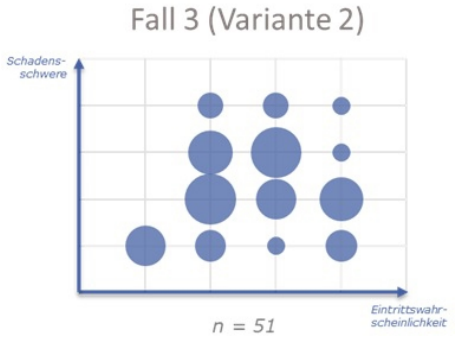
- Durch eine Bank in grösserer Zahl falsch versendete Kontoauszüge können die Befragten partout nicht richtig einordnen, möglicherweise weil sie unsicher sind, ob die Empfänger damit Missbrauch betreiben werden; den potenziellen Schaden schätzen sie aber als eher hoch ein (Nr. 7).
- Selbst bei Datenbearbeitungen zu nicht personenbezogenen Zwecken mit sehr beschränkter Aufbewahrungsfrist sind sich die Teilnehmer nicht wirklich einig, ob das wirklich kein besonderes Risiko darstellt (Nr. 9).
- Gleiches gilt beim Fahrzeughersteller, der alles, was in einem Auto seiner Kunden gesprochen wird, in seiner Cloud auswertet; manche halten es für unproblematisch (Nr. 10).
- Die Kreditprüfung ist im Gesetz zwar als überwiegendes Interesse vorgesehen, wenn aber ein Online-Shop-Betreiber hierbei eigene Wege geht, um den «Score» anhand ihm bereits vorliegender Daten zu berechnen, dann finden die Gruppe das besonders heikel (Nr. 11a); noch viel problematischer fänden sie es aber, wenn er personalisierte Preise berechnen würde (Nr. 11b).
- Offenbar kein Vertrauen haben die Teilnehmer in den Telefonhersteller, der seine Handies automatisch nach Kinderpornographie scannt und nötigenfalls die Polizei benachrichtigt (Nr. 12).

[25] Fazit dieser Fälle: Bei weit verbreiteten Datenbearbeitungen mit mutmasslich geringem Risiko findet sich die grösste Übereinstimmung im Publikum. Die Streuung wird insbesondere dort breit, wo sich in einem Fall das Risiko dadurch ergibt, dass eine in die Datenbearbeitung involvierte Person missbräuchlich agiert; hier zeigen die Antworten, dass oft nur geraten werden kann.

[26] Auch wenn diese Entscheide aus dem Bauch erfolgten, so können sie wichtige Hinweise liefern. Nach allem, was wir wissen, wird auch das breite Publikum so darüber urteilen, ob eine Datenbearbeitung richtig oder falsch ist. Dasselbe ist von den Entscheidern in den Aufsichtsbehörden und Gerichten zu erwarten, wobei separat zu prüfen wäre, ob sie nicht eine rollen- oder berufsbedingte Tendenz zu einer strengeren Beurteilung aufweisen als das «sorglosere» breite Publikum.

5. Selbstbestimmung macht den Unterschied

[27] Eine weitere Erkenntnis liefern die Antworten zu Fall 3. Er handelt von einer Standardsituation im Alltag: Ein Online-Shop ermittelt die Vorlieben seiner Kunden, um diese Informationen für personalisierte Werbung zu verwenden. Der Fall wurde in zwei Varianten abgefragt. In der ersten Variante wurde dem Publikum mitgeteilt, dass der Online-Shop über die Einwilligung der Kunden verfügt, während dies in der zweiten Variante nicht der Fall war. In der zweiten Variante waren Personen nicht informiert, in der ersten waren sie es aufgrund der Einwilligung. Die Beurteilung des Publikums fiel für die beiden Varianten völlig unterschiedlich aus:

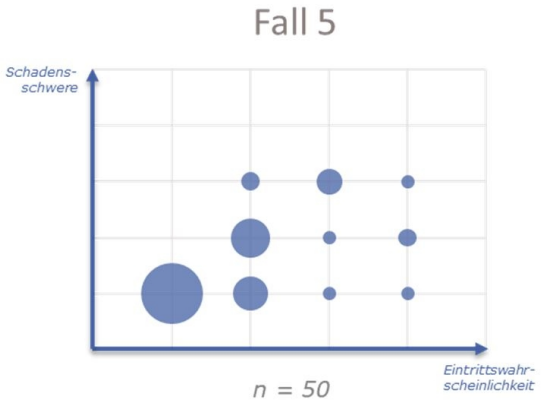
Fall 3 (Variante 1)	**Fall 3 (Variante 2)**
«Ein Unternehmen erhebt beim Verkauf von Waren in einem Online-Shop Kontaktdaten und Angaben über Warenkäufe. Es kann aufgrund dieser Angaben Vorlieben seiner Kunden ermitteln. Es will dieses Wissen verwenden, um den einzelnen Kunden auf ihre jeweiligen Vorlieben zugeschnittene Angebote zukommen lassen.»	
«Er hat die Einwilligung des Kunden»	«Er hat keine Einwilligung der Kunden und informiert sie nicht.»
	
Als typischer Schaden wurde genannt: Persönlichkeitsverletzung; Beeinflussung Kaufverhalten; keiner, da Einwilligung; Kundenbeeinflussung; Data Breach; Spam; Adresse an Dritte; Persönlichkeitsprofil; Profilingdaten-Diebstahl; falsches Profiling	Als typischer Schaden wurde genannt: Persönlichkeitsprofil; ungewolltes Profiling; Kappung Selbstbestimmung; Manipulation; Steuerung Konsumverhalten; Preisanpassungen; Kontrollverlust

[28] In beiden Fällen ist die Datenbearbeitung dieselbe. Trotzdem wurde sie vom Publikum im Hinblick auf das durch sie verursachte Risiko der betroffenen Person völlig unterschiedlich beurteilt. Dies erstaunt insofern, als dass eine Einwilligung der betroffenen Person an den möglichen unerwünschten Folgen einer Datenbearbeitung auf den ersten Blick nichts ändert. Auf den zweiten Blick lässt sich die unterschiedliche Beurteilung dadurch erklären, dass der durch die mangelnde Transparenz und das Nicht-Einholen einer Einwilligung in Variante 2 bewirkte Verlust des Selbstbestimmungsrechts per se als sehr gewichtiges Risiko gewertet wird, auch wenn sich am Verhalten des Online-Shops in beiden Fällen nichts ändert.

[29] Umgekehrt kann aus diesem Fall auch abgeleitet werden, dass die meisten Personen spontan die Meinung vertreten, dass sich eine hinsichtlich ihres Risikos für die Betroffenen als kritisch beurteilte Datenbearbeitung dadurch wirksam entschärft werden kann, dass vorgängig die Einwilligung der Betroffenen eingeholt wird. Allerdings wirft auch dies spannende Fragen auf: Das Vorliegen einer Einwilligung kann zwar das Risiko mangelnder Selbstbestimmung kompensieren, aber andere unerwünschte Folgen kann eine Datenbearbeitung für eine betroffene Person trotzdem noch haben. Auch in Variante 1 kam ein nicht irrelevanter Anteil der Teilnehmer Schluss,

dass selbst eine solch alltägliche Datenbearbeitung wie im Fall 3 beschrieben noch gewisse Risiken mit sich bringt: 20 der 52 Experten gingen bei Variante 1 von einem Risiko von 4 oder höher aus (38%), während 24 es mit Einwilligung als minimal (1) einschätzten (46%).

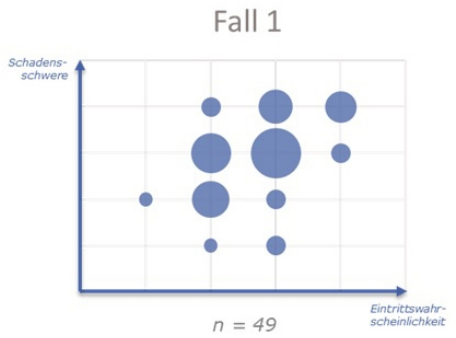
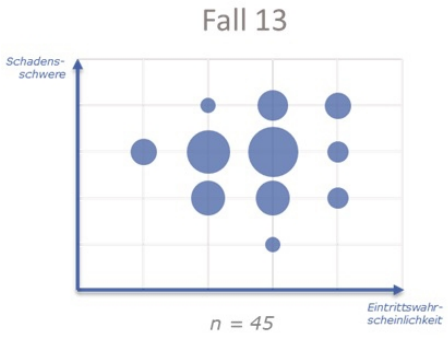
[30] Trotzdem scheint der Faktor *Selbstbestimmung der Betroffenen* aus Sicht vieler Befragten sich stark risikomindernd auszuwirken bzw. sollte so gewertet werden: Im Fall Nr. 5, wo es um die Überwachung von Arbeitnehmern durch das Tracking ihrer auch privat nutzbaren Geschäftsfahrzeuge geht (bei welchem auch ihre Fahrweise für präventive Wartungszwecke ausgewertet wurde), sahen 46 Prozent kein nennenswertes Risiko; weitere 20 Prozent erachteten das Risiko als etwas erhöht, den potenziellen Schaden aber trotzdem nur auf Stufe 1 von 4. Im Fall Nr. 5 wurde laut Fallbeschreibung nicht einmal eine Einwilligung eingeholt, sondern es wurde nur (aber immerhin) die Möglichkeit geboten, das Tracking für Privatfahrten auszuschalten (sog. *opt-out*):



6. Die Beurteilungen ändern sich

[31] In der Umfrage wurde auch geprüft, wie stabil die spontane Einschätzung des Risikos einer bestimmten Fallkonstellation ist, indem zwei Mal derselbe Fall präsentiert wurde (Fall 1 und 13). Hier ging es um das durch einen Data Breach verursachte Risiko. Dasselbe Publikum schätzte den Fall wie folgt ein:

Fall 1	**Fall 13**
«Ein Versicherungsbroker wird Opfer eines Ransomware-Angriffs. Die Dossiers seiner Kunden fallen in die Hände des Angreifers, der mit Veröffentlichung droht. Der Broker will kein Lösegeld bezahlen. Die Dossiers enthalten alle Angaben der Kunden, die Versicherungen für den Abschluss von Policen brauchen (z.B. Hausratsinventare, Fragebögen über frühere Schäden, Angaben zur Gesundheit).»	«Ein untreuer Mitarbeiter einer Versicherungsgesellschaft stiehlt die Dossiers von Versicherungsanträgen und erpresst inkognito die Gesellschaft mit der Veröffentlichung im Darknet, falls sie ihn nicht bezahlt. Diese will sich jedoch nicht darauf einlassen. In den Anträgen sind Angaben über die Gesundheit enthalten, über frühere Schäden aber auch Inventare des Hausrats.»

Fall 1	Fall 13
	

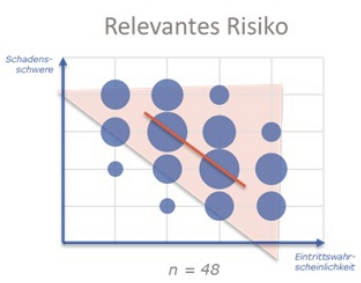
[32] Trotz der unterschiedlich formulierten, aber materiell selben Ausgangslage wurde das durch die Verletzung der Datensicherheit verursachte Risiko von derselben Gruppe als unterschiedlich erachtet, wenn auch nicht massiv unterschiedlich. Im Fall 1 kam wie erwähnt hinzu, dass der Moderator sich vor dem Publikum beispielhaft für eine Einstufung 3 x 3 aussprach. Im Fall 13 sagte er nichts. Im Fall 1 folgten 26.5% des Publikums der Einstufung des Moderators und 28.8% war strenger (d.h. kam zu einem höheren Risiko). Im Fall 13 schätzen noch 24.4% das Risiko auf 3 x 3 ein und nur noch 20% war strenger in ihrer Beurteilung des Risikos. Das Risiko wurde beim zweiten Durchlauf des gleichen Falls also deutlich geringer eingestuft als zu Beginn. Ob diese Differenz auf den fehlenden Hinweis des Moderators im ersten Fall zurückzuführen ist, auf die Zufälligkeit der Einschätzung eines jeden Beurteilers oder auf andere Ursachen, bleibt offen. Klar ist jedoch: Die Streuung der Einschätzung ist in beiden Fällen erneut deutlich.

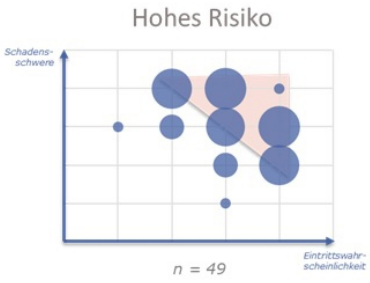
7. Was ist ein relevantes, was ein hohes Risiko?

[33] Für den Einsatz in der Datenschutz-Compliance ist es nicht nur erforderlich, das Risiko einer Datenbearbeitung oder Verletzung der Datensicherheit einzuschätzen. Es muss auch entschieden werden, ob ein «hohes» Risiko im Sinne des Gesetzgebers vorliegt. Das revidierte DSG stellt in verschiedenen Bestimmungen, so insbesondere im Rahmen der Datenschutz-Folgenabschätzung und betreffend die Meldepflicht von Data Breaches, auf dieses Kriterium ab; unter der DSGVO löst allerdings bereits jedes relevante Risiko eine Meldepflicht aus.

[34] Darum wurden die Teilnehmer auch befragt, ab welchem Risikowert (1–16) sie von einem für den Datenschutz relevanten Risiko und ab welchem Wert sie von einem «hohen» Risiko im Sinne des DSG bzw. der DSGVO ausgehen.

Hier die Antworten:





[35] Feststellen liess sich nur eine Tendenz, keine klare Antwort. Bei der Fragestellung des datenschutzrechtlich «relevanten» Risikos spricht sich die grösste Gruppe (13 Stimmen) für ein relevantes Risiko ab dem Wert 6 aus (auf einer Skala von 1-4 x 1-4, d.h. von 1-16). Das sind die zwei grossen Scheiben in der Mitte. Zwei ungefähr gleich grosse Gruppen erachten ein Risiko bereits ab einem Wert von 3 oder 4 (7+7) bzw. erst ab 8 oder 9 (8+8) als relevant, sind also strenger oder milder als die grösste Gruppe.

[36] Beim «hohen» Risiko ist die Situation ein wenig deutlicher: Hier geht eine Mehrheit davon aus, dass dieses ab einem Wert von 8 oder 9 (14+13) gegeben ist. In beiden Fällen zeigt die Erhebung allerdings, dass es Argumentationsspielraum gibt: Es kann mit guten Gründen vertreten werden, dass ein hohes Risiko erst vorliegt, wenn 12 Punkte oder mehr Punkte vorliegen. Umgekehrt kann vertreten werden, dass ein datenschutzrechtlich relevantes Risiko bereits ab 3 Punkten vorliegt. Wie gut sich das Argument verteidigen lässt, dass alle Risiken unter 8 oder 9 Punkten datenschutzrechtlich nicht relevant sind, ist hingegen fraglich, auch wenn sich immerhin mehr als ein Drittel der Gruppe dafür ausgesprochen hat.

8. Spontane Risikobeurteilungen als Lotterie?

[37] Die Erhebung macht vor allem eines deutlich: Werden datenschutzrechtliche Risikobeurteilungen spontan durchgeführt, sind sie in hohem Masse vom Zufall geprägt – selbst bei Personen mit Erfahrung in diesem Bereich. In ihrer Beurteilung «aus dem Bauch» heraus sind sie sich wie gezeigt mehrheitlich uneins.

[38] Warum dem so ist, kann das Experiment natürlich nicht beantworten. Diese Gründe werden ohnehin vielfältiger Natur sein; sie können innere und äussere Gründe sein. Die für die Umfrage verwendeten Szenarien sind beispielsweise nur grob beschrieben, weshalb die befragten Personen sich mindestens unbewusst weitere Elemente aus ihrer bisherigen Erfahrungswelt hinzudenken werden, um den ihnen präsentierten Fall besser einordnen und beurteilen zu können. Gefragt wurde zwar nur nach falltypischen Risiken, aber auch von diesen kann es mehrere geben. Je nach der bisherigen Berufs- und Lebenserfahrung werden einer Person spontan dabei unterschiedliche Dinge in den Sinn kommen. Jede Person wird zudem eigene Vorstellungen darüber haben, welche Werte – wie zum Beispiel das Selbstbestimmungsrecht, der Schutz vor Diskriminierung oder der eigene gute Ruf – ihm besonders wichtig sind und diese höher gewichten. Die Teilnehmer wurden auch gezwungen, sich auf einen Gesamtwert festzulegen und durften nicht differenziert antworten; sie mussten die einzelnen Risiken somit im Kopf gegeneinander abwägen. Selbst der Begriff des «Risikos» bzw. des Schadens wurde von den einzelnen Teilnehmern unterschiedlich verstanden; die von ihnen genannten «typischen» Schäden zeigen dies deutlich. Die in der Risikomatrix verwendete Skala ist mit 1–4 zwar klar begrenzt, unterliegt aber trotzdem gewissen Annahmen, die verschieden sein können: Für die eine Person wird ein jährliches Ereignis auf dieser Skala eine 1 sein, für einen anderen nur jene Dinge, die höchstens alle fünf bis zehn Jahre geschehen.

[39] Diese möglichen Ursachen für die scheinbare Zufälligkeit der Antworten mindert die Aussagekraft der Erhebung allerdings nicht, denn all diese Effekte können in der alltäglichen Datenschutzpraxis ebenfalls wirken, wenn Urteile spontan gefällt werden statt im Rahmen eines methodischen Ansatzes. Auch im Compliance-Alltag müssen Fälle von einzelnen Fachpersonen beurteilt werden, und zwar nicht selten ohne, dass ihnen hierzu klare Verfahren, Richtlinien oder Vergleichsfälle zur Verfügung stehen – auch bezüglich der Methodik solcher Beurteilungen. Sie

werden nicht selten zu vergleichbaren Bauchentscheiden gezwungen, die dann entsprechend unterschiedlich ausfallen. Manche werden nicht über die Erfahrung oder Fantasie verfügen, um zu wissen oder sich auszudenken, welches Ungemach eine Datenbearbeitung für eine betroffene Person mit sich bringen kann. Hinzu kommen die in der Person des Urteilenden und im Moment des Entscheids selbst liegenden persönlichen Faktoren wie Wertvorstellungen, Gemütszustand oder persönliche Erlebnisse, welche seine Urteile unbewusst beeinflussen werden.

[40] Die Zufälligkeit solcher prädiktiver Urteile ist allerdings keine überraschende Erkenntnis und nicht nur im Datenschutz anzutreffen. Das Phänomen ist für andere Branchen bereits eingehend untersucht und in der Wissenschaft gut bekannt, wobei sie selbst dort anzutreffen sind, wo erfahrenen Experten die nötige Zeit gewährt wird, eingehende Entscheide zu treffen.[21] Insofern bestätigt das vorliegende Experiment nur, was im Grunde zu erwarten – oder zu befürchten – war. Etwas überraschend ist immerhin, dass trotz der vergleichsweise grossen Zahl an Personen (44–52 Personen) sich bei keinem der Fälle eine Mehrheit für eine bestimmte Risikokombination fand. Einzig in den zwei genannten Fällen (Nr. 3.1 und 5) kam die Gruppe überhaupt erst in die Nähe der 50 Prozent Übereinstimmung, obwohl die Zahl der Risikokombinationen mit 4 x 4 vergleichsweise tief ist.

9. Schlussfolgerung: Zufall erwarten und bekämpfen

[41] Negativ formuliert könnte das Fazit lauten, dass spontanen Risikobeurteilungen nicht vertraut werden sollte, selbst wenn sie von Fachleuten abgegeben werden, da sie in hohem Masse vom Zufall geprägt sind. Positiv formuliert könnte hingegen gefolgert werden, dass die Vorstellung, dass es nur die eine objektiv «richtige» Risikobeurteilung einer Datenbearbeitung schlicht nicht gibt. Eine Risikobeurteilung ist immer eine Prognose der Zukunft, und die Zukunft kennt keiner.

[42] Es stellt sich mithin die Frage, ob die ermittelte Streuung der Ansichten zum Risiko tatsächlich nur das Ergebnis der Spontaneität der Beurteilungen ist oder ob sie einer Risikobeurteilung immanent ist, gerade weil keiner die Zukunft vorhersagen kann. Das würde wiederum bedeuten, dass solche Einschätzungen letztlich grundsätzlich Zufallsergebnisse sind, selbst wenn sie von den besten Experten durchgeführt werden. Das würde das Instrument der Risikobeurteilung – eine fundamentale Säule des Datenschutzes – grundsätzlich in Frage stellen. Sind wir also auf dem Holzweg damit? Machen wir uns nur etwas vor, wenn wir glauben, das Risiko einer Datenbearbeitung korrekt einschätzen zu können?

[43] Nein. Die Erwartung, dass es nur eine richtige Prognose gibt, ist schon im Ansatz falsch, weil sie davon ausgeht, *dass* wir die Zukunft vorhersagen können. Sie ist letztlich nur aber immerhin ein Hilfsmittel, um unsere Anstrengungen zum Schutz von Personendaten zu priorisieren. Die Alternative wäre das Giesskannenprinzip. Wie unsinnig dieses im Datenschutz ist, sagt uns nicht nur der gesunde Menschenverstand, sondern auch die praktische Erfahrung – etwa im Bereich der Vorgaben der DSGVO für Datenschutzerklärungen, die heute niemand mehr liest, gerade weil der Gesetzgeber hier auf eine Differenzierung verzichtet hat. Wenn wir also den Ansatz des risikobasierten Datenschutzes (zurecht) nicht aufgeben wollen, wir die Zukunft aber nicht vorhersagen

21 Vgl. zum Ganzen, m.w.H., Daniel Kahneman, Olivier Sibony, Cass R. Sunstein, Noise – Was unsere Entscheidungen verzerrt – und wie wir sie verbessern können, München, 2021.

können, müssen wir uns damit abfinden, dass wir ohne Prognosen nicht auskommen. Prognosen bieten eine Orientierungshilfe, an welcher wir unsere Massnahmen festzurren können, sind aber naturgemäss unsicher. Ohne Orientierungshilfe gibt es keine Prioritäten. Umso wichtiger ist, dass wir uns einerseits der Schwächen solcher Prognosen bewusst sind und andererseits die nötigen Vorkehrungen treffen, um diesen entgegenzuwirken. Gleichzeitig müssen wir akzeptieren, dass Prognosen eine Bandbreite aufweisen und es in der Tat nicht *die eine* richtige Vorhersage gibt. Wesentlich ist somit nicht das Ergebnis der Prognose oder ob sie eintritt, sondern dass sie sauber entsteht. Sauber bedeutet in aller Regel *methodisch*, ohne, dass es hier einen *numerus clausus* der Vorgehensweisen gibt. Dies ist insbesondere dort zu beachten, wo ein Datenschutzvorfall etwa im Rahmen eines Rechtsstreits rückblickend beurteilt wird und wir das, was wir in der Rückschau erklären können, gerne als naheliegend akzeptieren. War er nicht vorhergesagt, bedeutet das also nicht, dass die Prognose fehlerhaft war. Erfolgte die Prognose nicht methodisch oder gar nicht, liegt *darin* der Vorwurf und nicht im Ergebnis.

[44] Beurteilen wir einen Fall aus datenschutzrechtlicher Sicht, sollten wir uns ausserdem bewusst sein, dass das Ergebnis in erheblichem Masse von unseren *Wertungen* und anderen persönlichen Faktoren abhängt. Diese Wertungen wiederum sind subjektiv und können beinahe beliebig ausfallen – nachvollziehbar begründen lässt sich fast alles. Wir müssen daher davon ausgehen, dass datenschutzrechtliche Risikobeurteilungen in der Praxis nicht nur dann stark vom Zufall geprägt sind, wenn sie spontan erfolgen, sondern auch wohlüberlegt – gerade weil sie das Ergebnis eines Vorgangs der Wertung ist: Wie gewichtig wird eine bestimmte Folge als Schaden empfunden? Wie häufig ist mit welchem Schaden zu rechnen? Bei dieser zweiten Frage könnten im Prinzip objektive Erfahrungswerte vorliegen, doch ist dies in der Praxis so gut wie nie der Fall. Zudem bietet auch Erfahrungswissen seine Tücken: Wenn wir uns nur nach unserer Erfahrung ausrichten, treffen wir unsere Massnahmen für die Vergangenheit. Der Schaden, der einer betroffenen Person im nächsten Monat wiederfährt, bleibt unbedacht, weil es ihn bisher nie gab und wir zu wenig Fantasie, Mut oder Sorge hatten, um an ihn zu denken.

[45] Sind wir uns dessen bewusst, können wir diesem Umstand ebenfalls entgegenwirken. So lassen sich die Verrauschungen und Verzerrungen in der Beurteilung, wie sie das Experiment bei spontanen Entscheiden aufgezeigt hat, durch entsprechende Massnahmen erfahrungsgemäss massiv reduzieren.

10. Massnahmen für bessere Risikobeurteilungen

[46] Um Risikobeurteilungen sauber durchzuführen, sollten wir uns zunächst darauf einigen, dabei *methodisch* vorzugehen, d.h. den Entscheid nach einer bestimmten Struktur und Vorgehensweise herbeiführen. Diese sollten wir vorgängig festlegen, zum Beispiel in Form einer Checkliste, eines Templates für Datenschutz-Folgenabschätzungen mit vorbereiteten Fragen oder auch einer etwas komplexeren Berechnungsmethode.[22] Die Methode muss nicht «perfekt» sein, sondern verhindern, dass wir primär auf unseren «Bauch» hören. Auch hier wissen wir: Wir entscheiden sauberer, wenn wir nach zuvor von uns festgelegten Regeln urteilen, auch wenn diese Regeln einfach und lückenhaft sind.

22 Vgl. etwa das Beispiel des Autors für die Beurteilung des Risikos eines ausländischen Behördenzugriffs unter https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx.

[47] Im Rahmen der Methode sollten wir uns bewusst werden, *welches* Risiko wir beurteilen wollen. Einige Ausführungen dazu finden sich weiter vorne. Es ist wichtig, dass für die Beurteilung irrelevante negative Folgen als solche erkannt und ausgeblendet werden. Das Experiment hat gezeigt, dass dies bei einer spontanen Beurteilung mitunter nicht geschieht.

[48] Weiter sind die getroffenen Massnahmen zur Begrenzung oder Verhinderung von Risiko möglichst einfach zu berücksichtigen. In einer Datenschutz-Folgenabschätzung (**DSFA**) wird häufig zwischen einem Brutto- und Nettorisiko unterschieden, also den möglichen negativen Folgen mit und ohne den Schaden mitigierenden Massnahmen. Diese Unterscheidung ist in vielen Fällen jedoch reichlich theoretisch, da ein Grundstock an Massnahmen, etwa im Bereich der Datensicherheit, in der Praxis immer gegeben sein werden. Gleichzeitig erschwert eine solche theoretische Konstruktion die Einschätzung des Risikos, da eine künstliche Situation beurteilt werden muss, indem bereits getroffene Massnahmen «weggedacht» werden müssen. *Keep it simple* lautet hier das Motto für qualitativ bessere Prognosen: Zu beurteilen ist die Datenbearbeitung so, wie sie ist, mit allen bereits getroffenen Massnahmen. Diese sind zudem aufzuzählen, damit die Rahmenbedingung der Risikobeurteilung klar sind. Zeigt sich, dass bestimmte Risiken in Anbetracht dieser Massnahmen noch immer zu hoch sind, können als Ergebnis der Risikobeurteilung weitere Massnahmen vorgeschlagen werden.

[49] Eine Datenbearbeitung weist nicht einfach nur *ein* Risiko für eine betroffene Person, sondern es kennt deren viele – im Experiment wurde dies bewusst nicht berücksichtigt. Bei einer automatisierten Beurteilung von Stellenbewerbern mag das Risiko der Diskriminierung aufgrund des verwendeten Algorithmus im Vordergrund stehen, doch ist genauso denkbar, dass die Datenqualität wegen Fehlern schlecht ist, weil der Stellenbewerber bei der Dateneingabe im Bewerbungstool nicht die Gelegenheit erhält, seine Eingaben nochmals zu überprüfen. Hierbei haben wir eine Tendenz, zunächst an jene Risiken zu denken, die falltypisch sind, was im genannten Beispiel der Algorithmus und sicher nicht die fehlerhafte Datenerfassung ist, auch wenn sie gewichtiger sein mag. Für einen sauberen Beurteilungsprozess ist es daher wichtig, sich zunächst einmal aller möglichen unerwünschten Folgen bewusst zu werden, die eine Datenbearbeitung haben kann, etwa indem diese in einem ersten Schritt in einer Liste aufgezählt werden. Checklisten oder Templates im Falle von DSFA können hier helfen. Erst in einem zweiten Schritt sollten die einzelnen Risiken beurteilt werden. Diese Methode der Auftrennung des «Problems» in kleinere, leichter zu beurteilende Elemente ist ein wichtiges Instrument für saubere Beurteilungen.

[50] Hierzu gehört es auch, dass die Skalen der Risikomatrix klar definiert werden. Es sollte vor der Beurteilung der einzelnen Risiken festgelegt werden, was die einzelnen Schritte bedeuten. Hat die Risikomatrix 4 x 4 Felder, sollte definiert werden, was eine Eintrittswahrscheinlichkeit von 1, 2, 3 und 4 bedeutet, also beispielsweise:

Eintrittswahrscheinlichkeit	Rückblickend	Ausblickend
Gross / 4	Zu einem solchen Schaden kam es in den letzten sechs Monaten mindestens ein Mal	Mit einem solchen Schaden ist in den nächsten sechs Monaten zu rechnen
Substanziell / 3	Zu einem solchen Schaden kam es in den letzten zwölf Monaten mindestens ein Mal	Mit einem solchen Schaden ist in den nächsten zwölf Monaten zu rechnen
Überschaubar / 2	Zu einem solchen Schaden kam es in den letzten 2–3 Jahren mindestens ein Mal	Mit einem solchen Schaden ist in den nächsten 2–3 Jahren zu rechnen
Geringfügig / 1	Zu einem solchen Schaden kam es seltener	Mit einem solchen Schaden ist seltener zu rechnen

[51] Dasselbe gilt für die Schwere des Schadens. Hier hat sich bewährt, Beispiele aufzuführen (die nachfolgende Tabelle ist gekürzt und zeigt nur einige mögliche Nachteile auf):

Schadenskategorie	Geringfügig / 1	Überschaubar / 2	Substanziell / 3	Gross / 4
Gefahr für Leib und Leben			Gefahr einer leichten Körperverletzung	Lebensgefahr, Gefahr einer schweren Körperverletzung
Sachbeschädigung		Sachschaden von CHF 5'000 und mehr	Sachschaden an von CHF 50'000 und mehr	Sachschaden von CHF 250'000 und mehr
Geheimnisoffenbarung			Geheimnisoffenbarung hat Auswirkungen auf einen Teilbereich seines Lebens	Geheimnisoffenbarung hat Auswirkungen auf sein gesamtes Leben
Existenzgefährdung				Existenzgefährdung
Identitätsdiebstahl				Identitätsdiebstahl
Finanzieller Schaden	Weniger als ein Monatsgehalt	Ein Monatsgehalt	Mehrere Monatsgehälter	Jahresgehalt oder Verlust der gesamten persönlichen finanziellen Werte

Schadens-kategorie	Gering-fügig / 1	Über-schaubar / 2	Substan-ziell / 3	Gross / 4
Gesell-schaftliche oder wirtschaft-liche Nachteile	Keine bzw. sehr geringe Auswirkungen im täglichen Leben	Auswirkungen sind spürbar und führen zu kleinen Einschrän-kungen, Nachteilen Spürbare Auswirkungen im Amtsverkehr oder im Beruf	Auswirkungen haben Nachteile für den Betroffenen im täglichen Leben Einschränkungen im Beruf Einschrän-kungen im Verkehr mit Behörden	Auswirkungen haben grosse Nachteile auf den Betroffenen und ggf. auf sein persönliches Umfeld (z.B. Familie) Arbeitsplatz-verlust

[52] Mit einer solchen Definition ist nicht nur für den Leser klar, nach welchen Kriterien die Risiken beurteilt wurden. Sie hilft auch dem Beurteiler, das Risiko objektiver zu beurteilen, indem der Massstab vom konkreten Einzelfall entkoppelt und separat festgelegt bzw. beurteilt wird. Erweist sich das Risiko als unangemessen hoch oder tief, wird er sich überlegen müssen, ob er seinen Massstab (= Regel) anpassen muss, bevor er seinen Fall neu beurteilt (= Subsumption). Diese Auftrennung in einen Obersatz und einen Untersatz entspricht auch der in einer rechtlichen Beurteilung üblichen Vorgehensweise und hat sich bewährt.
[53] Bezüglich der obigen Beispiele ist zu beachten, dass diese für die Zwecke einer DSFA formuliert worden sind. Die Beurteilung des Risikos für betroffene Personen infolge einer Verletzung der Datensicherheit folgt nach anderen Kriterien.[23]
[54] Weitere Massnahmen können ebenfalls helfen, die Qualität von Risikobeurteilungen zu verbessern:

- **Keine Vorgaben:** Risikobewertungen sollten nicht durch die Datenschutzbeauftragten oder -experten der Unternehmen erfolgen, sondern durch das «Business», also den Prozesseigner. Dies entspricht auch dem Grundsatz des «Three Lines of Defense» Compliance-Modells, in welchem die Experten als *Second Line* die *First Line* nur beraten. Die First Line ist es auch, die den Risikoentscheid fällen und seine Konsequenzen tragen muss. Das sieht auch der Gesetzgeber so vor: Eine DSFA ist ebenfalls nicht vom Datenschutzbeauftragten durchzuführen, sondern von ihm lediglich zu kommentieren. Die Aufgabe des Datenschutzexperten (oder auch der Compliance-Stelle) sollte es jedoch sein, das Business so zu führen, dass es eine möglichst saubere Entscheidung zum richtigen Risiko[24] trifft, ohne sie dabei zu beeinflussen (wie dies im Experiment beim ersten Fall bewusst geschah). Gibt der Datenschutzbeauftragte seine Einschätzung zu Beginn preis, wird diese gerne einfach übernommen werden – jedenfalls soweit sie dem Interesse des Business entspricht. Das ist nicht das Ziel.

23 Vgl. dazu FN 19.

24 Also dem Risiko für die betroffene Person, und nicht dem Risiko für das Unternehmen, sowie bezüglich der Unterscheidung zwischen Brutto- und Nettorisiko, also vor und nach den Massnahmen zur Risikominderung.

- **Etablierung einer Fallpraxis:** Ein Datenschutzexperte muss in seiner Praxis immer wieder Fälle beurteilen. Hier hat sich gezeigt, dass uns die relative Beurteilung sehr viel leichter fällt als eine absolute Beurteilung. Muss ein bestimmtes Risiko einer Datenbearbeitung eingeschätzt werden, so fällt uns dies leichter, wenn wir das in Bezug auf einen anderen Fall tun können, den wir bereits eingeschätzt haben – also beurteilen, ob der neue Fall ein höheres oder geringeres spezifisches Risiko mit sich bringt als der bereits beurteilte Fall. Diesen Umstand können wir uns zunutze machen, indem wir uns mit bisherigen Beurteilungen eine Fallpraxis zur Orientierungshilfe aufbauen. Sie sorgt auch für mehr Konstanz in unseren Beurteilungen.
- **Berücksichtigung tatsächlicher Entwicklungen:** Kommt es aufgrund von Datenbearbeitungen zu Schäden, so sollten wir uns mit diesen auseinandersetzen und vor diesem Hintergrund früheren Risikobeurteilungen nachträglich daraufhin prüfen, ob und wie wir das sich verwirklichte Risiko als solches erkannt hatten. Dies hilft uns, von unseren Fehleinschätzungen zu lernen und die Fallpraxis um konkrete Erfahrungswerte zu ergänzen.
- **Die Gruppe weiss es besser:** Das Experiment des VUD lässt zwar vermuten, dass eine Beurteilung in der Gruppe nicht zwangsläufig zu klareren Ergebnissen führt. Wird dieselbe Beurteilung methodisch und von mehreren Personen getroffen, reduziert sich der Einfluss der Verrauschung und Verzerrung der Urteile des Einzelnen jedoch automatisch. Ergebnisse einer Gruppe von Beurteiler weisen daher eine grundsätzlich höhere Qualität auf, vorausgesetzt auch die Urteilsfindung in der Gruppe erfolgt nach einem bestimmten Schema, welches Störfaktoren minimiert. Dazu gehört beispielsweise, dass jeder Teilnehmer zunächst die Möglichkeit haben sollte, seine Bewertung von den anderen unbeeinflusst abzugeben, bevor über diese diskutiert wird.

[55] Es ist weiter darauf zu achten, dass eine Risikobeurteilung eine Momentaufnahme ist. Sie ist daher in ihrer «Gültigkeit» zeitlich zu begrenzen, d.h. in entsprechenden Abständen zu wiederholen. Das gilt nicht nur dann, wenn eine Datenbearbeitung tatsächlich zu unerwünschten Folgen führt, sondern auch ohne besonderen Anlass. DSFA sollten daher immer dann erneuert werden, wenn sich wesentliche Umstände ändern sowie beim Ausbleiben von augenfälligen Änderungen alle drei Jahre, wie eine Faustregel besagt.
[56] Wichtig ist schliesslich, dass Risikobeurteilungen schriftlich festgehalten werden. Eine Begründung der einzelnen Bewertungen wird nicht immer möglich sein. Mindestens aber die unerwünschte Folge, die beurteilt wird, sollte nachvollziehbar beschrieben sein, allenfalls auch die Umstände, welche nach Ansicht der Urteiler zu dieser Folge führen können und die Massnahmen, die dies verhindern oder mildern sollen. Die schriftliche Dokumentation einer DSFA ist in ihrer Wirkung nicht zu unterschätzen: Sie erschwert zum einen spontane Entscheide. Ist eine Beurteilung einmal zu Papier gebracht und nachvollziehbar, hat dies zum anderen einen entsprechenden Effekt auf den Leser. Es wird ihm erfahrungsgemäss schwerer fallen, zu einem anderen Ergebnis zu kommen. Wer daher einer Behörde seine Datenbearbeitung vorlegen will oder muss, sollte selbst eine DSFA durchführen. Damit wirkt er der Zufälligkeit der Beurteilung durch diese entgegen.

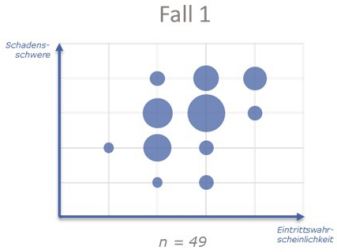
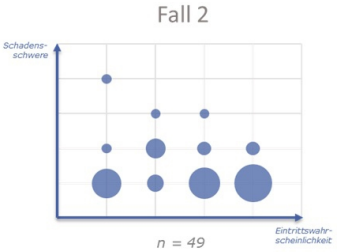
11. Kein Grund zur Beunruhigung

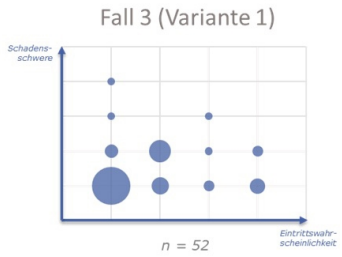
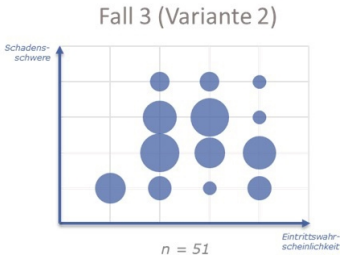
[57] Wer all diese Vorkehrungen treffen will, wird sich für eine Risikobeurteilung entsprechend Zeit nehmen und einräumen lassen müssen. Auch darum kann es sinnvoll sein, sie von der *First Line* vornehmen zu lassen, damit sie – sobald sie selbst in der Pflicht ist – realisiert, dass die Frage nach dem Risiko womöglich um einiges komplexer ist, als sie sich das vorstellt.
[58] Unter dem revidierten DSG sind solche Risikobeurteilungen in zwei Fällen im Gesetz sogar zwingend vorgesehen: Sie bilden einerseits den Kern einer jeden DSFA[25] und anderseits sind sie im Falle einer Verletzung der Datensicherheit erforderlich, um die Meldepflicht zu beurteilen[26]. Es ist davon auszugehen, dass sie jeweils dokumentiert werden müssen. Allerdings sieht das revidierte DSG weder für den einen noch den anderen Fall eine Busse im Falle Nichtbefolgung vor. Wer also das Risiko «falsch» beurteilt, muss nicht mit einer Sanktionierung rechnen. Bei einer DSFA ist aber ohnehin der Weg das Ziel: Es soll bewirkt werden, dass sich der Verantwortliche die Frage des Risikos seiner Datenbearbeitung für betroffene Personen überhaupt erst stellt. Es wird jedem klar sein, dass in der Praxis aus einer DSFA so gut wie nie ein «hohes» Risiko resultieren wird, da sonst die Datenschutzbehörde involviert werden müsste. Das will niemand. Angesichts der hohen Streuung bei Risikobeurteilungen stellt sich freilich abermals die Frage, ob nicht nur krasse Abweichungen bei der Einschätzung eines Risikos überhaupt als fehlerhaft bzw. als Datenschutzverletzung betrachtet werden können. Das ist angesichts des Gesagten wohl zu bejahen. Oder anders formuliert: Wer beim Lösen eines Falles bisher jeweils befürchtet hat, mit seiner Einschätzung des Risikos völlig «falsch» zu liegen, wird nun wissen, dass dem vermutlich nicht so ist. Wichtiger als das konkrete Ergebnis im Einzelfall ist eine nachvollziehbare, saubere Vorgehensweise – und deren Dokumentation.
[59] Dies alles gilt überdies nicht nur für die Privatwirtschaft, sondern auch bei Entscheiden von Datenschutzbehörden und Gerichten. Es gibt keinen Grund zur Annahme, dass diese in ihren Einschätzungen von Datenschutzrisiken weniger zufällig sind als das Experiment es gezeigt hat. Hinweise auf ein methodisches Vorgehen finden sich in ihren Risikobeurteilungen jedenfalls selten. Dieser Beitrag möchte in diesem Sinne auch ihnen Hinweise für qualitativ bessere Entscheide liefern.

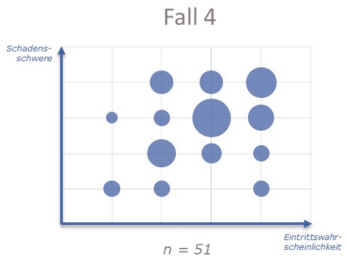
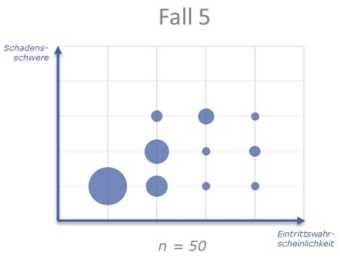
25 Art. 22 revDSG.

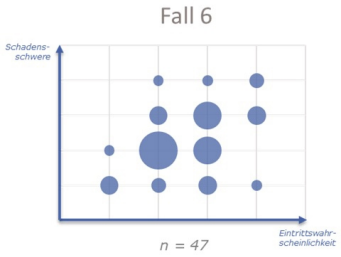
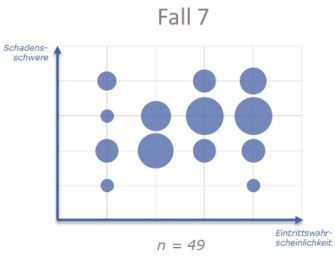
26 Art. 24 revDSG.

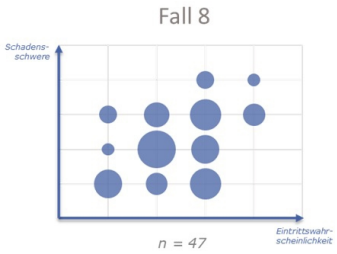
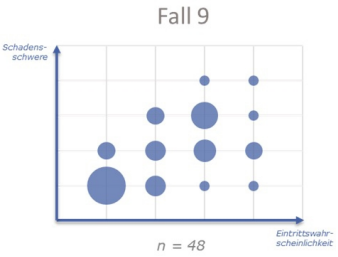
12. Anhang: Die Fälle und ihre Beurteilung

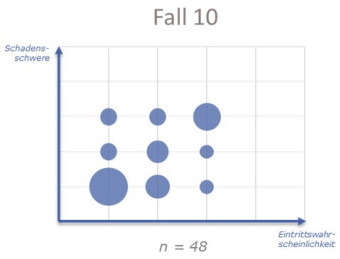
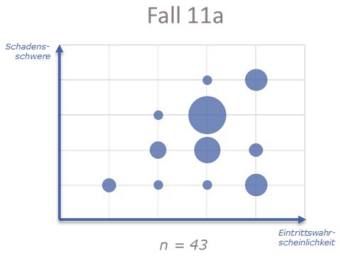
Fall	Szenario	Risikobeurteilung
1	Ein Versicherungsbroker wird Opfer eines Ransomware-Angriffs. Die Dossiers seiner Kunden fallen in die Hände des Angreifers, der mit Veröffentlichung droht. Der Broker will kein Lösegeld bezahlen. Die Dossiers enthalten alle Angaben der Kunden, die Versicherungen für den Abschluss von Policen brauchen (z.B. Hausratsinventare, Fragebögen über frühere Schäden, Angaben zur Gesundheit).	 Als typischer Schaden wurde genannt: Veröffentlichung; Erpressung; Reputationsschaden; Identitätsdiebstahl; Reputation; unsolicited marketing; Einbruch; Verkauf der Daten; zu teure Offerten [0 1 0 0 1 7 8 2 2 2 13 6 0 0 2 5][27]
2	Ein Lebensmittelhersteller will seine Tierfuttersparte verkaufen (in einem Asset Deal). Hierzu will er auch seinen Stamm an Kundendaten dem Erwerber verkaufen, damit dieser weiterhin Direktmarketing für das Tierfutter betreiben kann. In seiner Datenschutzerklärung hat der Verkäufer nichts für diesen Fall vorgesehen. Eine Einwilligung holt er ebenfalls keine ein.	 Als typischer Schaden wurde genannt: Unerwünschte Werbung; Spam; Unzulässige Kontaktaufnahme; Werbemails; Reputation; Zusatzaufwendungen; Zweckentfremdung; ungewolltes Profiling; Wechsel Anbieter [9 1 0 1 3 4 1 0 10 2 1 0 15 2 0 0]

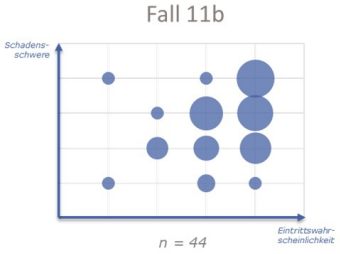
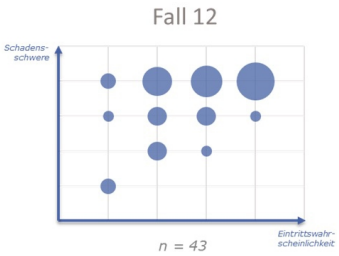
Fall	Szenario	Risikobeurteilung
3.1	Ein Unternehmen erhebt beim Verkauf von Waren in einem Online-Shop Kontaktdaten und Angaben über Warenkäufe. Es kann aufgrund dieser Angaben Vorlieben seiner Kunden ermitteln. Es will dieses Wissen verwenden, um den einzelnen Kunden auf ihre jeweiligen Vorlieben zugeschnittene Angebote zukommen lassen. Er hat die Einwilligung des Kunden.	 Als typischer Schaden wurde genannt: Persönlichkeitsverletzung; Beeinflussung Kaufverhalt; keiner, da Einwilligung; Kundenbeeinflussung; Data Breach; Spam Adresse an Dritte; Persönlichkeitsprofil; Profilingdaten-Diebstahl; falsches Profiling [24 3 1 1 5 8 0 0 2 1 1 0 4 2 0 0]
3.2	Ein Unternehmen erhebt beim Verkauf von Waren in einem Online-Shop Kontaktdaten und Angaben über Warenkäufe. Es kann aufgrund dieser Angaben Vorlieben seiner Kunden ermitteln. Es will dieses Wissen verwenden, um den einzelnen Kunden auf ihre jeweiligen Vorlieben zugeschnittene Angebote zukommen lassen. Er hat keine Einwilligung der Kunden und informiert sie nicht.	 Als typischer Schaden wurde genannt: Persönlichkeitsprofil; Ungewolltes Profiling; Kappung Selbstbestimmung; Manipulation; Steuerung Konsumverhalten; Preisanpassungen; Kontrollverlust [5 0 0 0 3 8 6 2 1 5 8 2 3 6 1 1]

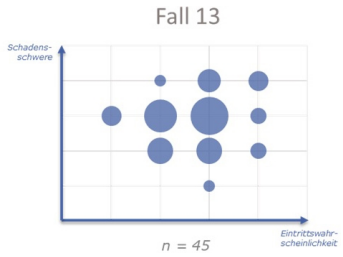
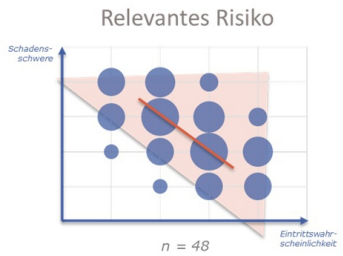
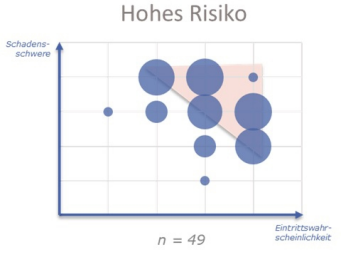
Fall	Szenario	Risikobeurteilung
4	Im Materiallager eines Krankenhauses kommt es immer wieder zu Diebstählen von Spritzen, Skalpellen und anderem Material des täglichen Gebrauchs. Die Spitalleitung baut heimlich versteckte Kameras ein, um den Lagerraum während drei Monaten zu überwachen und so den Täter zu überführen. Die gesamte Zeit wird aufgezeichnet und am Ende von der Security ausgewertet.	 Als typischer Schaden wurde genannt: Kündigung; Strafverfahren; Persönlichkeitsverletzung; Eingriff; soziale Nachteile; Traumatisierung; Sanktionierung Entlassung; Verletzung Privatsphäre [2 0 1 0 2 6 2 4 0 3 11 4 2 2 5 7]
5	Ein Aufzugswartungsfirma stellt ihren Aussendienstlern Wagen zur Verfügung, die diese auch privat nutzen dürfen. Eingebaut ist ein Tracker, der Standort und Fahrweise aufzeichnet. Das dient der Einsatzplanung und präventiven Wartung (aus der Fahrweise lässt sich die Abnutzung ermitteln). Zugang haben der Fahrer, die Einsatzplanung und die Fuhrparktechniker. Für private Fahrten können die Mitarbeiter das Tracking abschalten.	 Als typischer Schaden wurde genannt: kein Schaden; Profiling; Gefühl der Überwachung; Überwachung Arbeitsplatz; Verurteilung im Strafverfahren; Verlust Privatsphäre; Verletzung Zweckbindung; Verhaltensänderung; unzulässige Beobachtung; Unwohlsein; unfreiwillige Überwachung; Stress; Schadenersatz; Entlassung; psychischer Schaden [22 0 0 0 7 9 2 0 1 1 4 0 1 2 1 0]

Fall	Szenario	Risikobeurteilung
6	Ein Versicherer entdeckt, dass ein Verzeichnis der HR-Abteilung, in welchem sich Excels mit den Löhnen aller Kader-Mitarbeiter befinden, während einem halben Jahr für alle Mitarbeiter im Unternehmen offen zugänglich war. Hinweise auf Zugriffe durch andere Unberechtigte gibt es nicht, aber auch nicht, dass keine solche stattfanden. Gemeldet hat den Breach ein Mitarbeiter aus der Finanzabteilung.	 Als typischer Schaden wurde genannt: Cultural clash; Akzeptanz; Ungleichbehandlung; Stress mit dem Arbeitgeber; Rufschädigung; Rechtfertigungsbedarf; Neid; Missgunst; Lohnunterschiede; Kündigungen; psychischer Schaden; Vertraulichkeitsverletzung [3 1 0 0 2 13 3 1 3 7 7 1 1 0 3 2]
7	Eine Bank versendet wegen eines Problems in der Druckstrasse der monatlichen Kontoauszüge die Kontoauszüge von 200 Privatpersonen an die jeweils falschen Kontoinhaber. Der Fehler wird am Tag nach dem Versand wegen Rückmeldungen der Kunden, die fremde Kontoauszüge erhalten haben, bemerkt.	 Als typischer Schaden wurde genannt: Vertrauensverlust; Reputation; psychischer Schaden; privater Reputationsschaden; Veröffentlichung wegen Reichtums; Vertraulichkeitsverletzung; Vermögensschaden; Traumatisierung; Tax-Strafverfahren; Stopp der Bearbeitung; Sozialbetrug; Rufschädigung; Phishing; Offenlegung Finanzsituation; mediales Bashing; Kursverlust [1 3 1 2 0 7 5 0 0 3 8 3 1 3 8 4]

Fall	Szenario	Risikobeurteilung
8	Eine Beraterfirma will ein Computerprogramm verwenden, das von jeder Stellenbewerbung eines Beraters einen «Erfolgsscore» aufgrund seines bisherigen Werdegangs und seiner Noten berechnen. Der Score basiert auf den bisherigen Erfahrungen des Unternehmens mit vergangenen Einstellungen. Der Score dient nur der Information des Hiring-Partners. Es wird niemand automatisch aussortiert.	 Als typischer Schaden wurde genannt: Diskriminierung; Nichtberücksichtigung; Aussortierung; Absage; wirtschaftliche Nachteile; schwierige Stellensuche; keinen; Vermögensschaden; unzulässiges Profiling; Stelle nicht erhalten; non-hiring; Nichteinstellung; negative Vorselektion [5 1 2 0 3 9 4 0 6 5 6 2 0 0 3 1]
9	Eine private Forschergruppe hat ein Computerprogramm entwickelt, das die Attraktivität von Gesichtern beurteilen kann. Jeder kann auf der Website beliebige Bilder hochladen, die daraufhin vom Computer beurteilt werden. Die Bilder werden zudem genutzt, um das Computerprogramm noch besser zu machen. Hierzu werden sie Testteilnehmern zur menschlichen Beurteilung vorgelegt und danach gelöscht.	 Als typischer Schaden wurde genannt: Mobbing; Diskriminierung; Depressionen; psychischer Schaden; Verlust Selbstwertgefühl; Verletzung Recht am Bild; Upload fremder Bilder; Stigmatisierung; Stereotypisierung; Selbstzweifel; Selbstmord; Schäden durch Mobbing; Recht am Bild verletzt; psychologischer Schaden; None [14 3 0 0 4 4 3 0 1 5 7 1 1 3 1 1]

Fall	Szenario	Risikobeurteilung
10	Eine Fahrzeughersteller erweitert seinen Bordcomputer um einen Assistenten, der mit einem Sprachbefehl aktiviert werden kann (wie z.B. Alexa, Siri), d.h. er hört dauernd mit. Die Daten (d.h. Audiofiles) werden zur Auswertung und für das Training der Software in eine Cloud gesendet, allerdings ohne Kennung des Benutzers. Auf diese Eigenschaft wird hingewiesen; der Fahrzeughalter muss die Funktion selbst aktivieren.	 Als typischer Schaden wurde genannt: Profiling; n/a; kein Schaden; Veröffentlichung vertraulicher Gespräche; Verlust der Privatsphäre; Verknüpfung von Daten; Verfolgungswahn; unzulässiger Datentransfer; unerwünschte Werbung; Stimmenreplikation KI; Reidentifizierung; Profilerstellung [15 3 3 0 6 5 3 0 2 2 8 0 0 0 0 0]
11a	Der Betreiber eines Online-Shops will Zahlungsausfälle besser bekämpfen. Er hat festgestellt, dass es Korrelationen zwischen Nationalität, Wohnort, Alter, Geschlecht und bestimmter bestellter Ware und Zahlungsausfällen gibt. Statt auf traditionelle Kreditwürdigkeitsdaten abzustellen, berechnet er sich aufgrund dieser Angaben seinen eigenen Score, auf dessen Basis er über die Option zum Kreditkauf entscheidet.	 Als typischer Schaden wurde genannt: Diskriminierung; wirtschaftlicher Schaden; wirtschaftliche Nachteile; unzulässiges Profiling; Ungleichbehandlung; schlechtere Konditionen; Kundenverärgerung; Kreditverweigerung; Komfortverlust; keine Kreditkauf-Option; höhere Zinsbelastung [2 0 0 0 1 3 1 0 1 7 15 1 5 2 0 5]

Fall	Szenario	Risikobeurteilung
11b	Der Betreiber eines Online-Shops will seine Erträge optimieren. Er hat festgestellt, dass es Korrelationen zwischen Nationalität, Wohnort, Alter, Geschlecht und bestimmter bestellter Ware und der Preissensitivität gibt. Er berechnet nun mit diesen Angaben einen Score, auf dessen Basis er jeden Kunden in eine Kategorie einteilt, welchen er dieselbe Ware zu unterschiedlichen Preisen anbietet.	 Als typischer Schaden wurde genannt: Diskriminierung; Ungleichbehandlung; Übervorteilung Überhöhter Preis; z.B. Fotos eigener Kinder; wirtschaftlicher Schaden; keinen Schaden; freie Marktwirtschaft; Zusatzkosten; zu hohe Preise; Zahlung über Marktpreis; wirtschaftliche Nachteile; uninteressante Angebote [1 0 0 1 0 3 1 0 2 4 7 1 1 6 8 9]
12	Ein Telefonhersteller rüstet die Software in seinen Handies so um, dass alle Bilder auf bekannte Kinderpornographie gescannt wird. Werden mehr als 30 solcher Bilder gefunden, wird der Hersteller vom Gerät autonom benachrichtigt, der dann den Fall der Polizei melden kann. Das System soll von unabhängiger Stelle überwacht werden. Der Hersteller verspricht, Anfragen von Behörden zur Mitnutzung der Lösung nicht stattzugeben.	 Als typischer Schaden wurde genannt: Strafverfahren; wirtschaftlicher Schaden Überwachung; soziale Nachteile; psychischer Schaden; Unberechtigte Auswertung; Strafuntersuchung; Strafbarkeit; Stigmatisierung; Selbstzensur; Scheidung; Rufschädigung; misuse; lawful access [2 0 1 2 0 3 3 7 0 1 3 8 0 0 1 12]

Fall	Szenario	Risikobeurteilung
13	Ein untreuer Mitarbeiter einer Versicherungsgesellschaft stiehlt die Dossiers von Versicherungsanträgen und erpresst inkognito die Gesellschaft mit der Veröffentlichung im Darknet, falls sie ihn nicht bezahlt. Diese will sich jedoch nicht darauf einlassen. In den Anträgen sind Angaben über die Gesundheit enthalten, über frühere Schäden aber auch Inventare des Hausrats.	 Als typischer Schaden wurde genannt: Einbruch; Erpressung; Diskriminierung; Benachteiligung; wirtschaftlicher Schaden; soziale Nachteile; psychischer Schaden; Veröffentlichung meiner Krankheit; Versicherungsweigerung; Vermögensschaden; unsolicited marketing; Sicherheitsverlust; Identitätsklau; Identitätsdiebstahl; Gesundheitsdaten publik; Erpressung eines Versicherten [0 0 3 0 0 5 8 1 1 5 11 4 0 2 2 3]
	Ab welchem Risiko liegt ein datenschutzrechtlich relevantes Risiko vor?	 [0 2 7 7 2 7 13 8 7 13 9 3 7 8 3 0]
	Ab welchem Risiko liegt ein «hohes» Risiko im Sinne des DSG bzw. der DSGVO vor?	 [0 0 1 0 0 0 5 14 1 5 13 15 0 14 15 1]

27 Die Quellwerte, zuerst alle Werte für die Einrittswahrscheinlichkeit 1 (aufsteigende Schadensschwere 1 bis 4), dann für die Eintrittswahrscheinlichkeit 2 etc.

David Rosenthal ist Partner in einer Wirtschaftskanzlei in Zürich, Lehrbeauftragter der Universität Basel und ETH Zürich sowie Sekretär des Vereins Unternehmens-Datenschutz (VUD). Er ist erreichbar unter david@rosenthal.ch und drosenthal@vischer.com.

Der Autor dankt dem Vorstand des VUD, Maria Winkler und David Vasella für deren konstruktiv-kritischen Stellungnahmen, die zum Verbessern des Beitrags beigetragen haben. Danke auch an alle Mitglieder, die an der Umfrage teilgenommen haben.