Zeitschrift für Datenrecht und Informationssicherheit

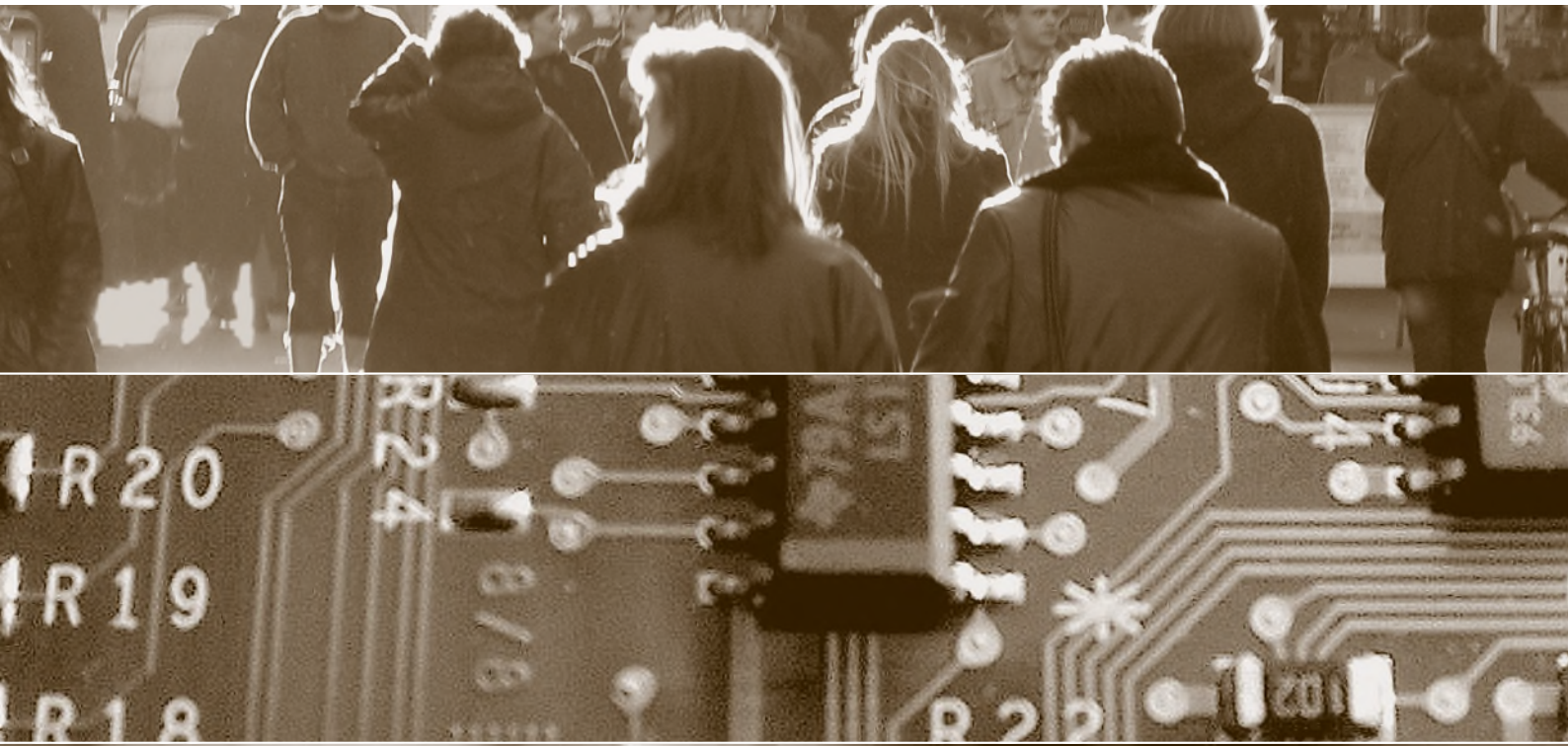
digma

www.digma.info 19. Jahrgang, Heft 4, Dezember 2019

Schwerpunkt:

Rechte an Daten

fokus: Datennutzung und Datensouveränität
fokus: Datenmärkte ohne «Dateneigentum»
report: Datenschutz auf der Intensivstation



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth
David Vasella

Schulthess §

inhalt

fokus

Schwerpunkt:
Rechte an Daten

Informationelle Selbstbestimmung

Was leistet das Datenschutzrecht für die Selbstbestimmung der Betroffenen? Welche Kontrollrechte sieht das DSG vor, und sind sie in der heutigen Zeit grundsätzlich überhaupt noch in der Lage, Datenkontrolle zu gewährleisten?

Datenmärkte ohne «Dateneigentum»

Das Datenschutzrecht ermöglicht den Handel mit Personendaten, schränkt ihn andererseits aber auch ein. Könnte die freie Widerrufbarkeit der datenschutzrechtlichen Einwilligung eingeschränkt werden, um den Handel zu fördern?

Sozialpflichtigkeit von Gesundheitsdaten

Damit der Forschung mehr Gesundheitsdaten zur Verfügung stehen, wird die Einführung einer generellen Widerspruchslösung gefordert. Ist das mit dem geltenden Recht und den Grundwerten unserer demokratischen Gesellschaft vereinbar?

Herausforderungen der Datenlöschung

Sensitive Daten müssen, wenn erforderlich, sicher gelöscht werden. Aber nicht immer ist es offensichtlich, ob diese Löschung irreversibel ist.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Prof. Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. (em.) Dr. iur. Rainer J. Schweizer, Prof. Dr. Günter Karjoth, Dr. iur. David Vasella

Redaktion: Dr. iur. Bruno Baeriswyl und Prof. Dr. iur. Beat Rudin

Rubrikenredaktor(inn)en: Dr. iur. Barbara Widmer, Dr. iur. Dominika Blonski

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, redaktion@digma.info

Erscheinungsplan: 4-mal jährlich (März, Juni, September, Dezember)

Bezugsbedingungen: Jahresabonnement: CHF 178.00 (für Studierende: CHF 98.00), Einzelheft: CHF 48.00, zzgl. Versandkosten. Alle Abo-Preise inkl. 2,5% MWST, zzgl. Versandkosten von CHF 6.00 innerhalb der Schweiz (Versandkosten für Lieferung ins Ausland: CHF 31.00). Studentenpreis gegen Vorlage eines gültigen Nachweises. Abonnementkündigungen sind mit einer Frist von 8 Wochen zum Ende des berechneten Bezugsjahres möglich.

Anzeigenverkauf und -beratung: Fachmedien Zürichsee Werbe AG, Laubisrütistrasse 44, CH-8712 Stäfa, Tel. +41 (0)44 928 56 17, marc.schaettin@fachmedien.ch

Verlag und Kundenservice: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach 2218, CH-8021 Zürich
Tel. +41 (0)44 200 29 29, Fax +41 (0)44 200 29 28, service@schulthess.com, www.schulthess.com

Datenschutz auf der Intensivstation

Ein bewusst provokativer Befund eines Privatrechtlers: Das geltende (und künftige) Datenschutzrecht ist nicht in der Lage, die heutigen Probleme überzeugend zu lösen. Wie sähen erste Schritte hin zu einem neuen Ansatz aus?

Vertrauensstiftende Videoüberwachung?

Kann ein soziotechnisches Konzept, das eine reversible Anonymisierung von Bilddaten mit einer Kontrollinstanz kombiniert, die berechtigten Bedenken gegenüber Videoüberwachung überwinden helfen?

Aus den Datenschutzbehörden

Wer hat an der Internationalen Konferenz der Datenschutzbeauftragten eine Auszeichnung erhalten? Wer diskutiert über Social Media und Fake News am ZFF Talk? Wer gewinnt den Datenschutz-Video-Wettbewerb 2019 des Datenschutzbeauftragten des Kantons Zürich? Und wer bietet neu eine Nachdiplom-Masterausbildung an?

Quo vadis KI? Neue OECD-Grundsätze

Künstliche Intelligenz fordert den Regulator heraus. Was sagen die neuen Grundsätze der OECD dazu? Und wo steht die Schweiz?

Gelöscht. Gelöscht?

Löschen. Gelöscht? Unser Cartoonist zeigt, was bleibt …

report

forum

Löschen und doch nicht löschen

Werden Personendaten nicht mehr benötigt, sind sie zu löschen. In der Praxis bereitet das enorme Schwierigkeiten.

David Rosenthal, lic. iur., Zürich
david@rosenthal.ch

Wie können die Anforderungen der EU-Datenschutzgrundverordnung und des Datenschutzgesetzes erfüllt werden?

An sich ist das Grundprinzip einfach, und eigentlich gilt es schon seit über 25 Jahren auch im Schweizer Datenschutzrecht: Wenn Personendaten für die Zwecke, für die sie beschafft worden sind, nicht mehr benötigt werden, sind sie zu löschen. Endgültig. Das ergibt sich aus dem Grundsatz der Verhältnismässigkeit[1]. Das Prinzip galt auch in der EU schon lange. Geändert hat sich mit der DSGVO lediglich der Leidensdruck, diesen Grundsatz der «Speicherbegrenzung»[2] auch einzuhalten. Wer ihn verletzt, kann massiv gebüsst werden[3], was mindestens in einem Fall bereits auch in Millionenhöhe geschah[4]. Das gilt auch für den Fall, dass das «Recht auf Vergessen» verletzt wird, wonach eine betroffene Person verlangen kann, dass die sie betreffenden Personendaten gelöscht werden, auch wenn sie noch benötigt werden (siehe *Box: Wie weit geht das Recht auf Vergessen?*)[5]. In der Schweiz kann die Verletzung dieser Grundsätze zwar nicht wirklich sanktioniert werden[6] und auch im revidierten DSG soll sich das nicht ändern. Dennoch kommt dem Löschen von Personendaten auch in der Schweiz sehr viel mehr Aufmerksamkeit zu. Der Grundsatz der Speicherbegrenzung soll im neuen DSG sogar ausdrücklich erwähnt werden[7].

In Anwendungen können Daten oft nicht gelöscht werden

So sinnvoll diese Grundsätze erscheinen mögen, so schwierig ist ihre Umsetzung. Viele Unternehmen haben realisiert, dass sie in vielen Fällen gar nicht in der Lage sind, die von ihnen bearbeiteten Personendaten zu löschen. Das gilt für KMU genauso wie Grossunternehmen. Betroffen sind insbesondere branchen- und fachspezifische Anwendungen, die mit strukturierten Daten arbeiten. Banken und Versicherungen, um ein Beispiel zu nennen, können in ihren Anwendungen nicht mehr benötigte Kundendaten zwar meistens archivieren und so den Zugriff auf einige wenige Personen im Unternehmen einschränken. Wenn sie Glück haben, können sie den Zugriff sogar für alle Benutzer einer Anwendung sperren. Doch wirklich gelöscht sind die Daten nach dem allgemeinen Sprachverständnis nicht; sie befinden sich nach wie vor auf den Festplatten der Server. Womöglich sind sie gar noch auf den Datenbanksystemen, auf welchen die Anwendungen gewissermassen «aufsetzen», als intakte Datensätze vorhanden und können von den Administratoren der Datenbanken in den Informatikabteilungen mit dem nötigen Fachwissen im Grunde beliebig abgerufen und sonst verarbeitet werden.

Das stellt diese Unternehmen vor die schwierige Frage, wie sie damit in Anbetracht der Vorgaben des Datenschutzes umgehen sollen. Werden Lösungen neu eingeführt, wird dem Aspekt der Datenlöschung inzwischen von Anfang an mehr Beachtung geschenkt. Doch viele Softwarelösungen können aus betrieblichen und wirtschaftlichen Gründen nicht ohne Weiteres abgelöst oder angepasst werden. Bei Standardsoftware kommt hinzu, dass die Unternehmen eine Anpassung ihrer Lösung nicht erzwingen können und somit von ihrem Lieferanten abhängig sind. Müssen sie nun für sehr viel Geld ihre Systeme umprogrammieren oder auf neue Lösungen wechseln – oder ist es möglich, die Löschpflichten gemäss DSGVO und DSG auch auf andere Weise einzuhalten?

Keine Begriffsdefinitionen

Glücklicherweise gibt es Lösungen dafür. Denn sowohl unter der DSGVO wie auch dem DSG ist der Begriff der «Löschung» nicht so absolut zu verstehen, wie dies auf den ersten Eindruck erscheinen mag. Und selbst wenn nicht im Sinne des Gesetzes gelöscht werden kann, gibt es Möglichkeiten, das Risiko einer Intervention oder Sanktion der Datenschützer massiv zu senken.

Dazu ist es zunächst erforderlich, den Begriff des «Löschens» etwas näher zu definieren. In der DSGVO wird er im Grundsatz der Speicherbegrenzung gar nicht verwendet. Dort ist stattdessen davon die Rede, dass Personendaten nur in «einer Form» gespeichert werden dürfen, «die die Identifizierung der betroffenen Person so lange ermöglicht», wie es für ihren Zweck erforderlich ist[8]. Im Rahmen des «Rechts auf Vergessen» ist wiederum ausdrücklich von «Löschen» von Personendaten die Rede[9]. Das bestehende DSG kennt den Begriff nicht; dort ist stattdessen immer vom «Vernichten» die Rede, das als Synonym verwendet wird.

Im revidierten DSG werden wiederum neu beide Begriffe – Löschen und Vernichten – verwendet, und zwar sowohl in der Definition des Begriffs des «Bearbeitens» als auch in den einzelnen Bestimmungen. Allerdings geschieht dies nicht konsistent. So wird im Rahmen des Grundsatzes der Speicherbegrenzung im gegenwärtigen Entwurf verlangt, dass Daten bei Nichtgebrauch «vernichtet oder anonymisiert» werden[10]. Das ist ein redaktionelles Versehen: Der Speicherbegrenzung ist auch durch ein Löschen Genüge getan; ein Vernichten ist nicht erforderlich[11]. In anderen Bestimmungen wie zum Beispiel den Rechtsansprüchen ist ausdrücklich davon die Rede, dass die Löschung oder die Vernichtung verlangt werden kann[12]. Eine Legaldefinition der Begriffe soll es jedoch auch im künftigen DSG nicht geben. Immerhin äussert sich die Botschaft zum revidierten DSG mit Verweis auf die Rechtsprechung[13] dazu. Demnach ist unter Vernichtung die irreversible und dauerhafte Zerstörung von Daten durch Zerstörung des eigentlichen Datenträgers, also etwa das Verbrennen oder Schreddern von Papier oder die Entmagnetisierung der Festplatte zu verstehen[14]. Dass diese Methode zur Löschung der Daten führt und daher genügt, bedarf keiner weiteren Erläuterung. Aus der Verwendung *beider* Begriffe ergibt sich aber auch, dass ein Löschen nicht erfordert, dass der Datenträger vernichtet bzw. seiner Eigenschaft als solchem beraubt wird. Löschen geht also weniger weit. Die Botschaft nennt als Beispiel «übliche Löschbefehle» oder eine «reine Umformatierung» von Daten[15], was in dieser Absolutheit natürlich nicht richtig ist und wohl auch nicht so gemeint war.

Was «Löschen» bedeutet

Zweifellos kann es Fälle geben, in welchen Daten zu vernichten und nicht bloss zu löschen sind[16]. In der Praxis interessiert aber primär der Begriff des Löschens. Nach herrschender Lehrer unter der DSGVO gelten Daten in jedem Fall dann als gelöscht, wenn sie nicht oder nur noch mit unverhältnismässigen Mitteln wiederhergestellt werden können, selbst unter Beizug von IT-Experten[17]. Gewisse Autoren sind etwas liberaler und der Ansicht, dass es bereits genügt, wenn die Daten «für den gewöhnlichen Gebrauch» nicht mehr nutzbar sind, und daher die Löschung aller Backups und aller sonst noch vorhandenen Datenträger daher nicht erforderlich ist, damit Personendaten als gelöscht gelten können[18]. Ein Autor vertritt sogar die Ansicht, dass es genügt, wenn die Information von der verantwortlichen Stelle (d.h. den Controllern) nicht mehr wahrgenommen werden kann[19].

Im revidierten DSG werden beide Begriffe – Löschen und Vernichten – verwendet, allerdings nicht konsistent.

Diesen liberalen Ansichten stehen die Ansichten der EU-Datenschutzbehörden entgegen. In einer Ende 2018 ergangenen Entscheidung befand die österreichische Aufsichtsbehörde, dass Personendaten nur dann gelöscht sind, wenn «weder der Verantwortliche selbst, noch ein Dritter ohne unverhältnismässigen Aufwand einen Personenbezug wiederherstellen kann»[20]. Andere Aufsichtsbehörden haben sich in vergleichbarer Weise verlauten lassen. So verlangt die Aufsichtsbehörde des deutschen Bundeslandes Mecklenburg-Vorpommern, dass die Löschung auf «irreversible Weise» bewirkt, dass aus den gelöschten Daten selbst mit verhältnismässig hohem Aufwand keine Informationen über bestimmte oder be-

Kurz & bündig

Die Pflicht zu Löschen ist unbestritten. Doch was bedeutet «Löschen» wirklich? Die Antwort liefert der Begriff des «Personendatums»: Löschen bedeutet nicht, dass es unter keinen Umständen mehr möglich ist, an die gelöschten Daten zu gelangen. Es genügt bereits, wenn sich Personendaten nur noch mit unverhältnismässigen Mitteln wiederherstellen lassen. Eine Anonymisierung von Personendaten genügt damit ebenso wie andere Verfahren, bei denen mit aller Wahrscheinlichkeit verhindert wird, dass die betroffenen Personen re-identifiziert werden können. Das wiederum hängt davon ab, wie hoch das Interesse an einer Re-Identifikation ist und welche Methoden hierfür zur Verfügung stehen. Dies wiederum hängt zum Beispiel davon ab, wie sensitiv die Daten sind. Sind Daten in einem System zwar noch vorhanden, kann das Unternehmen (und wer sonst noch Zugang dazu hat) aber mit verhältnismässigem Aufwand nicht mehr an sie gelangen, gelten sie als gelöscht. Es ist von einer «logischen» Löschung die Rede.

stimmbare Personen mehr gewonnen werden können[21].

Relative Methode gilt auch beim Löschen

Besonders hilfreich sind diese Definitionen nicht. Sie ergeben sich bereits aus der Definition des Begriffs des Personendatums. Denn liegen keine Personendaten mehr vor, fällt die Anwendung der DSGVO bzw. des DSG naturgemäss ausser Betracht. Keine Personendaten liegen vor, wenn die Identifikation nur noch mit Mitteln möglich ist, die der Verantwortliche oder ein Dritter «wahrscheinlich» nicht mehr einsetzt[22]. Dies erfordert einerseits, dass es Mittel zur Re-Identifikation gibt (objektive Komponente), und andererseits ein genügend grosses Interesse daran besteht, sie auch einzusetzen (subjektive Komponente). Kommt hierbei richtigerweise der sog. relative Ansatz zum Tragen, sind diese Komponenten nur aus Sicht jener zu prüfen, die tatsächlich Zugang zu den Informationen haben (d.h. nicht aus der Sicht aller möglichen Personen, selbst wenn diese keinen Zugang haben)[23].

Es genügt, wenn nach dem «Löschen» nichts mehr vorliegt, das als Personendatum gilt, weil die DSGVO und das DSG dann ohnehin nicht mehr gelten.

Daraus lassen sich zwei Schlussfolgerungen für vorliegende Fragestellung ziehen. Eine Anonymisierung von Personendaten ist erstens im Ergebnis aus datenschutzrechtlicher Sicht gleichbedeutend mit deren Löschung. Zweitens genügt es für die Zwecke der Löschung zu beurteilen, wie wahrscheinlich es ist, dass die Personen mit tatsächlichem Zugang zu den gelöschten oder anonymisierten Informationen Mittel zu deren Re-Identifikation einsetzen. Welcher Aufwand im Sinne der obigen Definitionen noch «verhältnismässig» ist, muss somit auch bezüglich der Löschung von Personendaten nach der relativen Methode beurteilt werden, also aus der Sicht derjenigen Personenkreise, die Zugang zu den Daten haben. Es genügt, wenn nach dem «Löschen» nichts mehr vorliegt, das als Personendatum gilt, weil die DSGVO und das DSG dann ohnehin nicht mehr gelten. Weitergehende Massnahmen können somit unter dem Titel des Löschens nicht erforderlich sein.

Anonymisierung genügt

Dass ein Anonymisieren dem Löschen gleichgesetzt ist, hat auch der bereits zitierte Entscheid der österreichischen Datenschutzbehörde bestätigt[24]. Zunächst stellte sie klar, dass der verantwortlichen Stelle ein «Auswahlermessen» bezüglich der Art und Weise der Löschung zusteht[25]. In diesem Sinne sei auch die Entfernung des Personenbezugs – also die Anonymisierung – «grundsätzlich ein mögliches Mittel zur Löschung»[26]. Als nicht ausreichend erachtete sie es, die Datenorganisation bloss so zu verändern, dass ein gezielter Zugriff auf die betreffenden Daten ausgeschlossen sei[27]. Wer also das Inhalts- und Stichwortverzeichnis eines Buches entfernt, hat die darin enthaltenen Personendaten damit noch nicht gelöscht. Das macht Sinn und dennoch mutet die Aussage im Entscheid etwas absolut an.

Nicht ganz richtig ist jedoch die Schlussfolgerung, dass, «[n]ur wenn der Verantwortliche die Daten im Ergebnis auf einer Ebene aggregiert, sodass keine Einzelereignisse mehr identifizierbar sind», der entstandene Datenbestand als anonym bezeichnet werden könne[28]. Das Aggregieren von Personendaten ist zwar zweifellos eine Methode zur Entfernung des Personenbezugs, aber nicht die einzige. Zuverlässig anonymisieren lassen sich Personendaten je nach Situation zum Beispiel auch durch die Veränderung, Schwärzung oder Löschung derjenigen Elemente der einzelnen Datensätze, anhand derer eine Re-Identifikation möglich wäre[29]. Wesentlich kann wie erwähnt nur sein, ob am Ende noch Personendaten vorliegen.

Dasselbe muss im Ergebnis auch unter dem DSG gelten, da es auf demselben Verständnis von Personendaten aufbaut wie die DSGVO.

Wie gut muss anonymisiert werden?

Wer also in einer Datenbank zwar Datensätze nicht entfernen kann, weil dies zum Beispiel die Integrität der Datenbank oder der Anwendung gefährden würde, kann Daten in einzelnen Datensätzen auch durch gezieltes Überschreiben oder Verändern mindestens jener Datenfelder löschen, welche für eine Re-Identifikation nötig wären. Dabei genügt es, dass dies erstens nur für jene Kreise gilt, die Zugang zu den Daten haben oder erhalten könnten, und zweitens auch bezüglich dieser Kreise nur so weit, als ihnen eine Re-Identifikation möglich wäre und sie die dazu erforderlichen Mittel wahrscheinlich auch einsetzen würden.

Somit muss im konkreten Fall beurteilt werden, wer noch Zugang zu den Daten haben könnte. Dies werden typischerweise gewisse Mitarbeiter des Unternehmens sein, doch nicht nur. Infrage kommen können je nach Fall auch externe Personen wie etwa Mitarbeiter von IT-Dienstleistern, die für Wartungszwecke auf die IT-Systeme des Unternehmens und deren Daten

zugreifen können. Zu denken ist auch an ungewollte Zugriffe, sei es durch unbefugte Benutzer (wie z.B. Hacker oder Malware), sei es durch staatliche Stellen (wie z.B. eine Behörde, die Daten auf IT-Systemen beschlagnahmt). Für jeden dieser Kreise muss separat beurteilt werden, wie wahrscheinlich erstens ein Zugang zu anonymisierten Daten ist und ob es zweitens zu einer erfolgreichen Re-Identifikation kommen könnte, d.h., welche Mittel ihm zur Verfügung stehen und ob er diese Mittel einsetzen würde. Ist eine Re-Identifikation insgesamt unwahrscheinlich, können die Personendaten im Sinne der DSGVO und des DSG als gelöscht gelten.

Pseudonymisieren und Verschlüsseln genügen nicht

Daraus ergibt sich umgekehrt, dass es nicht genügt, Personendaten bloss zu verschlüsseln oder auf andere Weise zu pseudonymisieren, also beispielsweise die identifizierenden Teile eines Datensatzes durch einen Code zu ersetzen. Diese Methoden können zwar vor unbefugten Zugriffen auf Personendaten im Klartext schützen und gehören insofern zu den technischen Schutzmassnahmen, zu denen ein Unternehmen ebenfalls verpflichtet sein kann. Wer jedoch den Schlüssel zur Entschlüsselung noch hat bzw. den zur Pseudonymisierung verwendeten Code noch realen betroffenen Personen zuordnen kann und Zugang zu den Daten hat, verfügt noch über Personendaten und hat sie nicht gelöscht.

Auch ein Archivieren von Personendaten führt noch nicht zu deren Löschung, auch wenn der Zugang zum Archiv auf wenige Personen beschränkt wird. Der Sinn und Zweck eines Archivs ist, dass bei Bedarf auf die darin abgelegten Daten oder Unterlagen zugegriffen werden kann und sie gerade nicht gelöscht oder vernichtet sind. Ein Archivieren kann datenschutzrechtlich durchaus angezeigt sein, so insbesondere, um sicherzustellen, dass Daten, die nur noch für Archivzwecke aufbewahrt werden, nicht anderweitig benutzt und damit missbraucht werden. Das gilt insbesondere, wenn der Zugriff auf die Daten zusätzlich beschränkt wird.

Verlangt die DSGVO bzw. das DSG hingegen deren Löschung, darf auch der Zugriff bei Bedarf mit verhältnismässigen Mitteln nicht mehr möglich sein. Dasselbe gilt notabene für Backups. Da sie aufgrund der Natur der Sache so angelegt sind, *dass* sich ihr Inhalt wieder einspielen lässt, sind auch sie in ein Löschkonzept einzubeziehen. Werden Backups längerfristig aufbewahrt, bietet sich im Rahmen des DSG immerhin die Möglichkeit an, ihre Nichtlöschung mit einem überwiegenden privaten Interesse des Datenbearbeiters zu rechtfertigen[30]. Eine längerfristige Aufbewahrung kann beispielsweise für den Fall eines über lange Zeit nicht entdeckten Cyberangriffs angezeigt sein, der die Daten eines Unternehmens einschliesslich der Backups systematisch zerstört.

Besser als nichts: «put beyond use»

Weiter als das Archivieren oder innerbetriebliche Zugriffsbeschränkungen ist das, was in der Praxis als «put beyond use» bekannt ist: Personenbezogene Daten sind technisch noch im System vorhanden, werden aber so gekennzeichnet, dass sie nicht mehr verwendet werden dürfen (d.h. sie werden so behandelt, als ob sie gelöscht worden wären), und die Verwendung solcher Daten wird durch Richtlinien grundsätzlich verboten. Aus diesem Grund wird das Unternehmen zumindest für seine Entscheidungen und Aktivitäten im normalen Geschäftsverlauf nicht mehr auf diese Daten abstellen. Der tatsächliche Zugriff auf diese Daten sollte streng eingeschränkt werden und die Verwendung dieser Daten sollte aufgezeichnet werden, um Missbräuche aufzudecken. Da die personenbezogenen Daten technisch noch verfügbar sind, kann ein Unternehmen nicht ausschliessen, dass es unter bestimmten Voraussetzungen (z.B. in einem Rechtsfall) auf die Daten zugreifen kann. Das «put beyond use» (zu Deutsch «von der Nutzung ausschliessen») von Daten ist somit eine vorübergehende Abhilfemassnahme, solange noch nicht wirklich gelöscht oder anonymisiert werden kann. Es ist somit noch keine Löschung im engeren Sinne, aber besser als nichts.

Ist eine Re-Identifikation insgesamt unwahrscheinlich, können die Personendaten im Sinne der DSGVO und des DSG als gelöscht gelten.

Die Grenzen sind allerdings fliessend, da Personendaten nur, aber immerhin dann als gelöscht gelten, wenn der Aufwand zu ihrer Wiederherstellung unverhältnismässig wird. Wann das genau der Fall ist, ist nicht klar zu beantworten und hängt ohnehin von den Umständen ab. Ist das Interesse an den zu löschenden Personendaten in einem konkreten Fall besonders hoch, wird auch davon ausgegangen werden müssen, dass ein entsprechend höherer Aufwand zu ihrer Wiederherstellung betrieben werden wird. Massnahmen zur Verhinderung

eines Zugriffs, die bei weniger begehrten Daten hinreichend wären, werden möglicherweise nicht genügen. Das Interesse an Daten kann sich dabei über die Zeit ändern. Hat ein Krankenhaus Patientendaten für Forschungszwecke anonymisiert und findet die Forschung in den Daten Hinweise auf eine lebensbedrohliche Situation gewisser Patienten, wird womöglich sehr viel investiert werden, um die Anonymisierung doch noch rückgängig zu machen und die Patienten warnen zu können.

Das «put beyond use» von Daten ist somit eine vorübergehende Abhilfemassnahme. Es ist somit noch keine Löschung im engeren Sinne, aber besser als nichts.

Die «logische» Löschung als Patentrezept?

Dies führt zu den bereits im Zusammenhang mit der Anonymisierung erwähnten Wahrscheinlichkeitsrechnungen zurück: Wer beurteilen will, ob die von ihm getroffenen Massnahmen zur Wiederherstellung von Personendaten genügen, muss erst die möglichen Szenarien ermitteln, in welchen ein Zugriff nötig werden könnte. Er muss dann prüfen, ob die Löschmassnahmen dem wahrscheinlich standhalten. Dies ähnelt der im Strafrecht für Sorgfaltspflichten[31] entwickelten Formel: Wer das, womit er nach dem gewöhnlichen Lauf der Dinge und den Erfahrungen des Lebens zu rechnen hat, mit zumutbaren Massnahmen höchstwahrscheinlich verhindert, handelt sorgfältig und wird selbst bei Fahrlässigkeitsdelikten nicht strafbar, wenn der Erfolg doch eintritt[32].

Der Datenschutz ist naturgemäss etwas weniger streng und erfordert – wie sich aus dem Begriff des Personendatums ergibt – nur, dass eine Re-Identifikation bzw. ein Zugriff *wahrscheinlich* verhindert wird. Salopp gesagt genügt es also, dass die Chancen mehr als 50% sind. Das entspricht auch der Vorgabe, dass Personendaten bereits dann als gelöscht gelten, wenn der Aufwand zur Wiederherstellung unverhältnismässig geworden ist, d.h., der Aufwand den Nutzen übertrifft. Unzumutbar muss der Aufwand demnach nicht sein. Es ist dies letztlich ein weiterer Ausfluss des im Datenschutz anerkannten *risikobasierten Ansatzes,* d.h., die Angemessenheit der Massnahmen richtet sich nach dem Risiko der Datenschutzverletzung, die sie verhindern sollen.

Hier kommt der Begriff der «logischen» Löschung ins Spiel: Personenbezogene Daten bleiben unverändert auf dem Datenträger, aber das System, das den Zugriff darauf kontrolliert, verweigert den Abruf, weil sie als «gelöscht» markiert wurden. Diese Technik findet sich zum Beispiel in vielen Datenverwaltungs- und Archivierungssystemen. Wenn jemand die von diesen Systemen verwendeten Festplatten physisch entfernen und auf die Festplatten zugreifen würde, könnte auf die Daten immer noch zugegriffen werden. Dies erfordert jedoch erhebliches Expertenwissen, Zugang zum System (physisch oder über eine Hintertür oder Hacking) sowie einiges an Aufwand. Daher ist die Löschung lediglich «logischer» Natur und nicht physischer. Trotz allem werden auf diese Weise gelöschte Daten aus datenschutzrechtlicher Sicht in der Regel als gelöscht betrachtet.

Wahrscheinlichkeitsüberlegungen

Die in der Praxis schwierige, aber wichtige Abgrenzungsfrage ist, ab welchem Moment die zur Verhinderung des Datenzugriffs getroffenen Massnahmen von einem «put beyond use» zu einer «logischen Löschung» werden und daher datenschutzrechtlich genügen.

Die Frage kann selbstverständlich nicht pauschal beantwortet werden. Wenn in einem Unternehmen beispielsweise die auf seinen Datenträgern gespeicherten Dateien in den «Papierkorb» geschoben werden, sind sie noch nicht gelöscht. Sie können vom Benutzer jederzeit wiederhergestellt werden. Leert er den Papierkorb, sind sie für ihn zwar weg, aber auf dem Datenträger seines Computers sind sie nach wie vor vorhanden, wenngleich vom System als «gelöscht» und der Speicherplatz als «ungenutzt» markiert. Die Daten auf dem Datenträger werden erst mit der Zeit überschrieben, nämlich wenn neue Daten auf dem betreffenden Speicherplatz abgelegt werden. Mit den passenden Softwareprogrammen lassen sich die Daten zwar im Prinzip wiederherstellen; dazu kommen wird es aber innerhalb eines Unternehmens normalerweise nicht. Solche Software wird nach dem gewöhnlichen Lauf der Dinge höchstens dann eingesetzt, wenn Daten versehentlich gelöscht worden sind. Diese Fälle sind aber datenschutzrechtlich unproblematisch, da die betreffenden Daten gerade *nicht* gelöscht werden sollten. Somit genügt diese Form – das Leeren des Papierkorbs – der Löschung normalerweise.

Anders verhält es sich jedoch, wenn Daten auf einem USB-Stick gespeichert werden, der ausserhalb des Betriebs zum Einsatz kommt. Geht er verloren oder wird er einem Dritten übergeben, ist die Wahrscheinlichkeit, dass der Finder oder der Dritte aus Neugier entsprechen-

Wie weit geht das Recht auf Vergessen wirklich?

Seit der DSGVO gibt es bezüglich des Rechts auf Vergessen zwei Missverständnisse: Erstens herrscht die Ansicht, dass dieses «Recht» erst mit der DSGVO eingeführt wurde. Das ist falsch. Es existierte schon zuvor, und auch das heutige DSG kennt es[36]. Zweitens glauben viele, jedes Personendatum einer Person müsse gelöscht werden, sobald sie dies verlangt. Auch das ist falsch. Ein Löschanspruch besteht letztlich in nur sehr wenigen Fällen.

Unter dem DSG kann zwar jeder die Löschung seiner Daten verlangen. Gelöscht werden muss jedoch nicht, wenn das betroffene Unternehmen sich auf ein überwiegendes privates oder öffentliches Interesse oder eine gesetzliche Pflicht nach Schweizer Recht berufen kann[37]. Vor allem die Rechtfertigung des überwiegenden Interesses – zum Beispiel der Abschluss oder die Abwicklung eines Vertrags – geht sehr weit. An diesem Konzept soll sich unter dem revidierten DSG nichts ändern.

Unter der DSGVO ist es etwas komplizierter: Stellt eine betroffene Person ein Löschgesuch, so muss das Unternehmen zuerst prüfen, ob einer der sieben Fälle von Art. 17 Abs. 1 DSGVO erfüllt ist. Solange jedoch ein Unternehmen Daten der betroffenen Person nicht für Direktmarketingzwecke oder auf Basis einer Einwilligung bearbeitet, es sich ansonsten an die DSGVO hält, es nicht um Daten über Kinder aus Online-Diensten geht und das EWR-Recht auch sonst nicht die Löschung verlangt, kann das Unternehmen eine Löschung unter Berufung auf ein überwiegendes berechtigtes Interesse verweigern. In der Mehrheit der relevanten Fälle kommt es somit auch unter der DSGVO zu einer Interessenabwägung. Selbst wenn das Unternehmen dabei unterliegen sollte, kann noch eine der Ausnahmen nach Art. 17 Abs. 3 DSGVO greifen. Dazu gehören gesetzliche Pflichten (z.B. Aufbewahrungspflicht nach EWR-Recht), Gerichts- und Behördenverfahren und Ausnahmen im Landesrecht der Mitgliedstaaten. Gemäss dem liechtensteinischen Datenschutzgesetz muss beispielsweise nicht gelöscht werden, wenn die Löschung «wegen der besonderen Art der Verarbeitung oder Speicherung nicht oder nur mit unverhältnismässig hohem Aufwand möglich» ist und «das Interesse der betroffenen Person an der Löschung als gering anzusehen» ist[38]. Das Liechtensteiner DSG erklärt sich dabei als weltweit anwendbar: Es soll immer dann Anwendung finden, wenn ein Unternehmen zwar keine Niederlassung in einem EWR-Mitgliedsstaat hat, aber in den Anwendungsbereich der DSGVO fällt[39]. Es kann somit mit guten Gründen vertreten werden, dass Schweizer Unternehmen im Anwendungsbereich der DSGVO sich auch dann auf diese Bestimmung berufen können, wenn sie nicht Personendaten von Personen anderer EWR-Mitgliedsstaaten bearbeiten.

de Tools einsetzt, um allenfalls früher auf diesem Datenträger gespeicherte Daten wieder sichtbar zu machen, wesentlich höher. Insbesondere in der Fallvariante des Finders dürfte die beschriebene Löschmethode nicht genügen; der zuvor für heikle Daten im Klartext benutzte USB-Stick müsste «sicher» gelöscht werden, beispielsweise durch gezieltes Überschreiben.

Logische Löschung dank organisatorischer Massnahmen

Vergleichbare Überlegungen sind auch für Geschäftsanwendungen mit strukturierten Daten möglich. Setzt ein Unternehmen beispielsweise eine Anwendung ein, welche zwar den Zugriff auf «gelöschte» bzw. inaktivierte Daten für die Benutzer der Anwendung sperrt, sind diese aber nach wie vor im Datenbanksystem des Unternehmens, auf welchem die Anwendung aufsetzt, vorhanden und im Grunde von jedem Mitarbeiter mit Administratorenrechten und Standardkenntnissen im Datenbankmanagement abrufbar, so dürften die Daten noch nicht als «logisch» gelöscht gelten.

Ab welchem Moment werden die zur Verhinderung des Datenzugriffs getroffenen Massnahmen von einem «put beyond use» zu einer «logischen Löschung» und genügen daher datenschutzrechtlich?

An diesem Punkt wird das Unternehmen organisatorische Massnahmen prüfen müssen. Es kann beispielsweise (1) den Administratoren untersagen, auf die als «gelöscht» markierten Datensätze zuzugreifen, selbst wenn ein Vorgesetzter dies verlangen sollte, (2) vorschreiben, dass Datenbankzugriffe nur nach dem Vier-

Augen-Prinzip erfolgen müssen, um die Durchsetzung dieser Weisung sicherzustellen und (3) die Einhaltung dieser Weisungen durch Protokolle überwachen und im Widerhandlungsfalle Sanktionen androhen. Werden solche oder vergleichbare Massnahmen getroffen, wird die Wahrscheinlichkeit, dass auf die gelöschten Daten zugegriffen wird, in der Praxis nur noch gering sein: Jeder Administrator müsste persönliche Sanktionen riskieren, nur um anderen Mitarbeitern Zugang zu gelöschten Daten zu verschaffen. Das werden sie wahrscheinlich nicht tun, und erst recht nicht zwei von ihnen. Das wird normalerweise genügen aus datenschutzrechtlicher Sicht, damit die Daten als gelöscht gelten können. Auch hier sind Anleihen ans Strafrecht und dem dort entwickelten Vertrauensprinzip möglich[33], wonach im Rahmen von arbeitsteiligen Unternehmungen im Hinblick auf die eigenen Sorgfaltspflichten grundsätzlich darauf vertraut werden darf, dass die mitwirkenden Personen sich pflichtgemäss Verhalten[34].

Bei der Rechtfertigung muss gezeigt werden, dass die Interessen der betroffenen Personen an einer Löschung geringer sind als die Interessen des Datenbearbeiters und weiterer Personen.

Im genannten Beispiel verbleibt noch das Risiko eines Behördenzugriffs, eines Zugriffs durch unbefugte Dritte und einer Fehlfunktion der Softwarelösung. Letzteres dürfte im Falle einer professionell entwickelten und ausreichend getesteten Anwendung normalerweise unter der Relevanzschwelle liegen. Ersteres dürfte in der Praxis keine Schwierigkeiten bereiten: Im Rahmen einer behördlichen oder gerichtlichen Edition wird normalerweise nur herauszugeben sein, was für das Unternehmen ohne Weiteres an Daten verfügbar ist. Die Chance, dass ein Gericht oder eine Behörde die Herausgabe der «rohen» Daten in der Datenbank verlangt, ist normalerweise ebenso gering wie die Aufforderung, alte Backups nach Daten abzusuchen. Beides kommt normalerweise nicht vor und ist daher auch datenschutzrechtlich für die Frage, ob die Daten als gelöscht gelten können, mangels anderer Erfahrungen nicht relevant. Dasselbe gilt schliesslich für den Fall des unbefugten Zugriffs durch Dritte: Ist mit einem solchen zu rechnen, befindet sich das Unternehmen ungeachtet der Frage der Löschung in einer Verletzung der DSGVO bzw. des DSG bezüglich Datensicherheit. Ist umgekehrt formuliert die Datensicherheit angemessen, so wird auch das Restrisiko eines Zugriffs auf die «nackte» Datenbank (und damit auch die gelöschten Datensätze) so gering sein müssen, dass die logische Löschung der Daten auch im Hinblick auf unbefugte Zugriffe durch Dritte nicht mehr in Frage zu stellen ist.

Rechtfertigungsgründe – auch unter der DSGVO?

Ist eine logische (oder weitergehende) Löschung, Anonymisierung oder Vernichtung von Personendaten trotz allem nicht möglich, bietet sich im Anwendungsbereich des DSG immerhin noch die Möglichkeit einer Rechtfertigung im Sinne von Art. 13 Abs. 1 DSG an. Es muss dazu gezeigt werden, dass die Interessen der betroffenen Personen an einer Löschung – mithin die Risiken einer Nichtlöschung – geringer sind als die weiteren Interessen des Datenbearbeiters und etwaiger weiterer Personen. Dazu gehört auch der (unvermeidbare) Aufwand der Löschung, wie er beispielsweise bei Backups naturgemäss entstehen würde, wenn einzelne Informationen daraus herausgefiltert werden müssten – ein enormer Aufwand.

Die DSGVO kennt eine solche Rechtfertigungsmöglichkeit zwar nicht. Wenn jedoch die Entfernung von Datensätzen aus einem Datenbanksystem ihrerseits Risiken[35] oder erhebliche Aufwendungen mit sich bringt, kann die Weiterbearbeitung der betreffenden Datensätze mitunter einen «kompatiblen» Zweck im Sinne von Art. 5 Abs. 1 Bst. b DSGVO darstellen und vor diesem Hintergrund zulässig sein. Das Ergebnis ist mit dem einer Rechtfertigung vergleichbar: Der Sekundärzweck bestünde in diesen Fällen gewissermassen in der Gewährleistung der Funktion und des stabilen Betriebs der verwendeten Softwarelösung, bis eine endgültige Löschung möglich ist. Zulässig wäre dieser Sekundärzweck allerdings nur, wenn die Kriterien nach Art. 6 Abs. 4 DSGVO erfüllt sind.

Dies dürfte im genannten Beispiel der Geschäftsanwendung der Fall sein, sofern sie keine besonders schützenswerten Personendaten im Sinne von Art. 9 und 10 DSGVO enthalten: Es besteht ein Zusammenhang zwischen dem ursprünglichen und dem neuen Zweck. Die Personendaten stehen weiterhin unter der Kontrolle des Unternehmens, welches sie zur Erfüllung eines Vertrages zwecks Verwendung im Rahmen der betreffenden Geschäftsanwendung erhoben hat. Im Rahmen der normalen Geschäftstätigkeit werden sie nicht mehr verwendet, womit das Risiko, dass auf sie zugegriffen wird und sie verwendet werden, gering ist. Schliesslich sind diverse Sicherheitsvorkehrungen getroffen worden, einschliesslich Zu-

gangsbeschränkungen, die dafür sorgen, dass gewöhnliche Benutzer keinen Zugang zu den Daten mehr haben. Wird davon ausgegangen, dass für diesen Sekundärzweck ein eigener Rechtsgrund im Sinne von Art. 6 Abs. 1 DSGVO erforderlich ist, dürfte sich vor diesem Hintergrund ein berechtigtes Interesse im Sinne von Bst. f ebenfalls vertreten lassen.

Restrisiken gibt es immer – Rückschaufehler auch

Selbstverständlich verbleibt in allen Fällen ein Restrisiko, dass an sich gelöschte Personendaten trotzdem in die Hände von Mitarbeitern, Behörden oder unbefugten Dritten gelangen. Wenngleich dieses Risiko vom Gesetzgeber durch sein Verständnis des Begriffs des «Löschens» – wie in diesem Beitrag dargelegt – akzeptiert ist, kann die Verwirklichung des Risikos einem Unternehmen dennoch erhebliche Schäden zufügen. Dabei stehen nicht nur Reputationsrisiken zur Diskussion, sondern auch datenschutzrechtliche Haftungs- und Sanktionsrisiken. Der Grund hierfür liegt im Hang der Datenschutzbehörden und Gerichte, es hinterher immer besser zu wissen und zu begründen, warum weitere oder andere Massnahmen hätten getroffen werden müssen. Dies wird in der Wissenschaft als «hindsight bias» oder auf Deutsch als «Rückschaufehler» bezeichnet. Immerhin können die dargelegten Überlegungen einem Unternehmen helfen zu begründen, warum seine Löschkonzepte den Anforderungen der DSGVO bzw. des DSG genügen, auch wenn die zur Diskussion stehenden Personendaten nicht gänzlich «weg» sind, sondern eben bloss kaum mehr zugänglich sind. Dies stellt bisher übrigens den Regelfall dar und ist angesichts des Sinns und Zwecks der Löschung auch nicht zu beanstanden: In allererster Linie dient die Löschung von Personendaten dazu, dass das Unternehmen selbst die fraglichen Daten nicht mehr für seine Zwecke bearbeitet. Selbstverständlich wird ein Unternehmen seine Löschkonzepte regelmässig überprüfen müssen, da sich die Mittel zur Re-Identifikation und das Interesse an deren Einsatz im Laufe der Zeit ändern können. ■

Die Datenschutzbehörden und Gerichte haben einen Hang, es hinterher immer besser zu wissen und begründen, warum weitere oder andere Massnahmen hätten getroffen werden müssen.

Fussnoten

1 Art. 4 Abs. 2 DSG.
2 Art. 5 Abs. 1 Bst. e DSGVO.
3 Art. 83 Abs. 5 Bst. a DSGVO.
4 Am 30. Oktober 2019 verhängte der Berliner Beauftragte für Datenschutz und Informationsfreiheit gegen die Deutsche Wohnen SE ein Bussgeld von rund 14,5 Mio. Euro, weil Mieterdaten in einem unlöschbaren Archiv gespeichert waren. Der Entscheid wurde angefochten.
5 Art. 17 DSGVO; in der Schweiz: Art. 12 Abs. 2 Bst. b DSG.
6 Immerhin kann die betroffene Person dagegen zivilrechtlich vorgehen (Art. 15 DSG) und auch der EDÖB kann einschreiten (Art. 29 DSG).
7 Art. 5 Abs. 4 E-DSG (Stand Beratung im Nationalrat, 25. September 2019): Personendaten «werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind».
8 Art. 5 Abs. 1 Bst. e DSGVO.
9 Art. 17 Abs. 1 DSGVO.
10 Art. 5 Abs. 4 E-DSG.
11 Ansonsten würde es keinen Sinn machen, die Anonymisierung zuzulassen. Der Fehler dürfte aufgrund der unbedachten Übernahme der bisherigen Regelung aus Art. 5 DSG entstanden sein, wo von Vernichten die Rede ist, dies aber synonym zu Löschen verwendet wird. So auch Rosenthal David, Der Entwurf für ein neues Datenschutzgesetz, in: Jusletter 27. November 2017, Rz. 28.
12 Art. 28 Abs. 4 E-DSG.
13 BVGE 2015/13, Erw. 3.3.4.
14 BBl 2017 7021.
15 Ebd.
16 Etwa, weil eine betroffene Person es geschafft hat, einen Richter davon zu überzeugen, dass aufgrund der Risiken nur eine Vernichtung angemessen ist und nicht bloss eine Löschung. Datenschutzrechtlich macht diese Begründung allerdings keinen Sinn, da es nur darauf ankommen kann, ob «danach» noch Personendaten im Sinne des Gesetzes vorliegen. Daher kann in solchen Fällen zwar ein dem Risiko angemessenes Löschverfahren verwendet werden; die Vernichtung des Datenträgers wird darüberhinaus aber nie erforderlich sein, ausser ein Löschen steht nicht zur Verfügung, wenn z.B. sich eine Schrift auf einer Unterlage nicht entfernen lässt, ohne die Unterlage zu zerstören.
17 Veil Winfried, in: Gierschmann Sibylle/Schlender Katharina/Stentzel Rainer/Veil Winfried (Hrsg.), Kommentar Datenschutzgrundverordnung, Köln 2018, Art. 17 N 84 f.; Herbst Tobias, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz – Kommentar, 2. Aufl., München 2018, Art. 4 Nr. 2 Rn. 36.
18 Härting Niko, Datenschutz-Grundverordnung, 1. Aufl., 2016 Köln, Rn. 701.

Fussnoten (Fortsetzung)

19 Dammann Ulrich, in: Simitis Spiros (Hrsg.)., Bundesdatenschutzgesetz – Kommentar, 8. Aufl., Baden-Baden 2014, § 3 Rn. 175.

20 Österreichische Datenschutzbehörde, Entscheid vom 12. Dezember, 2018 (DSB-D123.270/0009-DSB/2018), D.2.

21 <https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V1.1_60_L%C3%B6schen_V1.0_uagsdmbs_final.pdf>.

22 Erw. 26 DSGVO.

23 Dazu ausführlich: Rosenthal David, Personendaten ohne Identifizierbarkeit?, in: digma 4/2017.

24 Österreichische Datenschutzbehörde, Entscheid vom 12. Dezember, 2018 (DSB-D123.270/0009-DSB/2018), D.2.

25 Ebd., m.w.H.

26 Ebd.

27 Ebd., m.w.H.

28 Ebd.

29 Auch der Entscheid spricht in Erw. D.2 den Fall der «Schwärzung» als Löschungsmethode an, indem er auf einen anderen Entscheid zum Thema verweist, der allerdings nicht unter der DSGVO erging.

30 Art. 13 Abs. 1 DSG.

31 Art. 12 Abs. 3 StGB.

32 BGE 135 IV 56 E. 2.1; BGer v. 8. März 2019, 6B_1050/2018, E. 2.2; BGE 130 IV 7 E. 3.2; BGE 127 IV 34 E. 2.a; BGer v. 1. März 2018, 6B_351/2017, E. 1.3.1.

33 BGE 120 IV 300 E. 3.d.; Donatsch Andreas, Sorgfaltsbemessung und Erfolg beim Fahrlässigkeitsdelikt, Zürich 1987, 192; Donatsch Andreas/Tag Brigitte, Strafrecht I, Verbrechenslehre, Zürich 2013, 355; Stratenwerth Günter, Schweizerisches Strafrecht, AT I, Bern 2011, 511.

34 Stratenwerth Günter/Wohlers Wolfgang, Schweizerisches Strafgesetzbuch, Handkommentar, Zürich 2013, Art. 12 N 12; Donatsch/Tag (Fn. 32), 355.

35 Sieht eine Softwareanwendung ihrerseits nicht die Löschung von Datensätzen vor, dürfen Datensätze in der Datenbank normalerweise nicht einfach gelöscht werden, auch wenn ein direkter Zugriff auf die Datenbank technisch möglich ist. Eine solche direkte Löschung kann zu Fehlfunktionen und insbesondere Fehlzuordnungen führen, weil zum Beispiel durch das «eigenmächtige» Entfernen von Datensätzen die restlichen Datensätze sich nicht mehr dort befinden, wo die Software sie erwartet, weil die verbliebenen Datensätze in der Datenbank an die leeren Stellen «nachrücken».

36 Art. 12 Abs. 2 Bst. b DSG.

37 Art. 13 Abs. 1 DSG.

38 Art. 35 Abs. 1 FL-DSG.

39 Art. 2 Abs. 3 Bst. c FL-DSG.

Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement **digma** (4 Hefte des laufenden Jahrgangs) à **CHF 178.00**
(Versandkosten: Schweiz inklusive)

Name Vorname

Firma

E-Mail

Strasse/Nr.

PLZ Ort

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:

Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8001 Zürich
Telefon +41 44 200 29 29
Telefax +41 44 200 29 28
E-Mail: zeitschriften@schulthess.com
Homepage: www.schulthess.com

Schulthess §