cognitio

studentisches Forum für Recht und Gesellschaft

Data Breach Notification

Melde- und Benachrichtigungspflicht bei Datenschutzverletzungen

MEIKE SPITZ

Zitiervorschlag

SPITZ, Data Breach Notification,
in: cognitio 2020/2.

URL: cognitio-zeitschrift.ch/2020-2/Spitz

DOI: 10.5281/zenodo.4311213

ISSN: 2624-8417

cognitio

studentisches Forum für Recht und Gesellschaft

Data Breach Notification

Melde- und Benachrichtigungspflicht bei Datenschutzverletzungen

MEIKE SPITZ*

Cyberangriffe und Datenpannen häufen sich. Mit ihnen nehmen auch die Schäden für Unternehmen, vor allem aber für die natürlichen Personen zu, welche hinter den jeweiligen Daten stehen. Kaum ein Tag vergeht, ohne dass nicht davon berichtet wird – und das nicht erst seit Inkrafttreten der Datenschutzgrundverordnung (DSGVO) in der Europäischen Union (EU). Inwiefern können Meldepflichten hier Abhilfe verschaffen und wie steht es um die gesetzlichen Regelungen in der EU und der Schweiz? Die folgende Arbeit soll diesen Fragen nachgehen und kritisch beleuchten. Zudem wird auf gewisse Schwachpunkte und Unklarheiten der Regelungen hingewiesen.

Inhaltsübersicht

* Die Autorin studiert Rechtswissenschaften an der Universität Luzern. Verfasst wurde die Arbeit im Rahmen des Seminars «CH- und EU-Datenschutzrecht: Grundzüge und aktuelle Fragestellungen», geleitet von Dr. Mira Burri und Dr. Reto Fanger. Für Rückfragen wenden Sie sich bitte an: meike.spitz@stud.unilu.ch.

I. Einleitung

Am 22. Juni 2018 kam es bei der Fluggesellschaft *British Airways (BA)* zu einer Cyberattacke, die über zwei Monate lang nicht bemerkt wurde. Das Unternehmen hatte erhebliche Mengen an persönlichen Daten ohne angemessene Sicherheitsmassnahmen verarbeitet. Cyberkriminelle hatten dabei potenziell Zugriff auf persönliche Daten von rund 429'000 Kundinnen und Kunden und Belegschaftsmitgliedern. Darunter befanden sich unter anderem die Namen, Adressen und Kreditkarteninformationen von 244'000 Kundinnen und Kunden (in 77'000 Fällen davon war sogar der dazugehörige Sicherheitscode betroffen). Hinzu kamen Nutzernamen und Passwörter von Beschäftigten sowie von Administratorinnen und Administratoren. Als die Fluggesellschaft durch Dritte vom Datenleck erfuhr, informierte sie unverzüglich der DSGVO entsprechend die Aufsichtsbehörde und die von der Datenpanne Betroffenen.[1] Zudem versprach sie, alle Kundinnen und Kunden zu entschädigen, die durch einen Diebstahl ihrer Kartendaten finanzielle Verluste erlitten hatten.

Es hätte die höchste aller bisher verhängten Bussen nach der DSGVO werden können. Ursprünglich kündigte die britische Datenschutzbehörde, das *Information Commissioner's Office (ICO)*, der *BA* ein Bussgeld in Höhe von rund 180 Millionen Pfund wegen eines Verstosses gegen die Sicherheit der Verarbeitung (Art. 32 DSGVO) an.[2] Aufgrund der Corona-Pandemie und der damit einhergehenden schwierigen wirtschaftlichen Lage des Unternehmens wurde letztlich nur ein Bussgeld in Höhe von 20 Millionen Pfund verhängt.[3]

Es lässt sich nur ausmalen, wie hoch die finanziellen Schäden wären, wenn das Datenleck noch später bemerkt worden wäre oder der Vorfall nach der Entdeckung nicht publik gemacht worden wäre.

Für manche gelten Daten, insb. *Personendaten*, daher auch als das «Gold des 21. Jahrhunderts».[4] Der wirtschaftliche und monetäre Wert solcher Daten kann immens sein[5] und angesichts der stetig fortschreitenden Digitalisierung aller Lebensbereiche stellen sich laufend neue Herausforderungen bezüglich der Gewährleistung einer angemessenen Datensicherheit. Neue Technologien, wie bspw. *Cloud Computing* oder *Big Data*, bieten nicht nur neuen Nutzen, son-

1 Vgl. den Entscheid des ICO in Bezug auf BA vom 16. Oktober 2020, S. 17 ff. und S. 24.
2 Vgl. hierzu die Pressemeldung des ICO «Intention to fine British Airways £183.39m under GDPR for data breach» vom 8. Juli 2019.
3 Vgl. hierzu die Mitteilung des ICO «ICO fines British Airways £20m for data breach affecting more than 400,000 customers» vom 16. Oktober 2020; vgl. auch den Entscheid des ICO in Bezug auf BA vom 16. Oktober 2020.
4 Vgl. BAERISWYL BRUNO, Das «Datenleck» als Standard, in: digma (Zeitschrift für Datenrecht und Informationssicherheit), 2015/Heft 3, S. 80 f., S. 80.
5 Vgl. EBNETER MATTHIAS, Informationspflichten im Zusammenhang mit «Data Security Breaches», in: Jusletter vom 07.06.2010, Rz. 1.

dern stellen immer auch neue Gefahrenquellen dar: Aufgrund der immer umfangreicheren Datenerfassung und Verarbeitung sowie des stetig steigenden Interesses an Daten, erscheinen Szenarien sog. *Datenpannen* immer wahrscheinlicher – ja fast gar alltäglich.[6] Die zugrunde liegenden Konstellationen sind vielfältig: sei es durch schlichte Unaufmerksamkeit, Unwissen oder gar durch Angriffe von Kriminellen, welche eine Sicherheitslücke ausnutzen.[7] Die persönlichen und wirtschaftlichen Folgen einer Datenpanne können gravierend sein und oft nur sehr schwer überblickt werden.[8] Eine absolute Sicherheit der Dateninfrastruktur anzustreben erscheint daher illusorisch.[9] Eine Regulierung wird unumgänglich: In den Fokus rückt folglich eine Pflicht zur *Data Breach Notification*.[10]

Die vorliegende Arbeit soll einen Überblick über die Entwicklung einer solchen Meldepflicht bei Datenschutzverletzungen in der Schweiz und der EU[11] verschaffen und dabei deren Umgang erläutern. Aufgrund der Komplexität der Materie wird vereinzelt auf weiterführende Hinweise verwiesen. Den Schwerpunkt der Arbeit bilden das auslösende Moment einer *Melde- und Benachrichtigungspflicht* und die Fragen, wann überhaupt eine relevante Datenschutzverletzung besteht, innerhalb welches Zeitraums gemeldet werden muss und welchen Inhalt eine Meldung aufweisen muss.
Zunächst wird kurz auf die aktuelle Situation in der Schweiz unter dem geltenden Bundesgesetz über den Datenschutz (DSG) eingegangen. Sodann wird die Regelung der Melde- und Benachrichtigungspflicht in der DSGVO ausführlich behandelt, welche in gewissen Fällen auch auf in der Schweiz ansässige Unternehmen und Organisationen Anwendung finden kann.[12]
Die DSGVO gehört nicht zum Schengen-Acquis. Zwecks Erhaltung eines von der EU anerkannten Datenschutzniveaus soll das datenschutzrechtlich ohnehin überholte DSG jedoch den europäischen Anforderungen angenähert werden. Zudem enthält die von der Schweiz zu ratifizieren beabsichtigte revidierte Europäische Datenschutzkonvention (SEV Nr. 108) ähnliche Schutzanforderungen.[13] Da bei deren Ausarbeitung darauf geachtet wurde, dass sie mit den revidierten Regelungen der EU konform und insgesamt weniger detailliert ist (geregelt werden sollen nur Mindeststandards)[14], wird auf diese nicht weiter eingegangen. Ebenfalls nicht berücksichtigt wird die zum Schengen-Acquis gehörende Richtlinie (EU) 2016/680, welche in Art. 30 und 31 ebenso eine Melde- und Benachrichtigungspflicht vorsieht.

Schliesslich wird unter Berücksichtigung des Vorentwurfs zum Bundesgesetz über den Datenschutz (VE-DSG) auf die im Entwurf (E-DSG) geregelte Melde- und Benachrichtigungspflicht eingegangen und diese mit der Regelung in der DSGVO verglichen.

6 BAERISWYL (Fn. 4), S. 80 f.; EBNETER (Fn. 5), a.a.O.

7 Vgl. Agentur der Europäischen Union für Grundrechte (FRA), Handbuch zum europäischen Datenschutzrecht, 24.05.2018, S. 204; vgl. KLEINER JAN/STOCKER LUKAS, Data Breach Notifications, in: digma (Zeitschrift für Datenrecht und Informationssicherheit), 2015/Heft 3, S. 90 ff., S. 90.

8 Vgl. BAERISWYL (Fn. 4), a.a.O.

9 Vgl. HÄMMERLI BERNHARD M., Wie oft bin ich schon gehackt worden?, in: digma (Zeitschrift für Datenrecht und Informationssicherheit), 2015/Heft 3, S. 82 ff., S. 82 ff.; BAERISWYL (Fn. 4), a.a.O.; EBNETER (Fn. 5), Rz. 2.

10 KLEINER/STOCKER (Fn. 7), a.a.O.; ferner bereits Bundesamt für Justiz (BJ), Normkonzept zur Revision des Datenschutzgesetzes (Bericht der Begleitgruppe Revision DSG), 29.10.2014, S. 20 f.

11 Als miteinbezogen gelten auch die Mitgliedstaaten des Europäischen Wirtschaftsraums (EWR).

12 Hierauf wird nicht eingegangen, vgl. aber Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Die EU-Datenschutzgrundverordnung und ihre Auswirkungen auf die Schweiz, 06.12.2018, S. 3 f. und S. 6 ff.

13 Bundesrat, Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.09.2017, BBl 2017 6941 ff., S. 6943 f.; FREI NULA, Die Revision des Datenschutzgesetzes aus europarechtlicher Sicht, in: Jusletter vom 17.09.2018, Rz. 26.

14 FREI (Fn. 13), Rz. 8.

Zum Abschluss erfolgt eine Gesamtwürdigung der im Entwurf geregelten Meldepflicht, wobei im Rahmen einer kritischen Würdigung auf verbleibende Unklarheiten und Schwachpunkte hingewiesen wird.

Ferner ist darauf hinzuweisen, dass kurz vor Fertigstellung dieses Aufsatzes eine endgültige Fassung des zu revidierenden DSG (revDSG) veröffentlicht wurde. Die hier zu behandelten Themen haben dabei allerdings keine inhaltliche Änderung erfahren.[15]

II. Entwicklung der *Data Breach Notification* und Umgang

Ursprünglich kommt die Pflicht zur Meldung von *Data Breaches* aus den Vereinigten Staaten von Amerika (USA).[16] Mittlerweile treten Datenpannen immer häufiger auf, oftmals begleitet von grossen Schäden, insb. auch für die privaten Betroffenen. Um diese Schäden möglichst gering zu halten, müssen relevante Vorfälle gemeldet und publiziert werden. Ansonsten fehlen wichtige Erfahrungswerte, und die Aufsichtsbehörden und die betroffenen Personen können keine Vorkehrungen treffen.[17] Eine Offenlegung dient so präventiv auch der Vermeidung von gleichen oder ähnlichen Vorfällen. Cyberkriminelle etwa haben es nämlich häufig nicht nur auf ein konkretes Zielobjekt abgesehen.[18]
Zudem könnten die Verantwortlichen für die Verarbeitung von Personendaten durch Meldepflichten dazu bewegt werden, sich dem Thema *Datensicherheit* eingehender zu widmen. Denn die Meldung, Opfer eines Cyberangriffs geworden zu sein, kann unerwünschte Aufmerksamkeit nach sich ziehen und einen Ruf nachhaltig beschädigen.[19] Hinzu kommen zahleiche weitere negative (letztlich finanzielle) Folgen, welche eine *Data Breach* für ein Unternehmen mit sich bringen kann.[20] Letztlich kann eine Meldepflicht in dieser Hinsicht auch als *Nudge*[21] angesehen werden.

Im Folgenden wird untersucht, inwiefern die *Data Breach Notification* Eingang in die europäische und schweizerische Rechtsordnung gefunden hat.
Vorab ist noch zu bemerken, dass nicht jede Verletzung der Datensicherheit gleich eine vorliegend zu beachtende Datenschutzverletzung darstellt: Nur wenn *personenbezogene Daten* im Sinne von Art. 4 Nr. 1 DSGVO betroffen sind, kann diesbezüglich überhaupt eine relevante Datenschutzverletzung vorliegen.[22] Gemeint sind demnach Daten,

15 Es kam lediglich zu Normverschiebungen und redaktionellen Anpassungen, weswegen in diesem Aufsatz auf eine Überarbeitung in dieser Hinsicht verzichtet wurde. Beim jeweils ersten Artikel einer betreffenden Norm wird in den Fussnoten auf die Verschiebung hingewiesen.

16 ROSENTHAL DAVID, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter vom 20.02.2017, Rz. 93; KLEINER/STOCKER (Fn. 7), S. 92; EBNETER (Fn. 5), Rz. 4.

17 Vgl. FRA, Handbuch Datenschutzrecht (Fn.7), S. 204 f.; KLEINER JAN, Meldepflicht bei Datenschutzverletzungen, in: digma (Zeitschrift für Datenrecht und Informationssicherheit), 2017/Heft 3, S. 170 ff., S. 171; ferner bereits KLEINER/STOCKER (Fn. 7), S. 93; siehe auch MARTINI MARIO, in: Paal Boris P./Pauly Daniel A., Datenschutz-Grundverordnung Bundesdatenschutzgesetz (Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG), 2. Aufl., München 2018, N 5 zu Art. 33 DSGVO.

18 KLEINER (Fn. 17), a.a.O.; siehe auch MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 5 und 11 zu Art. 33 DSGVO.

19 KLEINER (Fn. 17), a.a.O.; ferner bereits KLEINER/STOCKER (Fn. 17), a.a.O.; siehe auch MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 11 zu Art. 33 DSGVO.

20 Vgl. ausführlich zu den möglichen Folgen bzw. Kosten einer *Data Breach* IBM Security/Ponemon Institute, Cost of a Data Breach, Report 2019.

21 Von einem *Nudge* kann insb. deshalb gesprochen werden, weil ein vernünftiges Unternehmen wohl ausreichend Zeit und Mittel in die Sicherheit der Dateninfrastruktur investieren wird, um eine Datenpanne möglichst zu verhindern (letztlich also ein erwünschtes Verhalten erbringt). Kommt es gar nicht erst zu einer Datenpanne, bedarf es auch keiner Meldung an eine Aufsichtsbehörde, wodurch eine unerwünschte Öffentlichkeit und finanzielle Folgen vermieden werden können.

22 MATTIG CORNELIA, Achtung, wir haben eine Datenpanne! Was nun?, in: Expert Focus,

die sich auf eine identifizierte oder direkt/indirekt identifizierbare *natürliche Person* beziehen.[23]

Diese Auffassung entspricht auch der künftigen Schweizer Regelung in Art. 4 lit. a E-DSG[24]. Im aktuellen DSG fallen unter Personendaten gemäss Art. 3 lit. a und b DSG zudem noch Daten *juristischer Personen*. Auf deren Schutz soll künftig in Übereinstimmung mit europäischen und anderen Rechtsordnungen verzichtet werden.[25] Zu bemerken ist, dass von Daten juristischer Personen in der Regel schnell auf eine natürliche Person geschlossen werden kann.[26]

III. Ausgangslage: Situation unter dem aktuellen DSG

Neben spezialgesetzlichen Meldepflichten findet sich im aktuellen DSG noch keine explizite Pflicht zur Meldung von Datenschutzverletzungen an eine Aufsichtsbehörde und/oder[27] die betroffene Person.[28] Auch der Begriff einer Datenschutzverletzung wird nicht definiert.[29] Gemäss der Lehre kann eine Meldepflicht einzig gegenüber der betroffenen Person bei gravierenden Verstössen erwogen werden. Theoretisch kann dieses Resultat aus dem Grundsatz der Datenbearbeitung nach *Treu und Glauben* gemäss Art. 4 Abs. 2 DSG hergeleitet werden.[30] Praktisch jedoch gibt es keine bekannten Fälle, für welche eine Meldepflicht nach Treu und Glauben gerichtlich bestätigt wurde.[31] Da aus Treu und Glauben also nur eine Meldepflicht bezüglich der betroffenen Person – und nicht bezüglich einer Aufsichtsbehörde – hergeleitet werden kann, und weil mit der Totalrevision ohnehin eine Meldepflicht in Bezug auf relevante Vorfälle eingeführt werden soll, wird die Lage unter dem aktuellen DSG vorliegend nicht weiter vertieft.[32]

IV. Regelung in der DSGVO (Art. 33/34)

Bis zum Inkrafttreten des E-DSG wird wohl noch einige Zeit vergehen.[33] Die DSGVO hingegen ist bereits am 24. Mai 2016 in Kraft getreten und ist seit dem 25. Mai 2018 in den EU-Mitgliedstaaten[34] anwendbares Recht.[35]

2019/Heft 6–7, S. 491 ff., S. 491; Artikel-29-Datenschutzgruppe der EU, 18/DE WP250rev.01, Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäss der Verordnung (EU) 2016/679 (deutsche Fassung), S. 8; KLABUNDE ACHIM, in: Ehmann Eugen/Selmayr Martin, Datenschutz-Grundverordnung (Ehmann/Selmayr, Kurzkommentar DS-GVO), 2. Aufl., München 2018, N 57 zu Art. 4 DSGVO.

23 Vgl. Erwägungsgrund 26 DSGVO; vgl. bezüglich der Identifizierbarkeit bereits BGE 136 II 508 E. 3.2 S. 513 f.

24 Die Norm findet sich neu in Art. 5 lit. a revDSG.

25 Nähere Hinweise unter BBl 2017 6941 (Fn. 13), S. 7011 und 7019; ROSENTHAL DAVID, Der Entwurf für ein neues Datenschutzgesetz - Was uns erwartet und was noch zu korrigieren ist, in: Jusletter vom 27.11.2017, Rz. 13/14.

26 RUGGLI MONIKA/RUGGLI SANDRO, Marktortprinzip, Verarbeitungstätigkeit, in: digma (Zeitschrift für Datenrecht und Informationssicherheit), 2019/Heft 1, S. 48 ff., S. 48; vgl. auch ERNST STEFAN, in: Paal Boris P./Pauly Daniel A., Datenschutz-Grundverordnung Bundesdatenschutzgesetz (Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG), 2. Aufl., München 2018, N 5–6 zu Art. 4 DSGVO.

27 Fraglich ist insb., ob nur eine Meldung an eine Aufsichtsbehörde erfolgen soll, oder ob auch die von einer Verletzung betroffene Person zu benachrichtigen ist.

28 KLEINER (Fn. 17), S. 171; siehe bereits KLEINER/STOCKER (Fn. 7), S. 92.

29 MATTIG (Fn. 22), S. 491.

30 MATTIG (Fn. 22), S. 494; BAERISWYL BRUNO, in: Baeriswyl Bruno/Pärli Kurt, Handkommentar zum Datenschutzgesetz (DSG) (Baeriswyl/Pärli, Handkommentar DSG), Bern 2015, N 18 zu Art. 4 DSGVO; EBNETER (Fn. 5), Rz. 11.

31 KLEINER/STOCKER (Fn. 7), S. 91 und 93; BAERISWYL (Fn. 4), S. 81.

32 Vgl. ROSENTHAL (Fn. 25), Rz. 63.

33 Vgl. BAERISWYL BRUNO, Mehr Transparenz im neuen DSG, in: digma (Zeitschrift für Datenrecht und Informationssicherheit), 2020/Heft 1, S. 6 ff., S. 6.

34 Bezüglich den EWR-Mitgliedstaaten seit dem 20. Juli 2018.

35 Siehe KELLER CLAUDIA, Datenschutz, Zürich 2019, S. 43.

In Art. 33 DSGVO wird eine *Meldepflicht* an die Aufsichtsbehörde bei Verletzungen des Schutzes personenbezogener Daten und in Art. 34 DSGVO eine *Benachrichtigungspflicht* der betroffenen Person statuiert.

A. Verletzung des Schutzes personenbezogener Daten

Der Begriff der *Verletzung des Schutzes personenbezogener Daten* aus Art. 33 und Art. 34 DSGVO wird in Art. 4 Nr. 12 DSGVO legaldefiniert: Eine *Verletzung* liegt vor, wenn (1.) eine Verletzung der Sicherheit eingetreten ist, die, (2.) ob unbeabsichtigt oder unrechtmässig, (3.) zur Vernichtung, zum Verlust oder zur Veränderung, oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, (4.) die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Der Begriff der *Verarbeitung* im Sinne von Art. 4 Nr. 2 DSGVO ist hierbei weit definiert zu verstehen.[36]

Eine Verletzung im Sinne von Art. 4 Nr. 12 DSGVO kann zudem nur vorliegen, wenn die *technischen und organisatorischen Massnahmen* gemäss Art. 32 DSGVO versagt haben, wodurch ein unbeabsichtigter oder unrechtmässiger Verarbeitungsvorgang erfolgen kann.[37] Werden keine solchen Massnahmen getroffen, kann auch keine Verletzung im Sinne von Art. 4 Nr. 12 DSGVO vorliegen.[38] Die Massnahmen nach Art. 32 DSGVO müssen dabei ein dem Risiko der jeweiligen Verarbeitung angemessenes Schutzniveau gewährleisten, wobei vor allem der *Stand der Technik* zu berücksichtigen ist. Insb. müssen die Massnahmen nach Art. 32 Abs. 1 lit. b DSGVO geeignet sein, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Systemen, die personenbezogene Daten verarbeiten, sicherzustellen.[39] Im Weiteren verwendet die DSGVO den unbestimmten Rechtsbegriff *Stand der Technik* mehrfach, definiert jedoch nicht näher, was darunter zu verstehen ist.[40] Abzugrenzen ist der Begriff vom *Stand der Wissenschaft und Technik*: Der *Stand der Technik* verlangt nur Massnahmen, welche zum jeweiligen Zeitpunkt marktfähig bzw. technisch realisierbar sind; die neuesten wissenschaftlichen Erkenntnisse dagegen sind nicht miteinzubeziehen. Dennoch müssen die Massnahmen einen hohen Sicherheitsstandard aufweisen: Im Gegensatz zu den *Regeln der Technik*[41] müssen sie sich in der Praxis (noch) nicht durchgesetzt haben.[42] Als Hilfestellung ist bezüglich dem *Stand der Technik* insb. auf die *ISO/IEC 27000-Normenreihe* zu verweisen.[43] Daneben sind nach Art. 32 Abs. 1 DSGVO stets auch die *Implementierungskosten* zu berücksichtigen. Die Kosten einer Massnahme sollten daher in einem angemessenen Verhältnis zum jeweiligen Verarbeitungsrisiko stehen.[44]

---

36 Für nähere Hinweise vgl. FRA, Handbuch Datenschutzrecht (Fn. 7), S. 117 ff.

37 KLABUNDE, (Fn. 22), in: Ehmann/Selmayr, Kurzkommentar DS-GVO BDSG, N 56 zu Art. 4 DSGVO.

38 Vgl. SPINDLER GERALD/DALBY LUKAS, in: Spindler Gerald/Schuster Fabian, Recht der elektronischen Medien Kommentar (Spindler/Schuster, Recht der elektronischen Medien), 4. Aufl., München 2019, N 27 zu Art. 4 DSGVO.

39 BARTELS KARSTEN U./BACKER MERLIN, Die Berücksichtigung des Stands der Technik in der DSGVO - Neue Anforderungen an die IT-Sicherheit im Datenschutz, in: Datenschutz und Datensicherheit (DuD), 2018/Heft 4, S. 214 ff., S. 215.

40 HARTUNG JÜRGEN, in: Kühling Jürgen/Buchner Benedikt, Datenschutz-Grundverordnung/BDSG Kommentar (Kühling/Buchner, DS-GVO BDSG), 2. Aufl., München 2018, N 21 zu Art. 25 DSGVO; BARTELS/BACKER, (Fn. 39), S. 214.

41 Hierbei handelt es sich um Sicherheitsmassnahmen, welche wissenschaftlich anerkannt sind und sich in der technischen Praxis bewährt und durchgesetzt haben.

42 JANDT SILKE, in: Kühling Jürgen/Buchner Benedikt, Datenschutz-Grundverordnung/BDSG Kommentar (Kühling/Buchner, DS-GVO BDSG), 3. Aufl., München 2020, N 10 zu Art. 32 DSGVO.

43 Vgl. MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 57-58 zu Art. 32 DSGVO; siehe auch JANDT, (Fn. 42), in: Kühling/Buchner, DS-GVO BDSG, N 10a zu Art. 32 DSGVO.

44 Vgl. LAUE PHILIP, in: Spindler Gerald/Schuster Fabian, Recht der elektronischen Medien Kommentar (Spindler/Schuster, Recht der elektronischen Medien), 4. Aufl., München 2019, N 7–8

Im Übrigen geht es bei der Verletzung nicht um die rechtliche Zulässigkeit der Datenverarbeitung nach Art. 6 DSGVO, welche unter anderem durch eine Einwilligung der Datenberechtigten gedeckt sein muss, sondern um den Grundsatz der Sicherheit nach Art. 5 Abs. 1 lit. f DSGVO.[45] Gezielte unzulässige Verarbeitungen von Verantwortlichen sowie Verarbeitungen unter Verstoss gegen (oder gar ohne) Rechtsgrundlagen stellen damit keine Verletzungen im Sinne von Art. 4 Nr. 12 DSGVO dar.[46] Ursächlich für einen unrechtmässigen Verarbeitungsvorgang ist diesfalls nämlich nicht eine Verletzung der Sicherheit.[47]

1. Gruppen von Sicherheitsverletzungen

Sicherheitsverletzungen bezüglich personenbezogener Daten lassen sich grob in drei Gruppen unterteilen: Die Verletzung der *Vertraulichkeit*, der *Integrität* und der *Verfügbarkeit* von Daten – wobei diese auch kombiniert auftreten können.[48]

Die *Vertraulichkeit* ist verletzt, sofern Daten unbefugt oder unbeabsichtigt offengelegt werden oder wenn eine unbefugte oder unbeabsichtigte Einsichtnahme erfolgt.[49] Es stellt sich insb. die Frage, ob dieser unbefugte Zugang letztlich auch erfolgen muss. Es ist dabei zu klären, ob die blosse Möglichkeit der Einsichtnahme ausreicht, um einen relevanten Sicherheitsvorfall anzunehmen. So kann es durch den Verlust eines Datenträgers selbst bei gegebener *Verschlüsselung*[50] theoretisch dazu kommen, dass sich darauf befindende Daten von Dritten eingesehen werden. Eine Verletzung der Sicherheit im Sinne von Art. 4 Nr. 12 DSGVO wäre daher bereits eingetreten.[51] Ob diese indes auch eine Meldepflicht nach sich zöge, beurteilt sich gemäss Art. 33 DSGVO bei der *Risikoabwägung*. Massgeblich wäre hier dann vor allem die Höhe des Risikos einer tatsächlichen Entschlüsselung.[52] Der grösste Teil der Lehre, einige Aufsichtsbehörden und der Europäische Datenschutzausschuss (EDSA) vertreten denn auch die Ansicht, dass eine *Verschlüsslung gemäss dem Stand der Technik*[53] die Meldepflicht entfallen lassen kann; ein Risiko für die betroffene Person bestünde dann nicht, vorausgesetzt die Daten sind anderweitig (vor allem mittels *Backups*) noch verfügbar.[54]

zu Art. 32 DSGVO und JANDT, (Fn. 42), in: Kühling/Buchner, DS-GVO BDSG, N 11 zu Art. 32 DSGVO.

45 BECKER FRANK, Meldungen nach Art. 33 DS-GVO, in: Zeitschrift für Datenschutz (ZD), 2020/Heft 4, S. 175 ff., S. 176; vgl. JANDT, (Fn. 42), in: Kühling/Buchner, DS-GVO BDSG, N 3–4 zu Art. 4 DSGVO.

46 SCHILD HANS HERMANN, in: Brink Stefan/Wolff Heinrich A., Beck'scher Online-Kommentar Datenschutzrecht (Brink/Wolff, BeckOK Datenschutzrecht), 32. Aufl., München 2020, N 133 zu Art. 4 DSGVO; vgl. auch KLABUNDE, (Fn. 22), in: Ehmann/Selmayr, Kurzkommentar DS-GVO BDSG, N 58 zu Art. 4 DSGVO.

47 Vgl. BECKER, (FN. 45), a.a.O.

48 HLADJK JÖRG, in: Ehmann Eugen/Selmayr Martin, Datenschutz-Grundverordnung (Ehmann/Selmayr, Kurzkommentar DS-GVO), 2. Aufl., München 2018, N 6 zu Art. 33 DSGVO; Artikel-29-Datenschutzgruppe (Fn. 22), S. 8 f.

49 Artikel-29-Datenschutzgruppe (Fn. 22), S. 8.

50 Technisch gesehen stellt die Verschlüsselung einen Vorgang dar, bei welchem Daten in Klartext unter Zuhilfenahme von Verschlüsselungsverfahren in eine nicht einfach interpretierbare Folge von Zeichen (Geheimtext) umgewandelt werden, so dass der Klartext nur unter Verwendung eines geheimen Schlüssels wiederhergestellt werden kann. Vgl. hierzu mit weiteren Hinweisen die Definition von JANDT, (Fn. 42), in: Kühling/Buchner, DS-GVO BDSG, N 19 zu Art. 32 DSGVO.

51 SPINDLER/DALBY, (Fn. 38), in: Spindler/Schuster, Recht der elektronischen Medien, N 28 zu Art. 4 DSGVO.

52 ERNST, (Fn. 26), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 94 zu Art. 4 DSGVO.

53 Vgl. zum Begriff Punkt IV.A.

54 LEIBOLD KEVIN, Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde nach Art. 33 DSGVO – auch bei Verschlüsselung?, in: ZD-Aktuell, 2019/Heft 11, 06650; andere Ansicht vgl. DIX ALEXANDER, in: Simitis Spiros/Hornung Gerrit/Spiecker genannt Döhmann Indra, Datenschutzrecht (Simitis/Hornung/Spiecker, Datenschutzrecht), Baden-Baden 2019, N 12 zu Art. 33 DSGVO, für welchen sich dies aus einem Umkehrschluss aus Art. 34 Abs. 3 lit. a DSGVO ergibt.

Eine Verletzung der *Integrität* besteht sodann in der unbeabsichtigten oder unrechtmässigen Veränderung von Daten.

Die *Verfügbarkeit* schliesslich ist verletzt, falls der Zugang zu Daten nicht mehr möglich ist. Diese Voraussetzung ist gegeben, wenn ein Verlust eingetreten ist oder indem Daten versehentlich oder absichtlich (unwiderruflich) vernichtet wurden.[55] Auch ein nur vorübergehender Verlust kann ausreichen. Eine Datenschutzverletzung im Sinne von Art. 4 Nr. 12 DSGVO besteht jedoch nur, wenn aufgrund des fehlenden Zugangs wesentliche Rechte und Freiheiten von natürlichen Personen tangiert sind, was bei einer geplanten Systemwartung z.B. nicht der Fall ist. Grundsätzlich ist stets eine *Einzelfallbetrachtung* vorzunehmen.[56]

2. Unbeabsichtigt oder unrechtmässig

Die Gründe, die zu einer Sicherheitsverletzung bezüglich personenbezogener Daten führen, sind grundsätzlich irrelevant: Egal ob durch Versäumnis eines Mitarbeiters oder aufgrund gezielten *Hackings*, relevant ist nur, dass es zu einer Sicherheitsverletzung kommt. Es ist also nicht relevant, ob diese durch fahrlässige und damit unbeabsichtigte Handlungen in Unternehmen oder durch gezielte Angriffe Dritter hervorgerufen wird.[57] Auf ein Verschulden der Verpflichteten kommt es somit nicht an. Ausschlaggebend ist vielmehr, ob eine Verletzung im Sinne von Art. 4 Nr. 12 DSGVO eingetreten ist.[58]

B. Bestehen einer Melde- und Benachrichtigungspflicht

Eine Meldepflicht im Falle einer Verletzung des Schutzes personenbezogener Daten besteht gemäss Art. 33 Abs. 1 Satz 1 DSGVO erst nach Bekanntwerden der Verletzung und entfällt nur, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Art. 34 Abs. 1 DSGVO greift hingegen nur bei einem hohen Risiko für die Rechte und Freiheiten von natürlichen Personen.
Da Art. 33 Abs. 1 DSGVO insgesamt sehr unbestimmt ist, ist dem EDSA gemäss Art. 70 Abs. 1 lit. g DSGVO der Auftrag erteilt worden, die Voraussetzungen für das Entstehen der Meldepflicht näher zu präzisieren.[59]

1. Bekanntwerden der Verletzung

Eine Meldepflicht gemäss Art. 33 Abs. 1 Satz 1 DSGVO kommt lediglich dann in Betracht, falls der oder dem Verantwortlichen eine Datenschutzverletzung im Sinne von Art. 4 Nr. 12 DSGVO bekannt wird bzw. sie oder er von ihr Kenntnis erlangt. Massgebend sind immer die *tatsächlichen Umstände*. Es ist daher unbedeutend, ob die oder der Verantwortliche den Sachverhalt selbst als Verletzung erkennt und einstuft.[60]

Eine Datenschutzverletzung kann als *bekannt* gewertet werden, sofern hinreichend klar ist, dass eine Sicherheitsverletzung aufgetreten

---

55 Artikel-29-Datenschutzgruppe (Fn. 22), S. 8.

56 Vgl. Artikel-29-Datenschutzgruppe (Fn. 22), S. 9 f. mit Beispielen.

57 FUHLROTT MICHAEL, Data Incident Management: Rechtlicher Umgang mit «Datenpannen», in: Neue Zeitschrift für Arbeitsrecht (NZA), 2019/Heft 10, S. 649 ff., S. 650.

58 ERNST, (Fn. 26), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 95 zu Art. 4 DSGVO; BRINK STEFAN, in: Brink Stefan/Wolff Heinrich A., Beck'scher Online-Kommentar Datenschutzrecht (Brink/Wolff, BeckOK Datenschutzrecht), 32. Aufl., München 2020, N 27 zu Art. 33 DSGVO; vgl. auch MANTZ RETO, in: Sydow Gernot, Europäische Datenschutzgrundverordnung Handkommentar (Sydow EU-DSGVO Handkommentar), 2. Aufl., Baden-Baden 2018, N 180 zu Art. 4 DSGVO.

59 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 20 zu Art. 33 DSGVO.

60 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 18 zu Art. 33 DSGVO; SCHULTZE-MELLING JYN, in: Taeger Jürgen/Gabel Detlev, Kommentar DSGVO – BDSG (Taeger/Gabel, Kommentar DSGVO – BDSG), 3. Aufl., Frankfurt am Main 2019, N 15 zu Art. 33 DSGVO; BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 29 zu Art. 33 DSGVO.

ist, die zu einer Beeinträchtigung des Schutzes personenbezogener Daten führt. Von einer *genügenden Kenntnis* ist auszugehen, wenn die oder der Verantwortliche zu einer sinnvollen Meldung gemäss den Vorschriften der DSGVO imstande ist.[61] Zudem müssen diese dafür Sorge tragen, dass sämtliche geeigneten technischen Massnahmen ergriffen wurden, um sofort feststellen zu können, ob eine Verletzung im Sinne von Art. 4 Nr. 12 DSGVO eingetreten ist, die einer umgehenden Meldung an die Aufsichtsbehörde und der betroffenen Personen bedarf. Die Berufung auf Nichtwissen wegen mangelnder Massnahmen ist somit nicht ausreichend.[62]

Wenn die oder der Verantwortliche bewusst bzw. absichtlich darauf hinwirkt, dass sie bzw. er im Falle einer Verletzung hiervon keine Kenntnis erhält, wird der Beginn der Meldepflicht auf diesen Zeitpunkt zurück fingiert.[63] Zu beachten ist indes, dass in Art. 33 Abs. 1 DSGVO von einem «bekannt sein», nicht von einem «bekannt sein müssen» die Rede ist; die fahrlässige Verschliessung der Kenntnisnahme ist demnach nicht erfasst.[64]

Weiter entsteht die Meldepflicht mit Eintritt einer relevanten Verletzung, allein die *Meldefrist*[65] setzt erst mit der Kenntnisnahme ein.[66] Der oder dem Verantwortlichen ist indessen ein gewisser erster Untersuchungszeitraum zu gestatten, bevor die Verletzung als ihr bzw. ihm bekannt zu gelten hat.[67]

Melden eine Auftragsverarbeiterin oder ein Auftragsverarbeiter gemäss Art. 33 Abs. 2 DSGVO eine Verletzung, ist ab diesem Zeitpunkt von der Kenntnisnahme durch die oder den Verantwortlichen und damit dem Beginn der Meldefrist auszugehen.[68]

Fraglich ist, da nicht ausdrücklich erwähnt, ob die Benachrichtigungspflicht gemäss Art. 34 Abs. 1 DSGVO auch an ein Bekanntwerden anknüpft. Dies erscheint dennoch folgerichtig: Die Auferlegung einer Benachrichtigungspflicht macht sodann nur Sinn, wenn eine Datenschutzverletzung der oder dem Verantwortlichen auch bekannt ist. Auch die Begrifflichkeit «unverzüglich» spricht hierfür.[69]

2. Voraussichtlich kein Risiko

Die Meldepflicht gemäss Art. 33 Abs. 1 Satz 1 DSGVO gilt nicht vorbehaltlos: Ein die Meldepflicht auslösender Sicherheitsvorfall liegt nur vor, wenn voraussichtlich auch ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht.

Wann genau von einem *voraussichtlich fehlenden Risiko* auszugehen ist, wird nicht definiert. In jedem Einzelfall ist insofern eine *Prognose* erforderlich, was sich aus der Verwendung

61 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, a.a.O.; SCHULTZE-MELLING, (Fn. 60), in: Taeger/Gabel, Kommentar DSGVO – BDSG, N 14 zu Art. 33 DSGVO; vgl. auch Artikel-29-Datenschutzgruppe (Fn. 22), S. 12 f. mit Beispielen.

62 Vgl. Erwägungsgrund 87 Satz 1 DSGVO; MATTIG (Fn. 22), S. 492.

63 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 19 zu Art. 33 DSGVO; SCHULTZE-MELLING, (Fn. 60), in: Taeger/Gabel, Kommentar DSGVO – BDSG, N 16 zu Art. 33 DSGVO.

64 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, a.a.O.; vgl. SCHULTZE-MELLING, (Fn. 60), in: Taeger/Gabel, Kommentar DSGVO – BDSG, N 17 zu Art. 33 DSGVO; andere Ansicht LAUE PHILIP, in: Laue Philip/Kremer Sascha, Das neue Datenschutzrecht in der betrieblichen Praxis (Laue/Kremer, Datenschutzrecht in der betrieblichen Praxis), 2. Aufl., Baden-Baden 2019, S. 267 (N 47).

65 Vgl. hierzu Punkt IV.E.

66 BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 29 zu Art. 33 DSGVO.

67 HLADJK, (Fn. 48), in: Ehmann/Selmayr, Kurzkommentar DS-GVO BDSG, N 9 zu Art. 33 DSGVO; Artikel-29-Datenschutzgruppe (Fn. 22), S. 13.

68 LAUE, (Fn. 64), a.a.O.; VON DEM BUSSCHE AXEL, in: von dem Bussche Axel/Voigt Paul, Konzerndatenschutz, 2. Aufl., München 2019, S. 152 (N 9).

69 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 31-34 zu Art. 34 DSGVO.

des Begriffs *voraussichtlich* ergibt.[70] Je nach Art der Datenschutzverletzung können dabei verschiedene Risiken für die Betroffenen vorliegen.[71]

Die in anderen Bestimmungen der DSGVO genannten Faktoren[72] können nur bedingt zur Bestimmung des Risikos herangezogen werden; dies deshalb, da das Risiko in Art. 33 Abs. 1 Satz 1 DSGVO nicht aus der Verarbeitung folgt, sondern aus der Verletzung der Sicherheit im Sinne von Art. 4 Nr. 12 DSGVO.[73]
Weiteren Aufschluss geben die allgemeine Bedeutung des Wortes *Risiko* und die Erwägungsgründe. Unter *«Risiko»* ist demnach die erhöhte Wahrscheinlichkeit des Eintritts eines potenziellen Schadens zu verstehen.[74]
Die möglichen Risiken sind zahlreich: zu nennen sind *physische, materielle und immaterielle Schäden.*[75]
Relevant für die Prognose sind damit vor allem die Eintrittswahrscheinlichkeit und die Schwere eines potenziellen Schadens.[76] Für die Annahme des *voraussichtlich fehlenden Risikos* wird kein ohnehin unmögliches Nullrisiko verlangt, sondern ein geringfügiges Risiko.[77] Von einem nur *geringfügigen Risiko* ist auszugehen, wenn unter Berücksichtigung der *potenziellen Schäden,* deren *Intensität* (Menge sowie Art der betroffenen Daten) und deren *Eintrittswahrscheinlichkeit* (Fähigkeiten Dritter, verarbeitungsspezifische Risiken) eine Meldung nicht erforderlich erscheint.[78] Je höher die Schadenssumme, desto geringere Anforderungen sind an die Eintrittswahrscheinlichkeit zu stellen.[79]

Die Meldepflicht besteht letztlich unabhängig von einem Schadenseintritt. Dahinter steckt die Idee eines *risikobasierten Ansatzes*, welcher der oder dem Verantwortlichen nur – aber immer dann – eine Meldepflicht aufbürden will, falls Schäden bei Betroffenen überhaupt möglich erscheinen: Die Meldepflicht entfällt also nur, sofern ein Schadenseintritt ausgeschlossen werden kann.[80]

Da Art. 33 Abs. 1 Satz 1 DSGVO an die Kenntnis der oder des Verantwortlichen anknüpft, ist in Bezug auf die Risikoprognose immer deren bzw. dessen Wissensstand massgebend.[81] Sie bzw. er unterliegt dabei dem Risiko, dass die Aufsichtsbehörde die getroffene Prognose für falsch erachtet.[82]

---

70 JANDT, (Fn. 42), in: Kühling/Buchner, DS-GVO BDSG, N 9 zu Art. 33 DSGVO; LAUE, (Fn. 64), in: Laue/Kremer, Datenschutzrecht in der betrieblichen Praxis, S. 265 f. (N 43).

71 Artikel-29-Datenschutzgruppe (Fn. 22), S. 28 mit Beispiel.

72 Vgl. Art. 24 Abs. 1 Satz 1, Art. 25 Abs. 1, Art. 32 Abs. 1 und Art. 35 Abs. 1 Satz 1 DSGVO.

73 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 23 zu Art. 33 DSGVO.

74 BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 35 zu Art. 33 DSGVO; vgl. auch SCHREIBER MARKUS, in: Haux Dario Henri/Picecchi Dario/Schreiber Markus, Recht und Risiko, Zürich 2019, S. 31.

75 DIX, (Fn. 54) in: Simitis/Hornung/Spiecker, Datenschutzrecht, N 14 zu Art. 33 DSGVO; bezüglich möglicher Schäden vgl. Erwägungsgrund 85 Satz 1 DSGVO.

76 SCHULTZE-MELLING, (Fn. 60), in: Taeger/Gabel, Kommentar DSGVO – BDSG, N 26 zu Art. 33 DSGVO.

77 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 22 zu Art. 33 DSGVO; vgl. auch SCHREIBER, (Fn. 74), S. 33, nach welchem sich ein Nullrisiko in technischen Bereichen nur durch ein Totalverbot durchsetzen liesse.

78 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 23–24 zu Art. 33 DSGVO; vgl. REIF YVETTE, in: Gola Peter, Datenschutz-Grundverordnung Kommentar (Gola DS-GVO Kommentar), 2. Aufl., München 2018, N 28 zu Art. 33 DSGVO; vgl. auch Erwägungsgrund 76 DSGVO.

79 BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 36 zu Art. 33 DSGVO; SCHULTZE-MELLING, (Fn. 60), in: Taeger/Gabel, Kommentar DSGVO – BDSG, N 28 zu Art. 33 DSGVO; DIX, (Fn. 54) in: Simitis/Hornung/Spiecker, Datenschutzrecht, N 11 zu Art. 33 DSGVO.

80 BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 7 und 34 zu Art. 33 DSGVO.

81 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 25-26 zu Art. 33 DSGVO; BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 37 zu Art. 33 DSGVO.

82 VON DEM BUSSCHE, (Fn. 68), in: Von dem Bussche/Voigt, S. 153 (N 13).

3. Voraussichtlich hohes Risiko und Ausnahmen gemäss Art. 34 Abs. 3 DSGVO

Hat die Verletzung *voraussichtlich ein hohes Risiko* für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt die oder der Verantwortliche die betroffene Person (Art. 34 Abs. 1 DSGVO). Wann eine Benachrichtigung des Betroffenen entfallen kann, bestimmt sich nach Art. 34 Abs. 3 lit. a–c DSGVO. Sinn und Zweck von Art. 34 DSGVO ist, dass Betroffene angemessen auf eine Datenschutzverletzung reagieren und präventiv geeignete Vorkehrungen zu ihrem Schutz treffen können.[83] Die Benachrichtigungspflicht dient zudem als Grundlage dafür, dass betroffene Personen ihre Rechte nach Art. 12 f. sowie Art. 82 DSGVO geltend machen können.[84]

a) Voraussichtlich hohes Risiko

Während Art. 33 Abs. 1 DSGVO die Meldepflicht entfallen lässt, sofern voraussichtlich kein Risiko vorliegt, setzt die Benachrichtigungspflicht gemäss Art. 34 Abs. 1 DSGVO ein voraussichtlich hohes Risiko voraus. Trotz des ähnlichen Wortlauts unterscheiden sich die beiden Vorschriften stark: Die Aufsichtsbehörde ist grundsätzlich immer zu informieren, es sei denn, es liegt nur ein geringfügiges Risiko vor. Eine betroffene Person dagegen ist nur bei einem voraussichtlich hohen Risiko zu informieren.[85]

Indem das Gesetz wiederum den Begriff *voraussichtlich* verwendet, wird klar, dass nicht jedes denkbare Risiko gemeint sein kann. Es bedarf einer *Risikoprognose*.[86] Wie auch in Art. 33 folgt die DSGVO hier dem risikobasierten Ansatz. Die Prognose dient bei Art. 34 DSGVO indes nicht der Pflichtenbegrenzung, sondern als Pflichtenauslöserin. Dies wiederum bezweckt die Reduzierung der Pflichten der oder des Verantwortlichen.[87] Aus der Formulierung von Art. 34 Abs. 1 DSGVO – dies im Gegensatz zu Art. 33 Abs. 1 DSGVO – lässt sich zudem schliessen, dass im Zweifelsfall nicht von einem hohen Risiko auszugehen ist.[88] Die DSGVO selbst definiert zwar nicht, wann ein Risiko als hoch einzustufen ist, betraut den EDSA gemäss Art. 70 Abs. 1 lit. h DSGVO aber mit der Aufgabe, die Umstände zu definieren, ab wann dieses als hoch einzustufen ist.[89]

Bei der Beurteilung des Risikos sind die Art der betroffenen Daten und deren Sensibilität, die wahrscheinlichen Folgen und die Umstände des Vorfalls (z.B. fahrlässige oder auf Vorsatz beruhende Verletzung) miteinzubeziehen.[90] Diese Parameter sind immer mit der Wahrscheinlichkeit eines Schadenseintritts in Bezug zu setzen. Ein Risiko gilt dabei als hoch, wenn die Prognose ergibt, dass ein Schadenseintritt unmittelbar droht. Droht ein hoher Schaden, genügt bereits eine geringe Eintrittswahrscheinlichkeit. Ist die Eintrittswahrscheinlichkeit hoch, kann aber auch ein voraussichtlich geringer Schaden genügen.[91] Weiteren Aufschluss zur

83 Vgl. Erwägungsgrund 86 Satz 1 DSGVO.

84 BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 2 zu Art. 34 DSGVO; MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 1 zu Art. 34 DSGVO.

85 Vgl. MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 4 zu Art. 34 DSGVO.

86 JANDT, (Fn. 42), in: Kühling/Buchner, DS-GVO BDSG, N 5 zu Art. 34 DSGVO.

87 BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 19 zu Art. 34 DSGVO.

88 SCHULTZE-MELLING, (Fn. 60), in: Taeger/Gabel, Kommentar DSGVO – BDSG, N 9 zu Art. 34 DSGVO; vgl. auch JANDT, (Fn. 42), in: Kühling/Buchner, DS-GVO BDSG, N 5 zu Art. 34 DSGVO.

89 Vgl. hingegen zur Unterscheidung der Risikohöhe die Beispiele in Artikel-29-Datenschutzgruppe (Fn. 22), S. 36-40.

90 RÄTHER PHILIPP, Die Anwendung der neuen EU-Datenschutz-Grundverordnung im Unternehmen, in: Zeitschrift für das gesamte Handels- und Wirtschaftsrecht (ZHR), 2019/Heft 2-3, S. 94 ff., S. 101.

91 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 30 zu Art. 34 DSGVO; BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 25 zu Art. 34 DSGVO; andere Ansicht vgl. LAUE, (Fn. 44), in: Spindler/Schuster, Recht der elektronischen

Frage des hohen Risikos gibt auch Art. 35 Abs. 3 DSGVO. Beispielhaft werden dort Verarbeitungsvorgänge aufgeführt, bei welchen ein voraussichtlich hohes Risiko für die Rechte und Freiheiten von natürlichen Personen anzunehmen ist. So geht z.B. von *Profiling*[92] und der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten gemäss Art. 9 Abs. 1 DSGVO oder von solchen über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 DSGVO häufig ein hohes Risiko aus.[93] Zwar nimmt Art. 35 DSGVO Bezug auf die Situation, bevor es überhaupt zur Datenverarbeitung kommt, dennoch wird daraus ersichtlich, in welchen Konstellationen die DSGVO überhaupt von einem hohen Risiko für die Rechte und Freiheiten von natürlichen Personen ausgeht.[94]

b) Ausnahme von der Benachrichtigungspflicht

In den von Art. 34 Abs. 3 lit. a–c DSGVO genannten Fällen kann die Benachrichtigung der betroffenen Person entfallen oder modifiziert erfolgen. Zudem können die Mitgliedstaaten unter engen Voraussetzungen von der *Öffnungsklausel* des Art. 23 Abs. 1 DSGVO Gebrauch machen und weitere Ausnahmen vorsehen. Das Ziel eines möglichst einheitlichen europäischen Datenschutzes kann so durch unterschiedliche mitgliedstaatliche Regelungen unterlaufen werden. Zudem wird eine grenzüberschreitende Rechtsanwendung verkompliziert.[95]

Die in Art. 34 Abs. 3 lit. a–c DSGVO vorgesehenen Ausnahmen müssen die einzelnen Mitgliedstaaten damit in jedem Fall vorsehen: diese können unter engen Grenzen[96] verlaufen, aber auch darüber hinausgehen.[97] Die Aufzählung in Art. 34 Abs. 3 DSGVO ist abschliessend, wobei lit. a–c je alternativ – nicht kumulativ – gelten. Aufgrund des unbestimmten Wortlauts sind diese restriktiv zu interpretieren, damit die Benachrichtigungspflicht nicht untergraben wird.[98]

Die Aufsichtsbehörde kann gemäss Art. 34 Abs. 4 Variante 2 DSGVO zudem per Beschluss feststellen, dass eine Ausnahme gemäss Art. 34 Abs. 3 lit. a–c DSGVO vorliegt. Dies schafft Rechtssicherheit für die Verantwortlichen, da eine Bestrafung wegen des Unterlassens einer Benachrichtigung so ausgeschlossen wird.[99] Jedoch ermächtigt Art. 34 Abs. 4 Variante 1 DSGVO die Aufsichtsbehörde auch dazu, die oder den Verantwortlichen zu verpflichten, dies nachzuholen, sofern eine Benachrichtigung noch nicht erfolgt ist und wenn unter Berücksichtigung der Wahrscheinlichkeit von einem hohen Risiko auszugehen ist. Dabei verleiht eine erhebliche Bussgeldandrohung bei Nichtbefolgung der Anweisung einer Aufsichtsbehörde[100] Art. 34 Abs. 4 Variante 1 DSGVO eine nicht zu unterschätzende Wir-

Medien Kommentar, N 4 zu Art. 34 DSGVO und REIF, (Fn. 78), in: Gola DS-GVO Kommentar, N 4 zu Art. 34 DSGVO.

92 Vgl. zum Begriff des *Profilings* Art. 4 Nr. 4 DSGVO.

93 Aus diesem Grund bedarf es bzgl. der dort genannten Verarbeitungsvorgänge auch einer *Datenschutz-Folgenabschätzung* nach Art. 35 DSGVO.

94 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 30a-30b zu Art. 34 DSGVO.

95 SYDOW GERNOT, in: Sydow Gernot, Europäische Datenschutzgrundverordnung Handkommentar (Sydow EU-DSGVO Handkommentar), 2. Aufl., Baden-Baden 2018, N 34 zur Einleitung; vgl. auch WOLFF HEINRICH AMADEUS, in: Schantz Peter/Wolff Heinrich Amadeus, Das neue Datenschutzrecht – Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, München 2017, S. 68 (N 220).

96 Eine weitere Ausnahme von der Benachrichtigungspflicht nach Art. 34 DSGVO muss nach Art. 23 DSGVO den Wesensgehalt der Grundrechte und Grundfreiheiten achten und in einer demokratischen Gesellschaft notwendig und verhältnismässig sein.

97 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 43 zu Art. 34 DSGVO.

98 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 35-36 zu Art. 34 DSGVO.

99 JANDT, (Fn. 42), in: Kühling/Buchner, DS-GVO BDSG, N 16 zu Art. 34 DSGVO; BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 46 zu Art. 34 DSGVO.

100 Vgl. Art. 83 Abs. 5 lit. e, Abs. 6 DSGVO.

kung in Bezug auf dessen Befolgung.[101] Die ähnlich lautende Vorschrift des Art. 58 Abs. 2 lit. e DSGVO knüpft bereits an eine blosse Verletzung des Schutzes personenbezogener Daten an. Um Widersprüche zu vermeiden, muss Art. 34 Abs. 4 Variante 1 DSGVO insofern als *lex specialis* angesehen werden.[102]

Gemäss Art. 34 Abs. 3 lit. a DSGVO kann eine Benachrichtigung entfallen, wenn durch *geeignete technische und organisatorische Sicherheitsvorkehrungen* ausgeschlossen werden kann, dass Dritte auf die von der Verletzung betroffenen Daten zugreifen können. Angesprochen sind namentlich *Verschlüsselungen*[103]. Dies können auch andere Massnahmen sein, sie müssen nur ebenso tauglich und zuverlässig sein. In Betracht kommen indes vor allem solche, die personenbezogene Daten für Unbefugte unzulänglich machen.[104] Nebst Verschlüsselungsverfahren kommen daher grundsätzlich auch Massnahmen zur *Pseudonymisierung*[105], räumliche Sicherheitsmassnahmen[106] oder interne Anweisungen in Frage.[107] Damit die Ausnahme greift, müssen die Massnahmen bereits vor der Schutzverletzung, also präventiv, eingesetzt worden sein und eine Verletzung gemäss Art. 34 Abs. 1 DSGVO muss dennoch eintreten. Insb. bei *Verschlüsselungen gemäss Stand der Technik*[108] sollte ein Risiko in der Regel dennoch ausgeschlossen werden können, weshalb eine Verletzung gar nicht anzunehmen wäre.[109] In dieser Hinsicht kommt Art. 34 Abs. 3 lit. a DSGVO maximal deklaratorische Bedeutung zu, er kann jedoch auch als Anreiz für Unternehmen verstanden werden, Verschlüsselungen einzusetzen.[110]

Zudem entfällt die Benachrichtigungspflicht gemäss Art. 34 Abs. 3 lit. b DSGVO, falls durch *nachfolgende Massnahmen* sichergestellt werden kann, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäss Art. 34 Abs. 1 DSGVO aller Wahrscheinlichkeit nach nicht mehr besteht. Art. 34 Abs. 3 lit. b DSGVO fungiert damit als *Auffangtatbestand*: definiert wird nur das Ziel; die Wahl der Mittel bleibt der oder dem Verantwortlichen überlassen. Die Massnahmen sind schnell zu treffen, damit nicht zwischenzeitlich ein Schaden eintritt, ansonsten muss unverzüglich eine Benachrichtigung erfolgen.[111]
Ein hohes Risiko gilt *aller Wahrscheinlichkeit* nach als ausgeschlossen, wenn die im Anschluss an die Verletzung getroffenen Schutzmassnahmen eine Verletzung der Rechte und Freiheiten der betroffenen Personen ganz verhindern oder zumindest sehr unwahrscheinlich erscheinen lassen.[112] Es bedarf damit keiner vollständigen Risikobeseitigung; verlangt wird nur der erfolgreiche Ausschluss des hohen Risikos.[113]

101 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 55 zu Art. 34 DSGVO.

102 BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 45 zu Art. 34 DSGVO; vgl. auch MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 56a zu Art. 34 DSGVO.

103 Vgl. zum Begriff der *Verschlüsselung* die Definition in Fn. 50.

104 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 38 zu Art. 34 DSGVO.

105 Vgl. zum Begriff der *Pseudonymisierung* Art. 4 Nr. 5 DSGVO.

106 Bspw. die Lagerung von Daten an einem sicheren und überwachten Ort wie in einem Rechenzentrum.

107 DIX, (Fn. 54) in: Simitis/Hornung/Spiecker, Datenschutzrecht, N 13 zu Art. 34 DSGVO; MARTINI, (Fn. 17), a.a.O.

108 Vgl. zum Begriff Punkt IV.A.

109 JANDT, (Fn. 42), in: Kühling/Buchner, DS-GVO BDSG, N 14 zu Art. 34 DSGVO; WILHELM MARIA, in: Sydow Gernot, Europäische Datenschutzgrundverordnung Handkommentar (Sydow EU-DSGVO Handkommentar), 2. Aufl., Baden-Baden 2018, N 10 zu Art. 34 DSGVO.

110 REIF, (Fn. 78), in: Gola DS-GVO Kommentar, N 8 zu Art. 34 DSGVO.

111 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 3 zu Art. 34 DSGVO; vgl. auch JANDT, (Fn. 42), in: Kühling/Buchner, DS-GVO BDSG, N 15 zu Art. 34 DSGVO.

112 HLADJK, (Fn. 48), in: Ehmann/Selmayr, Kurzkommentar DS-GVO BDSG, N 11 zu Art. 34 DSGVO.

113 WILHELM, (Fn. 109), in: Sydow EU-DSGVO Handkommentar, N 12 zu Art. 34 DSGVO; vgl. auch DIX, (Fn. 54) in: Simi-

Solche Massnahmen bestehen z.B. darin, dass bei Passwortdiebstählen unverzüglich nach dem Vorfall dafür gesorgt wird, dass die Betroffenen sich nur noch mit neu gesetzten Passwörtern einloggen können.[114] Wurden einzelnen Personen unbeabsichtigt personenbezogene Daten übermittelt, kommt als Massnahme auch der Abschluss von Vertraulichkeitsvereinbarungen in Betracht. Damit kommt Art. 34 Abs. 3 lit. b DSGVO insofern ebenfalls nur deklaratorische Bedeutung zu; denn sofern das hohe Risiko und damit auch ein Schaden aller Wahrscheinlichkeit nach ausgeschlossen werden kann, entsteht die Pflicht nach Art. 34 Abs. 1 DSGVO gar nicht erst.[115]

Gemäss Art. 34 Abs. 3 lit. c DSGVO genügt schliesslich eine *öffentliche Bekanntmachung* oder gleichsam wirksame Massnahme, wenn die Benachrichtigung mit einem unverhältnismässigen Aufwand verbunden oder aufgrund deren Vielzahl nahezu unmöglich wäre.[116] Nie darf die individuelle Benachrichtigung dazu führen, dass wegen eines zu grossen Zeitaufwands, vielen Betroffenen und schwer ermittelbaren Kontaktdaten weitere Schäden drohen.[117]

4. Dokumentationspflicht des Verantwortlichen

Die Dokumentationspflicht gemäss Art. 33 Abs. 5 DSGVO gilt unabhängig von einer erfolgten (erforderlichen) Meldung an die Aufsichtsbehörde. Wenn eine Verletzung im Sinne von Art. 4 Nr. 12 DSGVO eingetreten ist, müssen alle damit in Zusammenhang stehende Fakten dokumentiert werden. So kann die Aufsichtsbehörde die Einhaltung von Art. 33 DSGVO effektiv kontrollieren.

tis/Hornung/Spiecker, Datenschutzrecht, N 15 zu Art. 34 DSGVO.

114 BERANEK ZANON NICOLE, Melde- und Benachrichtigungspflichten nach EU DSGVO + revidiertes DSG, in: Jusletter vom 02.10.2017, Rz. 4.

115 REIF, (Fn. 78), in: Gola DS-GVO Kommentar, N 8 zu Art. 34 DSGVO.

116 BERANEK ZANON (Fn. 114), Rz. 6.

117 Vgl. MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 40 zu Art. 34 DSGVO.

Zudem dient es der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO. Auch falls die Meldepflicht wegen eines voraussichtlich nicht relevanten Risikos entfällt, ist die oder der Verantwortliche damit nicht von der Dokumentationspflicht entbunden.[118]

5. Selbstbelastungsfreiheit

Die Meldung nach Art. 33 DSGVO kann auch als Selbstanzeige aufgefasst werden und damit in Konflikt zur verfassungsrechtlich garantierten *Selbstbelastungsfreiheit („nemo tenetur, se ipsum accusare")* geraten: Die oder der Verantwortliche muss die zuständige Aufsichtsbehörde, welche auch für die Sanktionierung gemäss Art. 83 DSGVO zuständig ist (vgl. Art. 58 Abs. 2 lit. i DSGVO), über einen ihr zuvor möglicherweise nicht bekannten Sachverhalt informieren.[119]

Der Europäische Gerichtshof (EuGH) sieht die Selbstbelastungsfreiheit nicht verletzt, wenn nur rein tatsächliche Auskünfte abzugeben sind. Überschritten wird die Grenze laut EuGH erst, sofern durch die Meldung eine Zuwiderhandlung eingeräumt werden muss.[120] Im Ergebnis besteht damit nur noch ein *Geständnisverweigerungsrecht*.[121]
Die *zwingende Öffnungsklausel* des Art. 83 Abs. 8 DSGVO sieht jedoch vor, dass die

118 Vgl. MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 54-57 zu Art. 33 DSGVO; vgl. auch JANDT, (Fn. 42), in: Kühling/Buchner, DS-GVO BDSG, N 24-26 zu Art. 33 DSGVO.

119 BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 39-40 zu Art. 33 DSGVO; vgl. auch Erwägungsgrund 87 Satz 3 DSGVO, wonach eine entsprechende Meldung zu einem Tätigwerden der Aufsichtsbehörde im Einklang mit ihren in der DSGVO festgelegten Aufgaben und Befugnissen führen kann.

120 Urteil des EuGH vom 18. Oktober 1989, Rs. 374/87, *Orkem/Kommission*, Rz. 34 und 35; PAAL BORIS, Meldepflicht bei Datenschutzverstössen nach Art. 33 DSGVO – Praxisrelevante Rechtsfragen und Handlungsempfehlungen, in: Zeitschrift für Datenschutz (ZD), 2020/Heft 3, S. 119 ff., S. 123 f.; BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 41 zu Art. 33 DSGVO.

121 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 27 zu Art. 33 DSGVO; BRINK, (Fn. 58), a.a.O.

Mitgliedstaaten das Verfahren näher gestalten und insb. Verfahrensgarantien etablieren.[122] Insgesamt ist allerdings ein Verwertungsverbot bezüglich der durch die Meldetätigkeit gewonnen Informationen für spätere Verfahren zu fordern, welche sich auch auf die Mitarbeiterinnen und Mitarbeiter innerhalb der juristischen Person der oder des Verantwortlichen und der Auftragsverarbeiterin bzw. Auftragsverarbeiter erstreckt.[123]

C. Adressaten und Meldepflichtige

Adressatin oder Adressat der Meldung nach Art. 33 Abs. 1 DSGVO ist die gemäss Art. 55 DSGVO zuständige *Aufsichtsbehörde* im Sinne von Art. 4 Nr. 21 DSGVO.
Die Benachrichtigungspflicht in Art. 34 Abs. 1 DSGVO bestimmt als Adressatin oder Adressaten die von einer Verletzung betroffene natürliche Person.
Die Melde- und Benachrichtigungspflicht obliegt der oder dem *Verantwortlichen* im Sinne von Art. 4 Nr. 7 DSGVO, welche bzw. welcher allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von Personendaten entscheidet. In einem Unternehmen oder einer Organisation handelt es sich dabei in der Regel um die oder den Datenschutzverantwortlichen.[124]

Die *Auftragsverarbeiterin oder den Auftragsverarbeiter* im Sinne von Art. 4 Nr. 8 DSGVO trifft gegenüber der Aufsichtsbehörde zwar keine Meldepflicht. Indessen hat sie bzw. er gemäss Art. 33 Abs. 2 DSGVO, wenn ihr oder ihm eine potenziell relevante Verletzung bekannt wird, diese der oder dem Verantwortlichen zu melden, um einer Sanktionierung zu entgehen.[125]

Aus Art. 34 DSGVO ergibt sich zwar keine eigentliche Pflicht der Auftragsverarbeiterin oder des Auftragsverarbeiters, allerdings resultiert aus der *allgemeinen Unterstützungspflicht* nach Art. 28 Abs. 3 lit. f DSGVO eine Pflicht, die oder den Verantwortlichen im Rahmen von Art. 34 DSGVO zu unterstützen.[126]

D. Inhalt und Form der Meldung/Benachrichtigung

Art. 33 Abs. 3, Art. 34 Abs. 2 und Art. 12 DSGVO geben Aufschluss über Form und Inhalt der Meldung. In Art. 33 Abs. 3 lit. a–d DSGVO werden *Mindestanforderungen* in Bezug auf den Inhalt einer Meldung aufgeführt. Die oder der Verantwortliche muss daher, sofern für die Beurteilung durch die Aufsichtsbehörde relevant weitere Informationen zur Verfügung stellen.[127] Die Aufsichtsbehörde muss überprüfen können, ob ausreichende Massnahmen getroffen wurden. Zudem muss sie in die Lage versetzt werden, das tatsächliche Verletzungsausmass eruieren zu können, um so einen möglichst umfassenden Schutz von personenbezogenen Daten zu erreichen.[128] Verantwortliche sollten dabei beachten, dass auch freiwillige Angaben bei einer etwaigen Sanktionierung relevant werden können.[129]

Eine grobe inhaltliche Regelung des Melde- und Benachrichtigungsinhalts erscheint insgesamt sinnvoll und steht im Einklang mit

122 MOOS FLEMMING/SCHEFZIG JENS, in: Taeger Jürgen/Gabel Detlev, Kommentar DSGVO – BDSG (Taeger/Gabel, Kommentar DSGVO – BDSG), 3. Aufl., Frankfurt am Main 2019, N 119 zu Art. 83 DSGVO; siehe auch MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 33a zu Art. 31 DSGVO.

123 WILHELM, (Fn. 109), in: Sydow EU-DSGVO Handkommentar, N 29 zu Art. 33 DSGVO; BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 42 zu Art. 33 DSGVO.

124 BERANEK ZANON (Fn. 114), Rz. 8.

125 Vgl. MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 39 zu Art. 33 DSGVO; LAUE, (Fn. 64), in: Laue/Kremer, Datenschutzrecht in der betrieblichen Praxis, S. 270 f. (N 55).

126 LAUE, (Fn. 44), in: Spindler/Schuster, Recht der elektronischen Medien Kommentar, N 3 zu Art. 34 DSGVO.

127 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 44 zu Art. 33 DSGVO.

128 WILHELM, (Fn. 109), in: Sydow EU-DSGVO Handkommentar, N 17 zu Art. 33 DSGVO.

129 BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 50 zu Art. 33 DSGVO

einem effizienten Melde- und Benachrichtigungsverfahren.

Die Angaben nach Art. 33 Abs. 3 lit. b–d DSGVO stellen auch *Mindestangaben* für die Benachrichtigung der betroffenen Personen dar (Art. 34 Abs. 2 DSGVO). Einzig über die Art der Verletzung müssen Betroffene nicht benachrichtigt werden. Die oder der Verantwortliche geriete diesbezüglich aufgrund möglicher Schadenersatzansprüche von Betroffenen in der Regel wohl in einen Interessenkonflikt.[130]

1. In Bezug auf die Aufsichtsbehörde

Gemäss Umkehrschluss aus Art. 12 Abs. 1 DSGVO unterliegt die Meldung nach Art. 33 Abs. 1 DSGVO keiner bestimmten Form. Der schiere Umfang einer Meldung lässt eine (ausschliesslich) mündliche Meldung jedoch wenig praktikabel erscheinen.[131] Allein aus Beweiszwecken ist Verantwortlichen daher anzuraten die Schriftform zu verwenden.[132] Aufgrund der im Verhältnis zu einer *Data Breach* doch relativ langen Postlaufzeiten bietet es sich an, die oftmals von den Aufsichtsbehörden zur Verfügung gestellten *Meldeformulare*[133] zu benutzen.[134]

Gemäss Art. 33 Abs. 3 lit. a DSGVO muss die Meldung zwingend eine *Beschreibung der Art der Verletzung* des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO beinhalten. Um die Verletzung nachvollziehen zu können, sollten so weit möglich auch die vor der Verletzung eingesetzten technischen und organisatorischen Massnahmen aufgeführt werden. Ebenfalls sind, soweit möglich, auch Angaben zu den Kategorien und der ungefähren Zahl der betroffenen Personen, den betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze zu tätigen. Dass die oder der Verantwortliche soweit möglich zusätzliche Informationen liefern muss, ist nicht als Pflichtenbegrenzung zu verstehen. Es stellt lediglich einen Hinweis auf das Leistungsvermögen der oder des Verantwortlichen dar.[135] Fraglich erscheinen die Begriffe *Kategorien von betroffenen Personen oder personenbezogenen Datensätzen*. Ersterer Begriff handelt von den verschiedenen Gruppierungen einer Gesellschaft, die sich durch bestimmte persönliche Merkmale unterscheiden lassen: gemeint sind z.B. Kinder, andere schutzbedürftige Gruppen, Beschäftigte, Kundinnen und Kunden, Nutzerinnen und Nutzer eines sozialen Netzwerks oder einer Verwaltungsleistung.[136] Die Kategorien von betroffenen personenbezogenen Datensätzen, als zweiter Begriff, stellen die unterschiedlichen Arten von Datensätzen dar, die eine natürliche Person betreffen können: bspw. Gesundheitsdaten, Finanzdaten, Bankdaten, Reisepassnummern, Online-Kennungen, Standortdaten.[137]

Zwingend anzugeben sind gemäss Art. 33 Abs. 3 lit. b DSGVO zudem der *Name und die Kontaktdaten der oder des Datenschutzbeauftragten* oder einer sonstigen Anlaufstelle für

130 WILHELM, (Fn. 109), in: Sydow EU-DSGVO Handkommentar, N 19 zu Art. 34 DSGVO

131 BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 31 zu Art. 33 DSGVO; MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 29 und 31 zu Art. 33 DSGVO; DIX, (Fn. 54) in: Simitis/Hornung/Spiecker, Datenschutzrecht, N 21 zu Art. 33 DSGVO; vgl. JANDT, (Fn. 42), in: Kühling/Buchner, DS-GVO BDSG, N 15 zu Art. 33 DSGVO.

132 JANDT, (Fn. 42), a.a.O.; MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 31 zu Art. 33 DSGVO; SCHULTZE-MELLING, (Fn. 60), in: Taeger/Gabel, Kommentar DSGVO – BDSG, N 35 zu Art. 33 DSGVO.

133 Vgl. bspw. das Meldeformular des Bayerischen Landesamts für Datenschutzaufsicht.

134 Vgl. WILHELM, (Fn. 109), in: Sydow EU-DSGVO Handkommentar, N 25 zu Art. 33 DSGVO; vgl. auch LAUE, (Fn. 44), in: Spindler/Schuster, Recht der elektronischen Medien Kommentar, N 12 zu Art. 33 DSGVO.

135 BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 52-54 zu Art. 33 DSGVO.

136 Artikel-29-Datenschutzgruppe (Fn. 22), S. 16 f.; MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 33 zu Art. 28 und N 11 zu Art. 30 DSGVO.

137 Artikel-29-Datenschutzgruppe (Fn. 22), S. 17; MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 10b–10c zu Art. 30 DSGVO.

weitere Informationen. Dies dient bei Bedarf der vereinfachten Rückfragemöglichkeit der Aufsichtsbehörde.[138]

Ebenfalls zwingend ist gemäss Art. 33 Abs. 3 lit. c DSGVO auch eine *Beschreibung der wahrscheinlichen Folgen der Verletzung*. Dies dient der Koordinierung des weiteren Vorgehens der Aufsichtsbehörde; daher sind die wahrscheinlichen Folgen der Verletzung so genau wie möglich zu beschreiben. Es sind dabei nicht jedmögliche Folgen gemeint: Massgeblich sind solche, welche sich auf die freie Persönlichkeitsentfaltung (vgl. Art. 1 Abs. 1 und Abs. 2 DSGVO) auswirken.[139]

Erforderlich ist gemäss Art. 33 Abs. 3 lit. d DSGVO schliesslich eine Beschreibung der von den Verantwortlichen ergriffenen oder vorgeschlagenen Massnahmen zur Behebung der Verletzung und gegebenenfalls Massnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen. Bezüglich der vorgeschlagenen Massnahmen ist anzumerken, dass es nicht darum geht, der Aufsichtsbehörde Massnahmen vorzuschlagen. Gemeint ist, dass die oder der Verantwortliche zusätzlich zu bereits ergriffenen Massnahmen darüber informiert, welche weiteren Massnahmen sie bzw. er eventuell ergreifen möchte. Der Wortlaut «vorgesehene» Massnahmen wäre daher treffender.[140]
Bei den *Massnahmen zur Behebung der Verletzung* gilt es aufzuführen, welche Massnahmen ergriffen wurden, um die Sicherheit von personenbezogenen Daten wiederherzustellen. In Frage kommen sowohl technische[141] als auch organisatorische[142] Massnahmen.[143]

Die *Massnahmen zur Abmilderung möglicher nachteiliger Auswirkungen von Verletzungen* des Schutzes von personenbezogenen Daten[144] bezwecken den Schaden der Betroffenen möglichst auszuschliessen oder zumindest minim zu halten.[145] Relevant ist, dass sie von der oder dem Verantwortlichen überhaupt selbst ergriffen werden können.[146] Anhand der Informationen nach Art. 33 Abs. 3 lit. d DSGVO kann die Aufsichtsbehörde letztlich beurteilen, ob und welche weiteren Massnahmen (vgl. auch Art. 58 Abs. 2 lit. d und f DSGVO) sie zu ergreifen gedenkt.[147]

2. In Bezug zur betroffenen Person

Anders als in Art. 33 Abs. 1 DSGVO hat die Benachrichtigung der von einer Verletzung betroffenen Person gemäss Art. 34 Abs. 2 DSGVO in *klarer und einfacher Sprache* die Art der Verletzung zu beschreiben und muss zumindest die in Art. 33 Abs. 3 lit. b, c und d DSGVO genannten Informationen und Empfehlungen enthalten. In Ergänzung hierzu bestimmen Art. 12 Abs. 1 und 5 DSGVO, dass die Benachrichtigung grundsätzlich schriftlich zu erfolgen hat und unentgeltlich sein muss. Die Pflicht nach Art. 34 Abs. 1 DSGVO ist damit zwar weniger umfassend, hat dennoch individuell zu erfolgen. Der genaue Umfang und die genaue Art der Verletzung gemäss Art. 33 Abs. 3 lit. a DSGVO sind für die Betroffenen zumeist auch wenig hilfreich. Das Erfordernis einer klaren und einfachen Sprache verfolgt denn auch das Ziel, dass die oder der Betroffene verstehen kann, was ungefähr

138 BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 55-56 zu Art. 33 DSGVO.

139 Vgl. MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 49-49c zu Art. 33 DSGVO.

140 WILHELM, (Fn. 109), in: Sydow EU-DSGVO Handkommentar, N 23 zu Art. 33 DSGVO; MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 50a zu Art. 33 DSGVO; JANDT, (Fn. 42), in: Kühling/Buchner, DS-GVO BDSG, N 21 zu Art. 33 DSGVO.

141 Zu nennen ist bspw. die Behebung einer fehlerhaften Konfiguration.

142 In Betracht kommt hier z.B. die Anweisung oder Schulung der Mitarbeiterinnen und Mitarbeiter.

143 WILHELM, (Fn. 109), in: Sydow EU-DSGVO Handkommentar, a.a.O.

144 Eine geeignete Massnahme kann insb. auch die Benachrichtigung der Betroffenen darstellen.

145 WILHELM, (Fn. 109), in: Sydow EU-DSGVO Handkommentar, N 24 zu Art. 33 DSGVO.

146 WILHELM, (Fn. 109), in: Sydow EU-DSGVO Handkommentar, a.a.O.

147 BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 58 zu Art. 33 DSGVO; MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 50b zu Art. 33 DSGVO; REIF, (Fn. 78), in: Gola DS-GVO Kommentar, N 36 zu Art. 33 DSGVO.

vorgefallen ist, welche Vorkehrungen zu treffen sind und welche Rechte bestehen.[148]

E. Zeitpunkt der Meldung

Die oder der Verantwortliche hat, nachdem ihr bzw. ihm eine Verletzung bekannt wurde, diese unverzüglich und möglichst binnen 72 Stunden zu melden. Auch die Benachrichtigung nach Art. 34 Abs. 1 DSGVO hat unverzüglich zu erfolgen, wobei diese gewöhnlich der Meldung nach Art. 33 Abs. 1 DSGVO nachgehen wird, da Benachrichtigungen gemäss Art. 34 DSGVO in der Regel mit der Aufsichtsbehörde vorab besprochen werden.[149] Ebenfalls unverzüglich hat gemäss Art. 33 Abs. 2 DSGVO die Meldung durch die Auftragsverarbeiterin oder den Auftragsverarbeiter zu erfolgen.

Die Meldefrist gemäss Art. 33 Abs. 1 DSGVO wird in dem Moment ausgelöst, in welchem die oder der Verantwortliche von einer relevanten Datenschutzverletzung hinreichend Kenntnis erlangt.[150] Sodann hat unverzüglich und möglichst binnen 72 Stunden eine Meldung zu erfolgen. *Unverzüglich* meint, dass der oder dem Verantwortlichen nicht vorgeworfen werden können darf, dass eine Meldung auch früher hätte erfolgen können bzw. dass sie oder er schuldhaft gezögert hat. Anhaltspunkte bietet zudem Erwägungsgrund 87 Satz 2 DSGVO. Zudem ist der EDSA gemäss Art. 70 Abs. 1 lit. g DSGVO beauftragt, hierzu Leitlinien zur Verfügung zu stellen.[151]

Die *Frist von 72 Stunden* ist nur *als Leitvorgabe* zu verstehen: Die oder der Verantwortliche darf sie nicht überschreiten, es sei denn, dass ihr oder ihm eine sinnvolle Meldung vorher nicht möglich war, wobei dann gemäss Art. 33 Abs. 1 Satz 2 DSGVO eine Begründung für die Verzögerung beizufügen ist. Möglich ist auch, dass eine Meldung noch vor Ablaufen der 72 Stunden zu erfolgen hat, damit die Meldung als unverzüglich erfolgt gilt.[152] Die strafrechtliche Verfolgung von Cyberkriminellen kann bedingen, dass zunächst auf Massnahmen zur Behebung der Verletzung verzichtet wird. In Verbindung mit einer Strafanzeige können gezielt für Cyberkriminelle gelegte Fallen daher einen akzeptablen Grund für eine verspätete (vollständige) Meldung darstellen.[153]

Da es je nach den Umständen[154] eventuell nicht möglich ist, von Anfang an alle nötigen Informationen gemäss Art. 33 Abs. 3 DSGVO zu liefern, bestimmt Art. 33 Abs. 4 DSGVO, dass die Verantwortlichen auch *schrittweise* melden können, falls damit unangemessene weitere Verzögerungen verhindert werden.[155] Dennoch ist Art. 33 Abs. 4 DSGVO nicht als *Kann-Vorschrift*, sondern vor allem als Pflicht zu verstehen. Bereits die Begrifflichkeiten *(wenn und soweit, ohne unangemessene weitere Verzögerung)* deuten darauf hin, dass es sich nicht um einen Ermessensspielraum handelt und dass sich das Verbot einer unangemessenen weiteren Verzögerung auch auf die Meldung gemäss Art. 33 Abs. 1 DSGVO bezieht, sofern eine *Teilmeldung* als geboten erscheint. Eine zeitnahe, aber noch unvollständige Erstmeldung ist so betrachtet gewichtiger als eine vollständige Information.[156] In jedem Fall ist in Einklang mit Art. 33 Abs. 1 Satz 2 DSGVO aber zu

148 Vgl. BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 29-35 zu Art. 34 DSGVO.

149 REIF, (Fn. 78), in: Gola DS-GVO Kommentar, N 14 zu Art. 34 DSGVO; LAUE, (Fn. 44), in: Spindler/Schuster, Recht der elektronischen Medien Kommentar, N 11 zu Art. 34 DSGVO.

150 Vgl. hierzu Punkt IV.B.1.

151 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 34–36 zu Art. 33 DSGVO.

152 LAUE, (Fn. 64), in: Laue/Kremer, Datenschutzrecht in der betrieblichen Praxis, S. 267 f. (N 49); MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 33–34 zu Art. 33 DSGVO; vgl. zur Handhabung der Frist PRADEL MELANIE/PILTZ CARLO, Wie lange dauern 72 Stunden?, in: Zeitschrift für Datenschutz (ZD), 2019/Heft 4, S. 152–157.

153 Vgl. BERANEK ZANON (Fn. 114), Rz. 14.

154 So kann die Ursache für ein Datenleck noch unklar sein, wodurch es nicht möglich ist, diesbezüglich Massnahmen zur Behebung zu nennen.

155 Vgl. REIF, (Fn. 78), in: Gola DS-GVO Kommentar, N 39 zu Art. 33 DSGVO.

156 MARTINI, (Fn. 17), in: Paal/Pauly, Kompakt-Kommentar DS-GVO BDSG, N 51-52b zu Art. 33 DSGVO.

begründen, weshalb (nur) eine Teilmeldung erfolgt.[157] Massnahmen zur Schadensabwendung dürfen neben der Meldepflicht aber nicht vernachlässigt werden. Wurde eine Verletzung festgestellt, zählt häufig jede Minute: Massgeblich ist, dass das Risiko für die Rechte und Freiheiten der Betroffenen möglichst gering gehalten wird. Sofern durch eine Teilmeldung Schäden abgewendet werden können, ist diese als Pflicht zu verstehen. Unter Umständen erfolgt hierdurch eine Meldung, welche sich nachträglich als unnötig erweist.[158]

F. Sanktionen

Der Vollständigkeit halber sei angemerkt, dass bei einer Verletzung der Pflichten aus Art. 33 und 34 DSGVO, gemäss Art. 83 Abs. 2 i.V.m. Art. 83 Abs. 4 lit. a DSGVO erhebliche Sanktionen drohen können. Gleiches gilt im Übrigen auch für einen Verstoss gegen die Sicherheit der Verarbeitung nach Art. 32 DSGVO, welcher mit Art. 33 DSGVO einhergehen kann.[159]

V. Regelung im E-DSG (Art. 22)[160] und im Vergleich zur DSGVO

Auch in der Schweiz soll es künftig eine Meldepflicht für relevante Datenschutzverletzungen geben. Art. 22 Abs. 1 und 4 E-DSG sehen eine entsprechende *Melde- und Benachrichtigungspflicht* an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) bzw. an die betroffene Person vor.

A. Verletzung der Datensicherheit

In Art. 17 Abs. 1 VE-DSG war vorgesehen, dass eine Meldung an den EDÖB erfolgen muss, sofern eine unbefugte Datenbearbeitung oder ein Verlust von Daten vorliegt.

Während die DSGVO in Art. 4 Nr. 12 klarstellt, dass in Bezug auf die Verletzung des Schutzes personenbezogener Daten gemäss Art. 33 und 34 DSGVO nur Sicherheitsvorfälle gemeint sind, definiert der Vorentwurf nicht, was unter einer Verletzung des Datenschutzes zu verstehen ist. Art. 17 Abs. 1 VE-DSG spricht nur allgemein von einem Verlust von Daten oder einer unbefugten Datenbearbeitung. Geplant war, dass prinzipiell jede Art der unbefugten Bearbeitung eine relevante Datenschutzverletzung darstellen soll.[161] Dies ginge deutlich weiter als in der DSGVO: erfasst wären nicht nur die zahlreichen Sicherheitsvorfälle, sondern jedmögliche Datenschutzverletzungen, die voraussichtlich zu einem Risiko führen können. Eine *Meldeflut* und damit eine Überlastung des EÖDB wäre die Folge.[162]

Der Entwurf, im Vergleich zum Vorentwurf, definiert daher ebenso wie die DSGVO, wann eine relevante Datenschutzverletzung vorliegen soll. Art. 22 Abs. 1 E-DSG setzt eine Verletzung der Datensicherheit voraus, welche in Art. 4 lit. g E-DSG[163] legaldefiniert wird: Eine *Verletzung der Datensicherheit* liegt vor, wenn (1.) eine Verletzung der Sicherheit eingetreten ist, (2.) die ungeachtet der Absicht oder Widerrechtlichkeit (3.) dazu führt, (4.) dass Personendaten verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden. Bereits im Vorfeld muss gemäss Art. 7 Abs. 1 E-DSG[164] dafür gesorgt werden, dass durch *geeignete technische und organisatorische Massnahmen* eine dem Risiko angemessene Datensicherheit gewährleistet ist. Solche müssen es gemäss Art. 7 Abs. 2 E-DSG ermöglichen, Verletzungen

157 HLADJK, (Fn. 48), in: Ehmann/Selmayr, Kurzkommentar DS-GVO BDSG, N 16 zu Art. 33 DSGVO; Artikel-29-Datenschutzgruppe (Fn. 22), S. 18.

158 BRINK, (Fn. 58), in: Brink/Wolff, BeckOK Datenschutzrecht, N 59–61 zu Art. 33 DSGVO.

159 Vgl. BECKER, (FN. 45), S. 177.

160 Die Norm findet sich neu in Art. 24 revDSG.

161 Bundesamt für Justiz (BJ), Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, 21.12.2016, S. 62 f.

162 SIEVERS JACQUELINE/VASELLA DAVID, Der «Swiss Finish» im Vorentwurf des DSG, in: digma (Zeitschrift für Datenrecht und Informationssicherheit), 2017/Heft 1, S. 44 ff., S. 47; ROSENTHAL (Fn. 16), Rz. 94–96.

163 Die Norm findet sich neu in Art. 5 lit. h revDSG.

164 Die Norm findet sich neu in Art. 8 revDSG.

der Datensicherheit zu vermeiden. Werden keine solchen Massnahmen getroffen und Personendaten z.B. frei abrufbar gespeichert, so kann ein Zugriff durch Unbefugte auch keine Verletzung im Sinne von Art. 4 lit. g E-DSG darstellen.[165] Wie in der DSGVO kommt es also massgeblich darauf an, dass eine Sicherheitsverletzung besteht. Ob dadurch auch eine Meldepflicht ausgelöst wird, ist wie in der DSGVO im Rahmen der *Risikoeinschätzung* gemäss Art. 22 Abs. 1 E-DSG zu beurteilen.[166]
Die Definition nach Art. 4 lit. g E-DSG hat grosse Ähnlichkeit mit der Definition nach Art. 4 Nr. 12 DSGVO, weshalb hierzu auch auf oben verwiesen wird.[167]

B. Bestehen einer Melde- und Benachrichtigungspflicht

Eine Meldung im Falle einer Verletzung im Sinne von Art. 4 lit. g E-DSG hat gemäss Art. 22 Abs. 1 E-DSG zu erfolgen, falls die Verletzung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. In Art. 17 Abs. 1 VE-DSG war noch folgendes vorgesehen: Eine Meldung an den EDÖB hat zu erfolgen, es sei denn, dass die Verletzung des Datenschutzes voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte[168] der betroffenen Person führt. Bezüglich des Verhältnisses von Meldepflicht und deren Entfall sowie der Risikohöhe stimmt der Vorentwurf demnach mit der DSGVO überein, welche die Meldepflicht ebenso nur entfallen lässt, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.[169] In Art. 22 Abs. 1 E-DSG ist das Verhältnis von Meldepflicht und Entfall der Meldepflicht indes umgekehrt: Eine Meldung hat nur zu erfolgen, sofern die Verletzung voraussichtlich zu einem Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt; und dies auch nur, wenn von einem hohen Risiko auszugehen ist.

Eine Benachrichtigung gemäss Art. 22 Abs. 4 E-DSG ist nur zwingend, falls es zum Schutz des Betroffenen erforderlich ist oder der EDÖB es verlangt (was letztlich dasselbe bedeuten muss)[170]. Die Benachrichtigungspflicht gemäss Art. 17 Abs. 2 VE-DSG stimmte somit bereits fast wörtlich mit Art. 22 Abs. 4 E-DSG überein. Im Vergleich zu Art. 34 Abs. 1 DSGVO wird nicht grundsätzlich ein hohes Risiko vorausgesetzt. Jedoch muss die betroffene Person gemäss Art. 22 Abs. 4 E-DSG immer benachrichtigt werden, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt. Hier soll ein gewisser Ermessensspielraum bestehen, wobei es wesentlich darauf ankommen soll, ob die Risiken für die Persönlichkeit oder die Grundrechte der oder des Betroffenen durch eine Benachrichtigung und folgende entsprechende Vorkehrungen minimiert werden können.[171]
Für eine Relativierung der Benachrichtigungspflicht sorgen auch die Ausnahmen nach Art. 22 Abs. 5 E-DSG. Dennoch kann Art. 22 Abs. 4 E-DSG in gewisser Weise auch über die Benachrichtigungspflicht gemäss Art. 34 Abs. 1 DSGVO hinausgehen – auch wenn die Pflicht nicht grundsätzlich bei Vorliegen eines voraussichtlich hohen Risikos, wie es Art. 34 Abs. 1 DSGVO vorsieht, besteht. Aus einer Studie des *Ponemon Institute* aus dem Jahr 2014 ergibt sich ausserdem, dass die meisten Personen, die von einer *Data Breach* betroffen sind, Meldungen diesbezüglich ignorieren und keine Vorkehrungen zu ihrem Schutz treffen.[172] Es wäre da-

165 ROSENTHAL (Fn. 25), Rz. 64.
166 BBl 2017 6941 (Fn. 13), 7022 f.
167 Vgl. MATTIG (Fn. 22), S. 492; siehe auch Punkt IV.A.
168 «Grundrechte» bezieht sich nicht auf die Bearbeitung durch *private* Datenbearbeiter.
169 Vgl. Art. 33 Abs. 1 Satz 1 DSGVO.
170 Vgl. die Ausführungen in Fn. 76 bei ROSENTHAL (Fn. 16), Rz. 98.
171 BBl 2017 6941 (Fn. 13), S. 7065; vgl. PETER CHRISTIAN, DSGVO und E-DSG fordern Schweizer Spitäler, Praxen, Heime und Spitex, in: Jusletter vom 26.02.2018, Rz. 138–140 und KLEINER (Fn. 17), S. 172.
172 Vgl. Ponemon Institute, The aftermath of a mega data breach: Consumer Sentiment, 2014, S. 5; siehe auch BOLSON ANDREW, If not all data breaches are created equal, why are all data breach notifications treated the same?, Interna-

her sinnlos, die von einer *Data Breach* betroffenen Personen mit Meldungen zu überhäufen. Hierdurch könnte nämlich eine regelrechte *Data Breach Fatigue* entstehen, welche die Wirksamkeit derartiger Benachrichtigungen erheblich verringern würde.[173] Diesem Effekt wird allerdings dadurch entgegengewirkt, dass Art. 22 Abs. 4 E-DSG die Benachrichtigung nicht starr festschreibt, sondern nur verlangt, wenn es den Betroffenen überhaupt möglich ist, entsprechende Schutzmassnahmen einzuleiten. Da die Pflicht im Vergleich zur DSGVO unabhängig von einer Notifikation des EDÖB bestehen oder eher einsetzen kann, ist es möglich, dass eine Person, selbst wenn das Risiko nicht hoch ist, informiert werden muss, da auch dann ihr Schutz sichergestellt werden muss. In Anbetracht der Beweggründe dieser Revision macht dies Sinn, kann für Konzerne jedoch nachteilig sein, da europaweit agierende Unternehmen unter Umständen verschiedene Regelungen implementieren müssen.[174]

1. Bekanntwerden der Verletzung

Art. 22 Abs. 1 E-DSG knüpft nicht ausdrücklich wie Art. 33 Abs. 1 DSGVO an ein Bekanntwerden der Verletzung an. Gemäss Botschaft hat eine Meldung indessen ab dem Zeitpunkt der Kenntnisnahme so rasch als möglich zu erfolgen.[175] Deshalb – und weil eine Notifikationspflicht nur Sinn ergibt, wenn das Wissen um eine Verletzung besteht – ist dieser Punkt in Art. 22 Abs. 1 und 4 E-DSG hineinzulesen.[176]

2. Hohes Risiko

Eine Meldung an den EDÖB hat gemäss Art. 22 Abs. 1 E-DSG zu erfolgen, sofern die Verletzung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der oder des Betroffenen führt. Ebenso wie in der DSGVO wird im E-DSG nicht definiert, wann von einem hohen Risiko auszugehen ist.[177] Gemäss Botschaft soll so verhindert werden, dass selbst unbedeutende Verletzungen gemeldet werden müssen. Erforderlich sei eine *Prognose* bezüglich der möglichen Folgen der Verletzung für die Betroffenen.[178]

Damit von einem *hohen Risiko* auszugehen ist, sollte sich die Verletzung nicht nur qualitativ, sondern auch quantitativ (gemeint ist die Anzahl von Betroffenen) hinreichend auswirken können.[179] Werden bspw. vertrauliche Daten einer Person gestohlen, kann für diese unter Umständen zwar ein hohes Risiko für ihre Persönlichkeit vorliegen[180], eine Notifikation des EDÖB erscheint bisweilen nicht angezeigt. Die oder der Betroffene hingegen ist stets zu benachrichtigen, wenn es gemäss Art. 22 Abs. 4 E-DSG zu ihrem oder seinem Schutz erforderlich ist.[181] Da im heutigen digitalen Zeitalter z.B. schon eine *E-Mail-Newsletter-Datenbank* eine enorme Grösse annehmen kann, sollte bezüglich einer hinreichenden Quantität von 10'000 oder mehr Betroffenen ausgegangen werden.[182] Zwecks Verbesserung der Rechtssicherheit sind daher formale Kriterien zur Qualität und Quantität des hohen Risikos auf Verordnungsstufe zu fordern.[183] Um einer Meldeflut vorzubeugen, ist zu erwägen die Notifikation des EDÖB analog zu Art. 21 Abs. 4 E-DSG[184] für einen Grossteil der Fälle entfallen zu lassen, wenn sich eine *Datenschutzberaterin oder ein Datenschutzberater*

tional Association of Privacy Professionals (IAPP) vom 28.10.2014.

173 ROSENTHAL (Fn. 25), Rz. 67; vgl. BOLSON (Fn. 172).

174 ROSENTHAL (Fn. 25), Rz. 70.

175 BBI 2017 6941 (Fn. 13), 7064.

176 Für nähere Hinweise dazu, wann von einer Kenntnis auszugehen ist, siehe Punkt IV.B.1.

177 Vgl. zum hohen Risiko Punkt IV.B.3.a); vgl. auch ROSENTHAL (Fn. 25), Rz. 65.

178 BBI 2017 6941 (Fn. 13), 7064.

179 Vgl. ROSENTHAL (Fn. 25), Rz. 67 und die Beispiele in Rz. 66; vgl. bezüglich der Prognose auch die Risikoerwägungen zur DSGVO in Punkt IV.B.2 und 3.a)

180 In Betracht kommt bspw. die Gefahr des *Identitätsdiebstahls* bzw. des Missbrauchs von personenbezogenen Daten.

181 ROSENTHAL (Fn. 25), Rz. 67; vgl. ferner bereits ROSENTHAL (Fn. 16), Rz. 98.

182 ROSENTHAL (Fn. 25), a.a.O.

183 ROSENTHAL (Fn. 25), a.a.O.

184 Die Norm findet sich neu in Art. 23 Abs. 4 revDSG.

im Sinne von Art. 9 E-DSG[185] damit befasst.[186]

3. Ausnahme von der Benachrichtigungspflicht

Die oder der Verantwortliche kann gemäss Art. 22 Abs. 5 E-DSG die Information der Betroffenen einschränken, aufschieben oder darauf verzichten, wenn einer der Fälle gemäss lit. a-c gegeben ist.

Nach Art. 22 Abs. 5 lit. a E-DSG ist dies der Fall, sofern einer der Gründe von Art. 24 Abs. 1 lit. b oder Abs. 2 lit. b E-DSG[187] vorliegt oder eine gesetzliche Geheimhaltungspflicht besteht.

Die Ausnahme nach Art. 22 Abs. 5 lit. b E-DSG kommt in Betracht, wenn die Information *unmöglich* ist oder einen *unverhältnismässigen Aufwand* erfordert. Lässt sich die Benachrichtigung der Betroffenen in vergleichbarer Weise sicherstellen, so genügt nach Art. 22 Abs. 5 lit. c E-DSG eine öffentliche Bekanntmachung.

Unmöglich im Sinne von Art. 22 Abs. 5 lit. b E-DSG wäre die Information, falls die oder der Verantwortliche gar nicht weiss, welche Personen betroffen sind. Ein Aufwand dagegen wäre z.B. *unverhältnismässig*, wenn sehr viele Betroffene einzeln informiert werden müssten und die dadurch entstehenden Kosten in einem Missverhältnis zu deren Informationsgewinn stünde. Insb. dann sollte an eine *öffentliche Bekanntmachung* gemäss Art. 22 Abs. 5 lit. c E-DSG gedacht werden.[188] Die DSGVO fasst die Fälle nach Art. 22 Abs. 5 lit. b und c E-DSG in dieser Hinsicht denn auch zusammen.[189]

Die Ausnahmen im E-DSG sind damit im Vergleich zur DSGVO grundlegend anders geregelt, wobei die Benachrichtigung von Betroffenen ohnehin weniger starr ist. Wie oben bereits erörtert, kommt Art. 34 Abs. 3 lit. a und b DSGVO ohnehin nur deklaratorische Bedeutung zu.[190]

4. Dokumentationspflicht

Eine umfassende Dokumentationspflicht in Bezug auf Datenschutzverletzungen wie in Art. 33 Abs. 5 DSGVO ist im E-DSG nicht vorgesehen. Nach Art. 19 lit. a VE-DSG sollten die Verantwortlichen unter anderem hierzu noch verpflichtet werden. Allein weil eine relevante Datenschutzverletzung im VE-DSG nicht definiert wird, erschien diese Pflicht uferlos.[191] Sie ist im E-DSG nicht mehr vorgesehen, was sich als sinnvoll erweist.[192] Mehraufwand in Form neuer Pflichten (Risikofolgenabschätzung, Informationspflichten etc.) bringt die Revision für betroffene Unternehmen und Organisationen ohnehin genug.[193]
Im Falle einer Verletzung sollten sich betroffene Unternehmen vielmehr der Behebung dieser und der Abmilderung ihrer Folgen widmen. Zudem kann wohl angenommen werden, dass eine Verletzung allein durch eine Meldung selbst bereits in gewisser Form dokumentiert ist. Angesichts der Häufigkeit von Datenpannen ergibt es auch schlicht keinen Sinn, jede Verletzung der Datensicherheit, so wie in der DSGVO, zu dokumentieren.[194]

185 Die Norm findet sich neu in Art. 10 revDSG.
186 ROSENTHAL (Fn. 25), Rz. 72; vgl. auch Bundesamt für Justiz (BJ), Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens), 10.08.2017, S. 35.
187 Die Norm findet sich neu in Art. 26 revDSG.
188 BBI 2017 6941 (Fn. 13), S. 7065.
189 Vgl. Art. 34 Abs. 3 lit. c DSGVO.
190 Siehe Punkt IV.B.3.b).
191 ROSENTHAL (Fn. 16), Rz. 81.
192 Vgl. ROSENTHAL (Fn. 25), Rz. 69.
193 Vgl. auch HUSI-STÄMPFLI SANDRA, Die DSG-Revision oder: Ein Beziehungsdrama in drei Akten, in: Jusletter vom 07.05.2018, Rz. 24.
194 Vgl. zur Dokumentationspflicht in der DSGVO Punkt IV.B.4.

5. Selbstbelastungsfreiheit

Im Gegensatz zur DSGVO ist anzumerken, dass die Thematik zur *Selbstbelastungsfreiheit* im E-DSG immerhin Beachtung fand.[195] Gemäss Art. 22 Abs. 6 E-DSG darf eine Meldung im Sinne dieses Artikels in einem Strafverfahren gegen die oder den Meldepflichtigen nur mit deren bzw. dessen Einverständnis verwendet werden.

Erfasst werden soll dabei die Meldung durch Verantwortliche und Auftragsbearbeiterinnen oder Auftragsbearbeiter.[196] In verschiedener Hinsicht ist Art. 22 Abs. 6 E-DSG fragwürdig: So wird damit nur auf eine Meldung nach Art. 22 Abs. 1 und 3 E-DSG, nicht aber auf die Benachrichtigung gemäss Art. 22 Abs. 4 E-DSG Bezug genommen. Die oder der Meldepflichtige muss also bei der Benachrichtigung der Betroffenen besondere Vorsicht walten lassen, will er nicht ein Strafverfahren riskieren. Auch schützt Art. 22 Abs. 6 E-DSG nur im Strafverfahren, nicht vor zivilrechtlichen Ansprüchen. Das Hauptproblem besteht indes darin, dass die oder der Meldepflichtige häufig nicht diejenige Person ist, welche es vor strafrechtlicher Verfolgung zu schützen gilt (das wären die angestellten Hilfspersonen); so etwa in Fällen, wo die Verletzung der Datensicherheit gleichzeitig eine Verletzung des Berufsgeheimnisses darstellt. Daher ist zu fordern, dass Art. 22 Abs. 6 E-DSG nicht nur die Verantwortlichen und die Auftragsbearbeiterinnen und Auftragsbearbeiter erfasst, sondern auch die jeweiligen Hilfspersonen, womit auch deren Einverständnis erforderlich ist. Die Konsequenz daraus wäre, dass Mitarbeiterinnen und Mitarbeiter innerhalb derselben juristischen Person entgegen der Botschaft als Auftragsbearbeiterin oder Auftragsbearbeiter qualifiziert werden müssten, wodurch diese dann der Meldepflicht unterlägen. Allerdings wären sie durch Art. 22 Abs. 6 E-DSG dann auch geschützt.[197]

195 Vgl. FREI (Fn. 13), Rz. 45.
196 BBl 2017 6941 (Fn. 13), S. 7065 f.
197 ROSENTHAL (Fn. 25), Rz. 73.

C. Adressaten und Meldepflichtige

Adressatin bzw. Adressat der Meldung gemäss Art. 22 Abs. 1 E-DSG ist der EDÖB (vgl. Art. 3 Abs. 1 E-DSG[198]), Adressatin oder Adressat der Benachrichtigungspflicht gemäss Art. 22 Abs. 4 E-DSG die von einer Verletzung betroffene Person. Die Melde- und Benachrichtigungspflicht obliegt der oder dem *Verantwortlichen* im Sinne von Art. 4 lit. i E-DSG[199], welche bzw. welcher allein oder mit anderen über Zwecke und Mittel der Bearbeitung von Personendaten entscheidet. Nach Art. 22 Abs. 3 E-DSG sind die *Auftragsbearbeiterinnen und Auftragsbearbeiter* im Sinne von Art. 4 lit. j E-DSG[200] zudem verpflichtet, den Verantwortlichen eine Verletzung der Datensicherheit, sei sie noch so klein, zu melden. Hierbei liegt es an den Verantwortlichen zu entscheiden, inwieweit sie eine Meldung als nötig erachten. Um einer unnötigen Meldeflut an die Verantwortlichen vorzubeugen, sollte geregelt werden, wann die Auftragsbearbeiterinnen und Auftragsbearbeiter von einer Meldung absehen können.[201]

D. Inhalt und Form der Meldung/Benachrichtigung

Gemäss Art. 22 Abs. 2 E-DSG muss die Meldung mindestens die *Art der Verletzung* im Sinne von Art. 4 lit. g E-DSG, deren *Folgen* und die *ergriffenen oder vorgesehenen Massnahmen* enthalten. Es handelt sich demnach um *Mindestangaben*. Die Meldung soll es dem EDÖB ermöglichen, zeitnah zu intervenieren.[202] Formvorgaben sind dem E-DSG nicht zu entnehmen. Zur Vereinfachung des Meldeverfahrens erscheint es jedoch sinnvoll, ein *Online-Meldeformular* anzubieten.[203] Ebenfalls nichts entnehmen lässt sich zum Inhalt und der Form an die betroffene Per-

198 Die Norm findet sich neu in Art. 4 Abs. 1 revDSG.
199 Die Norm findet sich neu in Art. 5 lit. j revDSG.
200 Die Norm findet sich neu in Art. 5 lit. k revDSG.
201 ROSENTHAL (Fn. 25), Rz. 71.
202 Vgl. BBl 2017 6941 (Fn. 13), S. 7064 f. und die Ausführungen zur DSGVO unter Punkt IV.D.1.
203 ROSENTHAL (Fn. 25), Rz. 67.

son. Es ist aber davon auszugehen, dass sich die Mindestangaben nach Art. 22 Abs. 2 E-DSG, wenn auch nicht unbedingt in der geforderten Tiefe, auch auf Art. 22 Abs. 4 E-DSG beziehen. Eine Meldung für die betroffene Person ergibt schliesslich nur für den Fall Sinn, in dem diese infolgedessen Vorkehrungen zu ihrem Schutz treffen kann. Ebenfalls ist zu fordern, dass die betroffene Person wie in der DSGVO schriftlich informiert wird.

E. Zeitpunkt der Meldung

Die Meldung gemäss Art. 22 Abs. 1 E-DSG soll so rasch wie möglich erfolgen, im VE-DSG war unverzügliches Handeln vorgesehen. Dies hätte jedoch keinen Sinn ergeben, denn eine Datenschutzverletzung muss zunächst erkannt werden und sofern genügend Informationen beisammen sind, kann das weitere Vorgehen beurteilt werden.[204] Auch in der DSGVO wird ein erster Untersuchungszeitraum zugestanden, ehe eine Verletzung als bekannt gilt.[205]

Die Meldepflicht gemäss Art. 22 Abs. 1 E-DSG entsteht lediglich dann, wenn eine hinreichende Kenntnis in Bezug auf eine relevante Verletzung besteht. *So rasch wie möglich* meint dabei *so früh wie möglich*; die Meldung hat also grundsätzlich schnell zu erfolgen – jedoch immer unter Berücksichtigung der Umstände, insb. des Ausmasses der Gefährdung der Betroffenen.[206] Die Meldung muss also erst erfolgen, wenn alle nötigen Informationen vorliegen. Eine starre 72-Stundenfrist – wie sie in der DSGVO zu finden ist – und die Pflicht zu einer Teilmeldung sind nicht vorgesehen. Dies erscheint sinnvoll. Das Augenmerk sollte bei der Verletzung und der Abwendung und Minderung von Schäden liegen, nicht bei der Information des EDÖB.[207] Eine starre 72-Stundenfrist ist gerade für grössere Unternehmen in der Regel auch schwierig einzuhalten.[208] Die Meldung der Auftragsbearbeiterinnen und Auftragsbearbeiter nach Art. 22 Abs. 3 E-DSG hat ebenfalls nur so rasch als möglich zu erfolgen, wohingegen die DSGVO ebenso unverzügliches Handeln erfordert.

Bezüglich des Benachrichtigungszeitraums gegenüber den betroffenen Personen schreibt Art. 22 Abs. 4 E-DSG im Vergleich zur DSGVO keine zeitlichen Leitvorgaben vor. Da die Benachrichtigungspflicht im Vergleich zur DSGVO unabhängig von der Meldung an den EDÖB ist, kann die Benachrichtigung der betroffenen Person auch schon vor der Meldung an den EDÖB angezeigt sein.[209]

F. Sanktionen

Der Vorentwurf sah wie in der DSGVO noch eine Sanktionierung bei Verletzung der Meldepflicht vor.[210] Im E-DSG ist das Unterlassen einer Meldung gemäss Art. 22 E-DSG nun gänzlich straflos.[211] Zur Kompensation dieser und anderer gegenüber dem Vorentwurf weggefallenen Strafbestimmungen wurde Art. 57 E-DSG[212] geschaffen, welcher dem EDÖB die Kompetenz verleiht, gewisse Verwaltungsmassnahmen gemäss Art. 45 Abs. 3 E-DSG[213] unter Strafandrohung anzuordnen.[214] Daneben ist zu beachten, dass die vorsätzliche Nichteinhaltung der Mindestanforderungen an die Datensicherheit gemäss Art. 7 Abs. 3 E-DSG[215] nach Art. 55 lit. c E-DSG[216] bussgeldbewährt ist.

204 ROSENTHAL (Fn. 16), Rz. 99.
205 Siehe Punkt IV.B.1.
206 BBl 2017 6941 (Fn. 13), S. 7064.
207 ROSENTHAL (Fn. 25), Rz. 68.
208 Vgl. RÄTHER (Fn. 90), S. 100.
209 Siehe Punkt V.B.2.
210 Vgl. Art. 17 und 50 VE-DSG.
211 Vgl. ROSENTHAL (Fn. 25), Rz. 74 und 118.
212 Die Norm findet sich neu in Art. 63 revDSG.
213 Die Norm findet sich neu in Art. 51 Abs. 3 revDSG.
214 Vgl. BBl 2017 6941 (Fn. 13), S. 7103.
215 Die Norm findet sich neu in Art. 8 Abs. 3 revDSG.
216 Die Norm findet sich neu in Art. 61 lit. c revDSG.

VI. Fazit und Gesamtwürdigung der im Entwurf geregelten Meldepflicht

Nach ausführlichem Vergleich kann festgehalten werden, dass die Anforderungen an die Melde- und Benachrichtigungspflicht im E-DSG in weiten Teilen unter der DSGVO liegen werden.[217] Da die Notifikation des EDÖB nur bei einem hohen Risiko zu erfolgen hat, ist mit deutlich weniger Meldungen zu rechnen als in der EU unter der DSGVO. Dies entlastet sowohl Unternehmen als auch den EDÖB, vor allem angesichts dessen geringen Kapazitäten, und beugt einer Meldeflut vor. Der EDÖB soll sich nur mit den wirklich wichtigen Fällen beschäftigen müssen, also wenn es um eine Vielzahl von Betroffenen geht. Zudem sollte der EDÖB als Anlaufstelle für Probleme wahrgenommen werden und nicht umgekehrt. Deshalb ist es auch zu begrüssen, dass die Unterlassung einer Meldung, abgesehen von Aufsichtsbefugnissen des EDÖB und der möglichen Strafandrohung bei Nichtbefolgung, nun nicht mehr strafbewährt ist.[218]

Bezüglich der Frage des hohen Risikos wären zudem formale Kriterien auf Verordnungsstufe wünschenswert. Geregelt werden sollte insb. ab welcher Anzahl von Betroffenen grundsätzlich ein hohes Risiko anzunehmen ist. Zur weiteren Entlastung des EDÖB sollte auch geprüft werden, ob eine Meldung nicht entfallen könnte, wenn sich eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter im Sinne von Art. 9 E-DSG mit einer relevanten Datenschutzverletzung befasst.[219] Zudem gibt es keine starren zeitlichen Vorgaben in Bezug auf die Notifikation des EDÖB und die Benachrichtigung der Betroffenen. Auch muss eine Benachrichtigung nur erfolgen, wenn die Betroffenen überhaupt in der Lage sind, geeignete Schutzmassnahmen zu treffen. So kann dem Effekt, dass Meldungen aufgrund ihrer Häufigkeit nicht mehr ernst genommen werden *(Data Breach Fatigue),* wirksam entgegengewirkt werden.[220]

Es ist davon auszugehen, dass die europäischen Anforderungen in Bezug zur Melde- und Benachrichtigungspflicht grösstenteils eingehalten werden. Wie in der Gesamtwürdigung bereits festgehalten, werden durch die milde Ausgestaltung die Unternehmen, vor allem die kleineren, und der EDÖB, angesichts dessen geringen Kapazitäten, in einer sich immer mehr bürokratisierenden Welt weitgehend entlastet.

Dass eine vollständige Datensicherheit eine Illusion ist, wurde einleitend bereits erwähnt; jedoch ist auch klar, dass es eine Regulierung braucht, welche den neuen Anforderungen und auch der erheblich gestiegenen wirtschaftlichen Bedeutung von Personendaten gerecht wird. Eine zu strenge Regulierung wie in der DSGVO wäre allerdings angesichts der zunehmenden Anzahl von Datenpannen und Cyberangriffen der falsche Ansatz und wenig zielführend.[221] Zudem müssen Unternehmen und Organisationen in gewissen Fällen ohnehin auch die strengeren Vorschriften der DSGVO beachten.[222]

Mittlerweile ist die Revision des DSG abgeschlossen.[223] Es bleibt daher gespannt abzuwarten, ob die *Data Breach Notification* die gewünschten Effekte mit sich bringen wird.

Die Corona-Krise hat der Digitalisierung in sämtlichen Lebensbereichen einen enormen Schub verliehen. Was bis vor kurzem für viele undenkbar schien, ist Realität geworden. Allerdings darf die Datensicherheit nicht vernachlässigt werden. So nutzen Cyberkriminelle die durch die Digitalisierung neu geschaffenen Konstellationen und die

217 Vgl. BÜHLMANN LUKAS/METIN HATUN, Totalrevision des Schweizer Datenschutzgesetzes vor dem Hintergrund der DSGVO, in: Zeitschrift für Datenschutz (ZD), 2019/Heft 8, S. 356 ff., S. 359.

218 So auch schon ROSENTHAL (Fn. 16), Rz. 98; vgl. auch HUSI-STÄMPFLI SANDRA, (Fn. 193), Rz. 24–25.

219 Siehe Punkt V.B.2.

220 Siehe Punkt V.B.

221 Vgl. KLEINER (Fn. 17), S. 172.

222 Siehe bereits Punkt I.

223 Schweiz: Revision des Datenschutzes verabschiedet, in: ZD-Aktuell, 2020/Heft 17, 07323.

durch die rasche Umstellung bedingten Unsicherheiten bereits jetzt für ihre Zwecke aus.[224] Die neue Situation führt aber auch deutlich vor Augen, wie wichtig das Thema Datensicherheit geworden ist. Umso mehr ist daher alles daran zu setzen, sich so gut wie möglich zu schützen.

224 Vgl. zum Ganzen HEFER CORNELIA, Coronakrise: «Kriminelle nutzen das Chaos», in: VersicherungsJournal Deutschland vom 03.04.2020; vgl. auch HEFER CORNELIA, Coronakrise: Homeoffice: Experten warnen vor erheblichen IT-Risikofaktoren, in: VersicherungsJournal Deutschland vom 14.04.2020.