Jan-Hendrik Labusga

# Die Fristberechnung beim Data Breach

## Transparenz erfordert harte Fristen

Kommt es in einem Unternehmen zu einer Verletzung des Schutzes personenbezogener Daten (*Data Breach*) ist zügiges Handeln geboten. Sofern aus dem Vorfall Risiken für die Rechte und Freiheiten der betroffenen Personen erwachsen, besteht in einem solchen Fall eine Meldepflicht nach Art. 33 DSGVO. Der Beitrag macht Vorschläge, wie die vorgegebene 72-Stunden-Meldefrist in der Praxis zu berechnen ist.

### 1 Einführung

Bei einem Data Breach ist zügiges Handeln nicht nur aufgrund der möglichen Folgen für die betroffenen Personen geboten, sondern auch aufgrund des gesetzlichen Rahmens, der durch die Datenschutzgrundverordnung (DSGVO) geschaffen wurde. Denn mit der Verletzung dieses Rahmens gehen hohe Bußgelder einher. Insofern macht die DSGVO in Art. 33 Abs. 1 folgende Vorgabe:

> „*Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen*."

Es gilt demnach für die Meldung eines Data Breach an die Aufsichtsbehörde grundsätzlich eine 72-Stunden-Frist. Entscheidend ist dabei, dass die Meldung „unverzüglich und möglichst binnen 72 Stunden" zu erfolgen hat. Konkrete Vorgaben zur Berechnung dieser Frist existieren nicht. Weder gibt es Rechtsprechung noch gibt es eine einheitliche Vorgabe der Datenschutzbehörden. Klar ist: Je früher auf ein Data Breach reagiert wird, desto geringer wird meist der mögliche Schaden ausfallen. Dies gilt heute in Zeiten von Big Data umso mehr, da viele Unternehmen große Mengen an (sensiblen) personenbezogene Daten verwalten und demnach der (materielle und immaterielle) Schaden kaum überschaubar ist.

Es soll im Folgenden knapp dargelegt werden, wann ein Data Breach vorliegt (2) und welche Folgen ein solcher – insbesondere bei Nichteinhaltung der Frist – haben kann (3). Der Fokus soll jedoch auf der Frage liegen, wie die Meldefrist konkret berechnet wird bzw. werden sollte (4). Abschließend erfolgt ein kurzer Bezug zur Corona-Pandemie (5) und ein Ausblick (6).

### 2 Vorliegen eines Data Breach

Die Meldepflicht nach Art. 33 Abs. 1 DSGVO setzt zunächst zwingend einen Data Breach voraus. Die „Verletzung des Schutzes personenbezogener Daten" wird in Art. 4 Nr. 12 DSGVO als „eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden" definiert. Neben der Vertraulichkeit personenbezogener Daten wird demnach auch die Verfügbarkeit der Daten („Verletzung der Sicherheit die, […] , zur Vernichtung, zum Verlust führt […]") und die Datenintegrität („Verletzung der Sicherheit, die […] zur Veränderung führt […]") geschützt.[1]

Auf die Art der personenbezogenen Daten kommt es nicht an, sodass insbesondere nicht notwendig ist, dass besondere Kategorien personenbezogener Daten vorliegen. Dies unterscheidet sich von der vorherigen nationalen Regelung des § 42a BDSG a.F. Die dort geregelte Meldepflicht bezog sich lediglich auf die abschließend aufgelisteten besonders sensitiven Arten von personenbezogenen Daten. Die Erweiterung spricht dafür, dass in Zweifelsfällen eher von einer Meldepflicht auszugehen ist, da dies der gesetzgeberischen Intention an einem umfassenden Schutz der Betroffenen vor wirtschaftlichen und gesellschaftlichen Nachteilen gleicht.[2]

Trotz Vorliegens eines Data Breach kann die Meldepflicht durch den in Art. 33 Abs. 1 DSGVO normierten Vorbehalt entfallen. Die

**Jan-Hendrik Labusga**

ist Richter am Amtsgericht Schwarzenbek, Zuvor war er als Rechtsanwalt im Bereich Arbeitsrecht und als wissenschaftlicher Mitarbeiter im Bereich Datenschutz in einer internationalen Wirtschaftskanzlei tätig.
E-Mail janlabusga@hotmail.de

1 Reif in Gola, DSGVO, 2. Auflage 2018, Art. 33 Rn. 20.
2 Hessel/Potel, DuD 2020 S. 95.

Meldepflicht entfällt nach Art. 33 Abs. 1 S.1 HS 2 DSGVO, wenn „die Verletzung […] voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt". Vor dem Hintergrund des bürokratischen und finanziellen Aufwandes, der dem Verantwortlichen zugemutet wird[3], ist eine solche Risikoberücksichtigung notwendig und richtig. Zu berücksichtigen ist jedoch, dass Gesundheitsdaten schon bei rechtmäßiger Verarbeitung „ihrem Wesen nach" risikoträchtig sind, sodass hier der Vorbehalt kaum greifen dürfte.[4] Einzelheiten hierzu können und sollen hier nicht im Detail erläutert werden.

## 3 Folgen der Nichteinhaltung der Meldepflicht bzw. Meldefrist

Wird die Meldepflicht grundsätzlich nicht befolgt oder wird die Frist für die Meldung nicht eingehalten, kann dies nicht nur schwerwiegende Schäden bei den betroffenen Personen nach sich ziehen, sondern auch beträchtliche Konsequenzen haben für den Verantwortlichen.

Die sich aus Art. 33 DSGVO ergebende Folge der Nichteinhaltung der 72-Stunden-Frist klingt zunächst harmlos. So muss der Verantwortliche, wenn er seiner Meldepflicht nicht innerhalb von 72 Stunden nachkommt, die zeitliche Verzögerung gem. Art. 33 Abs. 1 S. 2 DSGVO gegenüber der Aufsichtsbehörde begründen. Dabei darf die 72-Stunden-Frist nur dann überschritten werden, wenn die Meldung vorher unmöglich war.[5] Zwar sind der Verordnung keine Vorgaben in Bezug auf die Qualität einer solchen Begründung zu entnehmen. Es muss jedoch davon ausgegangen werden, dass diese nicht bloß formelhaft sein darf und deren Anforderungen an die Belastbarkeit mit dem Ausmaß des Data Breach steigen.[6] Die Begründung kann indes eine nicht „unverzügliche" Meldung nicht heilen, da sich diese Möglichkeit lediglich auf die Fristvorgabe „binnen 72 Stunden" erstreckt. Auch eine nicht rechtzeitige Meldung kann zu aufsichtsrechtlichen Maßnahmen führen kann.[7] Die Begründung nach Art. 33 Abs. 1 S. 2 DSGVO kann demnach zwar den Pflichtenverstoß abwenden, zwingend ist dies aber nicht.[8]

Neben den aufsichtsrechtlichen Maßnahmen nach Art. 58 DSGVO kann insbesondere die Verhängung eines Bußgeldes nach Art. 83 Abs. 4 lit. a DSGVO die Folge einer Verletzung der Meldepflicht sein. Die Grundprämisse gemäß Art. 83 Abs. 1 DSGVO ist, dass Geldbußen „wirksam, verhältnismäßig und abschreckend" sein sollen. Zu berücksichtigen ist, dass eine solche Geldbuße nicht nur anstelle, sondern gemäß Art. 83 Abs. 2 S. 1 DSGVO auch zusätzlich zu einer aufsichtsrechtlichen Maßnahme verhängt werden kann. Hierbei sind Geldbußen in Höhe von bis zu 10.000.000 Euro oder im Falle eines Unternehmens von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres möglich. Da Art. 83 Abs. 4 lit. a DSGVO pauschal auf Art. 33 DSGVO verweist, liegt auch ein Verstoß vor bei einer unvollständigen Meldung nach Art. 33 Abs. 3, einer unterlassenen Teilmeldung nach Art. 33 Abs. 4 oder einer fehlenden/unvollständigen Dokumentation nach Art. 33 Abs. 5 DSGVO.[9]

## 4 Berechnung der Meldefrist

Gibt das Gesetz eine Frist für die Meldepflicht vor und drohen derart hohe Sanktionen, muss die Berechnung dieser Frist klar bestimmt und dadurch rechtssicher sein. Die vorgegebene Meldefrist aus Art. 33 DSGVO wirkt zunächst klar: 72 Stunden. Fraglich ist jedoch, wie diese Frist genau zu bestimmen ist. Zum einen gibt es EU-weite Regelungen. Zum anderen existieren die nationalen Regelungen zur Fristberechnung. Beide weichen jedoch voneinander ab, sodass sich die Frage stellt, welche Regelungen letztlich und insbesondere in welcher Form anzuwenden sind.

Wenn man die vielen nationalen Regelungen zur Berechnung von Fristen anwenden würde, würde dies zum einen dem vornehmlichen Ziel der Vereinheitlichung des Datenschutzes widerstreben.[10] Zum anderen steht der Anwendung der nationalen Regelungen im Rahmen der Meldepflicht der DSGVO der Anwendungsvorrang des Unionsrechts entgegen, welcher die Unanwendbarkeit der national kollidierenden Vorschriften anordnet.[11] Auf EU-Ebene existiert die „VO Nr. 1182/71 des Rates v. 03.06.1971 zur Festlegung der Regeln für Fristen, Daten und Termine" (im Folgenden „Fristen-VO"). Die Kollision würde vorliegend dadurch entstehen, dass man bei der Berechnung von in EU-weiten Rechtsakten geregelten Fristen – und damit im Rahmen des Anwendungsbereichs der Fristen-VO – nationales Recht (BGB u. ZPO) heranziehen würde.[12]

### 4.1 Fristbeginn

Die Fristen-VO normiert in Art. 3 Abs. 1, dass bei einer nach Stunden bemessenen Frist, bei der für den Fristbeginn der Zeitpunkt maßgebend ist, in welchem ein Ereignis eintritt oder eine Handlung vorgenommen wird, die Stunde nicht für die Berechnung der Frist mitgerechnet wird, in die das Ereignis oder die Handlung fällt.

Das fristauslösende Ereignis ist der Zeitpunkt, in dem ein Data Breach dem Verantwortlichen bekannt wird. Dabei genügt eine objektive Schutzverletzung, sodass es auf ein Verschulden des Verantwortlichen nicht ankommt.[13] Dem Sinn und Zweck der Vorschrift entsprechend muss auch bereits ein bestimmter Grad an Wahrscheinlichkeit der Datenschutzverletzung für das Vorliegen der Kenntnis von einem Data Breach genügen.[14]. Eine positive Feststellung ist nicht zu fordern. Notwendig ist jedoch ein ange-

3 Martini in Paal/Pauly, 2. Auflage 2018, DSGVO Art. 33 Rn. 3.
4 Petri, DUD 2018 S. 754.
5 Brink in BeckOK Datenschutzrecht, Wolff/Brink 32. Edition, Stand: 01.11.2019, Art. 33 Rn. 44.
6 Vgl. Martini in Paal/Pauly, DSGVO Art. 33 Rn. 37; Jandt in Kühling/Buchner, 2. Auflage 2018, DSGVO BDSG Art. 33 Rn. 16; Reif in Gola, DSGVO, Art. 33 Rn. 39.
7 Brink in BeckOK Datenschutzrecht, Art. 33 Rn. 45.
8 Jandt in Kühling/Buchner, DSGVO BDSG Art. 33 Rn. 16.
9 Brink in BeckOK Datenschutzrecht, Art. 33 Rn. 19.
10 Piltz/Pradel ZD 2019, 152 (153).
11 EuGH, U. v. 15.07.1964 – C-6/64, Rn. 47.
12 Piltz/Pradel a.a.O.
13 Brink in BeckOK Datenschutzrecht, Art. 33 Rn. 27.
14 Laue in Spindler/Schuster, 4. Auflage 2019, DSGVO Art. 33 Rn. 9; Brink in BeckOK Datenschutzrecht, Art. 33 Rn. 27; Dix in Simitis/Hornung/Spiecker, 1. Auflage 2019, DSGVO Art. 33 Rn. 7; Informationspapier des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zu Data-Breach-Meldungen nach Art. 33 DSGVO vom 15.11.2018, S. 6, abrufbar unter https://datenschutz-hamburg.de/assets/pdf/2018.11.15_Data%20Breach_Vermerk_extern.pdf; Artikel-29-Datenschutzgruppe, Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679, WP 250, zuletzt überarbeitet und angenommen am 06.02.2018, S. 12.

messener Grad an Sicherheit, dass ein Data Breach gegeben ist.[15] Schutzzweck der Meldepflicht ist es, betroffene Personen rechtzeitig vor einem Datenmissbrauch zu warnen und etwaige Folgeschäden zu vermeiden.[16] Eine solche Vermeidung von Folgeschäden kann jedoch in bestimmten Fällen unmöglich werden, wenn abgewartet wird, bis volle Gewissheit bezüglich einer Datenschutzverletzung besteht.[17] Insbesondere vor dem Hintergrund, dass gewiefte Hacker meist keinerlei Spuren hinterlassen, die auf ihre Identität oder einen vorgenommenen Data Breach hindeuten würden, würde die Meldepflicht nicht eingreifen, obwohl ein Missbrauch anhand der gewonnen Daten umso wahrscheinlicher wird.[18] Gibt es Hinweise auf einen Data Breach, trifft den Verantwortlichen zudem im Hinblick auf Art. 32 Abs. 1 DSGVO die Obliegenheit, weitere belastbare Informationen zu beschaffen.[19]

## 4.2 Fristende

Fraglich ist, wann die Frist des Art. 33 DSGVO endet. Vergleicht man die nationalen Regelungen mit der Fristen-VO, wird ein Unterschied deutlich. Die nationalen Regelungen berechnen bei Stundenfristen Sonntage, allgemeine Feiertage und Sonnabende nicht mit (vgl. § 222 Abs. 3 ZPO). Anders ist dies in Art. 3 Abs. 4 Fristen-VO, bei dem eine solche Herausnahme dieser Tage nicht erfolgt und nach dessen Wortlaut eine Frist demnach auch an einem Wochenende enden kann; dieser lautet insoweit: „Fällt der letzte Tag einer nicht nach Stunden bemessenen Frist auf einen Feiertag, einen Sonntag oder einen Sonnabend, so endet die Frist mit Ablauf der letzten Stunde des folgenden Arbeitstags."

Ohne explizit eine Frist nach Stunden zu benennen oder auszuschließen, normiert Art. 3 Abs. 5 Fristen-VO: „Jede Frist von zwei oder mehr Tagen umfasst mindestens zwei Arbeitstage". Dies führt dazu, dass alle Fristen, die mit mehr als zwei Tagen bemessen sind, mindestens zwei Arbeitstage umfassen. Da hier jedoch von Fristen die Rede ist, die Tage umfassen, ist fraglich, ob diese Regelung grundsätzlich auf Stundenfristen und insbesondere auf die 72-Stunden-Frist des Art. 33 Abs. 1 DSGVO angewendet werden kann mit der Konsequenz einer Fristverlängerung im Einzelfall.

**Wortlaut**

Der Wortlaut des Art. 3 Abs. 5 Fristen-VO bringt zunächst wenig Licht ins Dunkel. Die Formulierung „von zwei oder mehr Tagen" deutet zwar darauf hin, dass lediglich nach Tagen bemessene Fristen erfasst sein sollen.[20] Ein Ausnahme für nach Stunden bemessene Fristen existiert jedoch nicht und eine Auslegung in der Hinsicht, dass die Frist konkret in Tagen angegeben sein muss, könnte dem Wortlaut „Jede Frist" zunächst entgegenstehen.[21] Anders hingegen der Wortlaut des Art. 3 Abs. 4 Fristen-VO, welcher eindeutig Stundenfristen von dem Privileg ausnimmt, dass die Frist erst am folgenden Arbeitstag endet, sofern der letzte Tag der Frist auf einen Feier-, Sonn- oder Samstag fällt.

Das Argument, es würde deshalb rechtlich keinen Unterschied machen, ob eine Frist „3 Tage" oder „72 Stunden" umfasse, weil in beiden Fällen das Bedürfnis bestehe, für ein fristwahrendes Handeln auf vollständige Ressourcen zurückgreifen zu können, die an Wochenenden oder Feiertagen typischerweise nicht vorhanden seien[22], verfängt nicht. Stundenfristen sind außerhalb der DSGVO kaum zu finden. Allein in Wechsel- oder Scheckklagen sind Stundenfristen auf nationaler Ebene gesetzlich vorgesehen.[23] Üblicherweise werden Stundenfristen durch eine Behörde oder ein Gericht angeordnet und dies wohl auch nur bei besonderer Dringlichkeit.[24] Stundenfristen geben die Möglichkeit, exakte, von Feier-, Sonn oder Samstagen unabhängige Handlungspflichten zu statuieren.[25] Die Stundenfrist wurde demnach im Rahmen des Art. 33 DSGVO bewusst gewählt aufgrund des oben bereits erwähnten Sinn und Zwecks der Norm. Das genannte Bedürfnis nach einem Rückgriff auf alle Ressourcen muss demnach gegenüber der Notwendigkeit einer möglichst frühzeitigen Meldung zurücktreten.

Auch ist zu berücksichtigen, dass von der Kommission ursprünglich eine Meldefrist von 24 Stunden vorgesehen war.[26] Im Entwurf wurde insbesondere darauf hingewiesen, dass eine Verletzung des Schutzes personenbezogener Daten erhebliche wirtschaftliche Schäden und soziale Nachteile für die betroffene Person nach sich ziehen kann.[27]

**Sinn und Zweck des Art. 33 DSGVO**

Da der Wortlaut kein klares Ergebnis mit sich bringt, gilt es insbesondere, sich den Sinn und Zweck des Art. 33 DSGVO vor Augen zu halten. Neben einem vorbeugenden Schutz der informationellen Selbstbestimmung dient dieser der Minimierung der negativen Folgen von Datenschutzverletzungen durch Publizität und Transparenz gegenüber der Aufsichtsbehörde.[28] Es wird damit dem Umstand Rechnung getragen, dass aufgrund der allgegenwärtigen Datenverarbeitung in der digitalen Welt die Verletzlichkeit der Persönlichkeitsrechte ansteigt und damit nachhaltige Schäden entstehen können.[29] Eine – wenn auch nicht vollumfängliche – Meldung an die Aufsichtsbehörde ist daher möglichst frühzeitig vorzunehmen, damit diese an Stelle von oder ergänzend zu Maßnahmen des Verantwortlichen ggf. eigene aufsichtsbehördliche Maßnahmen zum Schutze des Persönlichkeitsrechts ergreifen kann.[30]

Das Vorbringen, eine Dringlichkeit, die eine „harte" 72-Stunden-Frist rechtfertigen würde, bestehe nicht bei jeder Datenschutzverletzung, da nicht bei jeder ein Eingreifen der Behörde

15 Informationspapier des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit v. 15.11.2018 S. 6; Art.-29-Datenschutzgruppe, WP 250, S. 12.

16 Reif in Gola, DSGVO, Art. 33 Rn. 32.

17 Reif in Gola, DSGVO, Art. 33 a.a.O.

18 Reif in Gola, DSGVO, Art. 33 a.a.O.

19 Orientierungshilfe des Bayerischen Landesbeauftragten für Datenschutz zur Meldepflicht und Benachrichtigungspflicht des Verantwortlichen vom 01.06.2019, Rn. 69.

20 Werkmeister/Brandt/Felcht, CR 2020, 89 (92).

21 Piltz/Pradel ZD 2019, 152 (156).

22 Werkmeister/Brandt/Felcht, CR 2020, a.a.O.

23 Vgl. § 604 Abs. 2 ZPO.

24 Vgl. Kallerhoff/Stamm in Stelkens/Bonk/Sachs, 9. Auflage 2018, VwVfG § 31 Rn. 42.

25 Orientierungshilfe des Bayerischen Landesbeauftragten für Datenschutz zur Meldepflicht und Benachrichtigungspflicht des Verantwortlichen a.a.O.

26 Vgl. Vorschlag für die Datenschutz-Grundverordnung vom 25.01.2012, 2012/0011 (COD) S. 32, abrufbar unter https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF.

27 Vgl. Vorschlag für die Datenschutz-Grundverordnung vom 2012/0011 a.a.O.

28 Brink in BeckOK Datenschutzrecht, Art. 33 Rn. 10; Martini in Paal/Pauly, DSGVO Art. 33 Rn. 11; Reif in Gola, DSGVO, Art. 33 Rn. 2.

29 Martini in Paal/Pauly, DSGVO Art. 33 Rn. 10.

30 Laue in Spindler/Schuster, DSGVO Art. 33 Rn. 2; Martini in Paal/Pauly, DSGVO Art. 33 Rn. 10;

in Betracht komme[31], ist nicht nachvollziehbar vor dem Hintergrund der Existenz des Art. 33 Abs. 4 DSGVO und des ErwG. 85 S. 3 DSGVO. Eine Meldung kann schrittweise erfolgen. Eine solche ist insbesondere dann durchzuführen, wenn detaillierte Informationen etwa zu der Zahl der Betroffenen oder Anzahl der betroffenen Datensätze noch fehlen. Wurde daher eine Datenschutzverletzung eindeutig festgestellt, ist aber deren Ausmaß noch nicht bekannt, ist eine schrittweise Meldung an die Datenschutzbehörde erforderlich und ratsam. Auch eine solche Meldung führt zur Wahrung der Frist. Schnelligkeit geht hier vor Richtigkeit und Vollständigkeit.[32] Zudem verfängt auch das Argument, dass der Verantwortliche bereits gesetzlich verpflichtet sei, soweit möglich auch an Wochenenden und Feiertagen unverzüglich Maßnahmen zur Schadensminimierung einzuleiten[33], nicht vor dem Hintergrund des bereits genannten Zwecks der Meldepflicht. Im Vordergrund steht hier die Publizität gegenüber der Aufsichtsbehörde. Ob diese erstmalig oder nur ergänzend zum Verantwortlichen Maßnahmen einleitet, kann dabei keine Rolle spielen.

Letztlich ist es ebenfalls wenig überzeugend, gegen eine „harte" Frist als Argument anzuführen, an Wochenenden oder Feiertagen seien typischerweise die vollständigen Ressourcen des Verantwortlichen nicht vorhanden[34]. In dieser Hinsicht schreibt die Artikel-29-Datenschutzgruppe richtig, dass Unternehmen dafür die Verantwortung tragen, Strukturen und Ressourcen einzusetzen, die der Art und Komplexität ihrer Geschäftstätigkeit angemessen sind.[35] Verantwortliche könnten daher Verstöße gegen das Datenschutzrecht gerade nicht mit fehlenden Ressourcen begründen.[36] Folglich können auch keine vom Gesetz klar als solche gewählten Stundenfristen mit diesem Argument erweitert werden. In Zeiten von datengetriebenen, hochmodernen Unternehmen und Big Data kann ein Feier- oder Wochenendtag im Rahmen eines Data Breach keinen Aufschub gewähren. Insbesondere dann nicht, wenn es um hochsensible und große Mengen von personenbezogenen Daten geht.

31 Werkmeister/Brandt/Felcht, CR 2020, a.a.O.
32 Brink in BeckOK Datenschutzrecht, Art. 33 Rn. 59.
33 Werkmeister/Brandt/Felcht, CR 2020, a.a.O.
34 Werkmeister/Brandt/Felcht, CR 2020, a.a.O.
35 Art-29-Datenschutzgruppe, Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679 WP 253 S. 13.
36 Artikel-29-Datenschutzgruppe, WP 253 S. 13.

Springer Vieweg

springer.com/informatik

Künstliche Intelligenz

U. Barthelmeß, U. Furbach
**Künstliche Intelligenz aus ungewohnten Perspektiven**
Ein Rundgang mit Bergson, Proust und Nabokov
2019, X, 190 S. 18 Abb., 10 Abb. in Farbe. Brosch.
€ (D) 29,99 | € (A) 30,83 | *CHF 33.50
ISBN 978-3-658-24569-6
€ 22,99 | *CHF 26.50
ISBN 978-3-658-24570-2 (eBook)

C. Beierle, G. Kern-Isberner
**Methoden wissensbasierter Systeme**
Grundlagen, Algorithmen, Anwendungen
6., überarb. Aufl. 2019, XVIII, 564 S. 165 Abb.
Mit Online-Extras. Brosch.
€ (D) 39,99 | € (A) 41,11 | *CHF 44.50
ISBN 978-3-658-27083-4
€ 29,99 | *CHF 35.50
ISBN 978-3-658-27084-1 (eBook)

**Ihre Vorteile in unserem Online Shop:**
Über 280.000 Titel aus allen Fachgebieten | eBooks sind auf allen Endgeräten nutzbar | Kostenloser Versand für Printbücher weltweit

€ (D): gebundener Ladenpreis in Deutschland, € (A): in Österreich. * : unverbindliche Preisempfehlung. Alle Preise inkl. MwSt.

Jetzt bestellen auf springer.com/informatik oder in der Buchhandlung

Part of SPRINGER NATURE

A85542

**Berücksichtigung auf Rechtsfolgenseite**

Es gilt nicht nur aufgrund der zuvor genannten Argumente die „harte Frist", sondern auch, weil anderweitige Mechanismen existieren, die eine notwendige Verhältnismäßigkeit im Rahmen der Meldepflicht schaffen. Im Rahmen der durch die Aufsichtsbehörde getroffenen Sanktionen haben diese begründete Umstände zu berücksichtigen, die einer schnelleren oder umfänglicheren Meldung entgegengestanden haben. Diese Umstände können demnach auf der Rechtsfolgenebene ausreichend berücksichtigt werden. So sind auch bei der Verhängung von Geldbußen im Rahmen des Art. 83 Abs. 2 S. 2 DSGVO von der Datenschutzbehörde neben der „Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens" auch „andere" erschwerende oder mildernde Umstände zu berücksichtigen. Zudem ist auch der „Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mildern", gebührend zu berücksichtigen. Es ist schon deshalb empfehlenswert, einen Data Breach lieber früher als später anzuzeigen.

Durch den im ErwG. 148 eingeführten Begriff des „geringfügigen Verstoßes" wird der Aufsichtsbehörde zudem in den Fällen, in denen nach ihrer Auffassung ein Verstoß unter den konkreten Einzelfallumständen keine erhebliche Gefahr für die Datenschutzrechte der betroffenen Personen darstellt und die fragliche Pflicht in ihrem Kern nicht beeinträchtigt, die Möglichkeit gegeben, die Geldbuße durch eine Verwarnung zu ersetzen.[37] Die Artikel-29-Datenschutzgruppe stellt insoweit fest, dass regulatorische Erfahrungen mit den Kontrollstellen nach Maßgabe der RL 95/46/EG gezeigt hätten, dass eine gewisse Flexibilität gegenüber den Verantwortlichen angemessen sein kann, wenn diese ihren Verstoß eingestanden und die Verantwortung dafür übernommen haben, dessen Auswirkungen zu korrigieren und zu beschränken.[38] Insbesondere nennt sie als Beispiel das rechtzeitige Tätigwerden des Verantwortlichen mit dem Ziel, den Verstoß zu beheben oder zu verhindern, dass schwerwiegendere Auswirkungen eintreten.[39]

## 5 COVID-19 / Corona

Im März 2020 wurde ein gesetzliches Fristen-Moratorium für Straf- und Zivilverfahren eingeführt.[40] Selbst wenn es auch im nationalen Datenschutzrecht zu einer Änderung kommen sollte, würde dies an der 72-Stunden-Frist nichts ändern. Die DSGVO kann durch nationale Regelungen nicht abgeändert werden. Zum einen steht dem der oben erwähnte Anwendungsvorrang entgegen. Zum anderen existiert für die Vorgaben in Art. 33 DSGVO keine Öffnungsklausel. Es bleibt demnach auch trotz Vorliegens der Corona Pandemie bei der 72-Stunden-Frist. Wenn jedoch der Verantwortliche aufgrund der Auswirkungen von COVID-19 an der Meldung gehindert war oder die Frist des Art 33 Abs. 1 DSGVO versäumt hat, dann wird die Datenschutzbehörde mit großer Wahrscheinlichkeit keine Strafe verhängen. In der Begründung für die Verzögerung sollte jedoch deutlich auf diese berücksichtigungswürdigen Umstände hingewiesen werden. Auch hier und nicht nur bei der grundsätzlichen Fristbestimmung ist demnach der bereits erwähnte Grundsatz wegweisend: Schnelligkeit vor Vollständigkeit.

## 6 Ausblick

Angesichts der bereits jetzt vorhandenen und in Zukunft noch hinzukommenden Technologien im digitalen Bereich und den damit einhergehenden Datenmengen und daraus folgenden Risiken für die betroffenen Personen gilt es, einen strengen Ansatz für die Bestimmung der Meldefrist anzusetzen. In unser sich stetig fortentwickelnden Informationsgesellschaft schließt das allgemeine Persönlichkeitsrecht Lücken, die sich aus neuartigen Gefährdungslagen in Folge des technischen Fortschritts ergeben.[41] Solche Lücken dürfen nicht bei an sich hart angesetzte Fristen im Bereich des Datenschutzes dadurch wieder geöffnet werden, dass diesen Fristen die harten Konturen entzogen werden. Eine Auslegung, bei der auch bei Stundenfristen mindestens zwei Arbeitstage umfasst sein müssten, ist auf die 72-Stunden-Frist nicht anwendbar und würde zudem auch dem Ziel des Datenschutzes widersprechen, welches in Art. 1 Abs. 2 DSGVO niedergelegt ist: der Schutz der Grundrechte und insbesondere dem Recht auf Schutz personenbezogener Daten natürlicher Personen.

An der Notwendigkeit einer Meldepflicht an sich bestand vor dem Hintergrund der zu gewährleistenden Transparenz wohl kein ernster Zweifel. Diese Transparenz wird im Falle der Verletzung des Schutzes personenbezogener Daten durch die Meldepflicht erst sichergestellt.[42] Eine solche Transparenz benötigt jedoch Klarheit. Aufgrund der oben aufgeführten Argumente ist daher die Anwendung einer „harten" Frist richtig. Auch wenn sich bis dato nur der Bayerische Landesbeauftragte für den Datenschutz[43] klar dahin positioniert hat, dass Art. 3 Abs. 5 Fristen-VO nicht zu einer Verlängerung der 72-Stunden-Frist führen kann, sollte eine solche Tendenz verfestigt und letztlich auch durch Gerichte bestätigt werden.

37 Artikel-29-Datenschutzgruppe, WP 253 S. 9.
38 Artikel-29-Datenschutzgruppe, WP 253 S. 13.
39 Artikel-29-Datenschutzgruppe, WP 253 S. 13.
40 Vgl. Gesetz zur Abmilderung der Folgen der COVID-19-Pandemie im Zivil-, Insolvenz- und Strafverfahrensrecht vom 27.03.2020.
41 Martini JA 2009, 839 (840).
42 Hornung ZD 2012, 99 (103).
43 Orientierungshilfe des Bayerischen Landesbeauftragten für Datenschutz zur Meldepflicht und Benachrichtigungspflicht des Verantwortlichen vom 01.06.2019, Rn. 80.