Robert Faußner, Christina-Maria Leeb

Die Melde- und Benachrichtigungspflichten nach Art. 33, Art. 34 DSGVO in der betrieblichen Praxis (Teil 1)

Der zweiteilige Beitrag widmet sich den drei wesentlichen Herausforderungen in der Praxis sowie zugehörigen Lösungsvorschlägen im Zusammenhang mit der Meldepflicht an die Aufsichtsbehörden nach Art. 33 DSGVO einerseits und der Pflicht zur Benachrichtigung der betroffenen Personen nach Art. 34 DSGVO andererseits. Diese betreffen die Frage, wann eine Verletzung des Schutzes personenbezogener Daten anzunehmen ist und wie die Maximaldauer der Meldefrist zu berechnen ist. Der Schwerpunkt der Darstellung liegt auf dem Risikobegriff, der für beide Pflichten des Verantwortlichen gleichermaßen Relevanz besitzt. Der vorliegende erste Teil des Beitrags führt in die Thematik ein und vermittelt die zum Verständnis notwendigen Grundlagen.

I. Einleitung

Die in Art. 33 und Art. 34 DSGVO geregelten Melde- und Benachrichtigungspflichten stehen nicht isoliert, sondern bilden wesentliche Elemente eines umfassenden Systems aktiver und passiver Informationspflichten (vgl. die übergreifende Darstellung bei *Kamps/Schneider,* K&R-Beil. 1 zu Heft 7/8/2017, 24 ff.). Dabei sprechen etwa die Zahlen aus dem erst kürzlich veröffentlichten Tätigkeitsbericht 2017/2018 des Bayerischen Landesamts für Datenschutzaufsicht mit Blick auf die Praxisrelevanz der Meldepflicht eine eindeutige Sprache: Mit insgesamt 2.471 Meldungen im Jahr 2018 wurde ein Rekordwert in der Geschichte der Aufsichtsbehörde verzeichnet; die Zahlen stiegen damit auf mehr als das 18fache im Vergleich zu 2017 und damit der Rechtslage unter § 42a BDSG a. F. (BayLDA, 8. Tätigkeitsbericht 2017/2018, abrufbar unter: www.lda.bayern.de/media/baylda_report_08.pdf, S. 18). Für den Berichtszeitraum 2019/2020 wird überdies eine weitere Steigerung erwartet (BayLDA, 8. Tätigkeitsbericht 2017/2018, abrufbar unter: www.lda.bayern.de/media/baylda_report_08.pdf, S. 19). Auch eine unionsweite Betrachtung der Meldepflicht zeichnet ein ähnliches Bild. Insgesamt aufaddiert wurden in der EU von sämtlichen nationalen Aufsichtsbehörden zum Stand Januar 2019 über 41.000 Meldungen getätigt (EU-Kommission unter Bezugnahme auf den EDSA, GDPR in numbers, abrufbar unter: https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf).

Bis dato sind sowohl zur Melde- als auch zur Benachrichtigungspflicht noch keinerlei (publizierten) Gerichtsentscheidungen verfügbar. Dies führt aufgrund einiger zentraler, bislang noch offener Detailfragen zu einer enormen Rechtsunsicherheit bei Unternehmen, zumal Verstöße gegen Art. 33, Art. 34 DSGVO als Ordnungswidrigkeiten mit Geldbußen von bis zu 10 Millionen Euro oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des Unternehmens bewehrt sind, Art. 83 Abs. 4 lit. a DSGVO. Daneben können Verletzungen der Benachrichtigungspflicht u. U. Schadensersatzansprüche aus Vertrags- und Deliktsrecht nach sich ziehen. Der vorliegende Beitrag möchte vor diesem Hintergrund aktuelle Herausforderungen aus Sicht der betrieblichen Praxis adressieren und gleichzeitig Lösungsvorschläge aufzeigen.

II. Die Meldung an die Aufsichtsbehörde nach Art. 33 DSGVO: Grundlagen und Arbeitshilfen

Art. 33 Abs. 1 Satz 1 DSGVO verlangt – als eine von diversen Ausgestaltungen gesetzlicher Meldepflichten (vgl. im nationalen Recht etwa für Betreiber elektronischer Kommunikationsdienste nach § 109a Abs. 1 TKG sowie für solche Kritischer Infrastrukturen nach § 8b Abs. 4, Abs. 1 BSIG) von dem Verantwortlichen im Fall einer Verletzung des Schutzes personenbezogener Daten i. S. d. Art. 4 Nr. 12 DSGVO eine Meldung an die zuständige Aufsichtsbehörde. Diese hat unverzüglich und möglichst binnen 72 Stunden nach dem Zeitpunkt zu erfolgen, zu dem einem Verantwortlichen die Verletzung bekannt wurde; ein Überschreiten der Frist ist nach Art. 33 Abs. 1 Satz 2 DSGVO zu begründen. Den Mindestinhalt der Meldung hat Art. 33 Abs. 3 DSGVO zum Gegenstand. Über laufende Sachverhalte ist die Behörde nach Art. 33 Abs. 4 DSGVO schrittweise in Kenntnis zu setzen. Ausnahmsweise entfällt die Meldepflicht im Sinne des risikobasierten Ansatzes (*Brink,* in: BeckOK-Datenschutzrecht, 28. Edit., Stand: 01.11.2017, Art. 33 DSGVO Rn. 34 m. w. N.), sofern die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, Art. 33 Abs. 1 Satz 1 DSGVO a. E. Eine Informationspflicht des Auftragsverarbeiters an den Verantwortlichen statuiert Art. 33 Abs. 2 DSGVO. Zum Zwecke der Überprüfbarkeit der Meldepflicht ist flankierend in Art. 33 Abs. 5 DSGVO eine umfassende Dokumentationspflicht des Verantwortlichen normiert.

Voraussetzung der Pflicht zur Meldung (und damit zugleich fristauslösendes Ereignis) ist, dass die Verantwortlichen von der Verletzung hinreichend Kenntnis erlangt haben – auf ein Verschulden des Verantwortlichen kommt es gerade nicht an (statt vieler *Martini,* in: Paal/Pauly, DSGVO BDSG, 2. Aufl. 2018, Art. 33 Rn. 16a, 18 ff.). Eine bestimmte Form der Meldung wird nicht vorausgesetzt, was sich aus einem Umkehrschluss zu Art. 12 Abs. 1 Satz 2, Satz 3 DSGVO ableiten lässt (statt vieler *Brink,* in: BeckOK-Datenschutzrecht, 28. Edit., Stand: 01.11.2017, Art. 33 DSGVO Rn. 31). Dennoch ist vor allem mit Blick auf Art. 33 Abs. 5 DSGVO die Wahl der Schriftform, jedenfalls aber der Textform anzuraten. Mit Ausnahme Brandenburgs halten sämtliche Aufsichtsbehörden der Länder sowie die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) elektronische Musterformulare bereit, die entweder rein webbasiert auszufüllen sind oder als downloadbare Online-Formulare über einen gesonderten Uploadbereich, via (ggf. mit PGP verschlüsselter) E-Mail, Telefax oder auf dem Postweg übermittelt werden können. Gesonderte Merkblätter bzw. unmittelbar auf den Online-Auftritten der Aufsichtsbehörden enthaltene Hinweise enthalten häufig zusätzliche Informationen als Ausfüllhilfen; vgl. im Einzelnen die nachfolgende Übersicht:

Aufsichtsbehörde	Formulartyp	Link
BfDI	Rein webbasiert	www.bfdi.bund.de/DE/Service/Datenschutzverstoesse/datenschutzverstoesse_node.html
Baden-Württemberg (Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg)	Rein webbasiert	www.baden-wuerttemberg.datenschutz.de/datenpanne-melden/
Bayern (Bayerisches Landesamt für Datenschutzaufsicht; BayLDA)	Rein webbasiert	www.lda.bayern.de/de/datenpanne.html
Berlin (Berliner Beauftragte für Datenschutz und Informationsfreiheit)	Downloadbar	www.datenschutz-berlin.de/wirtschaft-und-verwaltung/meldung-einer-datenpanne/datenpannenformular/
Brandenburg (Landesbeauftragte für Datenschutz und Akteneinsicht)	Nicht verfügbar	–
Bremen (Landesbeauftragte für Datenschutz)	Rein webbasiert	www.datenschutz.bremen.de/wir_ueber_uns/datenschutzverletzung_melden-15665
Hamburg (Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit)	Rein webbasiert	https://datenschutz-hamburg.de/meldung-databreach
Hessen (Hessischer Beauftragter für Datenschutz und Informationsfreiheit)	Downloadbar	https://datenschutz.hessen.de/service/meldungen-von-verletzungen-des-schutzes-personenbezogener-daten
Mecklenburg-Vorpommern (Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern)	Rein webbasiert	www.datenschutz-mv.de/kontakt/meldung-einer-datenpanne/
Niedersachsen (Landesbeauftragte für den Datenschutz Niedersachsen)	Rein webbasiert	www.navo.niedersachsen.de/navo2/portal/csend/8916/fileget/artikel_33.html
NRW (Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen)	Downloadbar	www.ldi.nrw.de/mainmenu_Aktuelles/Formulare-und-Meldungen/Inhalt2/Meldeformular---Verletzung-des-Schutzes-personenbezogener-Daten/formular_art33.pdf
Rheinland-Pfalz (Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz)	Rein webbasiert	www.datenschutz.rlp.de/de/themenfelder-themen/online-services/meldeformular-datenpanne-art-33-ds-gvo/
Saarland (Unabhängiges Datenschutzzentrum Saarland)	Rein webbasiert	https://datenschutz.saarland.de/online-services/datenpanne-melden-fuer-verantwortliche/
Sachsen (Sächsischer Datenschutzbeauftragter)	Downloadbar	www.saechsdsb.de/meldung-datenschutzverstoss
Sachsen-Anhalt (Landesbeauftragter für den Datenschutz Sachsen-Anhalt)	Rein webbasiert	https://datenschutz.sachsen-anhalt.de/service/online-formulare/datenschutzverletzung/?no_cache=1
Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein)	Downloadbar	www.datenschutzzentrum.de/meldungen/
Thüringen (Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit)	Downloadbar	www.tlfdi.de/tlfdi/wir/infomaterial-mustervordrucke/mustervordrucke/

Tab. 1: Übersicht Meldeformulare

Nach Art. 70 Abs. 1 Satz 2 lit. g DSGVO hat der Europäische Datenschutzausschuss (EDSA) die Aufgabe, Leitlinien, Empfehlungen und bewährte Verfahren zur Meldepflicht – konkret zur Feststellung von Verletzungen des Schutzes personenbezogener Daten, zur Festlegung der Unverzüglichkeit sowie zu den Umständen der Meldepflicht – bereitzustellen. Nachdem bislang seitens des EDSA noch keine eigenen Dokumente herausgegeben wurden, ist insoweit auf die noch von der Art. 29-Datenschutzgruppe erstellten „Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679" in der aktuellsten Fassung vom 06.02.2018, WP250rev.01 (abrufbar unter: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052) zurückzugreifen (vgl. allgemein *Schiedermair,* in: Simitis/Hornung/Spieker gen. Döhmann, Datenschutzrecht, 2019, Art. 70 DSGVO Rn. 6). Der EDSA hat diese Leitlinien auch explizit gebilligt (Endorsement of WP29 Documents, 1/2018, abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf, Ziffer 4).

Daneben ist nach wie vor das Kurzpapier Nr. 18 der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz; DSK) mit Stand vom 26.04.2018 (abrufbar unter: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/KP_18_Risiko.pdf) zur Konkretisierung des Risikos für die Rechte und Freiheiten natürlicher Personen heranzuziehen. Ausweislich des Vorworts soll dieses Kurzpapier auch vordringlich als Orientierungshilfe für den nicht-öffentlichen Bereich dienen.

III. Die Benachrichtigung betroffener Personen nach Art. 34 DSGVO: Grundlagen und Arbeitshilfen

Sofern die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein *hohes* Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat, hat der Verantwortliche nach Art. 34 Abs. 1 DSGVO zusätzlich die betroffenen Personen hiervon unverzüglich zu benachrichtigen. Hintergrund ist die angestrebte Vermeidung und Minimierung von Folgeschäden (*Franck,* in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2018, Art. 34 Rn. 1). Vorgaben zu Gestaltung, Formulierung und (Mindest-)Inhalt der Benachrichtigung enthält Art. 34 Abs. 2 DSGVO. Art. 34 Abs. 3 DSGVO beschreibt drei Konstellationen, in denen jeweils die Pflicht zur Benachrichtigung entfällt: (i) Anwendung geeigneter technischer und organisatorischer Sicherheitsvorkehrungen, (ii) Durchführung von Maßnahmen zur wahrscheinlichen Eliminierung des hohen Risikos und (iii) unverhältnismäßiger Aufwand. Art. 34 Abs. 4 DSGVO hat einen Teil der Handlungsoptionen der Aufsichtsbehörden zum Gegenstand – etwa eine Weisung an den Verantwortlichen, die Betroffenen zu benachrichtigen, vgl. auch Art. 58 Abs. 2 lit. e DSGVO.

Von besonderer Wichtigkeit in Bezug auf die konkrete Umsetzung der Benachrichtigungspflicht im Sinne einer „echten Informationsgrundlage" ist die von Art. 34 Abs. 2 DSGVO geforderte Wahl einer klaren und einfachen Sprache, die auch bereits im Rahmen der allgemeinen Vorgaben zu den Betroffenenrechten in Art. 12 Abs. 1 DSGVO zum Ausdruck kommt. In Parallelität zur Meldepflicht besteht zwar kein Formzwang, jedoch ist auch hierbei grundsätzlich zur Informationserteilung in Schrift- oder jedenfalls Textform zu raten (in dieselbe Richtung *Grages,* in: Plath, DSGVO/BDSG, 3. Aufl. 2018, Art. 34 DSGVO Rn. 9).

Nachdem sich die Benachrichtigungspflicht betroffener Personen noch stärker als die Meldepflicht gegenüber der Aufsichtsbehörde am Einzelfall orientiert, stehen im Gegensatz dazu hierfür in der Praxis weitaus weniger Arbeitshilfen und Muster zur Verfügung (eine begrüßenswerte Ausnahme in Gestalt einer Muster-Mitteilung findet sich hingegen bei *Koreng,* in: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2. Aufl. 2018, C. VI. 2.). Zumindest vereinzelt enthalten die Internetauftritte der Aufsichtsbehörden der Länder zusätzliche Informationen. Auch in diesem Zusammenhang von Relevanz sind jedoch die bereits erwähnten Leitlinien der Art. 29-Datenschutzgruppe, die gesonderte Ausführungen zu Art. 34 DSGVO sowie zur Bewertung eines hohen Risikos enthalten. Letztgenanntes hat nach Art. 70 Abs. 1 Satz 2 lit. h DSGVO wiederum im Ausgangspunkt der EDSA zu konkretisieren, wobei eigene Leitlinien bislang nicht veröffentlicht sind. Daneben ist zur Risikoabwägung wiederum auf das DSK-Kurzpapier Nr. 18 zu verweisen.

IV. Wesentliche Unterschiede zu § 42a BDSG a. F.

Die Vorschriften zur Meldung von und Benachrichtigung über Datenschutzverletzungen weichen stark von § 42a BDSG a. F. ab. Zunächst findet keine Unterscheidung zwischen öffentlichen und nicht-öffentlichen Stellen mehr statt. Für öffentliche Stellen des Bundes und die meisten öffentlichen Stellen der Länder bestanden vor dem 25.05.2018 keine Melde- und Benachrichtigungspflichten. Seither bestehen sie für öffentliche und nicht-öffentliche Stellen gleichermaßen.

Zudem sind Art. 33 und Art. 34 DSGVO viel weiter gefasst als § 42a BDSG a. F. Die Mitteilungspflichten traten nach § 42a Satz 1 BDSG a. F. nur ein, wenn (i) besondere Arten personenbezogener Daten nach § 3 Abs. 9 BDSG a. F. (nunmehr besondere Kategorien personenbezoge-

ner Daten, vgl. Art. 9 DSGVO), (ii) einem Berufsgeheimnis unterliegende personenbezogene Daten, (iii) personenbezogene Daten in Bezug auf strafbare Handlungen oder Ordnungswidrigkeiten oder (iv) personenbezogene Daten zu Bank- oder Kreditkartenkonten betroffen waren. Eine solche explizite Beschränkung auf bestimmte Datenkategorien sieht die DSGVO hingegen – wie bereits dargestellt – nicht mehr vor.

Des Weiteren war eine Meldung an die zuständige Aufsichtsbehörde sowie eine Mitteilung an die Betroffenen nur notwendig, wenn die vorgenannten Datenkategorien unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, § 42a Satz 1 BDSG a. F. Nach § 3 Abs. 4 Satz 2 Nr. 3 BDSG a. F. war unter Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft, zu verstehen. Eine unrechtmäßige Übermittlung war anzunehmen, wenn kein Erlaubnistatbestand wie beispielsweise eine Einwilligung nach § 4a BDSG a. F. vorlag. Alternativ hierzu enthielt § 42a Satz 1 BDSG den Auffangtatbestand der Kenntniserlangung auf sonstige Weise. Der Auffangtatbestand war erfüllt, wenn die Kenntnisnahme gegen oder ohne den Willen der verantwortlichen Stelle erfolgte (*Scheffczyk*, in: BeckOK Datenschutzrecht, § 42a BDSG 2003, 28. Edit., Stand: 01.11.2018, Rn. 28 m. w. N.). Hierunter fielen etwa das Ausspähen von Daten durch Dritte, eine Übermittlung von Daten an den falschen Empfänger, eine versehentliche Veröffentlichung der Daten im Internet oder das Abhandenkommen von Speichermedien wie Notebooks und USB-Sticks mit hierauf gespeicherten Daten (vgl. *Scheffczyk*, in: BeckOK Datenschutzrecht, § 42a BDSG 2003, 28. Edit., Stand: 01.11.2018, Rn. 28 f.).

Darüber hinaus musste für die Pflicht zur Meldung und Benachrichtigung gleichermaßen noch eine schwerwiegende Beeinträchtigung für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen, § 42a Satz 1 BDSG a. F.

Der Beitrag wird in der kommenden Ausgabe fortgesetzt.

Autoren: **Robert Faußner ist Rechtsanwalt bei der Heussen Rechtsanwaltsgesellschaft mbH in München und beschäftigt sich dort vorwiegend mit Fragen des Datenschutzrechts.**
Dr. Christina-Maria Leeb arbeitet als Wissenschaftliche Mitarbeiterin ebenfalls bei der Heussen Rechtsanwaltsanwaltsgesellschaft mbH in München, dort in der Praxisgruppe IT/IP/Media.

© Universität Passau/Hernandez