Robert Faußner, Christina-Maria Leeb

Die Melde- und Benachrichtigungspflichten nach Art. 33, Art. 34 DSGVO in der betrieblichen Praxis (Teil 2)

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. Der zweite Teil setzt auf den ersten auf, welcher grundlegende Zusammenhänge vermittelt (Datenschutz-Berater 2019, 156–159).

I. Aktuelle Herausforderungen und Lösungsvorschläge

1. Die Verletzung des Schutzes personenbezogener Daten i. S. d. Art. 4 Nr. 12 DSGVO

Sowohl die Meldepflicht nach Art. 33 DSGVO als auch die Benachrichtigungspflicht nach Art. 34 DSGVO verlangt eine Verletzung des Schutzes personenbezogener Daten. Hierunter ist nach Art. 4 Nr. 12 DSGVO eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur – unbeabsichtigten oder unrechtmäßigen – Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, zu verstehen.

Hieraus ergibt sich ein erstes wichtiges Praxisproblem: Es stellt sich die Frage, ob eine Verletzung tatsächlich bereits eingetreten sein oder ob diese nur möglich erscheinen muss. In der Praxis ist dies beispielsweise dann relevant, wenn bei einem Datenhack (etwa in Gestalt des sog. „Google Conditional Hack“) von der IT nicht geklärt werden kann, ob überhaupt ein Zugriff auf personenbezogene Daten erfolgte und daher lediglich die Möglichkeit eines Zugriffs bestand. Hier könnte der Tatbestand eines unbefugten Zugangs zu personenbezogenen Daten bereits erfüllt sein. Eine wortlautorientierte Auslegung des Art. 33 DSGVO führt zu dem Schluss, dass eine tatsächliche Verletzung gegeben sein muss. Die Vorschrift verweist – auch in der maßgeblichen englischsprachigen Fassung („in the case of a personal data breach“) – klar auf eine *Verletzung* des Schutzes personenbezogener Daten; eine bloße Gefahr oder lediglich mögliche bzw. wahrscheinliche Verletzung findet keine Erwähnung. Die rechtswissenschaftliche Literatur verhält sich hierzu indifferent; eine Gerichtsentscheidung ist bislang noch nicht bekannt. Aus Sicht der Verantwortlichen ist daher in Zweifelsfällen zur Kontaktaufnahme mit der Aufsichtsbehörde zu raten. Dies stellt – ebenso wie die Benachrichtigung der betroffenen Personen – bis zur eindeutigen Klärung der dargestellten Streitfrage eine sinnvolle Vorgehensweise dar.

2. Der Risikobegriff: Kriterien für die Prognoseentscheidung

Nach Art. 33 Abs. 1 Satz 1 DSGVO a. E. muss keine Meldung erfolgen, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Die Verordnung unterscheidet zwischen einem „Risiko“, „hohen Risiko“ sowie der in eingangs erwähnter Vorschrift zum Ausdruck gebrachten Formulierung „voraussichtlich nicht zu einem Risiko führend“. Nachdem eine Verarbeitung ohne jegliches Risiko für die betroffenen Personen nicht denkbar ist, ist eine Ausnahme von der Meldepflicht bei Bestehen eines *geringen* Risikos anzunehmen. Voraussetzung der Meldepflicht ist somit im Umkehrschluss (mindestens) das Vorliegen eines *mittleren* Risikos. Der Verantwortliche hat bei jedem möglichen Datenverstoß anhand einer eigenen Risikoprognose zu entscheiden, ob seiner Ansicht nach ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht und, falls ja, welchem „Intensitätsgrad“ dieses zuzuordnen ist.

Erwägungsgrund 85 führt in Satz 1 beispielhaft Kriterien für die Prognoseentscheidung des Verantwortlichen auf. Demnach sind hierbei physische, materielle oder immaterielle Schäden (wie etwa der Verlust der Kontrolle über personenbezogene Daten der Betroffenen oder Rufschädigung) oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person zu berücksichtigen. Daneben finden sich in den einschlägigen Leitlinien der Art. 29-Datenschutzgruppe ebenfalls bestimmte Kriterien für die Bestimmung des Risikos (WP250rev.01, S. 28 ff.): (i) Art der Datenschutzverletzung, (ii) Art/Sensibilität/Umfang der personenbezogenen Daten, (iii) Möglichkeiten der Identifikation von betroffenen Personen, (iv) potenzielle Konsequenzen des Vorfalls, (v) besondere Eigenschaften der betroffenen Personen oder des Verantwortlichen sowie (vi) Zahl der betroffenen Personen.

Überdies ist bei jeder meldepflichtigen Verletzung stets zusätzlich eine Prognose anzustellen, ob voraussichtlich ein *hohes* Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen besteht. In diesem Fall hat der Verantwortliche nach Art. 34 Abs. 1 DSGVO neben der Aufsichtsbehörde unverzüglich die Betroffenen zu benachrichtigen. Der Risikobegriff ist bei Art. 34 DSGVO im Gegensatz zu Art. 33 DSGVO materielle Tatbestandsvoraussetzung für die Benachrichtigungspflicht, während bei Art. 33 DSGVO eine Meldepflicht immer besteht und nur ausnahmsweise bei voraussichtlich nur geringem Risiko entfällt. Demzufolge gibt es zahlreiche Fälle, in denen zwar eine Melde-, aber keine Benachrichtigungspflicht besteht.

Ein hohes Risiko ist mit Blick auf den Wortlaut des Art. 34 Abs. 1 DSGVO anzunehmen, wenn eine hohe Eintrittswahrscheinlichkeit für eines der beschriebenen Risiken aus Erwägungsgrund 85 vorliegt, wobei auch das drohende Schadensausmaß einzubeziehen ist. Je größer der potenzielle Schaden und auch je sensibler die Art der Daten ist, desto geringer sind hierbei auch die Anforderungen an die Eintrittswahrscheinlichkeit anzusetzen, vgl. Erwägungsgrund 75 Satz 1 (ebenso statt vieler *Reif,* in: Gola, DSGVO, 2. Aufl. 2018, Art. 34 Rn. 4). Außerdem muss ein hohes Risiko auch dann bejaht werden, wenn ein hohes drohendes Schadensausmaß bezüglich des Vorliegens der Datenkategorien nach Art. 35 Abs. 3 DSGVO wie z. B. Gesundheits- und/oder Kontodaten gegeben ist. Ist Letzteres der Fall, darf im Gegenzug die Eintrittswahrscheinlichkeit nicht zu hoch angesetzt werden (so auch *Dix,* in: Simitis/Hornung/Spieker, Datenschutzrecht, 2019, Art. 34 DSGVO Rn. 4 m. w. N.).

3. Die Berechnung der Maximaldauer der Meldefrist

Eine Verletzung des Schutzes personenbezogener Daten ist nach Art. 33 Abs. 1 Satz 1 DSGVO unverzüglich und möglichst binnen 72 Stunden der gem. Art. 55 DSGVO zuständigen Aufsichtsbehörde mitzuteilen.

Der **Fristbeginn** fällt nach dem Wortlaut des Art. 33 Abs. 1 Satz 1 DSGVO auf den Zeitpunkt, in welchem dem Verantwortlichen die Verletzung bekannt wird. Der Normwortlaut enthält die Formulierung „bekannt" und nicht „bekannt sein muss", sodass die Frist nicht schon dann zu laufen beginnt, wenn dem Verantwortlichen – auch aufgrund Fahrlässigkeit – noch nicht alle notwendigen Informationen vorliegen (*Martini,* in: Paal/Pauly, DSGVO BDSG, 2. Aufl. 2018, Art. 33 DSGVO Rn. 19).

Gerade mit Blick auf die Möglichkeit einer schrittweisen Meldung nach Art. 33 Abs. 4 DSGVO, die in der Praxis insbesondere bei Cyber-Sicherheitsvorfällen relevant wird, müssen hierbei jedenfalls noch nicht alle Mindestinhalte für eine Meldung der Datenschutzverletzung nach Art. 33 Abs. 3 DSGVO vorliegen (*Reif,* in: Gola, DSGVO, 2. Aufl. 2018, Art. 33 Rn. 39). Vielmehr ist hierbei auf einen spezifischen „Kerninhalt" der Erstmeldung abzustellen, welcher seinerseits den Beginn der 72 Stunden-Frist markiert. Er umfasst Informationen über Art, Umstände und Zeitpunkt der Schutzverletzung sowie über die Kategorien der betroffenen Daten auf Seiten des Verantwortlichen (so *Dix,* in: Simitis/Hornung/Spieker, Datenschutzrecht, 2019, Art. 33 DSGVO Rn. 7 m. w. N.). Teilweise wird in den Kerninhalt auch noch die Wahrscheinlichkeit für einen Risikoeintritt miteinbezogen (so *Martini,* in: Paal/Pauly, DSGVO BDSG, 2. Aufl. 2018, Art. 33 DSGVO Rn. 18 f.). Der Verantwortliche darf bzw. muss somit erst die Sachlage klären, bevor die Frist zu laufen beginnt. Eine Verdachtsmeldung ist nicht erforderlich. Dies darf jedoch selbstverständlich nicht dazu führen, dass der Verantwortliche die erforderlichen Nachforschungen bewusst verzögert oder unterlässt. Ein Bekanntwerden der Kerninhalte einer initialen Meldung an die Aufsichtsbehörde ist somit jedenfalls dann anzunehmen, wenn der Verantwortliche bewusst und planmäßig darauf hingewirkt hat, sich Informationen und Indizien, aus denen sich eine Verletzung ergibt, zu verschließen (ebenso *Martini,* in: Paal/Pauly, DSGVO BDSG, 2. Aufl. 2018, Art. 33 DSGVO Rn. 19).

Mit Blick auf die Fristberechnung im Einzelnen herrscht bislang – wie im Allgemeinen in Bezug auf Fristen der DSGVO – in der Literatur Uneinigkeit darüber, ob sich diese im Ergebnis nach den nationalen Regelungen wie z. B. §§ 186 ff. BGB (so statt vieler *Eßer,* in: Auernhammer, DSGVO BDSG, 6. Aufl. 2018, Art. 12 DSGVO Rn. 25) oder nach der Verordnung (EWG, Euratom) Nr. 1182/71 des Rates v. 03.06.1971 zur Festlegung der Regeln für die Fristen, Daten und Termine (ABl. L 124, S. 1–2; im Folgenden: Fristen-VO; hierfür *Piltz/Pradel,* ZD 2019, 152 ff.) vollzieht. Dies ist deswegen – obschon der verhältnismäßig moderaten Fehlerfolge einer Begründungspflicht, vgl. Art. 33 Abs. 1 Satz 2 DSGVO – von Relevanz, da es hierbei mit Blick auf **Feiertage und Wochenenden** zu unterschiedlichen Ergebnissen kommt. Außerdem kann eine nicht rechtzeitige Meldung zu Sanktionen seitens der Aufsichtsbehörden, konkret in Gestalt einer Verwarnung oder der Verhängung eines Bußgeldes, führen (*Brink,* in: BeckOK-Datenschutzrecht, 28. Edit., Stand: 01.11.2017, Art. 33 DSGVO Rn. 45).

Bei der Berechnung der 72 Stunden-Frist sind unter Heranziehung des (§ 57 Abs. 2 VwGO i. V. m.) § 222 Abs. 3 ZPO bzw. § 193 BGB Sonntage, allgemeine Feiertage und Sonnabende nicht mitzurechnen. Dies führt dazu, dass bei einem Fristende beispielsweise an einem Sonntag die Frist erst im Laufe des Montags abliefe. Die Fristen-VO nimmt hingegen eine nach Stunden bemessene Frist von der dortigen, sinngemäßen Regelung (Art. 3 Abs. 4) explizit aus. Dasselbe regelt im Übrigen § 31 Abs. 6 VwVfG. Dennoch führt sie insoweit zu „besseren"

Ergebnissen für die Verantwortlichen. So regelt Art. 3 Abs. 5 Fristen-VO, dass jede Frist von zwei oder mehr Tagen – und jedenfalls nach streng wortlautorientierter Auslegung auch die Maximaldauer der Meldefrist nach Art. 33 Abs. 1 Satz 1 DSGVO – mindestens zwei Arbeitstage umfasst. Demnach würde eine am Freitag beginnende 72 Stunden-Frist erst an einem Dienstag ablaufen; vgl. im Einzelnen das nachfolgende Beispiel:

- Bekanntwerden der Datenschutzverletzung(en): Freitag, 14.15 Uhr
- Fristberechnungsbeginn, Art. 3 Abs. 1 UAbs. 1, Abs. 2 lit. a Fristen-VO: Freitag, 15.00 Uhr
- Fristende, Art. 3 Abs. 2 lit. a, Abs. 4, Abs. 5 Fristen-VO: Dienstag, 15.00 Uhr

Wie die Aufsichtsbehörden die Berechnung handhaben und ob sich eine – besonders wünschenswerte – einheitliche europäische Fristberechnung für die Meldepflicht nach Art. 33 DSGVO herauskristallisiert, bleibt abzuwarten.

II. Übergreifende Handlungsempfehlungen

Für Unternehmen sind mit Blick auf die Komplexität, Angriffsfläche und Bedeutung heutiger IT im Voraus klar definierte und mittels griffbereiter Werkzeuge auch umsetzbare Data Incident Management Prozesse von herausragender Bedeutung. Darin empfiehlt sich u. a. neben einer Regelung für eine Klassifikation von Sicherheitsvorfällen eine Festlegung der zu wählenden Form der Meldungen bzw. Benachrichtigungen; dasselbe gilt mit Blick auf die Meldepflicht für die zuständige Aufsichtsbehörde. Ein besonderes Augenmerk ist dabei auf die an den jeweiligen Umständen des Einzelfalls orientierte Prüfung zu legen, ob die Wahl auf das ggf. vorhandene behördliche Formular fällt. Aus Unternehmenssicht ist bei dem Ausfüllen der Formulare auf eine sorgfältige Vorgehensweise zu achten, nachdem nicht alle Felder gesetzliche Pflichtangaben beinhalten. Teilweise enthalten die Internetauftritte der Aufsichtsbehörden auch gesonderte Hinweisdokumente zu der Frage, welche verlangten Informationen gesetzliche Muss-Inhalte betreffen und welche rein freiwillig erteilt werden können.

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

Jetzt bestellen und im Bereich Datenschutz auf dem neuesten Stand sein!

- seit über 40 Jahren
- monatlich
- topaktuell informiert über die wichtigsten Neuigkeiten, Risiken und die aktuelle Rechtsprechung
- mit konkreten Handlungsempfehlungen, Arbeitsmitteln und Checklisten für die tägliche Praxis

https://www.datenschutz-berater.de

- Seit über 40 Jahren ist der monatlich erscheinende **DATENSCHUTZ-BERATER** der verlässliche Ratgeber für Datenschutz und Datensicherheit. Mit den täglich wachsenden Möglichkeiten der Datenerhebung, -verarbeitung und -nutzung wird Datenschutz immer wichtiger. Technische und rechtliche Neuerungen, Risiken und die aktuelle Rechtsprechung fordern von den Verantwortlichen, sich fortlaufend zu informieren. Der Fachleser profitiert von konkreten Handlungsempfehlungen, Arbeitsmitteln und Checklisten für die tägliche Praxis. Literaturtipps und Terminhinweise für Aus- und Weiterbildung runden das Angebot ab.
- Zielgruppe sind Fach- und Führungskräfte der Datenschutzabteilung, Personalabteilung, interne und externe Datenschutzbeauftragte, Datenschutzabteilungen, Geschäftsführer, IT-Sicherheitsexperten und Revisoren.
- Die **R&W-Online Datenbank** online.ruw.de – mit allen Inhalten der R&W-Zeitschriften und des R&W-Buchportfolios – bietet eine publikationsübergreifende, schnelle und zuverlässige Recherchemöglichkeit. Highlights sind die Übersichtlichkeit, Bedienerfreundlichkeit und besonders die pdf-Darstellung gemäß des Original-Seitenlayouts.

Per Faxantwort an 069/7595-1150

Name: ____________________

Firma: ____________________

Abteilung: ____________________

Straße: ____________________

PLZ | Ort: ____________________

Telefon: ____________________

E-Mail: ____________________

Datum | Unterschrift: ____________________

Sichern Sie sich Ihr individuelles Vorteilsangebot und bestellen Sie jetzt den DSB – Datenschutz-Berater

☐ **Testabo:** 3 Monate kostenlos lesen + 1 Zugang zur Online-Datenbank

Sie erhalten die nächsten 3 Ausgaben der Fachzeitschrift „Datenschutz-Berater" kostenlos. Falls Ihnen der „Datenschutz-Berater" gefällt, brauchen Sie nichts weiter zu unternehmen. Wenn Sie nicht innerhalb der Testzeit abbestellen, nutzen Sie den „Datenschutz-Berater" im Jahresabo weiter. Zunächst für ein Jahr (11 Ausgaben) zum Vorzugspreis von derzeit 319,- € inkl. aller Gebühren und MwSt. in Deutschland und anschließend bis auf Widerruf zum jeweils gültigen Jahrespreis. Das Abonnement kann bis 3 Monate vor Ablauf des Bezugszeitraumes schriftlich bei der Deutscher Fachverlag GmbH, Mainzer Landstr. 251, 60326 Frankfurt am Main gekündigt werden. Liegt dem Verlag zu diesem Zeitpunkt keine Abbestellung vor, verlängert sich das Abonnement automatisch um ein weiteres Jahr. Die Abonnementgebühren sind im Voraus zahlbar.

☐ **Jahresabo:** 11 Ausgaben + 1 Zugang zur Online-Datenbank

Sie erhalten die nächsten 11 Ausgaben der Fachzeitschrift „Datenschutz-Berater", sowie den Zugang zur Online-Datenbank. Der Abonnementvertrag wird für mindestens ein Jahr abgeschlossen. Das Abonnement kann jederzeit bis 3 Monate vor Ablauf des Bezugszeitraumes schriftlich bei der Deutscher Fachverlag GmbH, Mainzer Landstr. 251, 60326 Frankfurt am Main gekündigt werden. Liegt dem Verlag zu diesem Zeitpunkt keine Abbestellung vor, verlängert sich das Abonnement automatisch um ein weiteres Jahr. Die Abonnementgebühren sind im Voraus zahlbar und betragen 319,- € inkl. aller Gebühren und MwSt. in Deutschland.

DATENSCHUTZ-BERATER
Konrad Eckes | E-Mail: konrad.eckes@dfv.de | Tel.: 069 7595-1154

dfv Mediengruppe