Umgang mit Data-Breach-Meldungen nach Art. 33 DSGVO

Version 2, September 2023

Inhalt

1. Meldepflichtiger Data Breach

Art. 33 DSGVO statuiert eine Meldepflicht bei der Aufsichtsbehörde im „Falle einer Verletzung des Schutzes personenbezogener Daten“, „es sei denn, dass die Verletzung (…) voraussichtlich nicht zu einem Risiko führt“.

a) Verletzung des Schutzes personenbezogener Daten

Die Verletzung des Schutzes personenbezogener Daten ist in Art. 4 Nr. 12 DSGVO legaldefiniert 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, übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“.

Es kommt nicht darauf an, ob Daten von besonders sensiblen Kategorien abhandengekommen sind. Jede Art personenbezogener Daten ist umfasst.

Die deutsche Formulierung „Verletzung des Schutzes“ darf nicht dahingehend missverstanden werden, dass jede Datenschutzverletzung (also jedes rechtswidriges Verhalten) zu melden ist.[1] Die englischsprachige Formulierung „Data Breach“ ist dahingehend deutlicher, dass es sich um

[1] Martini, in: Paal/Pauly, DSGVO, Art. 33 Rn. 16.

einen Sicherheitsbruch handeln muss, bei dem Daten unrechtmäßig Dritten offenbart werden oder infolge eines Sicherheitsbruchs gelöscht oder zeitweise unzugänglich gemacht werden. Mögliche Beispiele sind Hacking und Datendiebstahl[2] sowie SQL-Lücken, Bugs im Webserver, verlorengegangene USB-Sticks oder Laptops sowie der Einbruch in Serverräume, die mit dem Verlust von Hardware einhergehen.[3]

Die „Verletzung der Sicherheit" im Sinne des Art. 4 Nr. 12 DSGVO meint nach einhelliger Literaturauffassung nicht die Unzulässigkeit der Datenverarbeitung, sondern betrifft die Datensicherheit, die nur durch technische und organisatorische Maßnahmen erreicht werden kann.[4] Der europäische Datenschutzausschuss (EDSA) erkennt an, dass es um „security incidents" geht,[5] und nimmt zum Teil auch Fälle der rechtswidrigen Datenübermittlung als Verletzung der Sicherheit an, wenn dadurch eine Offenlegung an Dritte erfolgt. Das Gremium definiert den Begriff „Sicherheit" zwar nicht, nennt aber unter anderem die Beispiele der versehentlichen Falsch-Adressierung von Briefen und E-Mails sowie die Versendung einer Massen-E-Mail unter Verwendung des cc- statt des bcc-Feldes (siehe Beispiele unten).[6] Entscheidend ist also für den EDSA, dass die Daten Dritten zu Kenntnis gegeben werden. Dies kann auch durch menschliches Versagen geschehen, das eine unzulässige Datenverarbeitung auslöst.[7]

Seit 2018 ist auch die vorübergehende Unerreichbarkeit der Daten oder dauerhafter Löschung infolge eines Sicherheitsbruchs von der Meldepflicht umfasst. Dies setzt eine längere Dauer voraus und kann z.B. hervorgerufen werden durch einen Stromausfall oder durch eine Denial-of-Service-Attacke.[8] Geplante Systemausschaltungen fallen nicht darunter, sondern nur unbeabsichtigte Zugangshindernisse sind Data Breaches.[9]

Der Verletzungserfolg muss eingetreten sein.[10] Der Erfolg ist der – beabsichtigte oder unbeabsichtigte – Zugriff auf die Daten.[11] Nicht erforderlich ist hingegen eine Kenntnisnahme des Inhalts.[12] Fand trotz Bestehens einer Sicherheitslücke nachweisbar kein Zugriff statt, besteht keine

[2] Hladjik, in: Ehmann/Selmayr, DSGVO, Art. 33 Rn. 5.
[3] BayLDA, Diskussionspapier zu Art. 33 und Art. 34 DSGVO v. 19.9.2016, S. 1.
[4] Jandt, in: Kühling/Buchner, DSGVO, 2. Aufl. 2018, Art. 4 Nr. 12 Rn. 3 f.; Klabunde, in: Ehmann/Selmayr, DSGVO, Art. 4 Rn. 39; Schild, in: BeckOK DSGVO, Art. 4 Rn. 133.
[5] EDSA Guidelines 9/2022, Version 2.0, S.7.
[6] Art.-29-Gruppe, WP 250, S. 32 f.; ebenso Sassenberg, in: Sydow, DSGVO, 2017, Art. 33 Rn. 18; vgl. EDSA Guidelines 01/2021, Version 1.0, Case 15 und 16, S. 27, 29.
[7] Vgl. EDSA Guidelines 9/2022, Version 2.0, S. 7.
[8] EDSA Guidelines 9/2022, Version 2.0, S. 7.
[9] EDSA Guidelines 9/2022, Version 2.0, S. 7.
[10] Brink, in: BeckOK DSGVO, Art. 33 Rn. 27; Jandt, in: Kühling/Buchner, DSGVO, 2. Aufl. 2018, Art. 33 Rn. 7; Martini, in: Paal/Pauly, DSGVO, Art. 33 Rn. 16a.
[11] Reif, in: Gola, DSGVO, Art. 33 Rn. 21.
[12] Sassenberg, in: Sydow, DSGVO, 2017, Art. 33 Rn. 7.

Meldepflicht.[13] Für das Ausbleiben eines Zugriffs braucht es dabei konkrete Belege wie beispielsweise Logfiles. Waren Daten für eine gewisse Dauer offen im Internet einsehbar, ist davon auszugehen, dass die Sicherheitslücke einen Data Breach bedeutet, solange das Gegenteil nicht belegt werden kann. Unerheblich ist es, ob daraufhin auch ein Schaden (also Vermögensschaden oder immaterieller Schaden) eingetreten ist.[14] Das kann aber bei der Frage des Risikos Berücksichtigung finden.

b) Risiko

Das Risiko bemisst sich aus der Relation zwischen Schwere des möglichen Schadens und seiner Eintrittswahrscheinlichkeit.[15] Je höher der anzunehmende Schaden ist, desto geringer sind die Anforderungen an die Wahrscheinlichkeit.[16] Der Europäische Datenschutzausschuss sieht bei der Risikobetrachtung die folgenden Kriterien vor:[17]

- Art des Data Breach (Unautorisierter Zugriff ist oft gravierender als Datenverlust)
- Art und Umfang der Daten
- Identifizierbarkeit (Wie einfach und wahrscheinlich ist es, dass ein Dritter, der unautorisierten Zugriff nimmt, den Personenbezug herstellen kann?)
- Spezielle Umstände hinsichtlich der Betroffenen (z.B. Kinder, Behinderungen)
- Spezielle Umstände hinsichtlich des Verantwortlichen (z.B. Medizinische Einrichtung)
- Anzahl der Betroffenen
- Zu erwartende Konsequenzen. Zu den Konsequenzen nennt EG 85 typische Fallgruppen:
    - Verlust der Kontrolle über die eigenen Daten
    - Einschränkung von Rechten
    - Diskriminierung
    - Identitätsdiebstahl oder -betrug
    - Finanzielle Verluste
    - Aufhebung der Pseudonymisierung
    - Rufschädigung
    - Verletzung des Berufsgeheimnisses
    - Andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile

Kein Risiko besteht z.B. in der Regel, wenn

- die Daten ohnehin öffentlich verfügbar sind,[18]

[13] Reif, in: Gola, DSGVO, Art. 33 Rn. 21.
[14] Jandt, in: Kühling/Buchner, DSGVO, 2. Aufl. 2018, Art. 33 Rn. 7.
[15] Jandt, in: Kühling/Buchner DSGVO, 2. Aufl. 2018, Art. 33 Rn. 7; Martini, in: Paal/Pauly, DSGVO, Art. 33 Rn. 23 f.
[16] Brink, in: BeckOK DSGVO, Art. 33 Rn. 36.
[17] EDSA Guidelines 9/2022, Version 2.0, S. 20 Rn. 86; siehe auch DSK Kurzpapier Nr.18.
[18] EDSA Guidelines 9/2022, Version 2.0, S. 22, Rn.97.

- die Daten wirksam verschlüsselt sind (außer es ist ein dauerhafter Datenverlust eingetreten, weil z.B. der einzige Datenträger verloren wurde und es keine Backups gibt).[19]

2. Information der Betroffenen

Zusätzlich zur Meldung bei uns muss der Verantwortliche in manchen Fällen auch die betroffenen Personen informieren. Die Informationspflicht nach Art. 34 Abs. 1 DSGVO besteht, wenn der Data Breach „voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten“ zur Folge hat. Im Gegensatz zu Art. 33 setzt Art. 34 also nicht nur ein Risiko, sondern ein hohes Risiko voraus. Die unter 1.b) genannten Kriterien und Fallgruppen greifen auch hier.[20] Darüber hinaus sind die Ausnahmen von der Informationspflicht gem. Art. 34 Abs. 3 DSGVO zu beachten.

3. Beispiele

Der Europäische Datenschutzausschuss erläutert in seinen Guidelines 01/2021[21] die Meldepflicht zahlreicher Beispiele. Diese dienen der Orientierung, wie sie mit Verletzungen des Schutzes von personenbezogenen Daten umgehen und welche Faktoren verantwortliche Stellen bei der Risikobewertung zu berücksichtigen haben.

a) Ransomware

Ein häufiger Grund für die Meldung einer Datenschutzverletzung ist ein sog. „Ransomware-Angriff“ auf den Verantwortlichen. In diesen Fällen verschlüsselt ein bösartiger Code die personenbezogenen Daten, und in der Regel verlangt anschließend ein Angreifer Lösegeld im Austausch für den Entschlüsselungsschlüssel. Diese Art von Angriff kann als eine Verletzung der Verfügbarkeit, Vertraulichkeit und/oder Integrität der Daten auftreten.[22]

	Fallbeschreibung	Art. 33 Meldung	Art. 34 Information	Anmerkungen
I.	Ransomware mit angemessener Sicherungskopie, ohne Exfiltration und verschlüsselten Daten[23]	Nein*	Nein	*Wenn schnelle Wiederherstellung der Sicherungskopie möglich - zumindest innerhalb der potenziellen 72 Stunden Meldefrist und die Hacker nur Zugriff auf verschlüsselte Daten hatten
II.	Ransomware ohne angemessene	Ja*	Nein**	*Überarbeitung der technischen und organisatorischen Maßnahmen sollte angeregt werden.

[19] EDSA Guidelines 9/2022, Version 2.0, S. 22, Rn.97, Sassenberg, in: Sydow, DSGVO, 2017, Art. 33 Rn. 8 f.
[20] Vgl. WP 250, S. 9.
[21] EDSA Guidelines 01/2021, Version 2.0.
[22] EDSA Guidelines 01/2021, Version 2.0, S. 8, Rn. 16.
[23] EDSA Guidelines 01/2021, Version 2.0, Fall Nr. 1, S. 9.

	Sicherungskopie und ohne Exfiltration[24]			**Die nicht erfolgte Exfiltration muss positiv und nachweisbar festgestellt werden.
III.	Ransomware ohne Exfiltration aber kein Zugriff auf Patientendaten in einem Krankenhaus (ca. 30 Stunden)[25]	Ja	Ja*	*Auch bei bestehenden Backups ist durch die Wiederherstellungszeit eine Gefahr für die Patientenversorgung gegeben.
IV.	Ransomware ohne Sicherungskopie und mit Exfiltration von Kunden und z.B. Kreditkartendaten.[26]	Ja	Ja*	*Die Information sollte individuell erfolgen. Wenn das nicht möglich ist, z.B. durch eine, sofort auffindbare, vollumfängliche Information / Banner auf der Website.

b) Angriffe – mit Exfiltration von Daten:

Angriffe, die Schwachstellen in Diensten ausnutzen, die der Verantwortliche Dritten über das Internet anbietet, z. B. durch Injektionsangriffe (z. B. SQL-Injection, Path Traversal), die Kompromittierung von Websites und ähnliche Methoden, ähneln Ransomware-Angriffen insofern, als dass das Risiko von unbefugten Dritten ausgeht.

Die Angriffe zielen in der Regel jedoch auf das Kopieren, Exfiltrieren und den Missbrauch personenbezogener Daten ab. Es handelt sich hauptsächlich um Verletzungen der Vertraulichkeit und möglicherweise auch der Integrität.[27]

	Fallbeschreibung	Art. 33 Meldung	Art. 34 Information	Anmerkungen
V.	Schadsoftware exfiltriert einen Monat lang Bewerbungsdaten von einer Website[28]	Ja	Ja	
VI.	Exfiltration von mit dem Stand der Technik gehashten Kunden Passwörtern von einer Website durch SQL Injektion[29]	Nein	Nein*	*Eine Benachrichtigung der Betroffenen ist nicht verpflichtend aber empfehlenswert um ihnen die Gelegenheit zu geben die Passwörter zu ändern.

[24] EDSA Guidelines 01/2021, Version 2.0, Fall Nr. 2, S. 11.
[25] EDSA Guidelines 01/2021, Version 2.0, Fall Nr. 3, S. 13.
[26] EDSA Guidelines 01/2021, Version 2.0, Fall Nr. 4, S. 15.
[27] EDSA Guidelines 01/2021, Version 2.0, S. 17. Rn. 50.
[28] EDSA Guidelines 01/2021, Version 2.0, Fall Nr. 5, S. 18.
[29] EDSA Guidelines 01/2021, Version 2.0, Fall Nr. 6, S. 19.

VII.	Angriff auf 100.000 Konten einer Bankwebsite mit Log-ins in ca. 2000 Kundenkonten aufgrund einer Schwachstelle in der Website.[30]	Ja	Ja*	*Information aller 100.000 Betroffenen, nicht nur die 2000 der erfolgreichen Log-ins.
VIII.	Hacker erbeuten Nutzernamen, Passwörter und Kaufhistorie der Kunden eines Onlineshops	Ja	Ja	
IX.	„Social-Engineering / Identitätsdiebstahl“ Veränderung der E-Mail-Weiterleitungen z.B. von Rechnungen eines Kunden an die E-Mailadresse von Dritten[31]	Ja	Ja*	*Wenn (echter) Kunde nicht über Änderung der Weiterleitung informiert wurde. Z.B. E-Mail an die ursprüngliche E-Mailadresse.

c) Interne Risikoquellen:

Die Rolle des menschlichen Versagens bei Verletzungen des Schutzes personenbezogener Daten muss aufgrund ihrer Häufigkeit hervorgehoben werden. Die Internationale Konferenz der Datenschutzbeauftragten (GPA) hat erkannt, wie wichtig es ist, sich mit solchen menschlichen Faktoren zu befassen und verabschiedete eine Entschließung, um die Rolle des menschlichen Versagens bei Verletzungen des Schutzes personenbezogener Daten im Oktober 2019. In dieser Entschließung wird betont, dass geeignete Schutzmaßnahmen ergriffen werden sollten, um menschliche Fehler zu vermeiden, sie enthält eine nicht abschließende Liste von Schutzmaßnahmen und Lösungsansätzen.[32]

	Fallbeschreibung	Art. 33 Meldung	Art. 34 Information	Anmerkungen
X.	Mitnahme von Geschäftsdaten eines ehem. Mitarbeiters um Kunden für sich zu gewinnen[33]	Ja	Nein*	*Die Sensibilität und der Umfang der betroffenen personenbezogenen Daten sind zu berücksichtigen.

[30] EDSA Guidelines 01/2021, Version 2.0, Fall Nr. 7, S. 21.
[31] EDSA Guidelines 01/2021, Version 2.0, Fall Nr. 17, S. 35.
[32] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf
[33] EDSA Guidelines 01/2021, Version 2.0, Fall Nr. 8, S. 23.

XI.	Versehentliche Übermittlung von Daten an eine vertrauenswürdige Drittpartei (z.B. Anwälte, Behörden etc.)[34]	Nein*	Nein	*Wenn Drittpartei als Berufsgeheimnisträger zur Vertraulichkeit verpflichtet ist, Löschung / Rücksendung sichergestellt wurde und keine Art.9 DSGVO Daten betroffen waren.

d) Verlorene oder gestohlene Geräte und Dokumente:

Im Falle von verlorenen oder gestohlenen Geräten muss der Verantwortliche die Umstände des Einzelfalles berücksichtigen, insbesondere die Kategorien der gespeicherten Daten sowie die ergriffenen Gegenmaßnahmen. All diese Elemente wirken sich auf die Bewertung der Schwere der Datenverletzung aus. Eine Risikobewertung erweist sich oftmals als schwierig, da die Geräte nicht mehr verfügbar sind und damit Aussagen über z.B. Kategorien der Daten erschwert werden.[35]

	Fallbeschreibung	Art. 33 Meldung	Art. 34 Information	Anmerkungen
XII.	Gestohlenes Gerät nach dem Stand der Technik verschlüsselt (USB-Stick, Festplatte etc.)[36]	Nein	Nein	Kein Art.-33-Fall aufgrund der Verschlüsselung. Meldepflicht besteht jedoch, wenn die Daten nicht anderweitig gesichert sind und somit die Verfügbarkeit beeinträchtigt ist.
XIII.	Gestohlenes Gerät nicht verschlüsselt[37]	Ja	Ja	Entsprechende Art. 32 DSGVO Maßnahmen hätten die Datenpanne verhindern können.
XIV.	Gestohlene Papierakten mit Gesundheitsdaten[38]	Ja	Ja	Entsprechende Art. 32 DSGVO Maßnahmen hätten die Datenpanne verhindern können.

e) Postversehen – Versand an falsche Empfänger:

Die Risikoquelle ist auch in diesem Fall ein internes menschliches Versagen. In diesen Fällen handelt es sich aber nicht um vorsätzliche Handlungen und die Verletzung ist das Ergebnis von Unachtsamkeit. Die verantwortliche Stelle kann im Nachhinein nur wenig unternehmen, so dass

[34] EDSA Guidelines 01/2021, Version 2.0, Fall Nr. 9, S. 25.
[35] EDSA Guidelines 01/2021, Version 2.0, S. 27, Rn. 85.
[36] EDSA Guidelines 01/2021, Version 2.0, Fall Nr. 10, S. 27.
[37] EDSA Guidelines 01/2021, Version 2.0, Fall Nr. 11, S. 28.
[38] EDSA Guidelines 01/2021, Version 2.0, Fall Nr. 12 S. 29.

vorbeugende Maßnahmen in diesen Fällen noch wichtiger sind als bei anderen Arten von Verstößen.[39]

	Fallbeschreibung	Art. 33 Meldung	Art. 34 Information	Anmerkungen
XV.	Versehentliche Versendung von Schülerdaten an eine Mailingliste	Ja	Ja*	*In der Regel
XVI.	Werbe-E-Mail mit offenem Verteiler (cc statt bcc)	Ja*	Ja**	*Art. 33 bei großer Empfängerzahl oder sensiblem Inhalt, z.B. Passwörter. ** Information sollte grds. durch nachfolgende Email mit einer Entschuldigung und Löschungsanweisung erfolgen. Ausnahme nur, wenn wenige Betroffene und kein sensibler Inhalt.
XVII.	Postversandfehler Online Waren[40]	Nein	Nein	*Der falsche Empfänger sollte gebeten werden alle Daten des korrekten Empfängers zu löschen.
XVIII.	Versehentlicher falsch-Versand vertraulicher Daten per E- Mail[41]	Ja	Ja	
XIX.	Postversandfehler Kfz- Versicherungspolice[42]	Ja	*Nein	*Den falschen Empfänger um Vernichtung oder Rücksendung bitten und unterrichten, dass die Daten nicht missbraucht werden dürfen. Keine Art. 9 DSGVO Daten.
XX.	Kontoauszug an falschen Kunden	Ja	Nein*	*Im Einzelfall i.d.R. nicht, bei Häufung schon.

f) EU- grenzüberschreitender Bezug und Meldepflichten

	Fallbeschreibung	Art. 33 Meldung	Art. 34 Information	Anmerkungen
XXI.	Angriff auf Kundendaten eines Unternehmens aus dem EU-Ausland mit Kunden im EU-Inland	Ja*	Ja	*Auch bei Benennung eines Vertreters gem. Art. 27 DSGVO, wird das One-Stop-Shop-Prinzip wird nicht ausgelöst.[43] Nach Art. 56 Abs.1 DSGVO ist jede Aufsichtsbehörde die zuständige Aufsichtsbehörde, soweit ein Bezug zum jeweiligen

[39] EDSA Guidelines 01/2021, Version 2.0, S. 26, Rn. 106.
[40] EDSA Guidelines 01/2021, Version 2.0, Fall Nr. 13, S. 31
[41] EDSA Guidelines 01/2021, Version 2.0, Fall Nr. 14, S. 32.
[42] EDSA Guidelines 01/2021, Version 2.0, Fall Nr. 16, S. 34
[43] EDSA Guidelines 9/2022, Version 2.0 Rn.73.

				Mitgliedsstaats vorliegt.[44] Es müssen demnach alle Aufsichtsbehörden informiert werden, in deren Zuständigkeitsbereich die EU Kunden Ihren Wohnsitz haben.

4. Rechtzeitigkeit der Meldung

Die Meldung muss unverzüglich, spätestens nach 72 Stunden bei der Aufsichtsbehörde eingehen. Die Frist beginnt ab Kenntnis von den erheblichen Tatsachen. Dabei genügt es, dass irgendwo im Unternehmen Kenntnis erlangt wird. Wenn die Meldung nach „allgemeinem Ermessen“ früher möglich ist, hat sie früher zu erfolgen (EG 86). Wird die 72-Stunden-Frist nicht eingehalten, hat der Verantwortliche dies zu begründen (Art. 33 Abs. 1 S. 2 DSGVO). Dabei müssen außergewöhnliche Umstände dargelegt werden.[45] Ein akzeptabler Grund liegt z.B. vor, wenn viele Hacker-Attacken in kurzem Zeitraum auftreten.[46]

Kenntnis ist dann erlangt, wenn der Verantwortliche einen angemessenen Grad an Sicherheit erlangt hat, dass ein Data Breach vorliegt.[47] Die Meldepflicht tritt demnach noch nicht ein, wenn zunächst nur vage Hinweise vorliegen. Dann hat er so schnell wie möglich Ermittlungen anzustellen und hat während der Ermittlungsphase keinen angemessenen Grad an Sicherheit.[48] Der Verantwortliche muss dann eine Meldung vornehmen, sobald sich in den Ermittlungen ein angemessener Grad an Sicherheit herauskristallisiert,[49] also schon bevor er den Sachverhalt vollständig ausermittelt hat. Ein angemessener Grad an Sicherheit liegt z.B. vor, wenn ein USB-Stick mit unverschlüsseltem Inhalt verloren gegangen ist, obwohl (noch) nicht nachvollzogen werden kann, ob Dritte die Daten ausgelesen haben.[50] Wenn der Verantwortliche einen Hinweis inklusive eines Beweises erhält, hat er ebenfalls Kenntnis,[51] nicht jedoch, wenn der Hinweis noch unsubstantiiert ist und weitere Ermittlungen notwendig sind. Leitet beispielsweise ein Betroffener eine Phishing-Mail an den Verantwortlichen weiter, die Kundendaten des Unternehmens des Verantwortlichen enthält, so hat der Verantwortliche nicht sofort eine Meldung abzusetzen. Zunächst hat er sein

[44] Sundermann in Freund/Schmidt/Heep/Roschek, DSGVO 1. Aufl. 2023, S. 477 Rn.13; vgl. auch EuGH v. 5.6.2018 – C 210/16, Rn. 62 ff.
[45] Vgl. Artikel-29-Datenschutzgruppe, WP 250, S. 16.
[46] EDSA Guidelines 9/2022, Version 2.0, S. 16, Rn.63
[47] EDSA Guidelines 9/2022, Version 2.0, S. 11, Rn. 31 f.
[48] EDSA Guidelines 9/2022, Version 2.0, S. 11, Rn. 31 f.
[49] EDSA Guidelines 9/2022, Version 2.0, S. 11, Rn. 31 f.
[50] EDSA Guidelines 9/2022, Version 2.0, S. 11, Rn. 31 f.
[51] EDSA Guidelines 9/2022, Version 2.0, S. 11, Rn. 31 f.

System auf unautorisierte Zugriffe zu überprüfen und hat erst dann Kenntnis, wenn er solche Zugriffe entdeckt.[52] Der Umfang der Meldung bestimmt sich nach Art. 33 Abs. 3 DSGVO.

Sind noch nicht alle vom Gesetz geforderten Inhalte bekannt (z.B. Datenkategorien oder Anzahl der Betroffenen), ist das aber kein Hinderungsgrund für eine rechtzeitige Meldung.[53] Dann hat die Meldung schrittweise zu erfolgen (Art. 33 Abs. 4 DSGVO), sodass die fehlenden Informationen später nachgereicht werden.

5. Form der Meldung

Die Meldung kann auf beliebigem Weg an die Aufsichtsbehörde herangetragen werden, wobei der Postweg aufgrund der kurzen Meldefirst regelmäßig praktisch ausscheidet. Es empfiehlt sich die Nutzung des Meldeformulars im Internet unter https://datenschutz-hamburg.de/meldung-databreach, da dort über eine gesicherte Verbindung und ohne Zeitverzug sensible Inhalte übertragen werden können. Die dort vorhandenen Eingabefelder bilden den gesetzlichen Inhalt der Meldung ab.

[52] Vgl. EDSA Guidelines 9/2022, Version 2.0, S. 11, Rn. 31 f.
[53] Artikel-29-Datenschutzgruppe, WP 29, S. 14.