15.11.2018

Data-Breach-Meldungen nach Art. 33 DSGVO

Sogenannte Data Breaches sind unter Umständen der Aufsichtsbehörde und ggfs. auch den Betroffenen anzuzeigen. Die Meldung bei uns sollte unter Verwendung des Online-Formulars unter https://datenschutz-hamburg.de/meldung-databreach erfolgen, kann aber auch auf jedem sonstigen Weg in Textform eingereicht werden.

1. Meldepflichtiger Data Breach

Art. 33 DSGVO statuiert eine Meldepflicht bei der jeweils zuständigen 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 mehr – wie unter der vorherigen Rechtslage – darauf an, ob Daten von besonderen Kategorien betroffen sind. Jede Art personenbezogener Daten ist umfasst.

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

[1] *Martini*, in: Paal/Pauly, DSGVO, Art. 33 Rn. 16.
[2] *Hladjik*, in: Ehmann/Selmayr, DSGVO, Art. 33 Rn. 5.

verlorengegangene USB-Sticks oder Laptops, unrechtmäßige Übermittlung sowie der Einbruch in Serverräume, die mit dem Verlust oder der Zerstörung von Hardware oder dem Auslesen von Datenträgern einhergehen.[3]

Die „Verletzung der Sicherheit“ im Sinne des Art. 4 Nr. 12 DSGVO bedeutet nach überwiegender Literaturauffassung nicht die Unzulässigkeit der Datenverarbeitung, sondern betrifft die Datensicherheit, die nur durch technische und organisatorische Maßnahmen erreicht werden kann.[4] Die Art.-29-Gruppe erkennt an, dass es um „security incidents“ geht[5], 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 das Gremium, dass die Daten Dritten zu Kenntnis gegeben werden. Dies kann auch durch menschliches Versagen geschehen, das eine unzulässige Datenverarbeitung auslöst.[7] Die Auslegung der Art.-29-Gruppe ist für die Datenschutz-Aufsichtsbehörden bindend, da die Working Papers dieses Vorgängergremiums vom Europäischen Datenschutzausschuss in dessen erster Sitzung adaptiert wurden. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit folgt daher der Auffassung, dass auch versehentliche Falschadressierungen einen meldepflichtigen Vorgang darstellen, sofern davon ein Risiko für die Betroffenen ausgeht.

Neu ist die Meldepflicht auch bei vorübergehender Unerreichbarkeit der Daten oder dauerhafter Löschung infolge eines Sicherheitsbruchs. 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, vielmehr sind nur unbeabsichtigte Zugangshindernisse Data Breaches im Sinne des Art. 33 DSGVO.[9]

Der Verletzungserfolg muss eingetreten sein.[10] Der Erfolg ist etwa der – beabsichtigte oder unbeabsichtigte – Zugriff auf die Daten.[11] Nicht erforderlich ist hingegen eine Kenntnisnahme des

---

[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] *Art.-29-Gruppe*, WP 250, S. 7; abrufbar unter https://datenschutz-hamburg.de/assets/pdf/wp250rev01_enpdf.pdf.
[6] *Art.-29-Gruppe*, WP 250, S. 32 f.; ebenso *Sassenberg*, in: Sydow, DSGVO, 2017, Art. 33 Rn. 18.
[7] Vgl. *Art.-29-Gruppe*, WP 250, S. 7.
[8] *Art.-29-Gruppe*, WP 250, S. 7.
[9] *Art.-29-Gruppe*, WP 250, 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.

Inhalts.[12] Fand trotz Bestehens einer Sicherheitslücke kein unberechtigter Zugriff statt, besteht keine Meldepflicht.[13] Für das Vorliegen einer Meldepflicht ist es unerheblich, ob daraufhin auch ein (Vermögens- oder immaterieller) Schaden eingetreten ist.[14] Das kann aber bei der Frage des Risikos Berücksichtigung finden.

b) Risiko

Das Risiko bemisst sich aus der Korrelation zwischen Schwere des Schadens und dessen Eintrittswahrscheinlichkeit.[15] Je höher der anzunehmende Schaden ist, desto geringer sind die Anforderungen an die Wahrscheinlichkeit seines Eintritts.[16] Die Art.-29-Gruppe 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

2. Information der Betroffenen

Zusätzlich zur Meldung bei der Aufsichtsbehörde 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

[11] *Reif*, in: Gola, DSGVO, Art. 33 Rn. 21.
[12] *Sassenberg*, in: Sydow, DSGVO, 2017, Art. 33 Rn. 7.
[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] *Art.-29-Gruppe*, WP 250, S. 24 f.

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.[18] Darüber hinaus sind die Ausnahmen von der Informationspflicht gem. Art. 34 Abs. 3 DSGVO zu beachten.

3. Beispiele

Das WP 250 der Art.-29-Gruppe enthält in Anhang B einige Beispiele, die nachfolgend zusammengefasst wiedergegeben werden.

Fallbeschreibung	Meldepflicht an die Aufsichtsbehörde	Informationspflicht an Betroffene	Anmerkungen
Gestohlener USB-Stick mit wirksam verschlüsselten Daten	Nein	Nein	Kein Art.-33-Fall aufgrund der Verschlüsselung. Meldepflicht besteht jedoch, wenn die Daten nicht anderweitig gesichert sind.
Datenzugriff durch Cyber-Attacke	Ja	Ja (abhängig von der Art der Daten)	
Mehrminütiger Stromausfall, dadurch zwischenzeitlich kein Zugriff möglich	Nein	Nein	Aber interne Dokumentation nach Art. 33 Abs. 5
Ransomware-Attacke, die Kundendaten verschlüsselt (Erpressungstrojaner)	Ja (in der Regel)	Ja (in der Regel)	Außer es gibt ein Backup, sodass die Daten zügig wiederhergestellt werden können.
Kontoauszug an falschen Kunden verschickt	Ja	Im Einzelfall i.d.R. nicht, bei Häufung schon	

[18] Vgl. *Art.-29-Gruppe*, WP 250, S. 9.

Hacker erbeuten Nutzernamen, Passwörter und Kaufhistorie der Kunden eines Onlineshops	Ja	Ja	
Kunden können aufgrund eines Programmierfehlers im Kundenportal fremde Kundendaten einsehen	Ja, wenn Daten abgerufen wurden	Kommt darauf an	
Cyber-Attacke auf Krankenhaus, dadurch für 30 Minuten kein Zugriff auf Patientendaten	Ja	Ja	
Versehentliche Versendung von Schülerdaten an eine Mailingliste	Ja	Ja (in der Regel)	
Werbe-E-Mail mit offenem Mailverteiler (cc statt bcc)	Ja (bei großer Empfängerzahl oder sensiblem Inhalt, z.B. Passwörter)	Ja (außer nur wenige Betroffene und kein sensibler Inhalt)	

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 durch die verantwortliche Stelle. Dabei genügt es grundsätzlich, dass jemand im Unternehmen oder der Behörde Kenntnis erlangt. Wenn die Meldung nach „allgemeinem Ermessen“ früher möglich ist, hat sie früher zu erfolgen (EG 86). Wird die 72-Stunden-Frist nicht gehalten, hat der Verantwortliche dies zu begründen (Art. 33 Abs. 1 Satz 2 DSGVO). Dabei müssen außergewöhnliche Umstände dargelegt werden.[19] Ein akzeptabler Grund liegt z.B. vor, wenn viele Hacker-Attacken in kurzem Zeitraum auftreten.[20]

[19] Vgl. *Art.-29-Gruppe*, WP 250, S. 16.
[20] *Art.-29-Gruppe*, WP 250, S. 16.

Kenntnis ist dann erlangt, wenn der Verantwortliche mit einen angemessenen Grad an Sicherheit davon auszugehen hat, dass ein Data Breach vorliegt.[21] Die Meldepflicht tritt demnach noch nicht ein, wenn zunächst nur vage Hinweise vorliegen. Dann hat die Stelle so schnell wie möglich weitere Ermittlungen anzustellen. Während der Ermittlungsphase liegt noch kein angemessener Grad an Sicherheit an Kenntnis über das Vorliegen eines Data Breach vor.[22] Der Verantwortliche muss die Meldung vornehmen, sobald sich in den Ermittlungen ein angemessener Grad an Sicherheit herauskristallisiert[23], also gegebenenfalls schon bevor der Sachverhalt vollständig ausermittelt ist. Ein angemessener Grad an Sicherheit liegt z.B. vor, wenn ein USB-Stick mit unverschlüsseltem Inhalt verloren gegangen ist, obwohl nicht nachvollzogen werden kann, ob Dritte die Daten ausgelesen haben.[24] Wenn der Verantwortliche einen Hinweis inklusive eines Beweises erhält, hat er ebenfalls Kenntnis[25], nicht jedoch, wenn der Hinweis zu unsubstantiiert ist und weitere Ermittlungen notwendig sind. Leitet beispielsweise ein Betroffener eine Phishing-Mail an den Verantwortlichen weiter, die Kundendaten des Verantwortlichen enthält, so hat der Verantwortliche nicht in jedem Fall sofort eine Meldung abzusetzen. Zunächst hat er sein System auf unautorisierte Zugriffe zu überprüfen und hat erst dann Kenntnis, wenn er solche Zugriffe entdeckt.[26] 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 dies kein Hinderungsgrund für eine rechtzeitige Meldung.[27] Dann hat die Meldung schrittweise zu erfolgen (Art. 33 Abs. 4 DSGVO), sodass die fehlenden Informationen später nachgereicht werden.

[21] *Art.-29-Gruppe*, WP 250, S. 11.
[22] *Art.-29-Gruppe*, WP 250, S. 11.
[23] *Art.-29-Gruppe*, WP 250, S. 11.
[24] *Art.-29-Gruppe*, WP 250, S. 11.
[25] *Art.-29-Gruppe*, WP 250, S. 11.
[26] Vgl. *Art.-29-Gruppe*, WP 250, 11.
[27] *Art.-29-Gruppe*, WP 29, S. 14.