AGAD

Partner im Wettbewerb.

DATENSCHUTZ ZUM FEIERABEND

Meldung von Datenpannen nach Art. 33 DSGVO

Christopher Pröpper

04.11.2021

AGAD
Partner im Wettbewerb.

Überblick

1. Grundsätzliches zur Meldung von Datenpannen gem. Art. 33 DSGVO
2. Was sind personenbezogene Daten?
3. Prüfung des Sachverhalts aufgrund der erlangten Informationen
4. Liegt eine meldepflichtige Datenpanne vor? (Risikostufen)
5. Meldeverpflichtung bei der Behörde/ kein meldepflichtiger Vorfall
6. Dokumentation des Vorfalls
7. Beispiele für meldepflichtige Datenpannen/ Bußgelder

1. Grundsätzliches zur Meldung von Datenpannen gem. Art. 33 I DSGVO

„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 gem. Art. 55 DSGVO 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.“

AGAD
Partner im Wettbewerb.

Inhalt und Umfang der Informationspflicht gem. Art. 33 III DSGVO

- Beschreibung der Art der Verletzung personenbezogener Daten.
  (Datenkategorien, Anzahl der betroffenen Personen, Anzahl der betroffenen Datensätze)
- Namen und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle
- Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten (pbD)
- Beschreibung der vom Verantwortlichen unternommen Maßnahmen zur Behebung der Verletzung oder Abmilderung der Verletzung pbD

→ Die geforderten Informationen ergeben sich idR direkt aus den Meldeformularen der jeweiligen Aufsichtsbehörden.

→ Die Formulare zur Meldung von Datenpannen sind über die Homepages der Aufsichtsbehörden abrufbar (NRW: https://ldi-fms.nrw.de/lip/form/display.do?%24context=BEB597D8DF64EA1F9E44)

2. Personenbezogene Daten mit Blick auf Art. 33 DSGVO

Was sind personenbezogene Daten?

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO).

- zwischen Information und Person muss eine Verbindung herstellbar sein, unmittelbar oder mittelbar.
- unmittelbare Verbindung liegt beispielsweise mit Namen, Anschrift oder Geburtsdatum vor.
- mittelbare Verbindung entsteht mittels Zusatzwissens, beispielsweise bei Telefon-, Matrikel- und Sozialversicherungsnummern. Ausreichend, wenn die Information die Identifizierung der betroffenen Person theoretisch ermöglicht. Kommt also nicht darauf an, ob Person tatsächlich identifiziert wird.

Was muss bei personenbezogenen Daten gemäß Art. 33 DSGVO beachtet werden?

- Informationen müssen sich auf einen lebenden Menschen beziehen. Einzelangaben über juristische Personen, wie Kapitalgesellschaften oder eingetragene Vereine, sind keine personenbezogenen Daten, außer wenn sich die Angaben auch auf die hinter der juristischen Person stehenden Personen beziehen, das heißt auf sie „durchschlagen“. Dies kann beispielsweise bei der GmbH einer Einzelperson oder bei einer Einzelfirma der Fall sein, wenn enge finanzielle, persönliche oder wirtschaftliche Verflechtungen zwischen der natürlichen und der juristischen Person bestehen.

- Besondere Kategorien personenbezogener Daten werden nach Art. 9 DSGVO besonders geschützt. Das sind zum Beispiel Gesundheitsdaten, Daten über die ethnische Herkunft sowie religiöse oder weltanschauliche Überzeugungen.

- Vor Inkrafttreten der DSGVO war Informationspflicht auf „besonders sensible personenbezogene Daten, die Dritten unrechtmäßig zur Kenntnis gelangen, und schwerwiegende Beeinträchtigungen für die Rechte darstellen oder schutzwürdige Interessen der Betroffenen bedrohen“ beschränkt.

Liegt eine meldepflichtige Datenpanne vor? (Risikostufen)

Die DSGVO senkt die Schwellen, ab wann eine Meldepflicht an die zuständige Aufsicht besteht, ab.
Früher bestand Meldepflicht nur bei der Verletzung besonders sensibler Daten (siehe oben).

Dagegen müssen die Meldungen an die betroffenen Personen eher seltener als bisher erfolgen.

So gilt:

§ **Grundsätzlich** hat eine Meldung an die Aufsichtsbehörde bei einer Verletzung pbD immer zu erfolgen.

§ **Ausnahme:** die Datenpanne führt *„voraussichtlich nicht zu einem Risiko“* für den Betroffenen.

§ **Aber:** Betroffene Person/en muss/müssen darüber hinaus gem. Art. 34 DSGVO benachrichtigt werden, wenn ein *hohes Risiko* für ihre Rechte und Freiheiten besteht

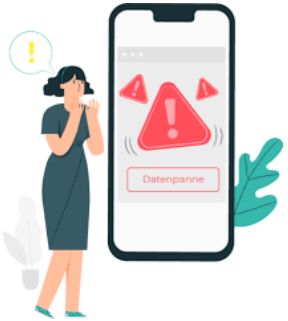
3. Prüfung des Sachverhalts aufgrund der erlangten Informationen

Hinweis auf Datenpanne: kann auf unterschiedlichsten Wegen an den Verantwortlichen (Unternehmen) herangetragen werden. Z.B. durch Mitarbeiter, durch Dritte (außerhalb des Unternehmens), durch öffentliche Quellen (Medien), Alarmierung durch unternehmensinternes Datenschutzmanagement.

Weitergabe und Überprüfung innerhalb des Unternehmens: Hinweise sollten schnellstmöglich den Verantwortlichen übermittelt werden. (Einrichtung einer Taskforce aus GF, IT- Verantwortlichen und (externen) Datenschutzbeauftragten.

Prüfung der Hinweise: Was ist passiert? In welchem Ausmaß sind Daten abhandengekommen? Ist das unternehmen überhaupt betroffen (bei größeren Datenpannen, wie z.B. Angriff auf Exchange-Server)? Kann der Verlust auf einen bestimmten Bereich eingegrenzt werden? Nachdem der Sachverhalt aufgearbeitet wurde muss die Entscheidung fallen:

Liegt eine meldepflichtige Datenpanne vor? (Risikostufen)



- Quelle LDI NRW -

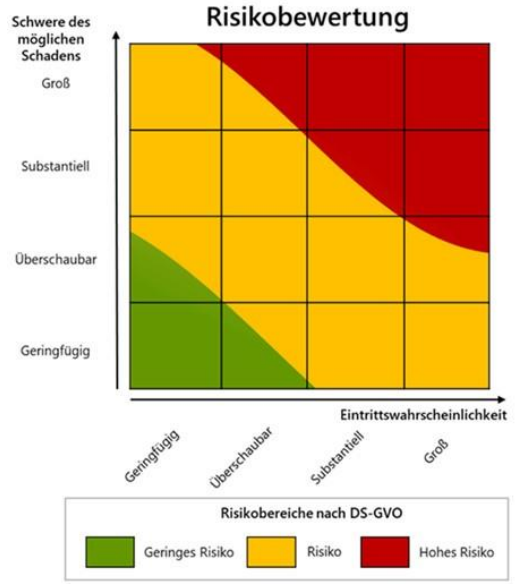
Risiko\Pflichten	Interne Dokumentationspflicht (Art. 33 Abs. 5 DSGVO)	Meldepflicht an zuständige Aufsichtsbehörde (Art. 33 Abs. 1 DSGVO)	Benachrichtigungspflicht gegenüber den betroffenen Personen (Art. 34 DSGVO)
Voraussichtlich kein bzw. nur geringes Risiko	ja	nein	nein
Risiko	ja	ja	nein
Hohes Risiko	ja	ja	Ja

Beurteilung der Risikostufen

Problem: welches Risiko besteht nach der Sachverhaltsanalyse und resultiert daraus eine Meldepflicht?

Keine pauschale Aussage darüber möglich, was erfüllt sein muss, damit eine bestimmte Risikostufe erfüllt ist oder auch nicht.

Eine Beurteilungsmöglichkeit zur Einordnung einer möglichen Verletzung ist die Erstellung einer Risikomatrix wobei es um ein Zusammenspiel zwischen Eintrittswahrscheinlichkeit und der möglichen Schwere des Schadens geht.



Zur Einordnung des Risikos in die vorgenannten Fallgruppen können folgende Überlegungen beispielhaft herangezogen werden:

Mögliche Schadensszenarien: Erwägungsgrund 85 enthält zahlreiche Beispiele für mögliche Schäden bei Datenschutzvorfällen z.B.: Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste oder Rufschädigung. Sind bei Datenpannen beispielsweise Datensätze mit vollständigem Namen und Privatadressen abhandengekommen, kommt ein Identitätsdiebstahl in Betracht.

Bei Beurteilung der Eintrittswahrscheinlichkeit sind zahlreiche Faktoren zu berücksichtigen. Werden z.B. Daten nur gegenüber einem sehr kleinen Personenkreis offenbart, kann dies bei bestimmten Schäden für eine geringere Eintrittswahrscheinlichkeit sprechen.

Hinsichtlich der Bestimmung der Schwere des Schadens gilt, je sensibler die Daten, desto höher ist die Schadenswahrscheinlichkeit. Dazu gehören die in Art. 9 DSGVO genannten Daten (Gesundheitsdaten).

4. Meldeverpflichtung bei der Behörde

Ausgangslage: es besteht ein Risiko oder ein hohes Risiko für die Verletzung personenbezogener Daten

1. Dokumentation aller durchgeführten Maßnahmen und weiterer Vorgehensweise gem. Art. 33 V DSGVO durch den Verantwortlichen (Unternehmen).

2. Erfüllung der Meldepflicht gem. Art. 33 I DSGVO durch den Verantwortlichen (für z.B. NRW ist hierfür ein entsprechendes Formular auf der Seite des LDI hinterlegt, das nach Ausfüllung direkt abgesendet werden kann).
   ACHTUNG! Falls das Risiko als gering eingestuft wird, ist ein Absenden des Formulars gar nicht erst möglich.

3. Die Meldung muss unmittelbar nach Bekanntwerden der Panne erfolgen, spätestens innerhalb von 72 Std.
   (*Fristberechnung richtet sich aber nicht nach BGB, sondern nach der europäischen Fristen-VO. Art. 3 Fristen-VO).*
   Bsp: Fristbeginn 22.12.2020 13.00 (Vorfall wurde um 12.17 bekannt- die Frist beginnt aber zu jeder vollen Stunde-).
   Fristende 25.12.2020 13.00.
   ACHTUNG ! Eine eventuelle Verzögerung der Meldung ist der Behörde zu erläutern.

4. Mindestangaben zur Meldeverpflichtung ergeben sich aus Art. 33 DSGVO (siehe oben)

AGAD
Partner im Wettbewerb.

5. Meldeverpflichtung bei der Behörde

5. Sofern ein hohes Risiko für die Verletzung personenbezogener Daten besteht, muss die betroffene/n Person/en zusätzlich gem. Art. 34 I DSGVO informiert werden, wobei dies in einfacher, verständlicher Art und Weise zu erfolgen hat. Der Inhalt der zu erteilenden Informationen ergibt sich aus Art. 33 III DSGVO.

6. *Die Benachrichtigung der Betroffenen gem. Art. 34 DSGVO trotz des hohen Risikos kann allerdings Ausnahmsweise unterbleiben, wenn:*
   - Entsprechende technische und organisatorische Maßnahmen (TOM) getroffen worden sind, die einen Zugang Dritter zu den Daten trotz Abhandenkommens unmöglich machen.
   - Der Verantwortliche sichergestellt hat, dass durch nachfolgende Maßnahmen ein Risiko für die Rechte und Freiheiten Dritter nicht mehr besteht.
   - Die Meldeverpflichtung mit unverhältnismäßigem Aufwand verbunden wäre. Stattdessen kann eine öffentliche Bekanntmachung o.ä. erfolgen.

7. Wichtig: Sofern ein Risiko oder hohes Risiko besteht, sollte die Meldung auf jeden Fall innerhalb der 72 Std. erfolgen, auch wenn der Sachverhalt noch nicht vollständig aufgeklärt ist. Eine „Nachmeldung“ ist ausdrücklich vorgesehen und gefordert!

AGAD
Partner im Wettbewerb.

5. Kein meldepflichtiger Vorfall wenn:

(voraussichtlich kein/geringes Risiko des Verlustes pbD)

Sofern der Verantwortliche im Rahmen der Sachverhaltsaufarbeitung zu dem Ergebnis kommt, dass durch den Vorfall kein oder nur ein geringes Risiko hinsichtlich der Verletzung personenbezogener Daten besteht, muss gem. Art. 33 DSGVO keine Meldung an die Datenaufsicht erfolgen.

Aber: Eine ausführliche Dokumentation wie bei den beiden anderen Risikostufen ist dennoch erforderlich.

6. Dokumentation des Vorfalls

- Unabhängig davon zu welcher Einschätzung man hinsichtlich der gezeigten Risikostufen kommt und welche konkreten Verpflichtungen daraus resultieren, muss eine ausführliche Dokumentation des gesamten Vorfalls erfolgen.
  Hierbei sind alle unternommenen Maßnahmen zu berücksichtigen (forensische Untersuchungen, Ergebnisse der IT-Abteilung/ Dienstleister), um auf Nachfragen der Behörde reagieren zu können.
- Auch im Hinblick auf nachträgliche Erkenntnisse sollte eine lückenlose Dokumentation erfolgen.
- Darüber hinaus sollten stets alle Beteiligten über den aktuellen Sachstand informiert sein. Daher ist eine enge Zusammenarbeit mit dem internen/ externen Datenschutzbeauftragten unerlässlich, damit dieser den Verantwortliche auch im Rahmen einer ggfs. erforderlichen Meldung unterstützen kann.

Beachte:
Nach Eingang der Meldung wendet sich die Behörde idR an den Verantwortlichen oder Datenschutzbeauftragten hinsichtlich etwaiger Rückfragen oder stellt die Sache letztlich, sofern den Verantwortlichen kein Verschulden hinsichtlich des Abhandenkommens personenbezogener Daten trifft, ein.

7. Beispiele für meldepflichtige Datenpannen

- Exchange Angriff März 2021 (Rundschreiben)
- Randsomewareangriff auf Klinikum in Nordrhein- Westfalen September 2020
- Angriff auf große Mediengruppe Dezember 2020

AGAD
Partner im Wettbewerb.

Herzlichen Dank für Ihre Aufmerksamkeit!

AGAD Service GmbH
Christopher Pröpper
Waldring 43-47
44789 Bochum
proepper@agad.de
Tel.: 0234/282533 20

AGAD
Partner im Wettbewerb.