Meldung von Datenschutzverletzungen: Wann und zu welchem Zweck?

Marit Hansen
Landesbeauftragte für Datenschutz
Schleswig-Holstein

Zürich, 15.05.2019

Überblick

Bild: stux via Pixabay

- „Datenpanne“ – was ist das?
- Meldepflicht – alles neu?
- Anforderungen an das Melden (Art. 33 DSGVO)
- Anforderungen an das Benachrichtigen (Art. 34 DSGVO)
- Erfahrungen als Aufsichtsbehörde
- Fazit

„Datenpanne“ – Verletzung des Schutzes personenbezogener Daten

- Englisch: „personal data breach“

„Verletzung der Datensicherheit“

- Definition in Art. 4 Nr. 12 DSGVO:
  Im Sinne dieser Verordnung bezeichnet der Ausdruck: [...]

  12. „Verletzung des Schutzes personenbezogener Daten“
  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, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

- Nicht im Einklang mit geplanter Datenverarbeitung
- Ausgelöst durch einen Vorfall („incident“)

Was ist davon umfasst?

- Vernichtung: Verletzung der Verfügbarkeit
- Verlust: Verletzung der Verfügbarkeit und der Vertraulichkeit
- Veränderung: Verletzung der Integrität (und ggf. Verfügbarkeit)
- Offenlegung: Verletzung der Vertraulichkeit
- Zugang: Verletzung der Vertraulichkeit (und ggf. Integrität)

Folgen der Verletzung des Schutzes personenbezogener Daten (Art. 33 Abs. 3 Buchst. c DSGVO)

Verletzung der Vertraulichkeit

[ ] Weitergabe der Daten an unberechtigte Dritte
[ ] Verknüpfung der Daten mit anderen Daten
[ ] Nutzung für unzulässige Zwecke
[ ] Unbefugte Einsichtnahme
[ ] Andere Verletzung der Vertraulichkeit

Verletzung der Integrität

[ ] Nicht mehr aktuelle Daten wurden genutzt
[ ] Daten wurden verfälscht
[ ] Herkunft der Daten nicht bekannt / feststellbar
[ ] Andere Verletzung der Integrität

Verletzung der Verfügbarkeit

[ ] Wichtige Daten sind dauerhaft nicht mehr verfügbar
[ ] Wichtige Daten waren zeitweise nicht ausreichend verfügbar
[ ] Andere Verletzung der Verfügbarkeit

Beschreibung der wahrscheinlichen Folgen

Geben Sie hier bitte Ihre eigene Einschätzung der Auswirkungen des Vorfalls auf die betroffenen Personen an.

Überblick

Bild: kalhh via Pixabay

- „Datenpanne“ – was ist das?
- Meldepflicht – alles neu?
- Anforderungen an das Melden (Art. 33 DSGVO)
- Anforderungen an das Benachrichtigen (Art. 34 DSGVO)
- Erfahrungen als Aufsichtsbehörde
- Fazit

Nicht alles ganz neu

Informationspflichten bei unrechtmässiger Kenntniserlangung von Daten:

- § 42a BDSG:
  - Besondere Arten pb Daten
  - Pb Daten über Straftaten + Ordnungswidrigkeiten
  - Pb Daten zu Bank- oder Kreditkartenkonten
- § 15a TMG
- § 109a TKG
- Teilweise LDSGe

Unterschied DSGVO: alle Arten von pb Daten

Ziele

Geeignete Risikovorsorge

Bild: Peggy und Marco Lachmann-Anke via Pixabay

Alarmierung (Detection)

Bild: 200 Degrees via Pixabay

Schadensbegrenzung

Bild: Myriams-Fotos via Pixabay

in gebotener Geschwindigkeit

Bild: annca via Pixabay

Überblick

Bild: Antranias via Pixabay

- „Datenpanne“ – was ist das?
- Meldepflicht – alles neu?
- Anforderungen an das Melden (Art. 33 DSGVO)
- Anforderungen an das Benachrichtigen (Art. 34 DSGVO)
- Erfahrungen als Aufsichtsbehörde
- Fazit

Meldung an die Aufsichtsbehörde (Art. 33 DSGVO)

- Wer meldet?
  - Der Verantwortliche an die Aufsichtsbehörde (Art. 33 Abs. 1 DSGVO)
  - Der Auftragsverarbeiter an den Verantwortlichen (Art. 33 Abs. 2 DSGVO)

- Wann?
  - Im Falle einer Verletzung des Schutzes pb Daten
  - Unverzüglich!
  - Und möglichst binnen 72 Stunden nach Bekanntwerden (sonst Verzögerung begründen!)

- Wann nicht (Ausnahme)?
  - Wenn die Verletzung des Schutzes pb Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt

Risiko – was ist das?

- Risiko für die Rechte und Freiheiten natürlicher Personen
- D.h. mehr als „nur“ Datensicherheit
- Definiert durch die Eintrittswahrscheinlichkeit und die Schwere eines möglichen Schadens (siehe EG 75)
- In Bezug auf Art, Umfang, Umstände und Zwecke der Verarbeitung; objektive Bewertung gefordert (siehe EG 76)
- Physischer, materieller oder immaterieller Schaden (siehe EG 75+85)

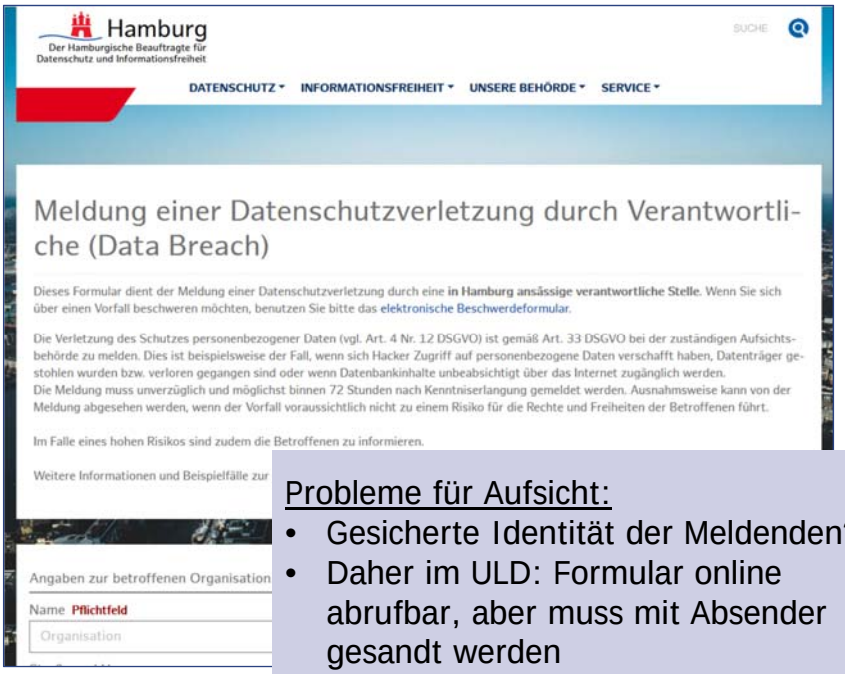
Bild: geralt via Pixabay

Beispiele aus EG 85:
- Diskriminierung
- Identitätsdiebstahl oder -betrug
- Finanzielle Verluste
- Unbefugte Aufhebung der Pseudonymität
- Rufschädigung
- Erhebliche wirtschaftliche oder gesellschaftliche Nachteile

Meldung an die Aufsichtsbehörde (Art. 33 DSGVO)

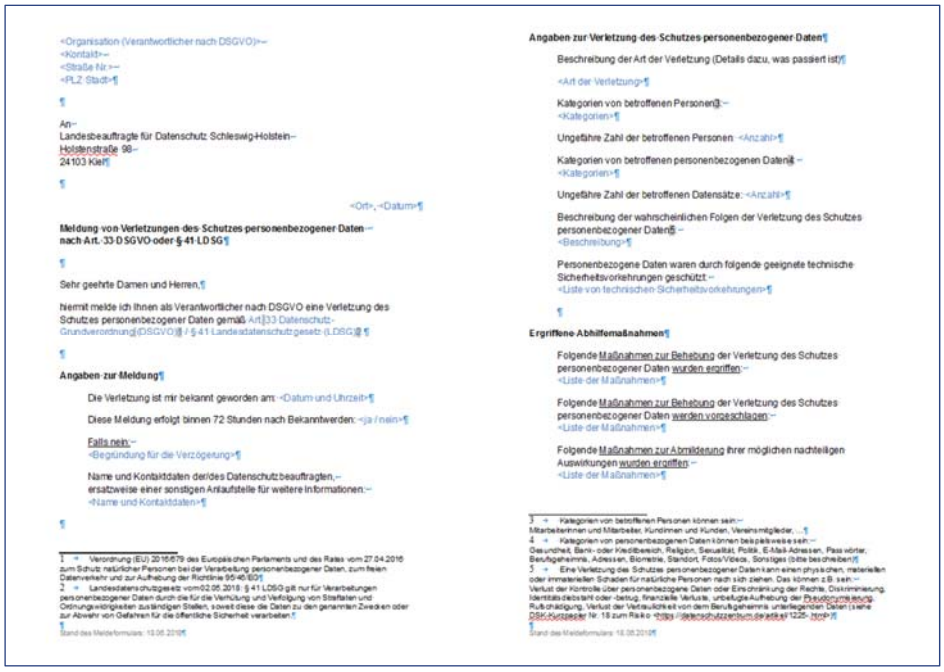
- Mindestinhalt der Meldung (Art. 33 Abs. 3 DSGVO)
  a) Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, Kategorien + ungefähre Zahl der betroffenen Personen bzw. personenbezogenen Datensätze;
  b) Namen + Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle;
  c) Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
  d) Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Massnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Massnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
- Ggf. schrittweise ergänzen (Art. 33 Abs. 4 DSGVO)

Meldung an die Aufsichtsbehörde – bspw. per Formular



Probleme für Aufsicht:
- Gesicherte Identität der Meldenden?
- Daher im ULD: Formular online abrufbar, aber muss mit Absender gesandt werden

Meldung an die Aufsichtsbehörde – bspw. per Standardschreiben



<Organisation (Verantwortlicher nach DSGVO)>
<Kontakt>
<Straße Nr.>
<PLZ Stadt>

An
Landesbeauftragte für Datenschutz Schleswig-Holstein
Holstenstraße 98
24103 Kiel

<Ort>, <Datum>

Meldung von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DSGVO oder § 41 LDSG

Sehr geehrte Damen und Herren,

hiermit melde ich Ihnen als Verantwortlicher nach DSGVO eine Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 Datenschutz-Grundverordnung (DSGVO) / § 41 Landesdatenschutzgesetz (LDSG):

Angaben zur Meldung

Die Verletzung ist mir bekannt geworden am: <Datum und Uhrzeit>

Diese Meldung erfolgt binnen 72 Stunden nach Bekanntwerden: <ja / nein>

Falls nein:
<Begründung für die Verzögerung>

Name und Kontaktdaten des/des Datenschutzbeauftragten,
ersatzweise einer sonstigen Anlaufstelle für weitere Informationen:
<Name und Kontaktdaten>

1 → Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG
2 → Landesdatenschutzgesetz vom 02.05.2018 - § 41 LDSG gilt nur für Verarbeitungen personenbezogener Daten durch die für die Verhütung und Verfolgung von Straftaten und Ordnungswidrigkeiten zuständigen Stellen, soweit diese die Daten zu den genannten Zwecken oder zur Abwehr von Gefahren für die öffentliche Sicherheit verarbeiten.

Stand des Meldeformulars: 10.06.2019

Angaben zur Verletzung des Schutzes personenbezogener Daten

Beschreibung der Art der Verletzung (Details dazu, was passiert ist):

<Art der Verletzung>

Kategorien von betroffenen Personen[3]:
<Kategorien>

Ungefähre Zahl der betroffenen Personen: <Anzahl>

Kategorien von betroffenen personenbezogenen Daten[4]:
<Kategorien>

Ungefähre Zahl der betroffenen Datensätze: <Anzahl>

Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten[5]:
<Beschreibung>

Personenbezogene Daten waren durch folgende geeignete technische Sicherheitsvorkehrungen geschützt:
<Liste von technischen Sicherheitsvorkehrungen>

Ergriffene Abhilfemaßnahmen

Folgende Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten wurden ergriffen:
<Liste der Maßnahmen>

Folgende Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten werden vorgeschlagen:
<Liste der Maßnahmen>

Folgende Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen wurden ergriffen:
<Liste der Maßnahmen>

3 → Kategorien von betroffenen Personen können sein: Mitarbeiterinnen und Mitarbeiter, Kundinnen und Kunden, Vereinsmitglieder, ...
4 → Kategorien von personenbezogenen Daten können beispielsweise sein: Gesundheit, Bank- oder Kreditbereich, Religion, Sexualität, Politik, E-Mail-Adressen, Passwörter, Berufsgeheimnis, Adressen, Biometrie, Standort, Fotos/Videos, Sonstiges (bitte beschreiben)
5 → Eine Verletzung des Schutzes personenbezogener Daten kann einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen. Das können z.B. sein: Verlust der Kontrolle über personenbezogene Daten oder Einschränkung der Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten (siehe DSK-Kurzpapier Nr. 18 zum Risiko <https://datenschutzzentrum.de/artikel/1225-.html>)

Stand des Meldeformulars: 10.06.2019

https://www.datenschutzzentrum.de/uploads/formular/Meldung-Datenpanne.odt

Meldung an die Aufsichtsbehörde – wichtig für Verantwortlichen: alles dokumentieren

- Wer?
  - Der Verantwortliche (Art. 33 Abs. 5 DSGVO)
  - Ggf. Informationen vom Auftragsverarbeiter einholen
- Was?
  - Verletzungen des Schutzes pb Daten,
  - d.h.: Fakten über Vorfall, Auswirkungen und ergriffene Abhilfemassnahmen
- Für welche Zwecke?
  - Zum Aufarbeiten und Vermeidung desselben Problems
  - Nachweis des korrekten Handelns (auch Art. 82 Haftung und Recht auf Schadenersatz)
  - Überprüfbarkeit durch Aufsichtsbehörde

u.a.:
- Zeitpunkte des Bekanntwerdens, der Meldung (Zugangsnachweis!) und ggf. der Benachrichtigung;
- Risiko-Bewertung

Überblick

Bild: cocoparisienne via Pixabay

- „Datenpanne“ – was ist das?
- Meldepflicht – alles neu?
- Anforderungen an das Melden (Art. 33 DSGVO)
- Anforderungen an das Benachrichtigen (Art. 34 DSGVO)
- Erfahrungen als Aufsichtsbehörde
- Fazit

Benachrichtigung der betroffenen Personen (Art. 34 DSGVO)

- Wann?
  - Bei voraussichtlich hohem Risiko
  - Unverzüglich
- Wie?
  - Beschreibung
  - In klarer und einfacher Sprache (s.a. Art. 12 Abs. 1 DSGVO)
  - Unentgeltlich (Art. 12 Abs. 5 DSGVO)
  - Wie in Art. 33 Abs. 3 Buchst. b, c + d, damit die betroffenen Personen nachfragen und selbst risikominimierende Massnahmen treffen können
- Korrespondiert mit Datenschutz-Grundsatz Transparenz (Art. 5 Abs. 1 Buchst. a DSGVO)

Benachrichtigung der betroffenen Personen (Art. 34 DSGVO)

- Wann keine Benachrichtigung (Ausnahmen)?
  a) Wenn geeignete TOMs zum Unzugänglichmachen (Verschlüsselung) oder

Wirksame Verschlüsselung nach Stand der Technik

  b) wegen nachfolgender Massnahmen das hohe Risiko aller Wahrscheinlichkeit nicht mehr besteht oder

Verantwortlicher muss dies korrekt einschätzen

  c) unverhältnismässiger Aufwand für Benachrichtigung – dann aber öffentliche Bekanntmachung o.ä.!

Bild: geralt via Pixabay

Benachrichtigung ja (wie?) oder nein? – wichtig für Verantwortlichen: alles dokumentieren

- Wie schon vorne:

- Aufsichtsbehörde kann Nachholen der Benachrichtigung verlangen (Art. 34 Abs. 4 DSGVO)

Blick ins BDSG-neu: „nemo tenetur“-Grundsatz

Art. 42 Abs. 4 BDSG-neu (Strafvorschriften):

(4) Eine Meldung nach Artikel 33 der [DSGVO] oder eine Benachrichtigung nach Artikel 34 Absatz 1 der [DSGVO] darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Abs. 1 der StPO bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

Im Zweifel also melden + benachrichtigen!

Probleme für Aufsicht:
- Over-Reporting?!
- Sanktionen?
- Aufbewahrungsfristen?

Bild: 1820796 via Pixabay

Geldbussen nach Art. 83 DSGVO

Art. 33+34 in Abs. 4 (kl. Bussgeld), Art. 5 Abs. 1 Buchst. f in Abs. 5 (gr. Bussgeld)

- Wirksame, verhältnismässige + abschreckende Geldbussen (Art. 83 Abs. 1 DSGVO)
- Berücksichtigung der Umstände des Einzelfalls (Art. 83 Abs. 2 DSGVO)
  - Art, Schwer, Dauer des Verstosses
  - Zahl der betroffenen Personen, Ausmass des Schadens
  - Verschulden: Vorsätzlichkeit / Fahrlässigkeit
  - Getroffene Massnahmen zur Minderung des Schadens
  - Grad der Verantwortung (inkl. TOM Art. 25+32 DSGVO)
  - Frühere Verstösse
  - Kooperation mit der Aufsichtsbehörde
  - Kategorien der pb Daten
  - Art des Bekanntwerdens / Mitteilung
  - Einhaltung von anordnenden Massnahmen
  - Einhaltung genehmigter Verhaltensregeln
  - Mildernde Umstände (inkl. wirtschaftliche Verhältnisse, EG 148)

Art. 83 Abs. 2 Buchst. h:
„Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;“

Beispiele der Art. 29-Datenschutzgruppe

WP250rev.01

Fall (immer pbD)	Melden	Benachr.	Bemerkung
USB-Stick verloren mit verschlüsseltem Backup	Nein	Nein	Solange die Verschlüsselung funktioniert
Hacker-Angriff auf Server mit Datenabfluss	Ja	Bei Risiko*)	*) „severity of likely consequences“: high
Wg. Stromausfalls kurz kein Zugriff auf pbD	Nein	Nein	Aber dokumentieren nach Art. 33 Abs. 5
Ransomware ohne Backup	Ja	Ja	Mit Backup ggf. „nein“
Einzelfehlzustellung	Ja	Bei Risiko	Wirklich Einzelfall?
Patientenakten im Krankenhaus für 30 h nicht verfügbar	Ja	Ja	
Studentendaten an falschen Mailverteiler gesandt	Ja	Bei Risiko	
E-Mails an TO statt BCC	Ja*)	Ja*)	*) Ggf. nicht, wenn keine sensiblen Daten und geringe Zahl

Überblick

Bild: silviarita Pixabay

- „Datenpanne“ – was ist das?
- Meldepflicht – alles neu?
- Anforderungen an das Melden (Art. 33 DSGVO)
- Anforderungen an das Benachrichtigen (Art. 34 DSGVO)
- Erfahrungen als Aufsichtsbehörde
- Fazit

Pflicht oder Kür der Aufsichtsbehörde?

- „Abheften mit Eingangsbestätigung“
- Auf Anfrage Beratung der Verantwortlichen zu Risiko-Bewertung & Massnahmen

zeitkritisch

- Anlassbezogene Prüfung des Vorfalls, speziell zu Risiko-Bewertung & Massnahmen (Benachrichtigung?)

- Vollständige Sachverhaltsermittlung und Bewertung bis zur Sanktion
- Weitergabe von Erkenntnissen an andere Aufsichtsbehörden mit möglicher Betroffenheit (wie detailliert? Betriebsgeheimnisse? Sprachen?)

ULD www.datenschutzzentrum.de

Pflicht oder Kür der Aufsichtsbehörde?

- Beantwortung von Presseanfragen zu den Vorfällen

- Weitergehende Prüfung der Verantwortlichen
  - bei gehäuften Meldungen (berechtigt? unberechtigt?)
  - in Bereichen ganz ohne Meldungen
  - bei Ausbleiben von Meldungen einiger Auftraggeber eines betroffenen Dienstleisters
  - Bei verspäteten Meldungen / Benachrichtigungen
- Zurückweisen von Fehl-Meldungen / Over-Reporting (z.B. aus Übervorsichtigkeit oder als „Leistungsnachweis“ eines betrieblichen Datenschutzbeauftragten)

Bild: gabrielle_cc via Pixabay

Balance zwischen Public Shaming und professionellem Fehlermanagement

Bild: Sabine van Erp via Pixabay

Andere Bilder:
Gerd Altmann via Pixabay

Überblick

Bild: stux via Pixabay

- „Datenpanne“ – was ist das?
- Meldepflicht – alles neu?
- Anforderungen an das Melden (Art. 33 DSGVO)
- Anforderungen an das Benachrichtigen (Art. 34 DSGVO)
- Erfahrungen als Aufsichtsbehörde
- Fazit

Fazit

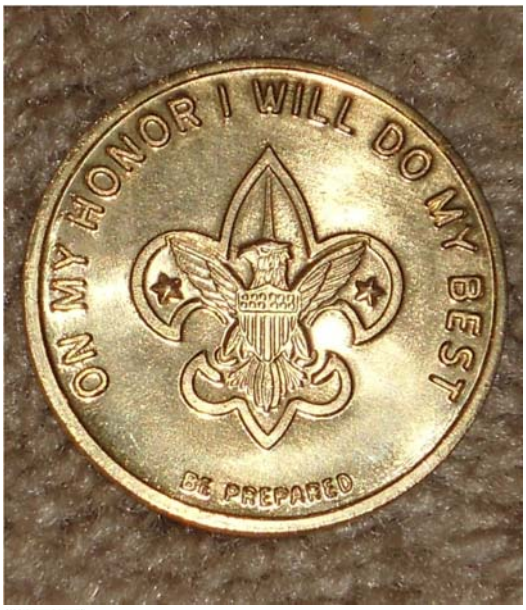


Bild: jclovis3 via Pixabay

- Meldung ist eine Komponente im Instrumentenkoffer der Aufsicht
- Ziel: Vorsorge und Bewusstsein
  - Verschlüsselung und Datentrennung vermindern das Risiko eines unbefugten Zugangs
  - Redundante Datenspeicherung für Verfügbarkeit
  - ISMS
  - Prozesse für den eingetretenen Fall
  - Wichtig: aufmerksame und sensibilisierte Beschäftigte
- Meldung schon bei „Risiko“ sinnvoll, nicht erst bei „hohem Risiko“ (DSFA)

Fazit

Bild: skeeze via Pixabay

Zum (Weiter-)Lesen

- **Art. 33 + 34 DSGVO**
- Zugehörige Erwägungsgründe: EG 85-88, EG 73 sowie EG 75ff.

- Art.-29-Datenschutzgruppe:
  Guidelines on Personal data breach notification under Regulation 2016/679, 18/EN, WP250rev.01,
  Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018 (bestätigt vom Europäischen Datenschutzausschuss),
  https://edpb.europa.eu/our-work-tools/our-documents/guideline/personal-data-breach-notifications_de

- Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Deutschland), DSK: **Kurzpapier „Risiko für die Rechte und Freiheiten natürlicher Personen“,**
  https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf