Verletzungen des Schutzes personenbezogener Daten („Datenpannen“)

Verletzung des Schutzes personenbezogener Daten

Begriffsbestimmung in Art. 4 Ziff. 12 DS-GVO

- 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**

Dokumentationspflicht: Verzeichnis muss geführt werden

Datenpannen müssen systematisch erfasst werden

- Art. 33 Abs. 5 DS-GVO
  Der Verantwortliche **dokumentiert Verletzungen des Schutzes** personenbezogener Daten **einschließlich aller im Zusammenhang** mit der Verletzung des Schutzes personenbezogener Daten **stehenden Fakten**, von deren **Auswirkungen** und der **ergriffenen Abhilfemaßnahmen**.
  Diese Dokumentation muss der **Aufsichtsbehörde** die **Überprüfung** der Einhaltung der **Bestimmungen dieses Artikels** ermöglichen.

→ ***Alle*** Datenpannen müssen dokumentiert werden

→ An Hand dieses Verzeichnisses kann die Aufsichtsbehörde prüfen, ob alle meldepflichtigen Vorfälle gemeldet wurden

Meldepflicht bei Datenpannen: Aufsichtsbehörde

Ggf. müssen Datenpannen der Aufsichtsbehörde gemeldet werden

- Art. 33 Abs. 1 DS-GVO
  „[...] Im Falle einer Verletzung des Schutzes personenbezogener Daten **meldet der Verantwortliche unverzüglich** und [...], nachdem ihm die Verletzung bekannt wurde [...]“

→ Grundsätzlich alle Verletzungen müssen gemeldet werden (Ausnahmen später)

→ Es meldet **nie** der Auftragsverarbeiter, immer nur der Verantwortliche

→ Meldefrist/-Zeit beginnt ab dem Zeitpunkt, wenn dem Verantwortlichen die Verletzung bekannt wurde

→ Cave: Auftragsverarbeiter gelten als „verlängerter“ Arm des Verantwortlicher, d.h. Auftragsverarbeiter hat Kenntnis = Verantwortlicher hat Kenntnis

Meldepflicht bei Datenpannen : Aufsichtsbehörde

Ggf. müssen Datenpannen der Aufsichtsbehörde gemeldet werden

- Art. 33 Abs. 1 DS-GVO
  „[...] es sei denn, dass die Verletzung des Schutzes personenbezogener Daten ***voraussichtlich*** **nicht zu einem Risiko** für die Rechte und Freiheiten natürlicher Personen **führt** [...]“

→ Keine Meldepflicht, wenn Datenpanne *voraussichtlich* kein Risiko beinhaltet

→ Bewertung für Verantwortlichen mitunter schwierig

→ Hinweis: Im Zweifelsfall Meldung
Cave: Verstoß gegen Meldepflicht bußgeldbewehrt
(„kleines“ Bußgeld)

Meldepflicht bei Datenpannen : Aufsichtsbehörde

Ggf. müssen Datenpannen der Aufsichtsbehörde gemeldet werden

- Art. 33 Abs. 1 DS-GVO
  „[...] Im Falle einer Verletzung des Schutzes personenbezogener Daten **meldet der Verantwortliche unverzüglich** und ***möglichst*** **binnen 72 Stunden**, nachdem ihm die Verletzung bekannt wurde [...]. Erfolgt die Meldung an die Aufsichtsbehörde **nicht binnen 72 Stunden**, so ist ihr eine **Begründung für die Verzögerung beizufügen**."

→ Meldefrist/-Zeit beginnt ab dem Zeitpunkt, wenn dem Verantwortlichen die Verletzung bekannt wurde

→ Meldung muss innerhalb von 72 Stunden erfolgen, egal ob Arbeitstag/Wochenende/Feiertag/...

→ Keine Meldung innerhalb von 72 Stunden:
Begründung, warum keine Meldung innerhalb von 72 Stunden erfolgte

Meldepflicht bei Datenpannen : Aufsichtsbehörde

Ggf. müssen Datenpannen der Aufsichtsbehörde gemeldet werden

(Mindest-) Inhalte der Meldung (Art. 33 Abs. 3 DS-GVO)

- Beschreibung der Art der Verletzung
- Angabe von Kategorien und ungefähre Zahl betroffener Personen
- Kategorien und ungefähre Zahl der betroffenen Datensätze
- Namen und Kontaktdaten des Datenschutzbeauftragten oder einer sonstiger Anlaufstelle
- Darstellung der wahrscheinlichen Folgen der Verletzung
- Beschreibung der ergriffene oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung
- Ggf. Maßnahmen zur Abmilderung der nachteiligen Auswirkungen

Meldepflicht bei Datenpannen: Betroffene Person

Ggf. müssen Datenpannen betroffenen Personen gemeldet werden

- Art. 34 Abs. 1 DS-GVO
  „Hat die Verletzung des Schutzes personenbezogener Daten **voraussichtlich** ein **hohes Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so **benachrichtigt** der Verantwortliche die **betroffene Person unverzüglich** von der Verletzung“

→ Voraussichtlich hohes Risiko: hohes Risiko muss nicht sicher (im Sinne von wahrscheinlich sicher, da Risiko = Wahrscheinlichkeit) sein, es reicht wenn es voraussichtlich ein **hohes Risiko darstellen könnte**

→ Unverzüglich = „ohne schuldhaftes Verzögern“

Meldepflicht bei Datenpannen : Betroffene Person

Ggf. müssen Datenpannen betroffenen Personen gemeldet werden

- Art. 34 Abs. 2 DS-GVO
  „Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in **klarer und einfacher Sprache** die **Art der Verletzung** des Schutzes personenbezogener Daten und enthält zumindest“

→ Vorgaben von Art. 12 DS-GVO bzgl. transparente Information gefordert

→ Verletzung und daraus resultierende oder evtl. resultierende Folgen müssen betroffener Person transparent erläutert werden.

Meldepflicht bei Datenpannen : Betroffene Person

Ggf. müssen Datenpannen betroffenen Personen gemeldet werden

(Mindest-) Inhalte der Meldung (Art. 33 Abs. 2 DS-GVO)

- Beschreibung der Art der Verletzung
- Namen und Kontaktdaten des Datenschutzbeauftragten oder einer sonstiger Anlaufstelle
- Darstellung der wahrscheinlichen Folgen der Verletzung
- Beschreibung der ergriffene oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung
- Ggf. Maßnahmen zur Abmilderung der nachteiligen Auswirkungen

Meldepflicht bei Datenpannen : Betroffene Person

Ggf. müssen Datenpannen betroffenen Personen gemeldet werden

- Benachrichtigung ist nicht erforderlich (Art. 34 Abs. 3 DS-GVO)
  - a) der Verantwortliche **geeignete** technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der **Verletzung betroffenen personenbezogenen Daten angewandt wurden**, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;
  - → Wenn kein Zugriff auf Daten möglich, kein Risiko für betroffene Person, keine Meldepflicht
  - → Welche TOM im Sinne dieser Regelung geeignet sind, aber den Zugriff auf Daten nicht verhindern: ???

Meldepflicht bei Datenpannen : Betroffene Person

Ggf. müssen Datenpannen betroffenen Personen gemeldet werden

– Benachrichtigung ist nicht erforderlich (Art. 34 Abs. 3 DS-GVO)

b) der Verantwortliche durch **nachfolgende Maßnahmen sichergestellt hat**, dass das **hohe Risiko** für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 **aller Wahrscheinlichkeit nach nicht mehr besteht**;

→ Beispiel: Remote-Wipe

Meldepflicht bei Datenpannen : Betroffene Person

Ggf. müssen Datenpannen betroffenen Personen gemeldet werden

– Benachrichtigung ist nicht erforderlich (Art. 34 Abs. 3 DS-GVO)

c) dies mit einem **unverhältnismäßigen Aufwand** verbunden wäre. In diesem Fall hat stattdessen **eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme** zu erfolgen, durch die die **betroffenen Personen *vergleichbar* wirksam informiert werden.**

→ Beispiel: Veröffentlichung in regionaler oder überregionaler (je nach Gruppe betroffener Personen) Tageszeitungen

Meldepflicht bei Datenpannen : Betroffene Person

Ggf. müssen Datenpannen betroffenen Personen gemeldet werden

– Feststellungs- und Anordnungsbefugnis der Aufsichtsbehörde
(Art. 34 Abs. 4 DS-GVO)
„Wenn der Verantwortliche die betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, **kann die Aufsichtsbehörde** unter **Berücksichtigung der Wahrscheinlichkeit**, mit der die **Verletzung** des Schutzes personenbezogener Daten **zu** einem **hohen Risiko führt**, **von** dem **Verantwortlichen verlangen**, **dies** ***[die Meldung]*** **nachzuholen**,
oder sie kann mit einem **Beschluss feststellen**, dass bestimmte der in Absatz 3 *[Tatbestande für Nicht-Meldung]* **genannten Voraussetzungen erfüllt sind**.

Umgang mit Datenpannen

Was also tun?

- Prozess zum Umgang etablieren
  - Was wird an wen gemeldet?
  - Wer hat welche Zuständigkeiten?
  - Wer ist Anlaufstelle für Auftragsverarbeiter?
  - Wer führt Verzeichnis?
  - ...
- Prozess bzgl. Risikomanagement integrieren
  - Wie erfolgt durch wen bis wann eine Risikobewertung?

Umgang mit Datenpannen

Was also tun?

- TOM ergreifen oder zumindest vorschlagen
  - Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten
  - Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
  - → Beides verlangt interdisziplinär agierendes Team:
    IT, Juristen, Mediziner, Entscheidungsträger
- Umgang mit Meldepflichten
  - Wer führt Meldungen an betroffene Person durch?
  - Wer führt Meldungen an Aufsichtsbehörde durch?
- Cave: 72-Stunden-Frist beinhaltet Erfassung der Datenpanne, Risikobeurteilung, TOM und ggf. Meldung