Deutsche Stiftung für Recht und Informatik

„DATENPANNEN“ – EIN IDEALES DATENSCHUTZMANAGEMENT BEIM UMGANG MIT DATENSCHUTZVORFÄLLEN AUS DER PERSPEKTIVE VON UNTERNEHMEN AUS DEM GESUNDHEITSWESEN

Conrad Sebastian Conrad
datenschutz nord GmbH

Herbstakademie 2021

Agenda

- Der Begriff der „Datenpanne“ (Definition)
- Prüfschritte (nach Art. 33 DSGVO und Art. 34 DSGVO)
- Fälle aus der Praxis
- Das richtige Datenschutzmanagement
- Risikoeinschätzung
- Fazit

Der Begriff der „Datenpanne“ (Definition)

- Was meint eigentlich eine „**Datenpanne**“?
- Ungenaue Begrifflichkeit hierzulande (Besser: „*data breach*“)

- **Definition**: Nach der Legaldefinition in Art. 4 Nr. 12 DSGVO ist die *„Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.*

- Entscheidend ist der „Erfolgseintritt“ der **Verletzung des Schutzes personenbezogener Daten** (z.B. durch Vernichtung oder Verlust der Daten, unbefugte Kenntnisnahme der Daten durch Offenbarung oder Zugangseröffnung, Verletzung des Patientengeheimnisses).

Der Begriff der „Datenpanne“ (Definition)

- **Definition**: Legaldefinition in Art. 4 Nr. 12 DSGVO geregelt.

- Erwägungsgrund 85, S. 1 DSGVO: *„Eine Verletzung des Schutzes personenbezogener Daten kann – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person.“*

- **Gesundheitsdaten:** Verlust der Vertraulichkeit / Verletzung des Berufsgeheimnisses (des Arztes), Diskriminierung, Rufschädigung, Verlust der Kontrolle (z.B. Diebstahl von Daten oder Systemausfall).

Prüfschritte: Meldung nach Art. 33 Abs. 1 DSGVO

- Voraussetzungen

1. „*Verletzung des Schutzes personenbezogener Daten*“

2. **Verletzungshandlung**
   - Nach objektiven Maßstäben (verschuldensunabhängig!)
   - Nicht zwingend eine „Verarbeitung“ im Sinne der DSGVO, praktisch jedes Handeln (z.B. auch ein Gespräch)

3. **Katalog aktueller Beispiele**
   - EDSA (Guidelines 01/2021 on Examples regarding Data Breach Notification, Version 1.0)
   - Frühere Art. 29-Gruppe (WP250rev.01)
   - Auch FAQ und Orientierungshilfen der Aufsichtsbehörden

Beispiele: EDSA, Guidelines 01/2021

Examples regarding Data Breach Notification, Version 1.0

Meldung - Art. 33 I

- Fall Nr. 3: Ransomware im Krankenhaus (+)
- Fall Nr. 9: Versicherungsvertreter (-)
- Fall Nr. 12: Gestohlene Papierakte mit Gesundheitsdaten (+)
- Fall Nr. 15: Liste mit 15 Personen mit Lebensmittelunverträglichkeit (-)
- Fall Nr. 16: Falschkuvertierung Kundenbrief KFZ-Versicherer (+)

Benachrichtigung - Art. 34 I

- Fall Nr. 3: Ransomware im Krankenhaus (+)
- Fall Nr. 9: Versicherungsvertreter (-)
- Fall Nr. 12: Gestohlene Papierakte mit Gesundheitsdaten (+)
- Fall Nr. 15: Liste mit 15 Personen mit Lebensmittelunverträglichkeit (-)
- Fall Nr. 16: Falschkuvertierung Kundenbrief KFZ-Versicherer (-)

Prüfschritte: Meldung nach Art. 33 Abs. 1 DSGVO

- Weitere Voraussetzungen

4. Frist

- 72 Stunden? *„unverzüglich und möglichst binnen 72 Stunden“* (Art. 33 DSGVO), aber: eher unverzügliches Handeln ratsam
- Abgestufte Meldung möglich (Art. 33 Abs. 4 DSGVO), d.h. Nachreichen von weiteren Angaben (Sachverhaltserforschung)

5. Form

- i.d.R. besteht ein Online-Formular der Aufsichtsbehörde
- Erforderliche Angaben aus Art. 33 Abs. 1 DSGVO
- Verantwortlicher und Kontaktdaten (für Rückfragen)
- Ggfs. weitere Angaben je nach Formular

Prüfschritte: Benachrichtigung nach Art. 34 Abs. 1 DSGVO

- Voraussetzungen

1. „*Verletzung des Schutzes personenbezogener Daten*“

2. Mit der Folge eines **„Hohen Risikos“** für die persönlichen Rechte und Freiheiten natürlicher Personen

3. **Ausnahmen** (Art. 34 Abs. 3 DSGVO) gegeben / umgesetzt?

4. **Frist**
   - 72 Stunden?, Keine Frist?
   - Grundsätzlich *„unverzüglich“ (ErwG. 86 der DSGVO)*

5. **Form** – keine Vorgaben (aber „klare und einfache Sprache“)

Prüfschritte: Benachrichtigung nach Art. 34 Abs. 1 DSGVO

- Ausnahmen nach Art. 34 Abs. 3 DSGVO

1. Geeignete technisch-organisatorische Maßnahmen (lit. a)
   - Bestanden vorher schon geeignete Sicherheitsvorkehrungen?
   - und wurden diese auch angewandt (z.B. Verschlüsselung; IT-Sicherheit)?

2. Nachfolgende Maßnahmen (lit. b)
   - Nachträgliche Schutzvorkehrungen getroffen?, schnelle Reaktion nötig
   - Bspw. IT-Sicherheit, Sperrung von Zugängen, Vernichtung von Irrläufern

3. Unverhältnismäßiger Aufwand (lit. c)
   - *„Die Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden“* (z.B. bei großer, unbekannten Personengruppe)
   - Dann aber: Öffentliche Bekanntmachung / Ähnliches vorzunehmen
   - Allerdings drohen dann Imageschaden und negative Publizität

Exkurs: Wer muss überhaupt melden?

- In der Praxis stellt sich regelmäßig die Frage: Wer hat den Vorfall zu melden bzw. die Benachrichtigung der betroffenen Person vorzunehmen?

- Antwort: Der Verantwortliche der Datenverarbeitung! (Vgl. Wortlaut von Art. 33, 34 DSGVO bzw. Nachweis wegen Rechenschaftspflichten gem. Art. 5 Abs. 2 DSGVO).

- Nicht:
  - Auftragsverarbeiter (Art. 28 DSGVO) -> Weiterleiten an Verantw.
  - Betrieblicher Datenschutzbeauftragte (Vgl. Art. 38, 39 DSGVO)
  - Externer Anwalt, Steuerberater, Wirtschaftsprüfer
  - Vertragspartner, Kunde, betroffene Person

Fälle aus der Praxis im Gesundheitswesen

- Datenschutzvorfall? Meldung erforderlich? Benachrichtigung?

- „Irrläufer“ durch:
  - Falschkuvertierung, Druckerfehler, vertauschte Blätter
  - Verwechslung, Tippfehler, Adressänderung, Umzug
  - Falsche Zustellung durch Postdienstleister
- Stromausfall im Krankenhaus, Wasserschaden im Keller
- Hackerangriff/Trojaner im System (z.B. emotet)
- Fehler in der IT-Sicherheit, „Lücken“ auf einer Webseite
- Gestohlene Akten/Dateien (durch Personal oder Dritte)
- Falscher Aktenvernichter, falsche Entsorgung im „Papiermüll“
- Gespräch beim „Abendessen“ oder am Gartenzaun

Das richtige Datenschutzmanagement

- **Beispiel eines Konzepts**

Folgende Schritte in dieser Reihenfolge bieten sich an bzw. sollten durch intern festgelegte Prozesse umgesetzt und sichergestellt werden:

- 1. **Existierende interne Prozesse**
  - Prüfung und Diagnose durch entsprechende Zuständigkeiten
  - Wissensmanagement (Schulungen, Sensibilisierung, Prozesse)
  - Ticketsystem zur Kommunikation und internen Dokumentation

- 2. **Einleitung interner Prüfung**
  - Erfassen des Sachverhalts (durch ExpertInnen, Personal, Leitung)
  - Ggfs. externe Experten hinzuziehen
  - Konsultation des Datenschutzbeauftragten

Das richtige Datenschutzmanagement

- **Beispiel eines Konzepts**

- 3. **Einleitung kurzfristiger Maßnahmen**
  - Schadensabwehr (Lücken schließen, IT-Sicherheit gewährleisten - können auch Maßnahmen gem. Art 34 Abs. 3 DSGVO darstellen)
  - Schnelle Vernichtung, Löschung der falsch versendeten Daten
  - Aktivierung eines Notfallkonzepts (Backups, IT-Sicherheit)

- 4. **Meldung und ggfs. Benachrichtigung**
  - Zuständigkeiten der AB und Formalitäten feststellen
  - Ggfs. (vorläufige) Meldung nach Art. 33 Abs. 1 DSGVO oder abgestufte Meldung vornehmen
  - Ggfs. Benachrichtigung nach Art. 34 Abs. 1 DSGVO

Das richtige Datenschutzmanagement

- **Beispiel eines Konzepts**

- 5. **Dokumentation**
  - Dokumentation des gesamten Vorgangs (inkl. Korrespondenz aller Meldungen / Schreiben), auch falls keine Meldung erging
  - Aufbewahrung für 3 Jahre an einem gesicherten Ort

- 6. **Etablierung langfristiger Maßnahmen**
  - Allgemeine Fehlerdiagnose (Prüfung der Systeme und Prozesse)
  - Schulung von MitarbeiterInnen; Sensibilisierungsmaßnahmen
  - Stichproben nehmen und ggfs. Whistleblowing anbieten
  - Personelle Veränderungen prüfen bzw. notfalls umsetzen
  - Regelmäßige Überprüfung des gesamten Konzepts vornehmen

Risikoeinschätzung

- **Denkbare Überlegungen des Verantwortlichen:**
  - Jeden Vorfall melden? Aber: Risikobasierter Ansatz der DSGVO
  - Keine oder verspätete, unvollständige Meldung ist bußgeldbewehrt

  - Vielleicht keine Meldung nach Art. 33 Abs. 1 DSGVO?
    - Da nur „*geringes*“ Risiko? Geringer Schadenseintritt?

  - Vielleicht keine Benachrichtigung nach Art. 34 Abs. 1 DSGVO?
    - Da kein „*hohes Risiko*“ (mehr) besteht? Ausnahmen greifen?

  - Fallbeispiel: Irrläufer zwischen Arzt – falscher Arzt
    - Wohl kein „*hohes*“ Risiko (falscher Empfänger ist auch Arzt)
    - Gar keine Datenschutzverletzung (wg. Patientengeheimnis)?

Risikoeinschätzung

- **Denkbare Überlegungen des Verantwortlichen:**
  - Jeden Vorfall melden? Aber: Risikobasierter Ansatz der DSGVO
  - Keine oder verspätete, unvollständige Meldung ist bußgeldbewehrt

  - Gilt der „*nemo tenetur*“-Grundsatz im Verfahren? [wohl ja]
  - Drohen daher keine Nachteile durch „Selbstanzeige“?
  - Erfolgt aber (dennoch) eine Kontrolle der Aufsichtsbehörde?
  - Erkennt diese strukturelle Fehler oder (neue) Schwachstellen?
  - Kosten für verbesserte Systeme und mehr Personal? Outsourcing?

  Alles unterliegt der allgemeinen Risikoeinschätzung der Geschäftsleitung bzw. dem unternehmerischen Risiko, wie mit Gefahren und rechtlichen Risiken umzugehen ist bzw. diesen angemessen begegnen werden soll.

Fazit

- Der Verantwortliche muss auf Grundlage einer eigenen Risikoeinschätzung und unter Berücksichtigung aller Umstände die weitreichende **Entscheidung** treffen, ob ein etwaiger Vorfall zur Meldung oder gar zur Benachrichtigung der betroffenen Person führt, und sodann diese innerhalb der zulässigen Frist vollumfänglich umsetzen.

- In jedem Fall ist der **Vorfall intern zu dokumentieren.**

- Die Praxis zeigt, dass die Meldung eines etwaigen Vorfalls gegenüber der zuständigen Aufsichtsbehörde in der überwiegenden Zahl an Fällen zu keinen **Maßnahmen** führt und darüber hinaus sogar das **Risiko von Sanktionen minimiert.**