Sommerakademie 2019

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Anstalt des öffentlichen Rechts

Datenschutzpannen aus der Praxis

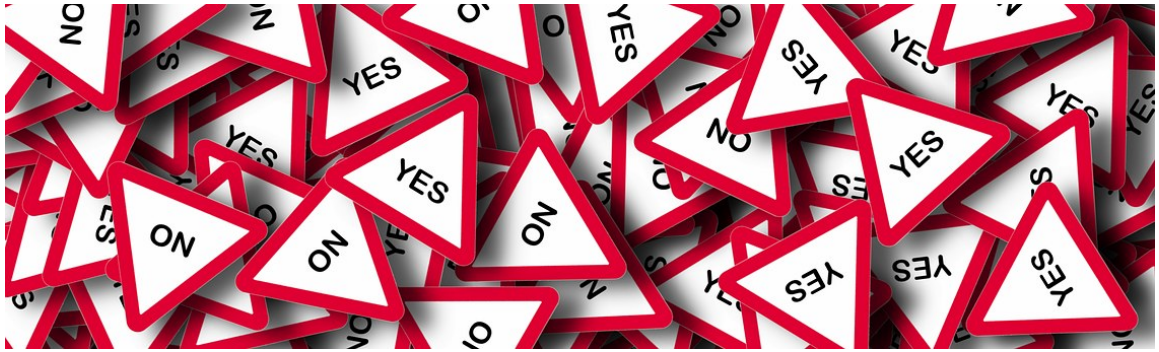
Heiko Behrendt
ISO 27001 Auditor
Fon: 0431 988 1212
Mail: uld72@datenschutzzentrum.de
Web: https://www.datenschutzzentrum.de/

Themen

- Meldungen aus der Praxis
- Anforderungen der Datenschutz-Grundverordnung
- Praktische Umsetzung in der Organisation
- Meldeprozess
- Fallbeispiele

Datenschutzpannen?!

Kann mir das auch passieren?



Quelle: https://pixabay.com/de/illustrations/banner-ja-nr-entscheidung-wahl-1183407//

Meldungen aus der Praxis

Verletzung des Schutzes personenbezogener Daten?!

- Virenbefall durch Kryptotrojaner mit Verschlüsselung der Kundendaten
- Einbruch in Arztpraxis und Entwendung von Datenspeicherungssystemen
- Alle Mitarbeiter können auf die Datenablage der Personalabteilung zugreifen
- Versendung von Sozialdaten per Mail (unverschlüsselt) an eine falsche E-Mailadresse
- Diebstahl eines Notebooks mit verschlüsselter Festplatte
- Zugriff auf Studentendaten über das Internet durch Eingabe eines URL-Pfades
- Übersendung eines Arztbriefes an einen anderen Arzt ohne Einwilligung des Patienten
- Zugriff auf alle Patientendaten durch unbefugte Mitarbeiter eines Krankenhauses
- Datenverlust von Kundendaten bei einem Cloud-Anbieter durch Systemausfall
- Mehrere Mitarbeiter speichern sensible personenbezogene Daten auf private Datenträger
- ...

Vorschriften der DSGVO richtig anwenden!

Quelle: https://pixabay.com/de/photos/dsgvo-datenschutzgrundverordnung-3958460/

Artikel 33 DSGVO

Meldung von Verletzungen des Schutzes personenbezogener Daten

Quelle: https://pixabay.com/de/photos/cyber-angriff-attacke-3327240/
https://pixabay.com/de/photos/datenklau-daten-dvd-passwort-1512249/

„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 gemäß Artikel 55 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.“

Artikel 34 DSGVO

Benachrichtigung der von einer Verletzung ... betroffenen Personen

Quelle: https://pixabay.com/de/photos/menschenmenge-menschen-silhouetten-2718833/

„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.“

Was muss ich melden?

Ereignisse, die den Schutz der pb Daten verletzen ...

Artikel 4 Nr. 12 DSGVO: „**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.“

Beispiele:

- Unbefugte Kenntnisnahme
- Unkontrollierter Datenabfluss
- Datenklau
- Verlust, Zerstörung oder Schädigung von pb Daten
- ...

↓

Ereignisse mit potenziellen Schäden für Betroffene?

Was sind Schäden für Betroffene?

Erwägungsgrund 85 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 pers. Daten
- 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

→ Schäden für Betroffene!

Besteht ein (hohes) Risiko für Betroffene?

Risikoanalyse

Ereignis: Unbefugter Datenabfluss

Entstehen Schäden für Betroffene?

Betroffene

Quellen:
https://pixabay.com/de/illustrations/identit%C3%A4tsdiebstahl-internet-online-2708855/
https://pixabay.com/de/illustrations/menschenmenge-menschen-silhouetten-3513217/

- Der Begriff „**Risiko**“ steht im Zusammenhang mit einem **Ereignis**, das mit einer möglichen (Eintrittswahrscheinlichkeit) negativen Auswirkung (Schaden) verknüpft ist.
- **Risikoanalyse:** Bei einer Datenschutzpanne ist ein Ereignis eingetreten, bei dem analysiert werden muss, ob es negative Auswirkungen (Schäden) für Betroffene haben kann.
- Ein **hohes Risiko** ist insbesondere dann gegeben, wenn **große Schäden** für den Betroffenen möglich sind. Darunter können insbesondere Ereignisse mit sensiblen Daten nach Artikel 9 DSGVO fallen.

Organisatorische Prozesse einführen!

Quelle: https://pixabay.com/de/photos/planen-ziel-strategie-prozess-2372176/

Ansprechpartner und Meldestelle

Organisatorische Regelungen

- **Nutzer/Mitarbeiter:** Internes Melden von Datenschutzpannen
- **Administratoren:** Entgegennahme von Meldungen und erste Entscheidungsvorbereitung sowie Einleitung der Eskalation
- **Fachverantwortliche:** Beteiligung als Datenverantwortliche der betroffenen Geschäftsprozesse und Anwendungen bei Entscheidungsfindung für Schadensbeseitigung
- **Informationssicherheitsbeauftragte(r):** Entgegennahme von Meldungen, Festlegung des Eskalationswegs und Einleitung notwendiger Maßnahmen
- **Datenschutzbeauftragte(r):** Einbindung
- **Informationssicherheits- und Datenschutzvorfallmanagement:** Ein aus Datenschutz- und Informationssicherheitsbeauftragten, IT- und Fachverantwortlichen und Leitungsebene zusammengesetztes **Team** zur Behandlung einer Datenschutzpanne

Klassifizierung nach Schweregrad

Wer soll und wer muss informiert werden?

- Bei Ereignissen **höherer Gewalt** wie Feuer, Wasser, Stromausfall, Einbruch und Diebstahl sind die örtlich verfügbaren Einsatzkräfte sowie die technische Einsatzleitung zu unterrichten, z. B. Feuerwehr, Haustechnik, Pforte, Wachdienst.

- Bei **hardware-technischen Problemen** oder bei Unregelmäßigkeiten bei Betrieb der IT-Systeme ist der zuständige Administrator bzw. der Benutzer-Support zu benachrichtigen.

- Bei **großflächigen Ausfällen** ist ggf. der Notfallbeauftragte (wenn vorhanden) und der Leiter des Krisenstabs zu informieren.

- Bei **vermuteten vorsätzlichen Handlungen** und bei ansonsten nicht zuzuordnenden Ereignissen, z. B. Datenmanipulationen, unerlaubte Ausübung von Rechten, Spionage- und Sabotageverdacht, ist der Datenschutz- und/oder der Informationssicherheitsbeauftragte zu benachrichtigen.

Eskalationsstufen und Meldepflichten

Intern

- Fachabteilung
- IT-Abteilung
- Informationssicherheits- und / oder Datenschutzbeauftragter
- Leitungsebene

Extern

- Datenschutz-Aufsichtsbehörden
- Betroffene
- Fach- bzw. Rechtsaufsichtsbehörden
- BSI bzw. Bundesnetzagentur bei kritischer Infrastruktur
- Ggf. Strafverfolgungsbehörden

Datenschutzpanne

Prozessablauf

1. **Feststellung der Datenpanne durch einen Mitarbeiter einer Fachabteilung und Meldung an den internen Service-Desk**

2. **Analyse des Ereignisses durch z. B. den DSB**

   Sofortmaßnahmen zur Schadensminimierung

   Datenschutzrechtliche Bewertung:

   Liegt ein (hohes) Risiko für Betroffene vor? Meldung an die Aufsichtsbehörde und Benachrichtigung der Betroffenen durch den Verantwortlichen

3. **Vollständige Beseitigung der Datenschutzpanne**

   Wiederherstellung und Verbesserung des Datenschutzes

   Nachbereitung und ggf. Anpassung der Prozessabläufe

   Dokumentation der Datenschutzpanne

Quelle: https://pixabay.com/de/illustrations/ampel-problem-analyse-l%C3%B6sung-rot-466950/

Dokumentation

Datenpanne und Benachrichtigung

- Der Verantwortliche dokumentiert die **Datenschutzpanne** 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 ermöglichen (Artikel 33 Abs. 5 DSGVO).
- Die **Benachrichtigung** (hohes Risiko) der Betroffenen beschreibt **verständlich**
  - die Art der Verletzung des Schutzes personenbezogener Daten,
  - zuständige Ansprechpartner,
  - die wahrscheinlichen Folgen sowie
  - die ergriffenen Maßnahmen zur Behebung (Artikel 34 Abs. 2 DSGVO).
- Ist der Aufwand unverhältnismäßig, ist stattdessen eine **öffentliche Bekanntmachung** durchzuführen (Artikel 34 Abs. 3 Buchst. c DSGVO).
- Eine **Benachrichtigung** kann entfallen, wenn der Verantwortliche durch Maßnahmen sichergestellt hat, dass **kein hohes Risiko mehr** für den Betroffenen besteht (Artikel 34 Abs. 3 Buchst. b DSGVO).

Meldung an die Aufsichtsbehörde (ULD)

Formular

<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)[1] / § 41 Landesdatenschutzgesetz (LDSG)[2].

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

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>

Folgende Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen werden vorgeschlagen:
<Liste der Maßnahmen>

Meldung an die Aufsichtsbehörde (ULD)

Formular

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen (Art. 34 DSGVO / § 42 LDSG)

Die Verletzung des Schutzes personenbezogener Daten hat voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge: <ja / nein>

Falls ja:

Die betroffenen Personen wurden gemäß Art. 34 DSGVO / § 42 LDSG unverzüglich über die Verletzung benachrichtigt:
<ja: Datum und Uhrzeit, Beschreibung / nein>

Falls nein, bitte mindestens einen der folgenden Gründe angeben:

1. Es wurden geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und auf die betroffenen personenbezogenen Daten angewandt (z.B. geeignete Verschlüsselung):
<Beschreibung>

2. Durch nachfolgende Maßnahmen wurde sichergestellt, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht:
<Beschreibung>

3. Eine Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden. Stattdessen erfolgt eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme, durch die die betroffenen Personen vergleichbar wirksam informiert werden:
<Beschreibung>

Vollständigkeit der Informationen

Folgende Informationen können zum Zeitpunkt dieser Meldung nicht bereitgestellt werden und werden nachgereicht:
<Liste der fehlenden Informationen>

Weitere Dokumentation

Als Verantwortlicher dokumentiere ich hiermit die Verletzungen des Schutzes personenbezogener Daten. Nach dieser Meldung dokumentiere ich alle im Zusammenhang mit dieser Verletzung des Schutzes personenbezogener Daten stehenden Fakten, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen.

Ich bestätige die Richtigkeit und Vollständigkeit der Meldung (ausgenommen der angegebenen fehlenden Informationen) sowie die Kenntnisnahme der Hinweise hinsichtlich der Benachrichtigung der betroffenen Personen sowie der weiteren Dokumentation.

(Ort, Datum, Unterschrift)

Hinweis zur Datenschutzerklärung:

https://www.datenschutzzentrum.de/datenschutzerklaerung/

Rechtsfolgen bei Verstoß gegen die DSGVO

- Geldbußen werden je nach den **Umständen des Einzelfalls** verhängt.
- Bei der Entscheidung über die **Verhängung einer Geldbuße** und über deren Betrag wird in jedem Einzelfall Folgendes berücksichtigt:
  - **Art, Schwere und Dauer** des Verstoßes
  - **Vorsätzlichkeit** oder **Fahrlässigkeit** des Verstoßes
  - Maßnahmen zur Minderung des den betroffenen Personen entstandenen **Schaden**
  - Grad der Verantwortung unter Berücksichtigung der getroffenen Schutzmaßnahmen
  - Etwaige einschlägige **frühere Verstöße**
  - **Kategorien** pb Daten, die von dem Verstoß betroffen sind
  - Zusammenarbeit mit der Aufsichtsbehörde, um den Verstoß abzuhelfen bzw. zu mindern
  - Einhaltung von Anordnungen im Rahmen von vorangegangenen Prüfungen
  - Einhaltung von Verhaltensregeln oder Zertifizierungsverfahren (DSGVO)
  - Durch den Verstoß erlangte **finanzielle Vorteile** oder **vermiedene Verluste**
- Bei Verstößen gegen die **Pflichten** der Verantwortlichen und der Auftragsverarbeiter werden Geldbußen von bis zu **10.000.000 Euro** oder bis zu **2 % des weltweiten Jahresumsatzes** des vorangegangenen Geschäftsjahrs verhängt (Artikel 83 DSGVO).
- Gegen **Behörden und sonstige öffentliche Stellen** werden **keine** Geldbußen verhängt (§ 43 BDSG, § 19 LDSG SH).

Fallbeispiele!

Quelle: https://pixabay.com/de/photos/europa-bipr-daten-datenschutz-3256079/

Datenschutzpanne „Notebook“

Bearbeitung – Prozess?

Einem Außendienstmitarbeiter wird auf der Dienstreise sein Notebook mit **vertraulichen Kundendaten** entwendet. Welche Schritte sind bei einer Datenschutzpanne abzuarbeiten, und was ist bedeutsam für die datenschutzrechtliche Bewertung?

Lösung

- Sofortige Meldung bei einer zentralen Meldestelle der Organisation
- Genaue Beschreibung des Ereignisses
- Analyse über den eingetretenen Schaden

Klärung z. B. folgender Fragen:

- Welche Daten befinden sich auf dem Notebook?
- Welche Sensibilität haben die Daten?
- Liegt eine Verletzung des Schutzes personenbezogener Daten vor?
- Welche negativen Auswirkungen (Schäden) können für Betroffene eintreten?
- Können über Anwendungen/Dienste Zugriffe auf Daten erfolgen?
- Sind Geschäftsprozesse gefährdet?
- Sind Sofortmaßnahmen erforderlich, z. B. Zugänge zu internen Systemen sperren?
- Sind Aufsichtsbehörde (Art. 33 DSGVO) und Betroffene (Art. 34 DSGVO) zu informieren?
- …

Datenschutzpanne „Datenleitung“

Meldepflichtig?

Bei einer Firma/Behörde fällt **während der Geschäftszeiten** die Datenkommunikations-verbindung (Netzverbindung, WAN) zum Rechenzentrum (Dienstleister) aus. Liegt eine Datenschutzpanne vor?

Lösung

Es kommt darauf an, welches Risiko damit verbunden ist:

- Fall 1: Es liegt eine **Datenschutzpanne** vor, wenn z. B. ein Hackerangriff erfolgte und pb Daten unbefugt zur Kenntnis genommen wurden.
- Fall 2: Es liegt eine **Störung** vor, wenn z. B. der Ausfall durch einen Defekt einer Netzkomponente verursacht wurde und nur **geringfügige Beeinträchtigungen** ohne unberechtigten Zugriff auf pb Daten vorliegen.

Datenschutzpanne „Personaldaten“

Wie gehe ich als DSB vor?

Ein **Azubi** aus der Personalabteilung der **Behörde „Zentrales Personalmanagement“** stellt fest, dass die **gesamten Personaldaten** von mehreren **tausend Beschäftigten** über eine Funktion der **Webseite** von jedem „Webseitennutzer“ aufgerufen werden können. Da sein Vorgesetzter nicht anwesend ist, informiert er ihn erst **zwei Wochen** später nach Rückkehr aus dem Urlaub. Der Vorgesetzte benachrichtigt den internen Datenschutzbeauftragten **per Mail**. Welche Schritte führen Sie in der Rolle des internen Datenschutzbeauftragten durch?

Lösung

Analyse – Gespräche mit IT, Fachabteilung, ggf. Dienstleister führen

- Was ist genau passiert?
- Welche Geschäftsprozesse, Systeme, Fachanwendungen und Daten sind betroffen?
- Welche Daten können/konnten „Unbefugte“ über das Internet auf der Webseite aufrufen?
- Sind unberechtigte Zugriffe nachweisbar (z. B. durch eine Protokollierung)?
- Wo liegt der Fehler (Web-Anwendung, Regelwerk der Firewall)?
- Wurden Berechtigungen falsch vergeben oder gab es einen Hackerangriff?
- ...

Datenschutzpanne „Personaldaten“

Wie gehe ich als DSB vor?

Lösung

Sofortmaßnahmen, Schadensbegrenzung

- Verantwortlichen (Chef) informieren
- Z. B. Webseite offline schalten oder Verbindung zum Internet trennen
- ...

Rechtliche Bewertung Artikel 33 und 34, Erwägungsgründe 85-88 DSGVO

- Eine Verletzung des Schutzes personenbezogener Daten liegt vor
- **Risikoanalyse:** Schäden können für Betroffene eintreten, z. B. Diskriminierung, Rufschädigung
- **Meldebogen** an Aufsichtsbehörde versenden mit Angaben zur Datenschutzpanne, zur Verletzung von pb Daten und Maßnahmen zur Abhilfe (siehe Vordruck Aufsichtsbehörden)
- Ggf. **Benachrichtigung** der Betroffenen in Abhängigkeit von der Schwere der Datenpanne

Datenschutzpanne „Personaldaten“

Wie gehe ich als DSB vor?

Lösung

Beseitigung der Datenpanne

- Fehlerbeseitigung mit Test und Freigabe durch Verantwortliche (IT- und Fachabteilung)
- Dokumentation der Datenpanne mit allen Abläufen und umgesetzten Maßnahmen z. B. in einem Ticketsystem
- Verbesserung des Meldeprozesses (sofort, persönlich, telefonisch, schriftlich, Mail mit cc)
- Schulung und Sensibilisierung von Beschäftigten im Umgang mit Datenschutzpannen
- Ggf. Abläufe in der Personal- und IT-Abteilung verbessern, so dass Fehler rechtzeitig erkannt werden

Vielen Dank für Ihre Aufmerksamkeit!

Heiko Behrendt
ISO 27001 Auditor
Fon: 0431 988 1212
Mail: uld72@datenschutzzentrum.de
Web: https://www.datenschutzzentrum.de/