Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Anstalt des öffentlichen Rechts

Sommerakademie 2018

Datenschutzpannen

Feststellung, Klassifizierung und Management von Datenschutzvorfällen

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

Inhalt

- Was sind Datenschutz- und Informationssicherheitsvorfälle?
- Welche organisatorischen Maßnahmen sind für das Erkennen von Vorfällen umzusetzen?
- Wie ist ein Datenschutz- und Informationssicherheitsvorfallmanagement zu gestalten?
- Wann muss ich die Aufsichtsbehörde und wann den Betroffenen informieren?
- Nach welchen Kriterien bewerte ich, ob ein Risiko für den Betroffenen vorliegt?
- Welche Schritte sind für die Bearbeitung eines Datenschutz- und Informationssicherheits-vorfalls umzusetzen?
- Beispiele aus der Praxis

Artikel 33 DS-GVO

Meldung von Verletzungen des Schutzes personenbezogener Daten

Auszug Gesetzestext

- Im Falle einer **Verletzung des Schutzes personenbezogener Daten** meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden der zuständigen **Aufsichtsbehörde, wenn ein Risiko für die Betroffenen vorliegt**.

- „Wenn dem **Auftragsverarbeiter** eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem **Verantwortlichen unverzüglich**."

- Die **Meldung** enthält **Informationen** über Art der Verletzung, Kategorien der Daten, Anzahl betroffene Personen und Datensätze, Kontaktdaten des Datenschutzbeauftragten, Beschreibung der Folgen der Verletzung des Schutzes personenbezogener Daten sowie **Maßnahmen zur Behebung des Vorfalls**.

- Vollständige **Dokumentation des Vorfalls** einschließlich der durchgeführten Schritte.

Artikel 33 DS-GVO

Meldung von Verletzungen des Schutzes personenbezogener Daten

Auslegung – Kommentar (Becksche Kompakt-Kommentare Paal /Pauly)

- Die Mitteilungspflicht des Verantwortlichen gegenüber der Aufsichtsbehörde entsteht in dem Zeitpunkt, in welchem ihm die Verletzung **bekannt** wird. Der **Auftragsverarbeiter hat die Pflicht**, den Verantwortlichen bei dessen Pflichterfüllung zu unterstützen (Art. 28).

- Art. 4 Nr. 12 Definition **„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.

- Der Verantwortliche muss **eine Verletzung nicht** melden, wenn diese voraussichtlich nicht zu einem Risiko bzw. nur zu einem **geringfügigen Risiko** für die persönlichen Rechte und Freiheiten der Betroffenen führt (Verhältnis Eintrittswahrscheinlichkeit und Schadenshöhe).

- Die **Bemessungskriterien** für die Risikobeurteilung sind **nicht** festgelegt.

Artikel 33 DS-GVO

Meldung von Verletzungen des Schutzes personenbezogener Daten

Erwägungsgründe 85, 87, 88

- ... 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

Artikel 34 DS-GVO

Benachrichtigung der von einer Verletzung betroffenen Personen

Auszug Gesetzestext

- „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.“

- Die Benachrichtigung beschreibt in **verständlicher Sprache** die Art der Verletzung des Schutzes personenbezogener Daten, zuständige Ansprechpartner, die möglichen Folgen sowie die ergriffenen Maßnahmen zur Behebung. Ist der Aufwand unverhältnismäßig, ist stattdessen eine **öffentliche Bekanntmachung** durchzuführen.

- Eine Benachrichtigung kann entfallen, wenn der Verantwortliche durch Maßnahmen sichergestellt hat, dass der Schutz der Daten gewährleistet wird und **kein Risiko mehr** für den Betroffenen besteht.

Artikel 34 DS-GVO

Benachrichtigung der von einer Verletzung betroffenen Personen

Auslegung – Kommentar (Becksche Kompakt-Kommentare Paal /Pauly)

- Die Benachrichtigungspflicht gegenüber den Betroffenen wird auf **bestimmte Risiko-situationen** begrenzt. Besteht nachweislich kein hohes Risiko, trifft den Verantwortlichen **keine** Benachrichtigungspflicht. Wann ein Risiko hoch ist, wird in Art. 34 DS-GVO **nicht** definiert. Art. 35 DS-GVO Datenschutz-Folgenabschätzung definiert jedoch ein hohes Risiko für die Rechte und Freiheiten Betroffener, wenn z. B. **Daten nach Art. 9 DS-GVO** verarbeitet werden.

- Die Benachrichtigung soll es dem Betroffenen ermöglichen, auf bestehende Risiken **zu reagieren** sowie **selbst zum Schutz** seiner Freiheiten und Rechte durch geeignete Vorkehrungen beizutragen.

- Es ermöglicht ihm, gegen den Verantwortlichen **gerichtlich** vorzugehen oder **Haftungsansprüche** geltend zu machen (Art. 82 Abs. 1 DS-GVO).

- Die Aufsichtsbehörde kann den Verantwortlichen zur **Beseitigung der Schwachstellen** auffordern sowie eine Geldbuße auferlegen (Art. 83 DS-GVO).

Datenschutz- und Informationssicherheitsvorfälle

Kann mir das auch passieren?

- Als **Datenschutz- und Informationssicherheitsvorfall** wird ein **unerwünschtes Ereignis** bezeichnet, das Auswirkungen auf den Betroffenen und/oder die Informationssicherheit der Organisation hat und in der Folge (große) Schäden nach sich ziehen kann.

- Typische **Datenschutz- und Informationssicherheitsvorfälle** sind beispielsweise
  - Fehlkonfigurationen, die zur Offenlegung vertraulicher Daten, zu Verlust der Integrität schutzbedürftiger Daten oder zu Datenverlusten führen,
  - Auftreten von Sicherheitslücken in Hard- oder Softwarekomponenten,
  - Auftreten von Schadsoftware,
  - Verlust eines Notebooks mit Geschäfts- und Kundendaten oder
  - kriminelle Handlungen, wie z. B. Hacking von IT-Systemen oder Diebstahl von Daten.

- **Datenschutz- und Informationssicherheitsvorfälle** können durch eine Vielzahl von Gefährdungen ausgelöst werden. Datenschutzvorfälle im Sinne der DS-GVO liegen immer dann vor, wenn von einer **Verletzung des Schutzes personenbezogener Daten** auszugehen ist.

Ansprechpartner und Meldestellen

- **Nutzer/Mitarbeiter:** Melden von Datenschutz- und Informationssicherheitsvorfällen
- **Administratoren:** Entgegennahme von Meldungen und erste Entscheidungsvorbereitung sowie Einleitung der Eskalation
- **Fachverantwortliche:** Beteiligung als Datenverantwortliche der betroffenen Geschäftsprozesse und Anwendungen bei Entscheidungsfindung für Schadensbeseitigung
- **Datenschutz- und Informationssicherheitsbeauftragter:** Entgegennahme von Meldungen und Entscheidungsfindung zwischen Datenschutz- und Informationssicherheits-vorfall, Einschaltung des Eskalationswegs und Einleitung notwendiger Maßnahmen
- **Datenschutz- und Informationssicherheitsvorfallmanagement:** Ein aus Datenschutz- und Informationssicherheitsbeauftragten, IT- und Fachverantwortlichen und Leitungsebene zusammengesetztes **Team** zur Abwicklung eines Datenschutz- und Informationssicherheitsvorfalls

Meldewege, Klassifizierung

Wer ist bei welchem Ereignis zu informieren?

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

- 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 Krisenstab 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.

- Die **Meldungen** von Datenschutz- und Informationssicherheitsvorfällen sind zentral z. B. in einem Ticketsystem zu dokumentieren (Art. 33 Abs. 3 + 5 DS-GVO).

Eskalationsstufen, Dokumentations- und Meldepflichten

Intern

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

Extern

- BSI bzw. Bundesnetzagentur bei kritischer Infrastruktur
- Aufsichtsbehörden
- Landes- bzw. Bundesbeauftragte für Datenschutz (DS-GVO, BDSG, LDSG)
- Betroffene

Datenschutz- und Informationssicherheitsvorfall

Beispiel: „Virenbefall“

Prozess:

annehmen, bewerten, analysieren, beheben, nachbereiten

1. Meldung
2. Analyse
3. Sofortmaßnahmen
4. Wiederherstellung
5. Nachbereitung

Quelle: https://pixabay.com

1. Meldung

- Wer hat Auffälligkeiten festgestellt?
- Wie wird der Vorfall gemeldet (telefonisch, Formular etc.)?
- Gibt es eine zentrale Meldestelle?
- Wer analysiert und priorisiert den Vorfall?
- Wer ist befugt, Sofortmaßnahmen einzuleiten?
- ...

2. Analyse

Perspektive „Geschäftsprozesse“ und „Betroffene“

- Wann und an welcher Stelle hat sich der Vorfall ereignet?
- Welche Anwendungen, IT-Systeme, Dienste und **Daten** sind betroffen?
- Können Folgeschäden auch durch die Vernetzung der IT-Systeme entstehen?
- Für welche Anwendungen, IT-Systeme, Dienste und **Daten** können Schäden und Folgeschäden ausgeschlossen werden?
- Liegt eine Verletzung des Schutzes personenbezogener Daten vor?
- Besteht für Betroffene (Kunden, Mitarbeiter etc.) ein (hohes) Risiko?
- Wie hoch kann der durch den Vorfall verursachte direkte Schaden oder Folgeschaden sein?
- Wodurch wurde der Vorfall ausgelöst, z. B. durch Unachtsamkeit oder Angreifer?
- ...

3. Sofortmaßnahmen

- Können Systeme vom „Netz“ genommen werden?
- Können/müssen Festplatten vor Schadensbehebung gesichert werden (Beweissicherung)?
- Welche Datenverantwortlichen (Fachabteilung) und Mitarbeiter müssen informiert werden?
- Müssen die Aufsichtsbehörde oder ggf. der Betroffene informiert werden?
- Welche technischen Maßnahmen können für die Schadensbehebung umgesetzt werden?
- ...

4. Wiederherstellung

- Betriebssysteme untersuchen
- Protokolldateien analysieren
- Originaldateien von geschützten Datenträgern zurückspielen
- Passwörter auf den betroffenen IT-Systemen ändern
- ...

5. Nachbereitung

- Wie schnell wurde der Vorfall bemerkt?
- Welche Informationen standen für die Bewertung zur Verfügung?
- Ggf. Nachrüstung technischer Detektionsmaßnahmen
- Ggf. Optimierung der Wiederherstellungsschritte
- ...

Warn- und Informationsdienste

- https://www.cert-bund.de/

Warn- und Informationsdienst WID
Eine maßgebliche Aufgabe des Teams CERT-Bund ist der Betrieb eines Warn- und Informationsdienstes - WID. Über den WID werden Informationen zu neuen Schwachstellen und Sicherheitslücken sowie aktuellen Bedrohungen für IT-Systeme publiziert. Zu den Anwendern des WID zählen die Bundesverwaltung, Unternehmen kritischer Infrastrukturen, CERTs sowie Bürgerinnen und Bürger.

- https://www.cert-verbund.de/

Der CERT-Verbund ist die Allianz deutscher Sicherheits- und Computer-Notfallteams mit über 40 Mitgliedern

- https://de.wikipedia.org/wiki/Computer_Emergency_Response_Team

Definition CERT

Beispiel 1

Einem Außendienstmitarbeiter wird während der Dienstreise sein Notebook mit **vertraulichen Kundendaten** entwendet. Welcher Prozess ist im Rahmen eines Datenschutz- und Informationssicherheitsvorfallmanagements abzuarbeiten und was ist bedeutsam für die Bewertung?

- Sofortige Meldung bei einer zentralen Meldestelle der Organisation
- Genaue Beschreibung des Vorfalls
- Analyse über den eingetretenen Schaden
- Klärung folgender Fragen:
  - Welche Daten befinden sich auf dem Notebook?
  - Welche Sensibilität haben die Daten?
  - Lieg eine Verletzung des Schutzes personenbezogener Daten vor?
  - Können über Anwendungen/Dienste weitere Zugriffe auf Daten erfolgen?
  - Sind Geschäftsprozesse gefährdet?
  - Sind Sofortmaßnahmen erforderlich, z. B. Zugänge zu internen Systemen sperren?
  - Sind Aufsichtsbehörde und Betroffene zu informieren?
  - ...

Beispiel 2

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

- Es kommt darauf an, wie der Vorfall entstanden ist:
  - Es liegt ein **Informationssicherheitsvorfall** vor, wenn z. B. wesentliche Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren.
  - Es liegt darüber hinaus ein **Datenschutzvorfall** vor, wenn z. B. ein Hackerangriff erfolgte und z. B. Daten unbefugt zur Kenntnis genommen wurden.
  - Es liegt eine **Störung** vor, wenn z. B. der Ausfall durch einen Defekt einer Netzkomponente verursacht wurde und nur **geringfügige Beeinträchtigungen** vorliegen.

Beispiel 3

In einer Firma/Behörde wird von einem Mitarbeiter telefonisch beim Helpdesk eine Systemstörung gemeldet. Der Helpdesk **vermutet** eine Infektion mit dem Verschlüsselungsvirus „WannaCry“ und informiert den Datenschutzbeauftragten. Welche Schritte führen Sie in der Rolle des Datenschutzbeauftragten durch?

- Analyse des Vorfalls
  - Auf welchem System ist der Vorfall aufgetreten?
  - Was ist genau passiert?
  - Welche Systeme, Geschäftsprozesse, Fachanwendungen und Daten sind betroffen?
  - Liegt eine Verletzung des Schutzes personenbezogener Daten vor?
- Sofortmaßnahmen ergreifen
  - System(e) vom Netz nehmen
  - ggf. Unternehmensleitung informieren
  - ggf. Notfallmanagement aktivieren
  - ggf. Beweissicherung durchführen
- Wiederherstellung einleiten
  - Backup einspielen
  - ...
- Nachbereitung durchführen
  - Sicherheitsmaßnahmen verbessern
  - ...

Datenschutzpannen

Feststellung, Klassifizierung und Management von Datenschutzvorfällen

Vielen Dank für Ihre Aufmerksamkeit!

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