Meldungen und Benachrichtigungen bei Datenschutzverletzungen

Sommerakademie
am 11. September 2023
in Kiel

Alexander Hauptmann/Dr. Thomas Probst
0431 988-1200
mail@datenschutzzentrum.de
https://www.datenschutzzentrum.de/

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Überblick

1. Wann (unter welchen Voraussetzungen) muss eine Meldung nach Art. 33 DSGVO erfolgen?

2. Wie erfolgt eine Meldung nach Art. 33 DSGVO?

3. Weitere Bearbeitung des ULD nach Eingang der Meldung

4. Beispiele aus der Praxis

5. Zusammenfassung / Abschluss

1. Wann muss eine Meldung nach Art. 33 DSGVO erfolgen?

Art. 33 Abs. 1 DSGVO

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 der betroffenen Personen führt.

1. Wann muss eine Meldung nach Art. 33 DSGVO erfolgen?

Verletzung des Schutzes personenbezogener Daten

-> Begriffsbestimmung gem. Art. 4 Nr. 12 DSGVO

Der Ausdruck „Verletzung des Schutzes personenbezogener Daten" bezeichnet 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.

1. Wann muss eine Meldung nach Art. 33 DSGVO erfolgen?

Art. 4 Nr. 12 DSGVO Verletzung der Sicherheit

-> Art. 32 DSGVO Sicherheit der Verarbeitung

Art. 32 Abs. 1 DSGVO: Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

1. Wann muss eine Meldung nach Art. 33 DSGVO erfolgen?

Art. 33 Abs. 1 DSGVO

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 der betroffenen Personen führt.

1. Wann muss eine Meldung nach Art. 33 DSGVO erfolgen?

Risiko gem. ErwGr. 75 und 76 DSGVO

Ein Risiko im Sinne der DSGVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das **selbst** einen Schaden darstellt oder zu einem **weiteren Schaden** für eine oder mehrere natürliche Personen führen kann.

Es hat zwei Dimensionen:

- erstens die **Schwere des Schadens** und
- zweitens die **Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten**.

1. Wann muss eine Meldung nach Art. 33 DSGVO erfolgen?

Schaden – physisch, materiell oder immateriell

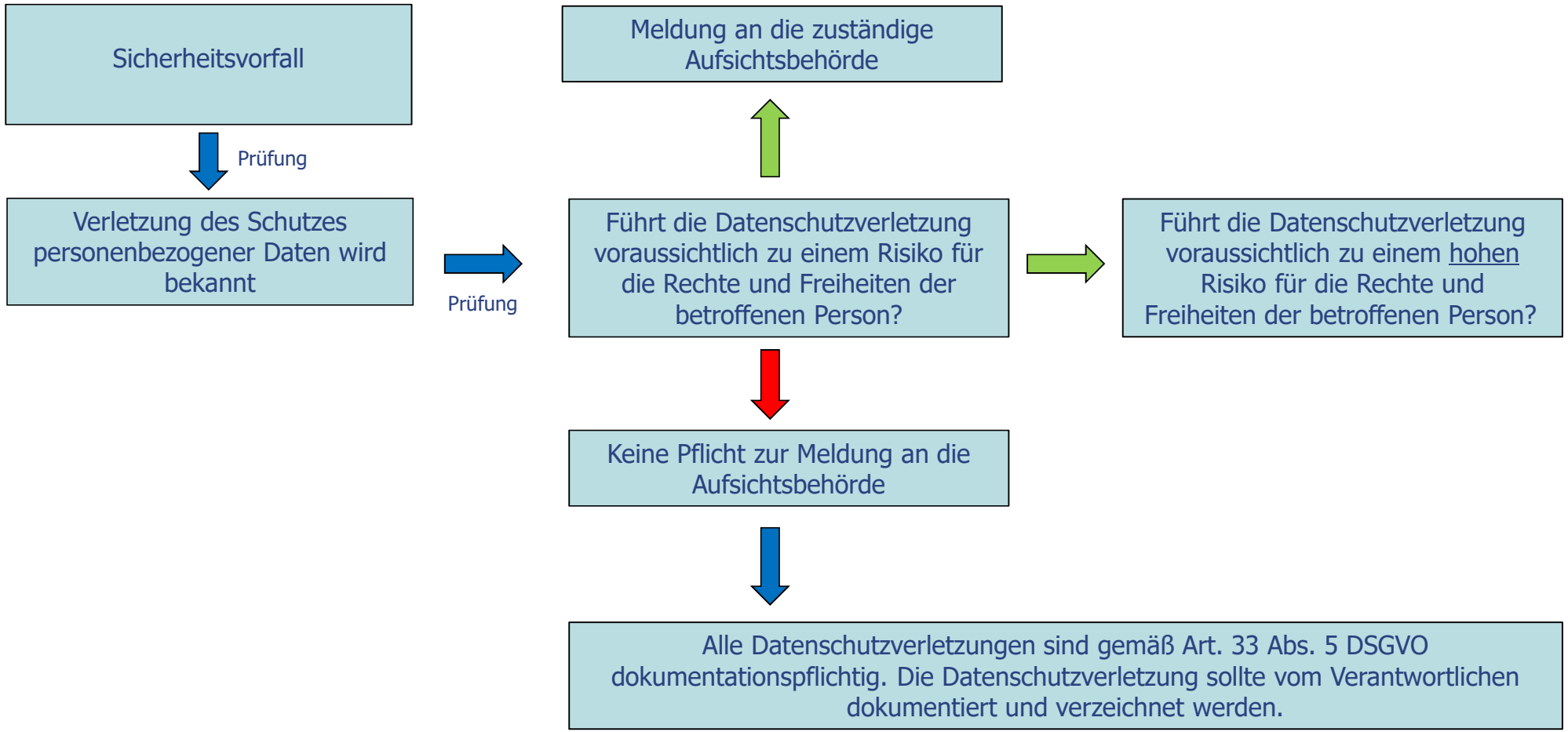
- finanzieller Verlust
- wirtschaftliche Nachteile
- Identitätsdiebstahl
- gesellschaftliche Nachteile
- Rufschädigung
- Diskriminierung

1. Wann muss eine Meldung nach Art. 33 DSGVO erfolgen?

Eintrittswahrscheinlichkeit

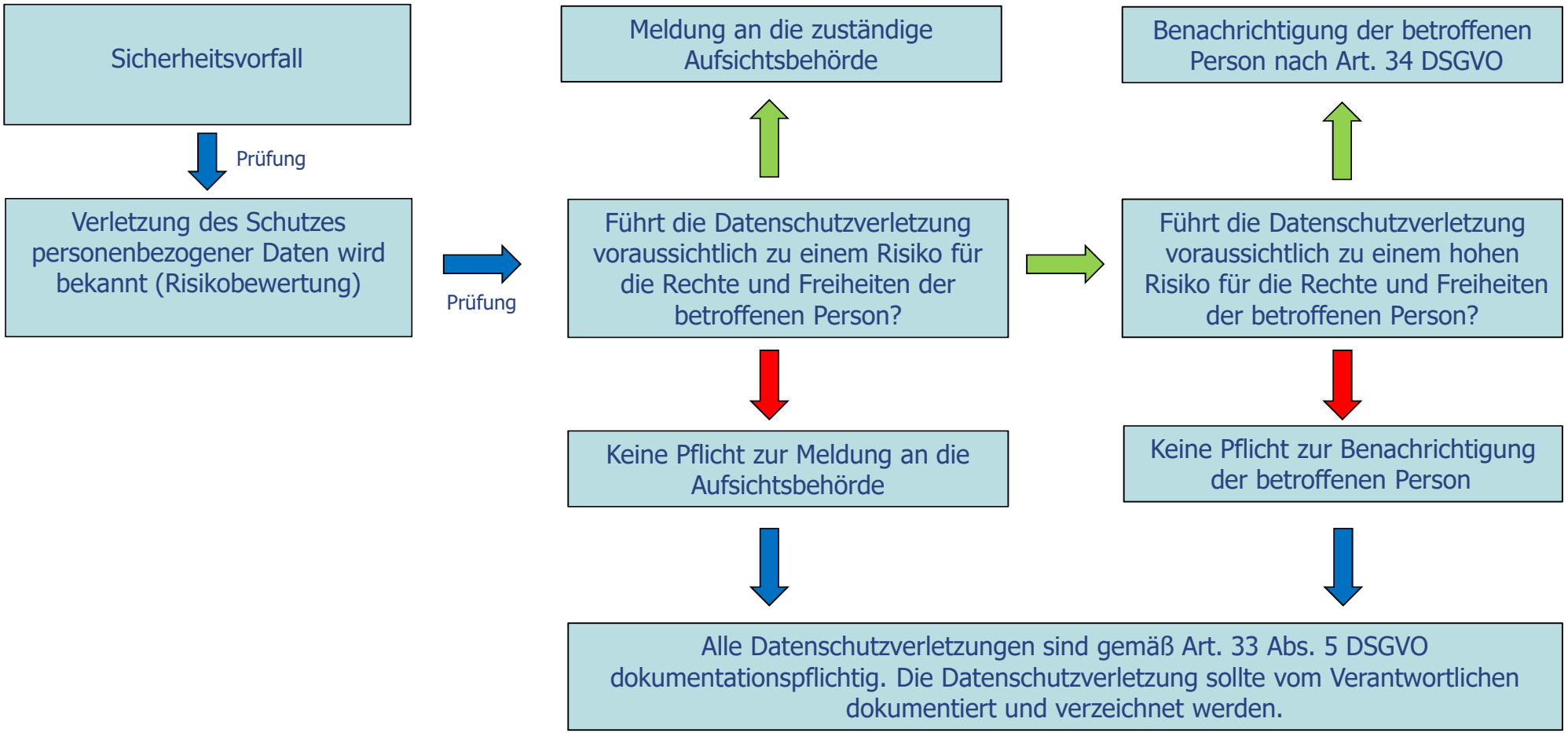
Die Eintrittswahrscheinlichkeit eines Risikos beschreibt, mit welcher Wahrscheinlichkeit ein bestimmtes Ereignis (das selbst auch ein Schaden sein kann) eintritt und mit welcher Wahrscheinlichkeit es zu Folgeschäden kommen kann.

Ablauf einer Meldung nach Art. 33 DSGVO



Pflicht zur Benachrichtigung gem. Art. 34 Abs. 1 Buchst. d DSGVO

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.


Sicherheitsvorfall
Prüfung
Verletzung des Schutzes personenbezogener Daten wird bekannt (Risikobewertung)
Prüfung
Führt die Datenschutzverletzung voraussichtlich zu einem Risiko für die Rechte und Freiheiten der betroffenen Person?
Meldung an die zuständige Aufsichtsbehörde
Keine Pflicht zur Meldung an die Aufsichtsbehörde
Führt die Datenschutzverletzung voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Person?
Benachrichtigung der betroffenen Person nach Art. 34 DSGVO
Keine Pflicht zur Benachrichtigung der betroffenen Person
Alle Datenschutzverletzungen sind gemäß Art. 33 Abs. 5 DSGVO dokumentationspflichtig. Die Datenschutzverletzung sollte vom Verantwortlichen dokumentiert und verzeichnet werden.

2. Wie erfolgt die Meldung nach Art. 33 DSGVO?

Gem. Art. 33 Abs. 3 DSGVO enthält die Meldung zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen

2. Wie erfolgt die Meldung nach Art. 33 DSGVO?

Gem. Art. 33 Abs. 3 DSGVO enthält die Meldung zumindest folgende Informationen:

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten

d) eine 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

3. Was passiert mit den Meldungen gem. Art. 33 DSGVO?

Die Aufsichtsbehörde muss in ihrem Hoheitsgebiet die Anwendung der DSGVO überwachen und durchsetzen (Art. 57 Abs. 1 Buchst. a DSGVO)

- Prüfung, ob die Meldung den Vorgaben des Art. 33 DSGVO entspricht

- Prüfung, ob die personenbezogenen Daten zum Zeitpunkt des Vorfalls in einer Weise verarbeitet wurden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistete (Art. 5 Abs. 1 Buchst. f DSGVO i.V.m. Art. 32 DSGVO).

3. Was passiert mit den Meldungen gem. Art. 33 DSGVO?

Sicherheit der Verarbeitung gem. Art. 32 Abs. 1 Buchst. d DSGVO

Die durch den Verantwortlichen zu treffenden technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, schließen unter anderem Folgendes ein:

- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

-> Welche Maßnahmen wurden ergriffen, um einen erneuten gleichartigen Vorfall zu verhindern?

4. Beispiele aus der Praxis

- vertauschte E-Mail-Anhänge
- vertauschte Postsendungen
- E-Mail-Versand cc statt bcc – „offener E-Mail-Verteiler“
- (Massen-)Fehldrucke durch Formatierungsfehler
- falsche Zugriffsberechtigungen in Dateisystemen
- Einbruchsdiebstahl von Papieren, Datenträgern, Computern
- missbrauchte (Online-)E-Mail-Konten
- unbefugter Zugriff auf E-Mail-Konten
- Angriff mit Ransomware („Verschlüsselungstrojaner“)

4. Beispiele aus der Praxis

Vertauschte E-Mail-Anhänge und vertauschte Postsendungen

- meist Einzelfälle
- Betroffene haben häufig bereits Kenntnis

- Typische Verbesserungsmaßnahme: Sensibilisierung+ Hinweis auf Kontrolle

4. Beispiele aus der Praxis

E-Mail-Versand cc statt bcc – „offener E-Mail-Verteiler"

- verschiedene Stufen, vom Einzelfall mit betrieblichen E-Mails bis hin zum Massenversand bei Kunden

- Typische Verbesserungsmaßnahmen:
  - konfigurative Änderungen in E-Mail-Clients/Servern
  - Nutzung von Verteilerlisten

4. Beispiele aus der Praxis

(Massen-)Fehldrucke durch Formatierungsfehler

z. B. doppelseitiger Druck statt einseitiger Druck von einseitigen Briefen

- Typische Verbesserungsmaßnahme:
  - Stichprobenkontrollen
  - Plausibilitätskontrollen
  - wenn möglich: konfigurative Anpassungen im Drucksystem

4. Beispiele aus der Praxis

falsche Zugriffsberechtigungen in Dateisystemen

- Folge: unbefugte Zugriffsmöglichkeiten für Dritte

- Typische Abhilfemaßnahmen:
  Zugriff sperren; Fehlerbeseitigung

- Typische Verbesserungsmaßnahmen:
  - Berechtigungskonzept haben und Umsetzung regelmäßig überprüfen
  - Wirksamkeit der Berechtigungsprüfung überprüfen
  - Datenbestände aufräumen; Archiv

Quelle: Open Clipart, https://openclipart.org/detail/288229/read-write-delete-crud

4. Beispiele aus der Praxis

- (Einbruchs-)Diebstahl von Papieren, Datenträgern, Computern

- Typische Verbesserungsmaßnahmen:
  - Einbruchsschutz
  - Verschluss von Unterlagen + Geräten
  - Verschlüsselung von Datenträgern/Laptops

Quelle: Open Clipart,
https://openclipart.org/detail/221843/crowbar
https://openclipart.org/detail/204662/digital-encryption-icon

4. Beispiele aus der Praxis

missbrauchte (Online-)E-Mail-Konten
unbefugter Zugriff auf (Online-)E-Mail-Konten

- Typische Analyse: Was ist genau passiert?
  - Missbrauch zum Spamversand?
  - Zugriff/Auslesen von Adressbüchern?
  - Zugriff/Auslesen von E-Mails?

- Typische Verbesserungsmaßnahmen:
  - Zwei-Faktor-Authentisierung
  - Einschränkungen auf Geräte/Netze

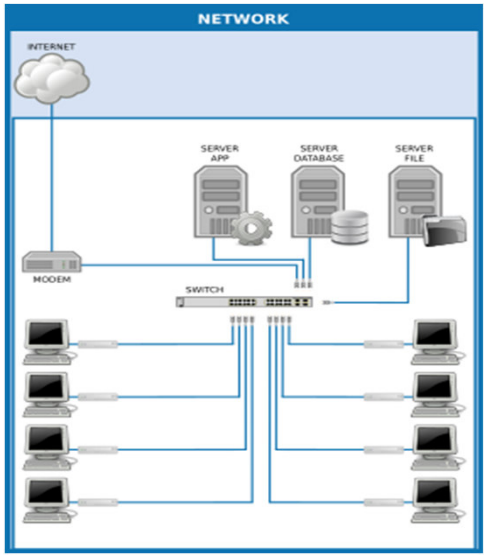
Quelle: Open Clipart, https://openclipart.org/detail/95077/spam-mail-to-trash

4. Beispiele aus der Praxis

Angriff mit Ransomware („Verschlüsselungstrojaner“)

- Typische Analyse: Was ist genau passiert?
  - Einfallstor bekannt?
  - Umfang: nur Verschlüsselung oder auch Datenabfluss?
  - Umfang: auch andere Systeme oder Netze kompromittiert?

  => forensische Analyse



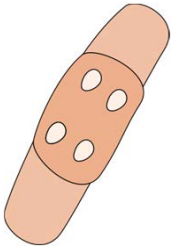
- Betroffenenrechte: auch hinsichtlich Verfügbarkeit!

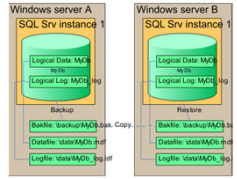
Quelle: Open Clipart,
https://openclipart.org/image/400px/36571
https://openclipart.org/detail/195971/network-rede

4. Beispiele aus der Praxis

Typische Verbesserungsmaßnahmen:

- aktuelle Software-/Hardwareversionen
- zeitnahes Einspielen von Sicherheitspatches
  - Patchprozesse prüfen
  - ggf. vertragliche Anpassungen bei Dienstleistungen
- Backup
  - separiert (Netz, Betriebssystem, Zeit)
  - ggf. extern





Quelle: Open Clipart,
https://openclipart.org/detail/196038/patch
https://openclipart.org/detail/16889/lto
https://openclipart.org/detail/19334/sql-backup

Zusammenfassung

1. Wann (unter welchen Voraussetzungen) muss eine Meldung nach Art. 33 DSGVO erfolgen?
2. Wie erfolgt eine Meldung nach Art. 33 DSGVO und was ist Inhalt der Meldung?
3. Was passiert nach Abgabe der Meldung?
4. Relevanz der Prüfung, ob eine Verletzung des Schutzes personenbezogener Daten vorliegt und ob diese Verletzung zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen führt
5. Anforderungen der Aufsichtsbehörde an die Meldung nach Art. 33 DSGVO
6. Beispiele aus der Praxis und Umgang mit Datenschutzverletzungen

Vertiefende Literatur

- Kurzpapier Nr. 18 der DSK „ Risiko für die Rechte und Freiheiten natürlicher Personen“
- EDSA: Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten
- EDSA: Guidelines 09/2022 on personal data breach notification under GDPR
- Webseite des ULD: www.datenschutzzentrum.de