Art. 33 und 34 DS-GVO

Wann was gemeldet werden muss...

Was ist eine „Datenschutzverletzung“?

Datenschutzverletzung im Sinne der DS-GVO bedeutet eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung von oder einem unbefugten Zugang zu personenbezogenen Daten führt. Somit handelt es sich um einen Verstoß gegen die IT-Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität.

Was sind hierfür typische Kategorien?

- Cyberattacken
- Ransomware
- Malware
- Verlust oder Diebstahl
- Software- oder Konfigurationsfehler
- Fehlversand

Welche Meldepflichten bestehen?

Art. 33 DS-GVO: Meldung bei der Aufsichtsbehörde, falls ein Risiko für die betroffene Person besteht
Art. 34 DS-GVO: Benachrichtigung der betroffenen Person, falls das Risiko für diese hoch ist

Wann muss gemeldet werden?

Die Aufsichtsbehörde ist innerhalb von 72 Stunden nach Kenntniserlangung zu informieren – die betroffenen Personen bei hohem Risiko unverzüglich.

Meldepflicht nach Art. 33 DS-GVO:

Kommt es in einer Organisation zu einer Datenschutzverletzung, bei der ein Risiko für die betroffenen Personen besteht, muss die zuständige Datenschutzaufsichtsbehörde innerhalb von 72 Stunden darüber informiert werden.

Versäumt ein Verantwortlicher diese Meldung oder reicht sie ohne triftigen Grund verspätet ein, so besteht wegen des Verstoßes gegen die Vorschriften der DS-GVO die Gefahr einer Geldbuße.

Über unser Online-Angebot können bayerische Verantwortliche aus dem nicht-öffentlichen Bereich Datenschutzverletzungen nach Art. 33 DS-GVO schnell und sicher melden, um so ihrer gesetzlichen Verpflichtung nachzukommen. Bei Nutzung des Online-Services erhält der Absender unmittelbar eine Meldebestätigung und kann diese als ersten Nachweis der fristgemäßen Meldung verwenden.

www.lda.bayern.de

HERAUSGEBER
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 18
91522 Ansbach

Bayerisches Landesamt für Datenschutzaufsicht

Datenschutzverletzung nach Art. 33 DS-GVO

Hinweise zum Umgang mit Sicherheitsvorfällen

Cyberattacken

SQL-Injection, XSS, Brute-Force, DDoS...

Was versteht man unter „Cyberattacke“?

Cyberattacken umfassen gezielte Angriffe, die über das Internet stattfinden. Dabei kann das Abgreifen von personenbezogenen Daten im Fokus stehen (z. B. Passwörter und Kundendaten aus einem Online Shop), aber auch reine Beeinträchtigungen bei einem Dienst an sich (z. B. DDoS-Attacke auf Server).

Ist eine Cyberattacke meldepflichtig?

Ja, in vielen Fällen – sofern personenbezogene Daten betroffen sind. Schließlich haben Cyberkriminelle in diesen Fällen ein Interesse, die gestohlenen Daten nach einem Angriff zu Geld zu machen, z. B. durch Erpressung, Betrug durch gestohlene digitale Identitäten oder Ausnutzen vertraulicher Informationen.

Tipps zur Reaktion:

- Befallene Systeme identifizieren und isolieren
- Einschaltung von Forensik-Spezialisten prüfen
- Strafanzeige stellen (ZAC Polizei)
- Manipulationen finden (Log-Analyse, Datenbank)
- Schadensausmaß feststellen (Risiko bestimmen)
- Schwachstelle/Lücke finden und Angriff stoppen
- Patch Management: Security Updates einspielen
- Veränderte Datensätze berichtigen (z. B. Backup)
- Penetrationstest durchführen

Ransomware

WannaCry, NotPetya, GandCrab, TeslaCrypt...

Was versteht man unter „Ransomware“?

Ransomware sind Programme, die Dateien verschlüsseln und somit unbrauchbar machen. Von ihren Opfern verlangen sie dann ein Lösegeld, um die verschlüsselten Dateien wieder freizugeben. Daher wird hierfür oft auch der Begriff Erpressungs- und Verschlüsselungstrojaner verwendet.

Ist ein Ransomware-Befall meldepflichtig?

Meistens. Durch die Folgen eines Ransomware-Angriff wird die Verfügbarkeit von Daten eingeschränkt. Der Ausfall des Systems bzw. von Dateien kann dann ein Risiko für betroffene Personen bedeuten, z. B. wenn wichtige Gesundheitsdaten nicht zur Behandlung eines Patienten zur Verfügung stehen.

Tipps zur Reaktion:

- Ausbreitung stoppen: Alle befallenen Systeme isolieren bzw. vom Netz nehmen
- Strafanzeige stellen (ZAC Polizei)
- Kein Lösegeld zahlen
- Nach Entschlüsselungswerkzeug suchen: **nomoreransom.org**
- Einfallstor finden, um eine erneute Infektion zu vermeiden

> mehr auf lda.bayern.de/schadcode

Malware

Spyware, Viren, Trojaner (u. a. Emotet)....

Was versteht man unter „Malware“?

Malware bezeichnet schädliche Programme, die sich weiter verbreiten wollen und dabei Daten im System ausspähen, manipulieren oder löschen. Der Trojaner „Emotet“ z. B. liest nach Infektion u. a. die vergangene E-Mail-Korrespondenz aus, welche später genutzt wird, um personalisierte Phishing-Angriffe zu starten.

Ist ein Malware-Befall meldepflichtig?

Teilweise – es kommt auf den konkreten Schädling an. Nicht jeder Virenbefall muss gemeldet werden. Sobald jedoch eine Malware personenbezogene Daten abgreift oder in einer Art und Weise beeinflusst, die ein Risiko für die betroffenen Personen darstellt, muss der Vorfall gemeldet werden.

Tipps zur Reaktion:

- Befallene Systeme identifizieren und isolieren
- Mit nachgeladenen Schadcode rechnen
- Strafanzeige stellen (ZAC Polizei)
- Schadensausmaß feststellen (Risiko bestimmen)
- Prüfen, welche (Zugangs-)daten betroffen sind
- Bei Emotet: Kommunikation mit betroffenen Personen nach Art. 34 DS-GVO führen
- Vollständige Security-Scans durchlaufen lassen
- Awareness-Schulung für Mitarbeiter durchführen