EDPS

DER
EUROPÄISCHE
DATENSCHUTZBEAUFTRAGTE

VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN KURZ ERKLÄRT

WAS IST EINE VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN?

Eine **Verletzung des Schutzes personenbezogener** Daten ist ein Sicherheitsvorfall, der unbeabsichtigt oder rechtswidrig zu Vernichtung, Verlust, Veränderung, oder unbefugter Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Nicht jeder Informationssicherheitsvorfall stellt eine Verletzung des Schutzes personenbezogener Daten dar, umgekehrt stellt jedoch jede Verletzung des Schutzes personenbezogener Daten einen Informationssicherheitsvorfall dar.

Verletzungen des Schutzes personenbezogener Daten können folgende Ursachen haben:

- menschliches Versagen, wenn Informationen per E-Mail der falschen Person übermittelt werden;
- Verlust oder Diebstahl von Geräten, die unverschlüsselte personenbezogene Daten enthalten;
- schwache Authentifizierungsmethoden, die einen unbefugten Zugriff auf Datenbanken ermöglichen.

WAS IST BEI EINER VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN ZU TUN?

- Ermitteln Sie den Vorfall, der zu einer Verletzung des Schutzes personenbezogener Daten geführt hat.
- Melden Sie die Verletzung dem Datenschutzbeauftragten (DSB); dies stellt eine **Verpflichtung** nach den Datenschutzvorschriften der EU dar.
- Befassen Sie sich **sofort** mit den Verletzungen des Schutzes personenbezogener Daten, um unmittelbare Risiken für personenbezogene Daten natürlicher Personen zu mindern.
- Dokumentieren Sie den Verstoß; dies entspricht dem Grundsatz der **Rechenschaftspflicht**.
- Beurteilen Sie die Auswirkungen der Verletzung des Schutzes personenbezogener Daten auf die Rechte und Freiheiten natürlicher Personen.
- Falls Sie **Auftragsverarbeiter** sind, müssen Sie sofort den **Verantwortlichen** Ihrer Organisation oder EU-Einrichtung benachrichtigen.
- Als ein Organ, eine Einrichtung oder sonstige Stelle der EU sind Sie verpflichtet, den Europäischen Datenschutzbeauftragten unverzüglich und nach Möglichkeit spätestens innerhalb von 72 Stunden nach dem Verstoß darüber in Kenntnis zu setzen.
- Teilen Sie den betroffenen Personen wenn nötig die Verletzung des Schutzes ihrer personenbezogenen Daten mit.
- Überprüfen Sie Ihre Verfahren und aktualisieren Sie Ihre Maßnahmen.

WELCHE ARTEN VON VERSTÖßE SIND MÖGLICH?

Verstoß gegen die Geheimhaltung: eine Einrichtung oder Person greift auf personenbezogene Daten zu, zu denen sie nicht berechtigt ist.

Verstoß in Bezug auf die Datenverfügbarkeit: Verlust des Zugangs zu oder der Kontrolle über ihre personenbezogenen Daten oder Löschung zweckentfremdeter personenbezogener Daten.

Verstoß gegen die Datenintegrität: jede zweckwidrige Änderung personenbezogener Daten.

WER SIND DIE BETEILIGTEN BEI EINER VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

- Die oberste Führungsebene (rechenschaftspflichtig)
- Die im Geschäftsbereich zuständige Person
- Der DSB
- Die IT-Abteilung (falls erforderlich)
- Die Verarbeiter (falls erforderlich)
- Das Kommunikationsteam (falls erforderlich)

WAS TUT EIN DSB?

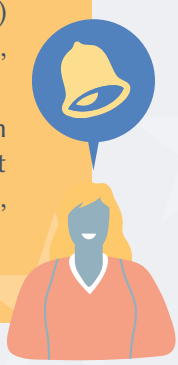
Ein DSB:

- berät bei der Beurteilung der Auswirkungen auf die betroffenen Personen und zur Notwendigkeit von Meldungen bei Verletzungen des Schutzes personenbezogener Daten (auf Antrag);
- empfiehlt Risikominderungsmaßnahmen;
- ist der Ansprechpartner für natürliche Personen;
- ist der Ansprechpartner für den EDSB;
- kommuniziert mit den Sicherheitsbeauftragten über das Risikomanagement im Bereich der Informationssicherheit und die Richtlinien in Bezug auf Datenschutzverletzungen;
- erstellt Sensibilisierungsprogramme für Mitarbeitende und führt diese durch.

WIE IST DEM EDSB EINE VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN ZU MELDEN?

Alle Organe, Einrichtungen oder sonstige Stellen der EU sind bei einer Verletzung des Schutzes personenbezogener Daten folgendermaßen zu benachrichtigen:

- über das spezielle Webformular, bei dem die Kommunikation verschlüsselt wird;
- so schnell wie möglich, spätestens innerhalb von 72 Stunden nach Entdeckung (sofern machbar) der Verletzung des Schutzes personenbezogener Daten. Falls Sie den Verstoß verspätet melden, sollten Sie den Grund dafür erläutern;
- Falls nicht alle Informationen über den Vorfall vorliegen, sollten Sie den Verstoß in mehreren Phasen melden. Dies bedeutet, dass eine Erstmeldung und eine erste Risikobewertung gesendet werden müssen. Anschließend müssen Sie so bald wie möglich weitere Informationen übermitteln, um Ihre erste Meldung zu ergänzen.



WANN IST EINE VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN NATÜRLICHEN PESONEN ZU MELDEN?

Die Benachrichtigung natürlicher Personen über eine Verletzung des Schutzes ihrer personenbezogenen Daten ist obligatorisch, wenn die Verletzung voraussichtlich **hohe Risiken für die Rechte und Freiheiten der von der Verletzung betroffenen Personen mit sich bringt.**

Es gibt jedoch einige Ausnahmen, z. B.:

- wenn in Bezug auf die von der Verletzung betroffenen Daten bereits technische oder organisatorische Maßnahmen ergriffen wurden, wie z. B. eine Verschlüsselung;
- wenn anschließend Maßnahmen ergriffen wurden, um sicherzustellen, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen keine Bedrohung mehr darstellt.

WIE IST NATÜRLICHEN PERSONEN EINE VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN ZU MELDEN?

- In deutlicher und einfacher Sprache, vorzugsweise in schriftlicher Form, sowie durch Vermeidung technischer Begriffe, die den Einzelnen verwirren.
- Durch Beschreibung des Vorfalls und Erläuterung, was geschehen ist und warum, außerdem wie die personenbezogenen Daten kompromittiert wurden und welche Folgen dies hat.
- Durch Mitteilung der Kontaktdaten Ihres Datenschutzbeauftragten und der Maßnahmen, die Sie als Verantwortlicher ergriffen haben, um gegen die Verletzung des Schutzes personenbezogener Daten vorzugehen.
- Gegebenenfalls indem den Personen Maßnahmen zu ihrem Schutz vorgeschlagen werden (z. B. wenn Passwörter gestohlen wurden, durch die Empfehlung, die Passwörter zu ändern, wenn sie dieselben Passwörter für andere Websites verwenden).

Falls die Mitteilung dieses Verstoßes mit einem unverhältnismäßigen Aufwand verbunden ist, ist eine öffentliche Kommunikation oder eine ähnliche Maßnahme möglich, die jedoch sicherstellen muss, dass die betroffenen Personen gleichermaßen wirksam informiert werden.

HANDELN SIE PROAKTIV, UM VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN SO WEIT WIE MÖGLICH ZU VERMEIDEN!

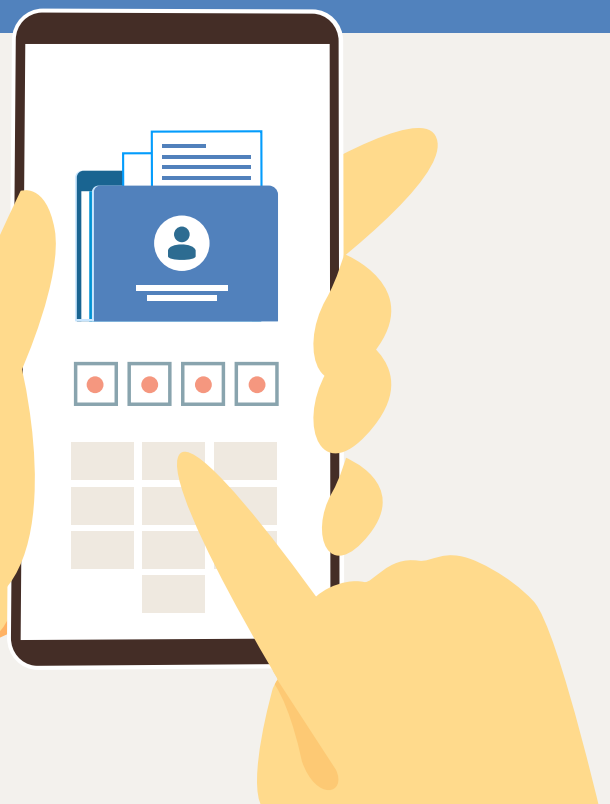
Um das Potenzial für Verletzungen des Schutzes personenbezogener Daten zu minimieren, empfiehlt der EDSB, in Ihrer Organisation eine Kultur des Datenschutzes, einschließlich der Datensicherheit zu schaffen. Mit anderen Worten: Gestalten Sie Ihre Datenverarbeitungsvorgänge so um, dass dabei Sicherheitsüberlegungen standardmäßig im Mittelpunkt stehen. Vor allem sollten diese Überlegungen Folgendes umfassen:

- eine E-Mail-Strategie und Schulung des Personals für die sorgfältige Nutzung von E-Mails;
- die Verwendung sicherer Passwörter und eines zweiten Authentifizierungsfaktors;
- Sicherungskopien Ihrer Systeme;
- regelmäßige und obligatorische Systemaktualisierungen;
- Vermeidung der Exposition Ihrer Dienste im Internet;
- die Verschlüsselung Ihrer Geräte.

FALLS SIE ZWEIFEL HABEN, WENDEN SIE SICH BITTE AN UNS!

Weitere Informationen:

- Schauen Sie sich unser Informationsvideo zur Verletzung des Schutzes personenbezogener Daten an;
- Rufen Sie die Webseite des EDSB über die Verletzung des Schutzes personenbezogener Daten auf;
- Lesen Sie die Leitlinien des EDPS zur Meldung von Verletzungen des Schutzes personenbezogener Daten.



edps.europa.eu

@EU_EDPS

EDPS

European Data Protection Supervisor

QT-02-21-587-DE-N ISBN: 978-92-9242-691-0 DOI: 10.2804/405048