

Datenschutzpannen erkennen und handeln - Formen, Präventionsmaßnahmen und Beispiel eines funktionierenden Incident-Managements

DHBW - Ringvorlesung Cyber-Security
24.11.2025
Astrid Ernst | Lehrbeauftragte



ASTRID ERNST



- ❖ Ich bin gebürtige Bremerin, 59 Jahre alt,
- ❖ habe eine Familie mit 3 Männer,
- ❖ habe auch bei der DHBW studiert,
(einst staatliche BA),
- ❖ war fast 40 Jahre bei Mercedes-Benz
beschäftigt mit u.a. den Hauptthemen
 - Produktmanagement
Mercedes-Zubehör,
 - Produktmanagement, Key-Accounting, Marketing für gepanzerte Fahrzeuge (Mercedes-Benz Guard),
 - Mercedes-Benz Driving Academy
(Fahrsschule bei Mercedes-Benz) und Verkehrserziehungsprogramm für Jugendliche – RoadSense,
 - Eventmanagement Circle of Excellence zur Betreuung VIPs,
 - Verantwortung Website Mercedes-benz.com
 - Datenschutz – LCO ,
(Local Compliance Officer) für CEO-Bereich Digitalization&Marketing.

Agenda

-
- 01** Risiken bei Datenschutzverstößen
 - 02** Informationssicherheit - Datensicherheit - Datenschutz
 - 03** Kurzüberblick in geplante Datenschutz-Erliechterung
 - 04** Datenschutzpannen – Definition – Auslöser - Ursachen
 - 05** Datenschutz-incidentmanagement und Relevanz von TOMs
 - 06** Quiz
-

Jedes Jahr im Dezember passiert es wieder.

Welche Datenschutzpanne ist ein Klassiker?



MoD fined after email blunder risked Afghan interpreters' lives

13 December 2023

Share Save

Liv McMahon & Chris Vallance
Technology reporters



British troops in Afghanistan in 2008

The Ministry of Defence (MoD) has been fined £350,000 over an email blunder that exposed details of interpreters fleeing Afghanistan.

HUNDERTE ADRESSEN IM VERTEILER**Hunderte Adressen im Verteiler: Merseburger muss für Wut-Mails über 2.000 Euro zahlen**

Von Undine Freyberg 13.02.2019, 10:57

Merseburg/Magdeburg Ein theoretischer Verteiler ist eine eingehaltene Landesbeauftragte gezeigt, was passiert gesetzlichen Vorgaben. Zwischen dem 10. August und dem 9. September seien bis zu 187 Personenbezogene Mail-Adressen für jedermann im Verteiler offen einsehbar gewesen. Bei den Mails handelte es sich um Beschwerden, Stellungnahmen, Verunglimpfungen aber auch Strafanzeigen gegen die unterschiedlichsten Vertreter aus Wirtschaft, Presse, Kommunal- und Landespolitik. Der Inhalt der Mails war aber nicht Grund für die Geldbuße.

Gegen einen Merseburger Grund sind eklatante Strafverordnungen und Verfahrens tragen

-Anzeige-

Merseburger verschickte Verunglimpfungen oder Strafanzeigen an Hunderte Adressen**Merseburger empfindliche**

„Der Mann hat sich uns gegenüber immer wieder auf die Meinungsfreiheit berufen, aber diese gestattet keine solchen offenen Verteiler“, sagte der oberste Landesdatenschützer, Harald von Bose, der Mitteldeutschen Zeitung. „Der Grund ist, dass dadurch ja Rechte Dritter berührt werden. Wir waren in dieser Sache sehr akribisch, haben jeden einzelnen Verstoß sehr genau aufgelistet, um das Ganze auch gerichtsfest zu machen, falls das nötig werden sollte.“

Mann bezahlt Bußgeld - verstößt aber weiter gegen Datenschutz

Die Mitteilung über die Geldbuße war am 5. Februar zugestellt worden. Am 6. Februar hatte der Betroffene bezahlt. Von Bose: „Allerdings ist die zweiwöchige Einspruchfrist noch nicht abgelaufen. Da könnte also noch etwas kommen.“ Was passiert, wenn der Mann wieder gegen die Datenschutzrichtlinien verstößt? „Das hat er ja schon getan. Deshalb könnte es neue Bußgeldbescheide geben“, so von Bose.

Quelle

Man warf dem Mann im Sommer 2018 zehn Verstöße und 153 personenbezogene E-Mails im Schreiben des Landesbeauftragten vor.

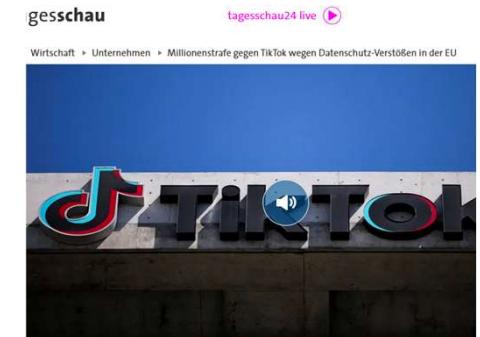
Datenschutzverstöße können teuer werden

- Unzureichende Schutzmaßnahmen
- Fehlende Rechtsgrundlage
- Rechtswidrige Übermittlung von Daten an Dritte oder in Drittstaaten
- Verarbeitung von Daten Minderjähriger
- Säumnis der Informationspflichten

....und und und.....

- Bußgelder bis zu 20 Mio EUR oder 4% des Vorjahresumsatzvolumens

<https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank/>



FAQ Maßnahme gegen TikTok
530 Millionen Euro Strafe wegen Datenschutz-Verstößen
Stand: 02.05.2025 12:43 Uhr
TikTok soll wegen Verstößen gegen den europäischen Datenschutz mehr als eine halbe Milliarde Euro zahlen. Es ist nicht die erste Strafe. Worum es diesmal geht – und was China damit zu tun hat.





Geldbußen für Datenschutzverstöße

<https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank/>

DSGVO - PORTAL
© Compliance Essentials

NEWS BUSSGELDER + URTEILE SICHERHEITSVORFÄLLE RECHTSTEXTE + DATENSCHUTZBEAUFTRAGTER

Geldbußen für DSGVO-Verstöße
und für Verletzungen anderer Datenschutzgesetze

Nach Land filtern Suchen

Datum	€ Bußgeld	Empfänger	Land	Vergehen
24.07.2019	4.536.999.350 €	Facebook, Inc.	US	Verstoß gegen frühere FTC-Datenschutzanordnungen und FTC-Gesetz »Details
22.05.2023	1.200.000.000 €	Meta Platforms Ireland Limited	IE	Rechtswidrige Übermittlung personenbezogener Facebook-Daten an die USA. »Details
21.07.2022	1.165.011.903 €	DiDi	CN	Verstöße gegen Gesetze zur Netzwerksicherheit, Datensicherheit und zum Schutz persönlicher Informationen. »Details
30.07.2021	746.000.000 €	Amazon Europe Core S.à.r.l.	LU	Verstöße im Zusammenhang mit der Anzeige von Werbung und der Weitergabe von Daten an Dritte. »Details
02.05.2025	530.000.000 €	TikTok Technology Limited	IE	Unzureichender Datenschutz bei Übermittlung nach China, mangelnde Transparenz während der Untersuchungen. »Details



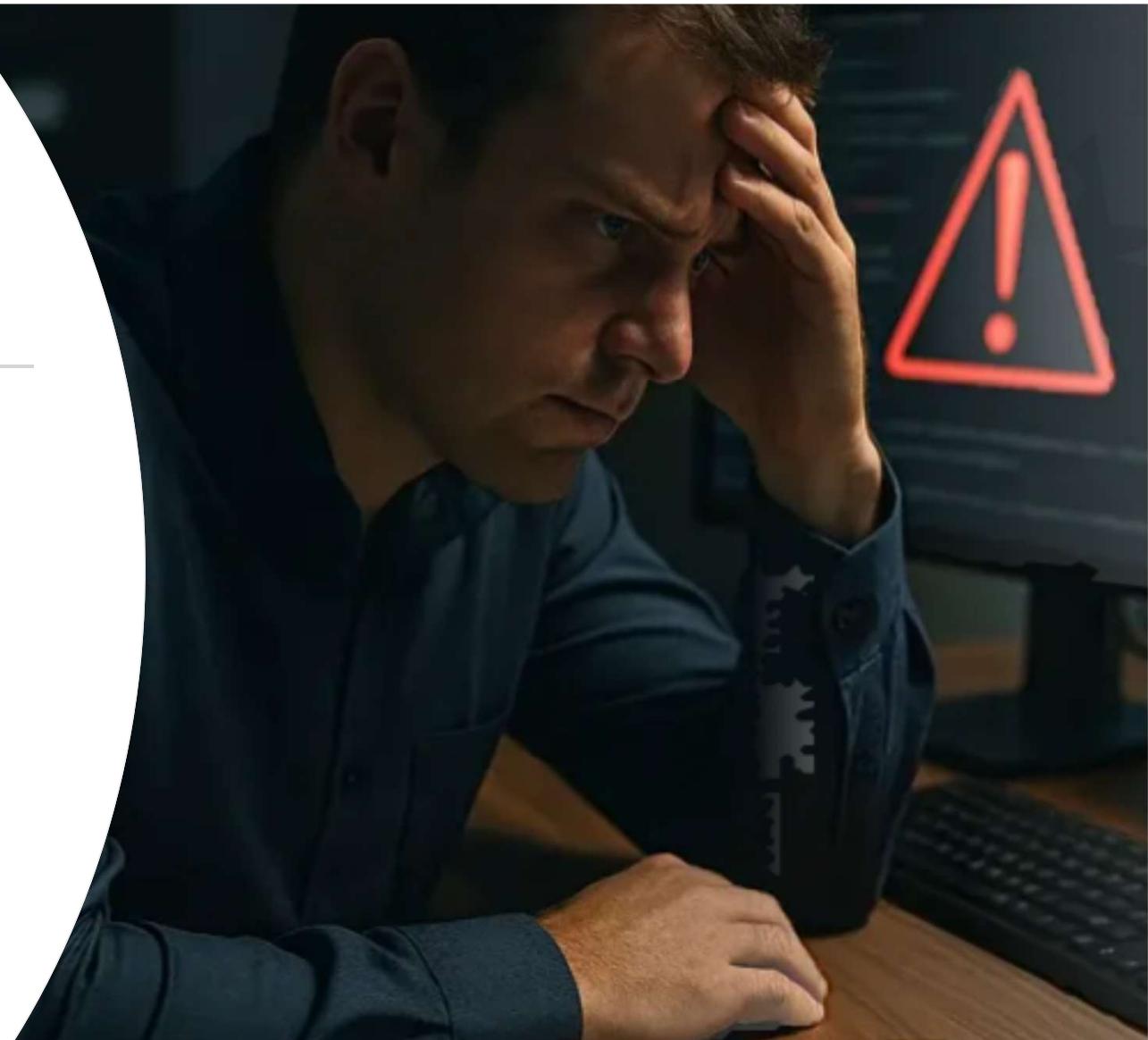
Folgen fürs Unternehmen

- Bußgelder bis 20 Mio. € oder 4 % Umsatz
- Imageverlust und Vertrauensschaden
- Kundenabwanderung
- Interne Kosten für Aufklärung und Forensik
- Demotivation und Verängstigung der Belegschaft



Mögliche Folgen für Betroffene

- Identitätsdiebstahl
- Finanzieller Schaden
- Diskriminierung
- Verlust der Privatsphäre
- Psychische Belastung durch Kontrollverlust
- Beschwerden oder Klagen gegen Verantwortliche



Informationssicherheit ist ein großer Begriff

Der Schutz aller geschäftlichen Informationen und Daten mit Unternehmenswert beruht auf drei Säulen „Vertraulichkeit“, „Integrität“, „Verfügbarkeit“ CIA-Triade (Confidentiality, Integrity, Availability)



Einfache Abgrenzung - grober Überblick

Begriff	Fokus	Was wird geschützt?	Bezug zu IT	Rechtsrahmen	Beispiele
Informations-sicherheit	Ganzheitlicher Schutz von Information	Alle Informationen	nicht zwingend IT	ISO 27001, BSI-Standards	Zutrittskontrolle, Notfallkonzepte
IT-Sicherheit	Schutz der Technik & IT-Systeme	Hardware, Software, Netzwerke	rein IT	IT-SiG, NIST, ISO 27002	Firewall, Antivirus, Patching
Datensicherheit	Schutz der Datenqualität & -verfügbarkeit	Alle Daten	meist IT, aber auch analog	DSGVO Art. 32, ISO 27002	Backup, Verschlüsselung, feuerfester Aktenschrank
Datenschutz	Schutz personenbezogener Daten & Rechte	Daten von natürlichen Personen	IT ist nur ein Teil	DSGVO, BDSG	Einwilligung, Löschkonzept, Datenschutzfolgeabschätzung

Warum ist Datenschutz wichtig?



Schutz der
Persönlichkeitsrechte



Schutz vor Missbrauch
sensibler Informationen



Vertrauen in digitale Prozesse
und Produkte



Wirtschaftliche Stabilität von
Unternehmen

Was sind personenbezogene Daten?



Was sind personenbezogene und -beziehbare Daten

Art. 4 (1), DSGVO

Informationen, die eine Person identifizieren oder identifizierbar machen

- Beispiele: Name, Adresse, Geburtsdatum, E-Mail, IP-Adresse
- Kombination scheinbar harmloser Daten kann Personenbezug herstellen
- Besonders sensibel: Gesundheits-, Religions- oder Standortdaten (Artikel 9)
- Auch Video- und Audiodaten gelten als personenbezogen



Datenschutzprinzipien der DSGVO



Art. 24 und 32 DSGVO – Sicherheit der Verarbeitung



Rechenschaftspflicht:
Verantwortliche müssen geeignete **technische und organisatorische Maßnahmen umsetzen**, deren Wirksamkeit nachweisen (Dokumentationspflicht) können und sie bei Bedarf **regelmäßig überprüfen und aktualisieren**.



Risikobasierter Ansatz:
Technische und organisatorische Maßnahmen müssen dem **Risiko für Rechte und Freiheiten natürlicher Personen angemessen** sein (unter Berücksichtigung von Technikstand, Kosten, Art und Umfang der Verarbeitung).



Schutzmaßnahmen:
Einsatz u. a. von Pseudonymisierung/ Verschlüsselung, Sicherstellung von **Vertraulichkeit, Integrität, Verfügbarkeit** und Belastbarkeit der Systeme sowie Verfahren zur **regelmäßigen Wirksamkeitsprüfung**.



Notfallfähigkeit:
Schnelle **Wiederherstellung** von **Daten** und **Systemzugängen** bei technischen oder physischen Zwischenfällen.



Risikoarten:
Berücksichtigung von Risiken wie unbeabsichtigter/ unerlaubter **Vernichtung, Verlust, Veränderung, Offenlegung oder Zugriff** auf personenbezogene Daten.



Verantwortlichkeiten:
Verarbeitung personenbezogener Daten durch **Mitarbeitende nur auf Anweisung**; Nachweis der Maßnahmen möglich durch anerkannte Verhaltensregeln oder Zertifizierungen.

Datenschutzmodell 3.1 - 7 Gewährleistungsziele



Quelle

Absichten zur aktuell geplanten Datenschutz-Erleichterung

	1. Weniger Bürokratie für Klein- und Mittelständer Vereinfachte Dokumentations- und Nachweispflichten Fokus auf risikoreiche Datenverarbeitungen		2. Klare Rechtsgrundlage „Berechtigtes Interesse“ Einheitlichere Auslegung EU-weit Mehr Handlungsspielraum ohne zusätzliche Einwilligungen auch bei Cookie-Bannern		3. Zentralisierung der Datenschutzaufsicht Eine bundesweite Stelle statt vieler Landesbehörden Einheitlichere Entscheidungen und schnellere Verfahren		4. Realistischere Meldefristen bei Datenpannen Fristbeginn erst nach tatsächlicher Bewertung der Panne Reduzierung unnötiger Frühmeldungen		5. Praxisgerechte Regeln für KI & Big Data Vereinfachte Nutzung anonymisierter oder synthetischer Daten Anpassung der DSGVO an technologische Entwicklungen		6. Stärkere EU-Koordination („One-Stop-Shop“) Einheitliche Verfahren bei grenzüberschreitenden Fällen Schnellere und konsistente Behördenentscheidungen
-----------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------

Ziel der Vereinfachung.

Ziel: Effizienterer Datenschutz, nicht mehr Bürokratie



EU-weit einheitlichere
Verfahren → weniger
Abstimmungsverluste
zwischen Behörden



Zentralisierung &
Digitalisierung der Aufsicht →
schnellere Entscheidungen
und klarere Zuständigkeiten



Planbare Reaktionszeiten →
Unternehmen wissen früher,
woran sie sind



Weniger Verwaltungsstau
durch Standardisierung und
KI-gestützte Prüfroutinen



Rechtssicherheit durch
Geschwindigkeit:
Entscheidungen in Wochen
statt Monaten



Kerngedanke – Schnelligkeit
soll Unsicherheit reduzieren,
aber **nicht den Datenschutz
schwächen!**

!!! Kritische Würdigung zur geplanten Neuauslegung der DSGVO von Max Schrems bereits gegeben:
<https://noyb.eu/de/digital-omnibus-eu-commission-wants-wreck-core-gdpr-principles>

Wann spricht man von einer Datenschutzpanne?

Definition (Art. 4 Nr. 12 DSGVO):

Eine Datenschutzpanne liegt vor, wenn es zu einer **Verletzung der Sicherheit personenbezogener Daten** kommt,

die **versehentlich oder unrechtmäßig** zur

**Vernichtung, Verlust, Veränderung,
unbefugten Offenlegung oder unbefugtem Zugriff** führt.



Einfallstore für Datenpannen

Datenschutzpannen entstehen dort, wo **Mensch, Technik oder Organisation** versagen.



Menschliche Ursachen

- Fehlbedienung/unvorsichtiger **Umgang**, freigeben oder löschen von Daten
- **Datenmissbrauch** bewusste oder unbewusste Weitergabe von Daten an Intern oder Externe
- **Geringe Awareness** oder keine klare **Meldeschwelle**



Technische Ursachen

- **Veraltete Systeme**, fehlende/fehlgeschlagene Sicherheits-Updates
- **Ausfälle** können zu Beschädigungen oder Verlusten führen
- **Fehlkonfigurationen** in Anwendungen oder Schnittstellen
- **Schatten-IT** oder unsichere Tools im Einsatz



Organisatorische Schwächen

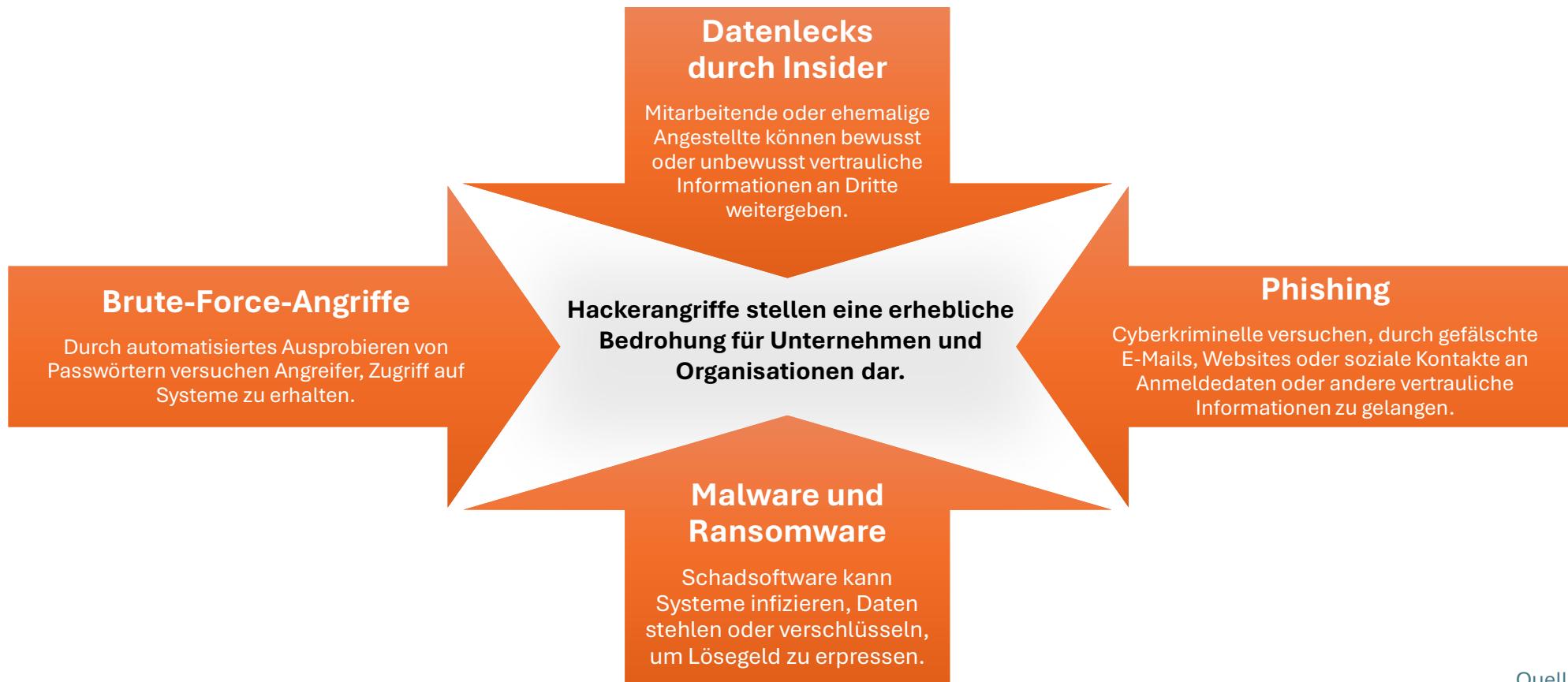
- **Unklare Verantwortlichkeiten**
- **Fehlende Prozesse** für Erkennung und Meldung
- **Keine dokumentierten Abläufe** oder Reaktionspläne

Anzeichen und Verdachtsgeschehen für Datenpannen



- **Unberechtigter Zugriff** auf personenbezogene Informationen
- **Unbeabsichtigte Offenlegung, Veränderung oder Verlust** von Daten
- **Diebstahl oder Verlust von Datenträger** (z. B. Akten, USB-Sticks, Laptop, Smartphone)

Cyberangriffe



Quelle



Phishing/Social Engineering

Manipulation von Menschen

Social Engineering umfasst Techniken, bei denen Personen gezielt manipuliert werden, um vertrauliche Informationen preiszugeben.

Phishing-Angriffe

Ein typisches Beispiel ist Phishing, bei dem z.B. täuschend ähnliche Email-Adressen verwendet werden um damit das Vertrauen und die Preisgabe von Daten und Informationen zu erlangen.

Psychologische Tricks

Angreifer nutzen psychologische Tricks, um das Vertrauen von Opfern zu gewinnen und Zugang zu sensiblen Daten zu erhalten.



Quelle

Ransomware

Verschlüsselung von Daten

Ransomware verschlüsselt Dateien auf Computern und verhindert die Integrität und Verfügbarkeit, also den Zugriff, auf wichtige Daten, bis ein Lösegeld gezahlt wird.

Verbreitungswege

Schadsoftware gelangt häufig durch infizierte E-Mail-Anhänge oder schadhafte Webseiten auf Computer.

Bekannte Vorfälle

Weltweit führten bedeutende Ransomware-Angriffe wie WannaCry und Emotet zu erheblichen Schäden und brachten zahlreiche Computersysteme zum Stillstand.

Arten von Malware



Computerviren
und Würmer



Trojaner



Spyware



Ransomware



Keylogger



Bots



Rootkits



Adware

WannaCry | Ein Cyberangriff, der die Welt lahmlegte

Was ist WannaCry?

- **Wurm** – Verschlüsselt Dateien auf infizierten Rechnern und verlangt Lösegeld in Bitcoin.
- Einer der größten globalen Cyberangriffe aller Zeiten; zeigte Verwundbarkeit staatlicher und privater IT-Infrastrukturen.

* Wirkung & Funktionsweise

1. **Ausgenutzte Schwachstelle:** WannaCry nutzte die bekannte Windows-Sicherheitslücke *EternalBlue*, die vielerorts trotz verfügbarem Patch ungeschlossen war.
2. **Startmechanismus:** Der zugrundeliegende NSA-Exploit wurde von Hackergruppen veröffentlicht und ermöglichte die automatisierte Infektion.
3. **Funktionsweise:** Nach Eindringen in ein System verschlüsselt die Ransomware Dateien und fordert Lösegeld in Bitcoin.
4. **Selbstständige Verbreitung:** WannaCry verbreitete sich wie ein Wurm über Netzwerkfreigaben und infizierte weitere ungepatchte Systeme ohne Nutzerinteraktion.
5. **Wirkung:** Innerhalb weniger Stunden wurden weltweit tausende Rechner lahmgelegt – darunter Krankenhäuser, Unternehmen, Verkehrssysteme und Behörden.

⚠ Folgen und weitere Potenziale

- > 200.000 betroffene Systeme in rund 150 Ländern.
- Aufdeckung massiver Sicherheitsdefizite: fehlende Updates, veraltete Systeme (z. B. Windows XP).
- Zeigte, wie einfach sich Schadsoftware in schlecht abgesicherten Netzwerken ausbreiten kann.

WannaCry selbst ist heute weitgehend entschärft, kann aber noch Wirkung haben bei unsicheren und veralteten Protokollen, die bis heute noch in Systemen existieren.

Aber Angriffsmuster wie WannaCry (Ransomware-Würmer, die Schwachstellen automatisiert ausnutzen) sind weiterhin möglich und stellen nach wie vor ein erhebliches Risiko dar.

Emotet | Eine der gefährlichsten Malware der Welt



Was ist Emotet?

- **Hochmodulare Malware** – früher Banktrojaner, heute „Türöffner“ für weitere Angriffe
- Verbreitet sich über **täuschend echte Spam-Mails** mit infizierten Anhängen oder Links

★ Wirkung & Funktionsweise

1. **Infektion:** Öffnen von infizierten Anhängen lädt Schadsoftware nach
2. **Einnistung:** Sammelt E-Mail-Adressen, Passwörter & Zugangsdaten
3. **Nachladen:** Installiert weitere Malware (z. B. Ransomware, Banking-Trojaner)
4. **Verbreitung:** Breitet sich selbstständig im Netzwerk und an Kontakte aus

⚠ Gefahren & Folgen

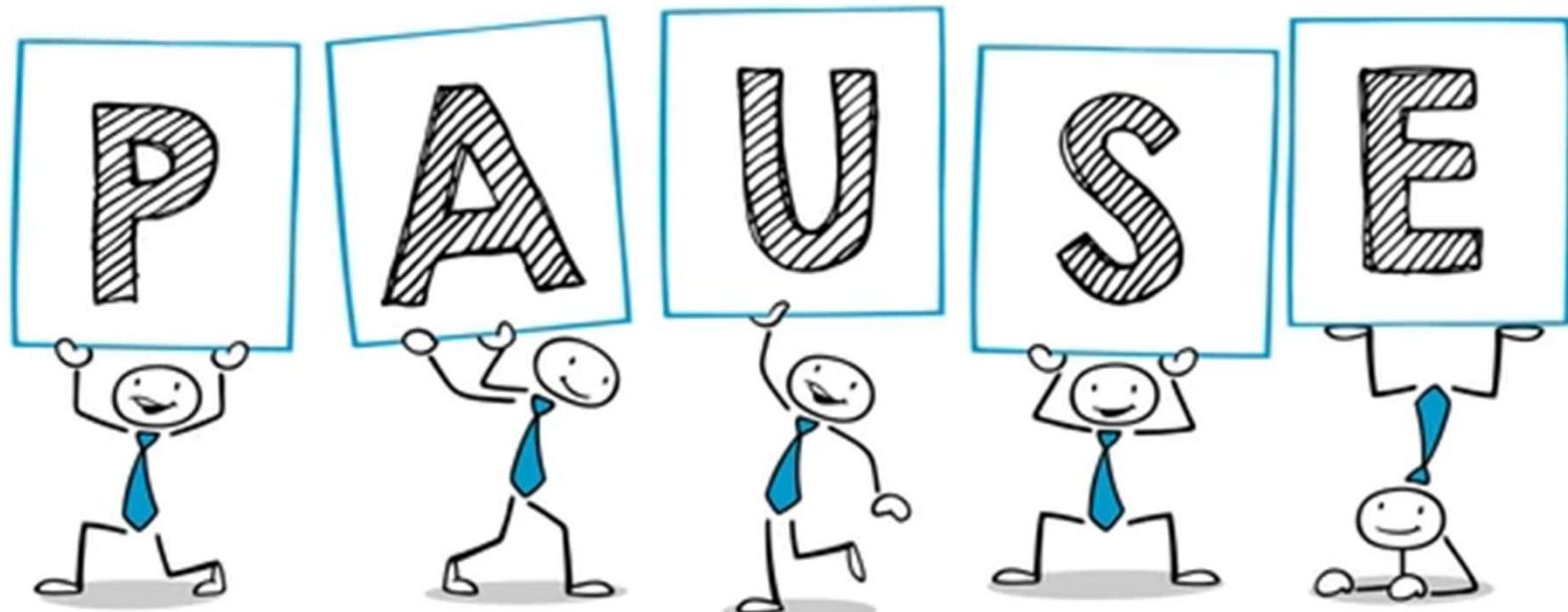
- Verschlüsselung & Erpressung (Ransomware, z. B. Ryuk)
- Daten- und Identitätsdiebstahl
- Komplette Systemübernahme durch Angreifer
- Missbrauch eigener E-Mail-Adressen → Reputationsschaden

Die Folgen einer Emotet-Infektion sind gravierend und führen oft zum vollständigen Systemausfall oder Datenverlust.





Überlege Dir klassische
Datenschutzpannen und
mögliche Auslöser.
Wir sprechen nach der Pause darüber



10 Minuten



Nenne klassische
Datenschutzpannen und
mögliche Auslöser.

Verletzung der Schutzziele

Schutzziel	Bedeutung	Typische Ursache / Beispiel
Vertraulichkeit	Nur Berechtigte dürfen Daten einsehen.	Fehlversand einer E-Mail, Hackerangriff, falsche Zugriffsrechte
Integrität	Daten müssen vollständig und unverändert bleiben.	Softwarefehler, Manipulation, fehlerhafte Systemupdates
Verfügbarkeit	Daten müssen bei Bedarf zugänglich und nutzbar sein.	Datenverlust durch Hardwaredefekt, Diebstahl, fehlendes Backup



Beispiele aus der Praxis:

- Montag, 9:30 Uhr: Der Marketing-Mitarbeiter gibt Kundendaten (B) in ChatGPT ein, um eine Zielgruppen-Analyse zu erstellen.
- Dienstag, 14:15 Uhr: Die Personalabteilung lässt sich von Co-Pilot ein Stelleninserat formulieren - inklusive spezifischer Anforderungen des Unternehmens.
- Mittwoch, 11:00 Uhr: Der Vertrieb erstellt GEMINI-generierte Angebote mit echten Kundennamen (B).

Typische Problemfelder der Daten:

- Unbewusste Übermittlung personenbezogener Daten
- Weitergabe interner Geschäftsinformationen
- Unsicherheit bei der Nutzung der KI-Ergebnisse (Richtigkeit, Diskriminierung)

Wer ist verantwortlich?

- Das Unternehmen bleibt für alle eingegebenen Daten datenschutzrechtlich verantwortlich, auch ohne expliziten KI-Einsatz.
- OpenAI wäre theoretisch Auftragsverarbeiter – praktisch fehlt meist der Vertrag.
→ Risiko: Unternehmen haftet für DSGVO-Verstöße, selbst bei unbemerkt Nutzung.

KI-Beispiel aus der Praxis:

Risiken und Datenschutz-Fallstricke

- **Datenschutzverletzung:** Personenbezogene Daten (Kundennamen, Firmendaten) werden an einen externen Anbieter übermittelt – fehlende Rechtsgrundlage.
- **Fehlerhafte oder rechtlich problematische KI-Texte:** Haftungsrisiko gegenüber B liegt beim Unternehmen.
- **Informationspflichten:** Kunden/Betroffene müssen darüber informieren, dass deren Daten möglicherweise in KI-Systemen verarbeitet werden.
- **Betroffenenrechte** kaum erfüllbar

! **Komplettes KI-Verbot würde die Beschäftigten frustrieren und die Produktivität senken.
Zudem nutzen viele Mitarbeiter KI-Tools heimlich weiter - dann gibt es erst recht keine Kontrolle.**

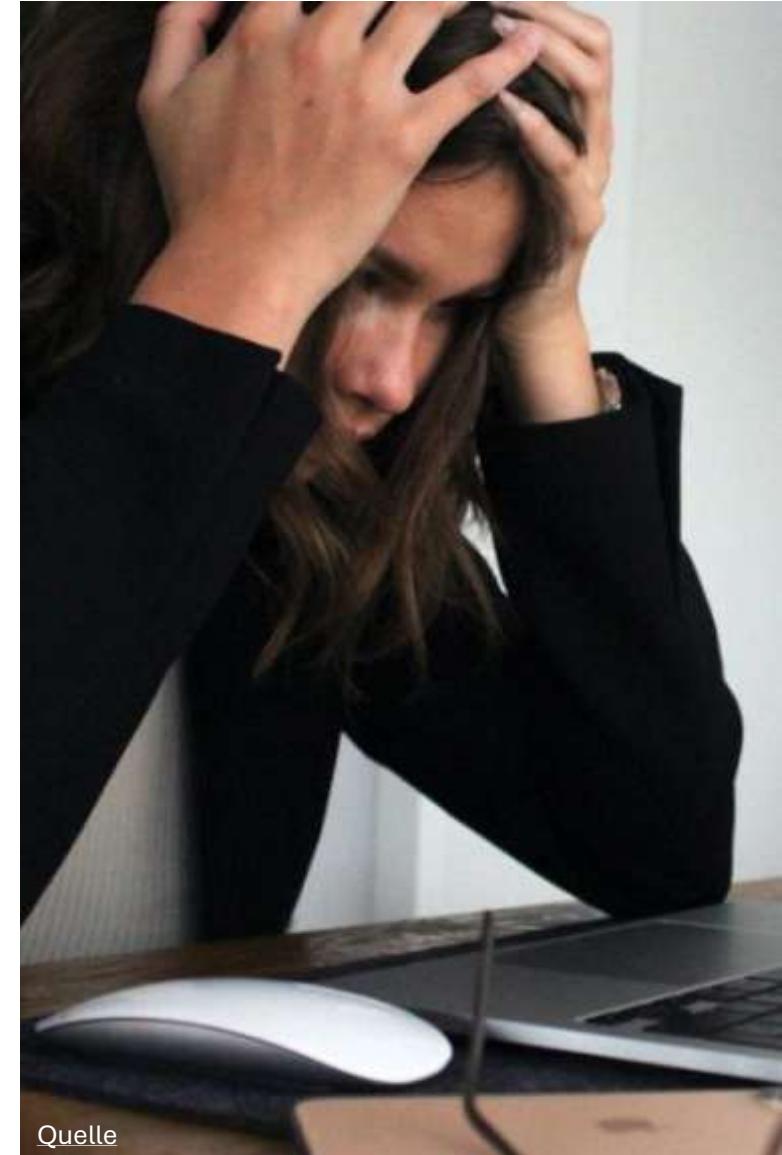
Maßnahmen

- **Klare interne Regeln:** Was darf in KI eingegeben werden – und was nicht?
- **Datensparsamkeit:** Keine echten Kundennamen oder internen Informationen eingeben; Inhalte anonymisieren.
- **Schulung der Mitarbeitenden:** Sensibilisierung für Datenschutz, Alternativen aufzeigen.
- **Technische Lösungen:** Nutzung datenschutzfreundlicher KI-Systeme oder Unternehmens-Accounts.

Wann ist ein Datenschutzverstoß meldepflichtig?

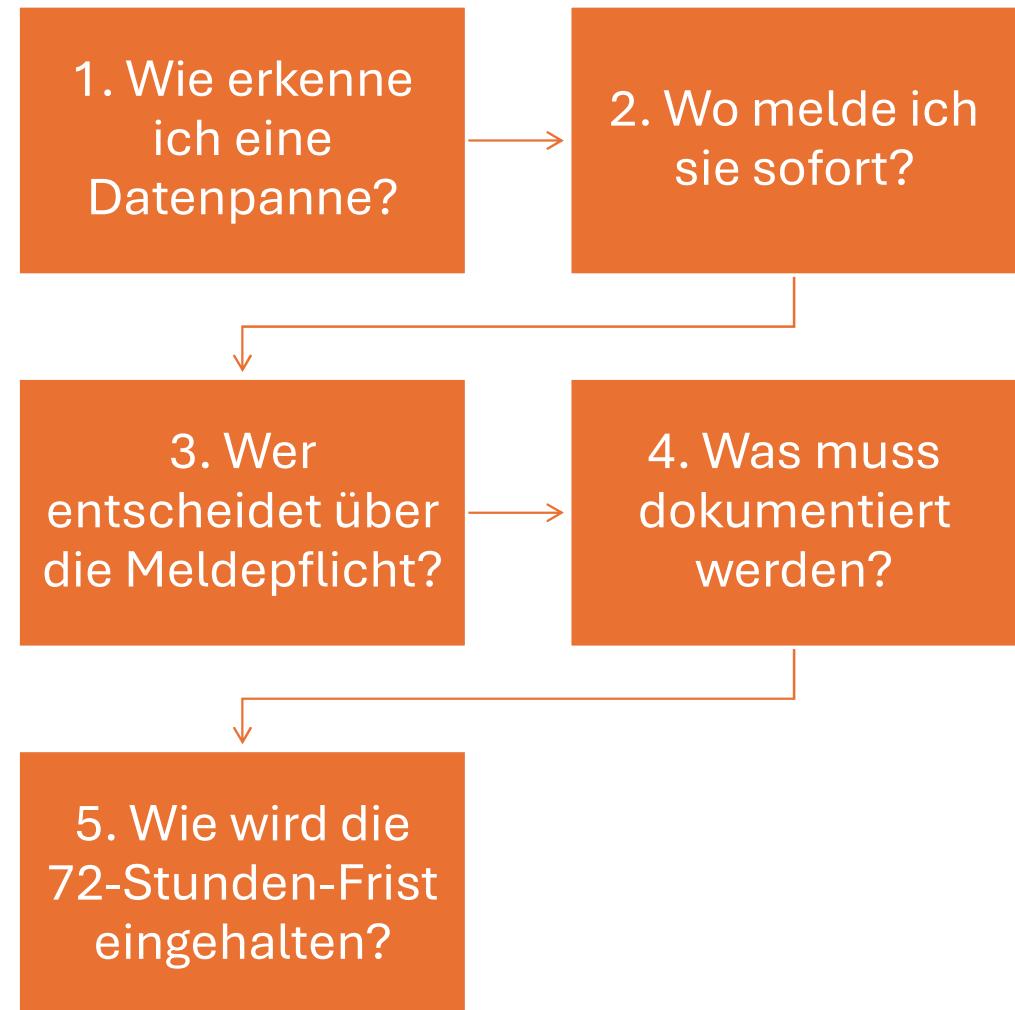
Definition (Art. 33 DSGVO):

⚠ Eine Meldepflicht innerhalb 72 Stunden besteht, wenn die Störung **voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen** darstellt.

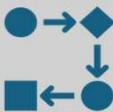


Quelle

Notfallprozess im Unternehmen - Was Beschäftigte wissen müssen:



Prävention und Organisation im Unternehmen

				
Klare Verantwortlichkeiten	Prozesse & Meldewege definieren	Technische und organisatorische Maßnahmen (TOMs)	Schulung & Sensibilisierung	Dokumentation & Nachbereitung
Datenschutz- und IT-Sicherheitsbeauftragte benennen Vertretungsregelungen und Eskalationswege festlegen	Einheitliches Verfahren zur Incident-Erkennung, Bewertung und Meldung Meldeketten intern + zum Auftragsverarbeiter klar dokumentieren 24/7-Erreichbarkeit für Vorfälle sicherstellen	Zugriffsschutz, Verschlüsselung, Backup, Protokollierung Regelmäßige Updates und Schwachstellenmanagement Entwicklung nach Vorgaben der „Privacy by Design and Default“	Mitarbeiterschulungen zu Phishing, Datenverlust, Meldepflichten Simulationsübungen: „Was tun im Ernstfall?“	Datenschutz-Notfallplan und Checklisten Lessons Learned nach jedem Vorfall zur Prozessverbesserung 

Feststellen – Bewerten - Melden



Erfassung der Datenpanne

- a) Welche Daten sind betroffen?
- b) Wie viele Personen sind betroffen?
- c) Wann und wie wurde die Panne entdeckt?

Analyse der Risiken

- Welche möglichen Folgen ergeben sich für Betroffene?
- Identifizierung von Risiken wie Identitätsdiebstahl, Betrug oder andere Schäden?

Im Fall von Risiko für Rechte und Freiheiten Betroffener



Meldung an die Aufsichtsbehörde ggf. auch Betroffene

- erfolgt durch den **Verantwortlichen**
- Frist: **innerhalb von 72 Stunden**
- **DSB unterstützt** bei Inhalt & Kommunikation

Schadensbegrenzung und Ergreifen von Gegenmaßnahmen

- Schutzmaßnahmen (z. B. Verschlüsselung) und betroffene Systeme absichern,
- Passwörter zurücksetzen und Zugänge sperren,
- Sicherheitslücken identifizieren und schließen
- Ergebnis dokumentieren (auch bei keiner Meldung!)
- Mitarbeitende für zukünftige Fälle sensibilisieren.

Zweck & Grundlagen der Risikobeurteilung bei Datenschutzvorfällen



Warum ist eine Risiko-beurteilung wichtig?

- Grundlage für Meldepflicht nach Art. 33 / 34 DSGVO
- Risiko = Eintrittswahrscheinlichkeit × Schadensschwere
- Ziel: Schutz der Rechte und Freiheiten Betroffener



Typische Schäden

- Identitätsdiebstahl, finanzielle Verluste
- Diskriminierung, Rufschädigung
- Verlust der Datenkontrolle, psychische Folgen



**Fokus liegt nicht auf Unternehmensinteressen,
sondern auf Risiken der Betroffenen !!!**

[Quelle](#)

Risikobeurteilung (1): Identifikation, Ereignisse, Risikoquellen

Risiken der Rechte und Freiheiten natürlicher Personen erkennen und verstehen

1. Risikoidentifikation

- Welche Daten? (z. B. Gesundheits-, Finanz- oder Logindaten)
- Wie viele Personen? Besonders schutzbedürftige Gruppen?
- Welche Grundwerte betroffen? (Vertraulichkeit, Integrität, Verfügbarkeit)



2. Ereignisse (Was ist passiert?)

- Fehlversand, unbefugter Zugriff, Datenverlust
- Technischer Defekt, Ransomware, Löschversäumnis



3. Risikoquellen

- Menschliches Fehlverhalten
- Technische / organisatorische Schwachstellen
- Cyberangriffe, fehlerhafte Auftragsverarbeitung



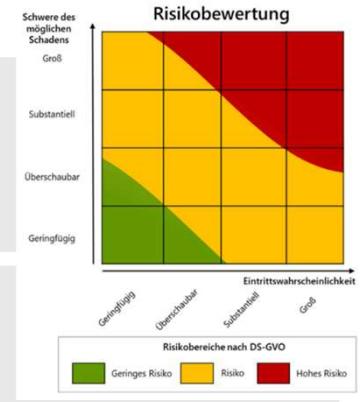
Quelle

Risikobeurteilung (2): Bewertung & Eindämmung

Wahrscheinlichkeit, Schaden, Maßnahmen

4. Eintrittswahrscheinlichkeit

- Missbrauch der Daten wahrscheinlich?
- Faktoren: Datenart, Umfang, Schutzmaßnahmen



5. Schwere der Schäden

- Abhängig von Sensibilität, Anzahl, Irreversibilität
- Einstufung: gering – mittel – hoch – sehr hoch (Einzelfallbetrachtung)



Bewertung des Meldebedarfs

6. Eindämmung des Risikos

- Technisch: Sperren von Zugängen, Passwortreset, Wiederherstellung
- Organisatorisch: Incident-Team aktivieren, Dokumentation, Kommunikation
- Ziel: Risiko mindern, Transparenz sichern

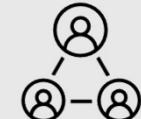


Quelle

Rolle der Auftragsverarbeiter & Meldefristen

Datenschutzvorfall beim Auftragsverarbeiter

- Der Verantwortliche bleibt haftbar (Art. 24, 28 DSGVO)
 - Auftragsverarbeiter muss unverzüglich Verantwortlichen informieren
 - Offenlegung notwendiger Informationen: Art der Daten, Umfang, erste Maßnahmen
 - Zeitfaktor:
 - Interne Meldefrist (z. B. 12–24 h an Verantwortlichen)
 - Verantwortlicher: 72 h Frist an Aufsichtsbehörde
 - Einbindung des Auftragsverarbeiters in das Incident- und Bewertungsverfahren
- Ziel: vollständige, dokumentierte Risikoabschätzung



Quelle

Wenn Altsysteme zum Sicherheitsrisiko werden



Wie lassen sich Datenpannen vermeiden?

T echnische Maßnahmen

sichere Passwortrichtlinien: starke Passwörter, MFA, keine Wiederverwendung

regelmäßige Updates und Patches: Sicherheitslücken durch veraltete Software vermeiden

Firewalls und Antivirensoftware: Schutz vor externen Angriffen und Malware

Zwei-Faktor-Authentifizierung: zusätzliche Sicherheitsebene für den Zugang zu sensiblen Systemen

Verschlüsselung von Daten: Schutz sensibler Informationen auf Speichermedien und in der Cloud

regelmäßige Backups und Kontrollen: kritische Daten sicher speichern

Videoüberwachung

O rganisatorische Maßnahmen

Schulungen und Awareness-Programme: Information über Datenschutzrisiken für Mitarbeitende und regelmäßige Auffrischungen

interne Datenschutzrichtlinien: klare Vorschriften zur Nutzung und Speicherung sensibler Daten

Zugriffsrechte und Zutrittsrechte: durch angemessene Gebäudesicherung und IT-Peripherie

Löschkonzept für manuelle und automatisierte Lösungen einschl. regelm. Prüfungen nachweisbar

regelmäßige Sicherheitsüberprüfungen: durch Audits Schwachstellen identifizieren und beheben.

Notfallpläne für Datenpannen: detaillierte Abläufe für den Ernstfall vorbereiten und regelmäßig testen

Quelle

Aktuelles

The screenshot shows a news article from the DsIN (Deutschland sicher im Netz) website. The headline reads "Milliarden gestohlene Passwörter und Mailadressen im Netz entdeckt". Below the headline is a photograph of a person sitting on a couch, using a laptop and holding a credit card. At the bottom of the article is a link "11.11.2025 -Quelle".

- >10 Mrd. gestohlene Zugangsdaten (email-Adressen und Passwörter) im Internet entdeckt, davon 625 Mio. erstmals kompromittiert
- Erhöhtes Risiko, da Cyberkriminelle solche Sammlungen für **Credential Stuffing Angriffe** nutzen

Empfehlungen für Betroffene:

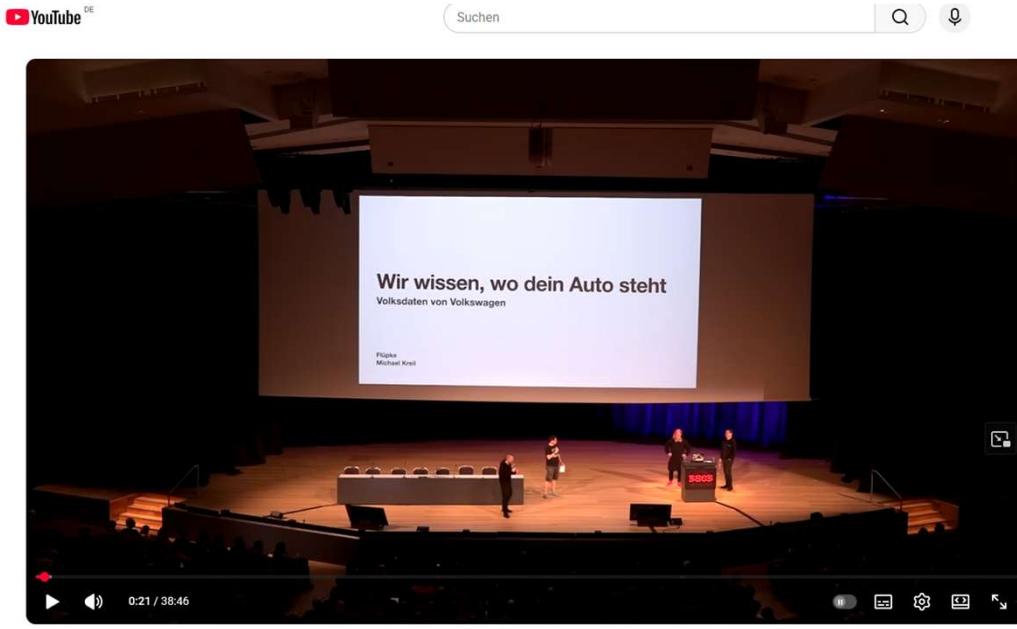
- E-Mail-Adresse bei **Have I Been Pwned** prüfen
- **Einzigartige, starke Passwörter** pro Dienst nutzen (am besten per Passwortmanager)
- **Zwei-Faktor-Authentifizierung (2FA)** aktivieren
- Auf **verdächtige E-Mails/Logins** achten

Empfehlungen für IT-Verantwortliche:

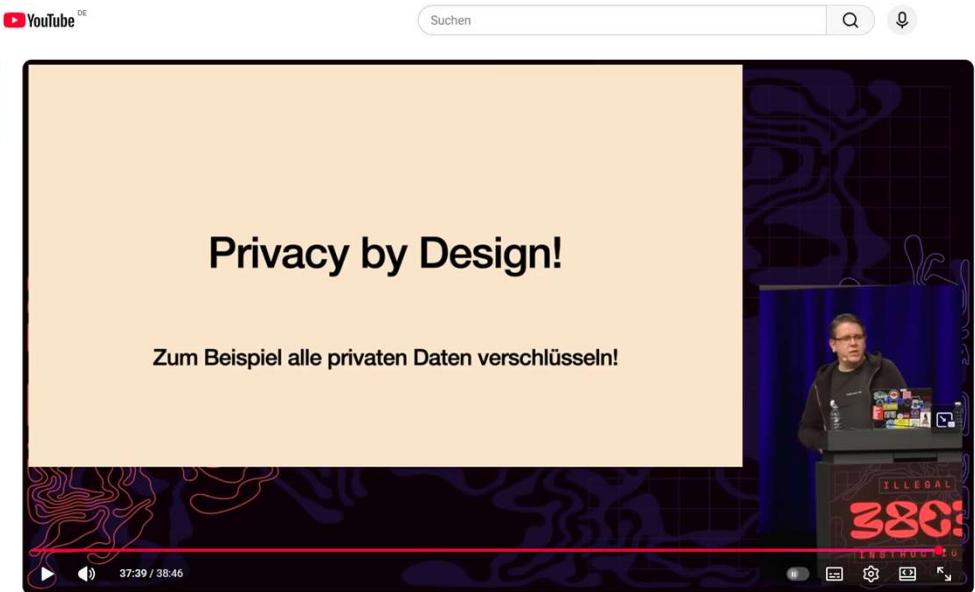
- Systeme auf **Credential-Stuffing-Versuche** überwachen und Schutzmechanismen verstärken
- **Passwort-Richtlinien** und 2FA für Nutzer verpflichtend oder empfohlen umsetzen
- **Monitoring & Logging** für ungewöhnliche Login- oder Traffic-Muster ausbauen
- Nutzer regelmäßig mit **Security Awareness** sensibilisieren



CCC – Privacy by Design



38C3 - Wir wissen wo dein Auto steht - Volksdaten von Volkswagen



38C3 - Wir wissen wo dein Auto steht - Volksdaten von Volkswagen

<https://www.youtube.com/watch?v=iHsz6jzbRc>

Warum TOMs wichtig sind ...



Behörden bewerten
Reifegrad und
Dokumentation



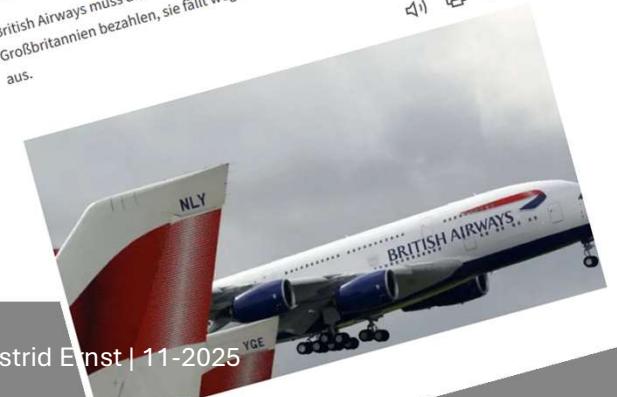
TOMs beweisen
Sorgfalt und
Pflichterfüllung
des Verantwortlichen



Gute TOMs können
Bußgelder deutlich
reduzieren (Fehlen von
TOMs -> Bußgeldgefahr)

- Datenschutzpannen sind nicht vermeidbar, aber beherrschbar
- Prävention ist möglich durch Technik, Awareness und klare Prozesse
- Incident-Management ermöglicht kontrollierte Reaktion
- TOMs sichern Nachweis und Vertrauen im Ernstfall

heise online > Netzpolitik > Datenschutzpanne: British Airways muss 22 Millionen Euro zahlen – statt 204
Datenschutzpanne: British Airways muss 22 Millionen Euro zahlen – statt 204
British Airways muss die bislang höchste Strafe für ein Datenschutzvergehen in Großbritannien bezahlen, sie fällt wegen der Corona-Pandemie aber niedriger aus.



Meldepflicht-Umfang

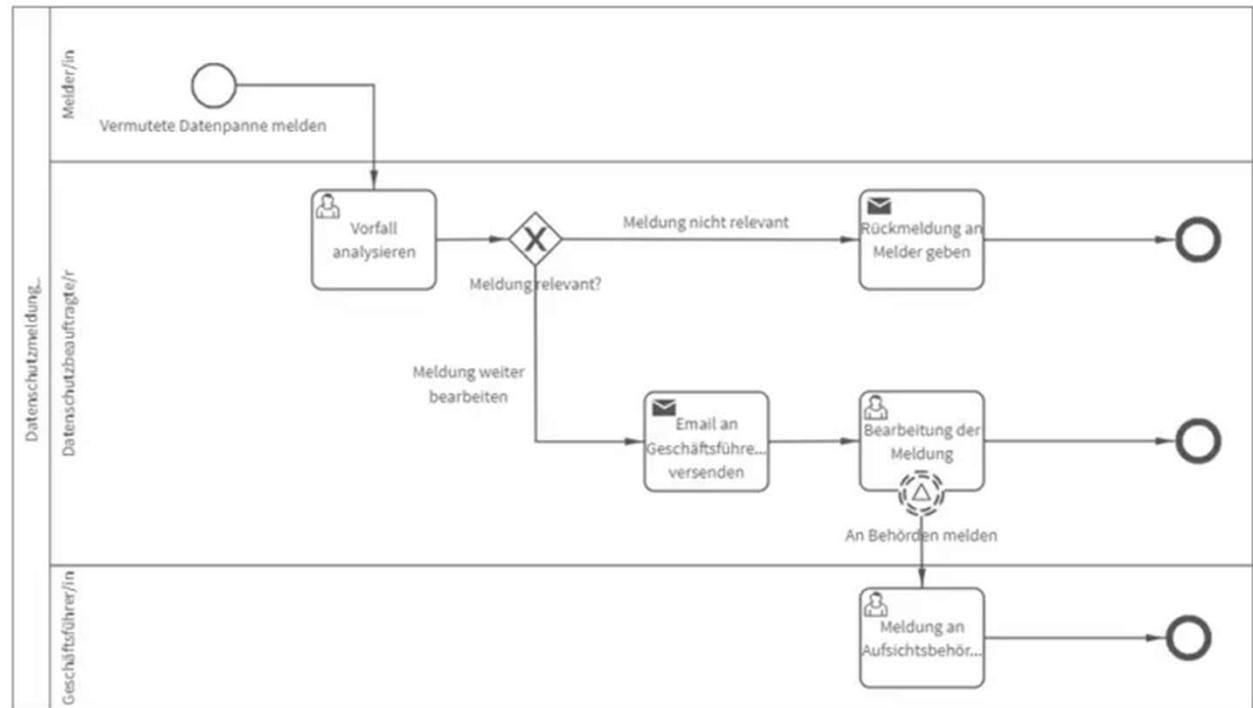
- Datum, Uhrzeit, Umfang der Datenpanne
- Kategorie und Art der Daten (Kontakt, Bank, Gesundheit, etc.)
- Anzahl betroffener Personen / Datensätze
- Kontaktdaten des Datenschutzbeauftragten oder sonstige Anlaufstellen für weitere Informationen
- Beschreibung möglicher Folgen der Verletzung des Schutzes der pbDaten
- Ergriffene oder geplante Gegenmaßnahmen zur Behebung der Verletzung, ggf. Maßnahmen zur Abmilderung möglicher nachteiliger Auswirkungen für Betroffene

The image shows two side-by-side screenshots of online reporting forms for data breaches.

Niedersachsen Form: This form is titled "Meldung einer Datenpanne nach Art. 33 DS-GVO, bzw. § 54 LDS". It includes fields for reporting a data breach to the Landesbeauftragte for Datenschutz Niedersachsen. It asks for the type of breach ("Benachrichtigung (* = Pflichtangaben) Art der Meldung") and provides a "Vollständige Neumeldung" option. The form also includes sections for organizational details, reporting contact information, and a detailed description of the breach.

Thüringen Form: This form is titled "Meldung einer Datenpanne nach Art. 33 Datenschutz-Grundverordnung". It follows a similar structure, asking for the type of breach ("Schadensart") and providing a "Vollständige Neumeldung" option. It includes sections for reporting contact information and a detailed description of the breach, including specific fields for the nature of the violation and the affected data subjects.

Beispiel: Prozess einer Datenschutz- meldung



Quelle

Beispiel: Rückmeldung vom Datenschutz- beauftragten an Datenpannenmelder



Guten Tag Vorname Nachname (Melder/in),
vielen Dank für Ihre Meldung "Titel". Nach eingehender
Prüfung wurde festgestellt, dass diese Meldung keine
Relevanz für den Datenschutz nach § 33 DSGVO hat.

Trotzdem möchten wir uns dafür bedanken, dass Sie das
Thema Datenschutz ernst nehmen.

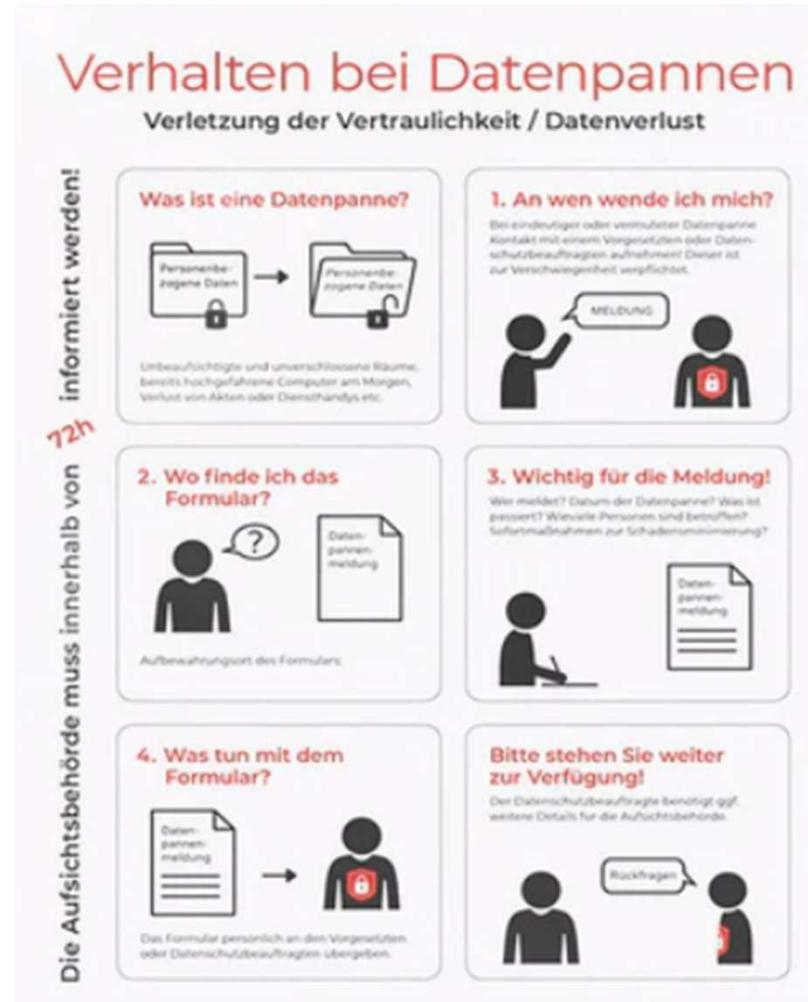
Mit freundlichen Grüßen
Vorname Nachname (Datenschutzbeauftragte/r)



Guten Tag Vorname Nachname (Geschäftsführer/in),
wir haben eine neue relevante Datenschutzmeldung
erhalten. Wir werden die Meldung bearbeiten.

Vorname Nachname (Datenschutzbeauftragte/r)

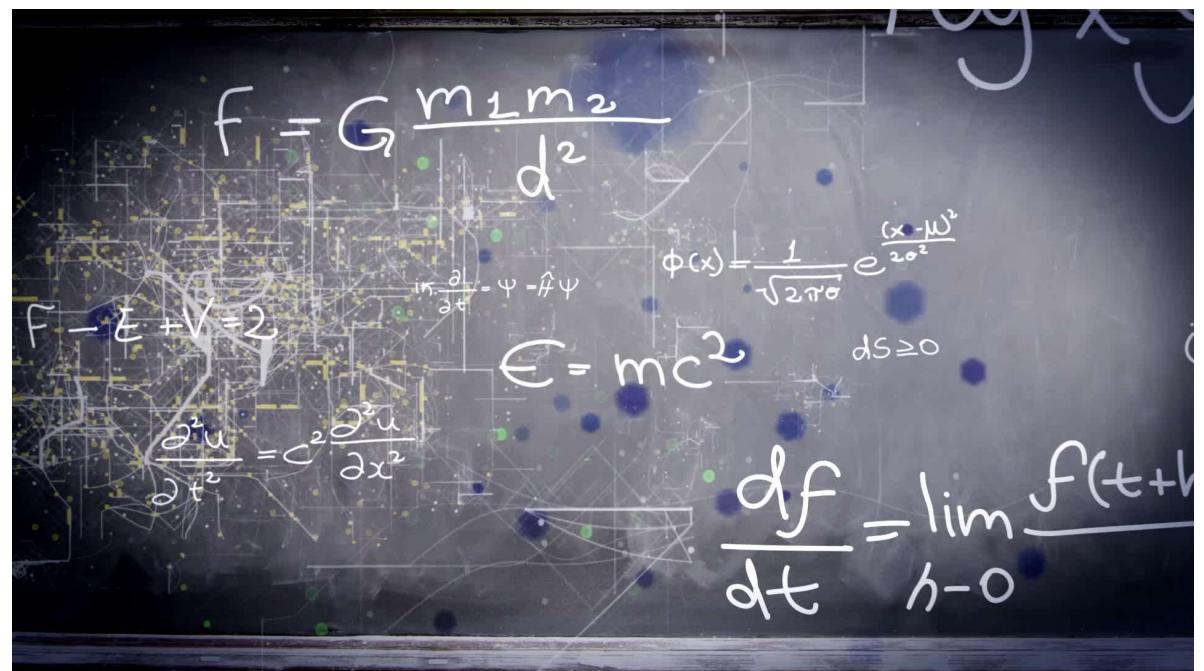
Beispiel Geregelter Prozess für Beschäftigte fördert Sicherheit bei der Umsetzung



Bereich	Quelle	Verpflichtung
Datenschutz	DSGVO Art. 32–34	TOMs + Meldepflicht (72 h) + Benachrichtigung Betroffener
Cybersicherheit	NIS 2 / BSIG / IT-SiG 2.0	Incident-Detection, Reporting an BSI
KRITIS	§ 8a BSIG	ISMS + Nachweis & Meldung BSI-Gesetz (BSIG) & IT-Sicherheitsgesetz 2.0
Branchenreguliert	BAIT / MaRisk (BaFin) / EnWG / SGB V / TKG	branchenspezifisches Incident-Management
Stand der Technik	ISO 27035, NIST 800-61, ENISA	Normen und Best Practices

Normen | Standards | Verordnungen

Incident- Management am Beispiel eines Großkonzerns



Kontaktlisten und Unterlagen

- Umfassende Informationen für alle Beschäftigten im INTRANET
- LCO / Multiplier-Netzwerk
- Eskalationskontaktliste
- Liste für Rufbereitschaft 24/7
(Konzerndatenschutz, CEO-Bereich: Führungskräfte und LCO)
- Sprachregelung im Falle Meldebedarf (PR)

Handreichung Datenschutz Incident Management - Eingangskanäle

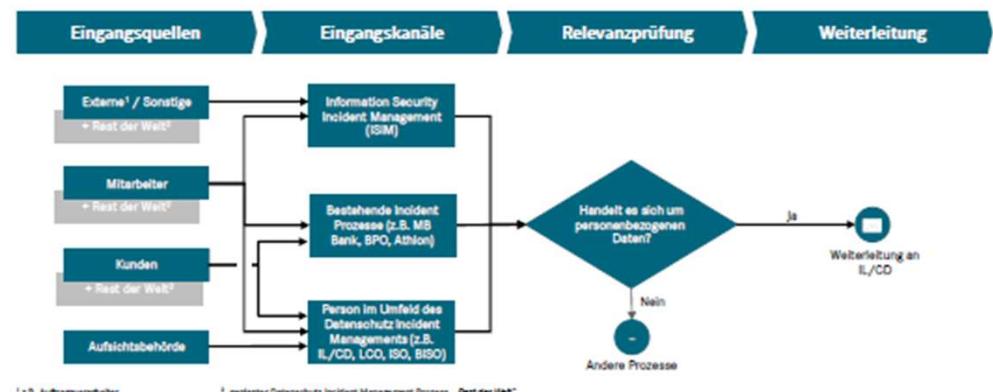
Version 5, 30.07.2024

Inhaltsverzeichnis

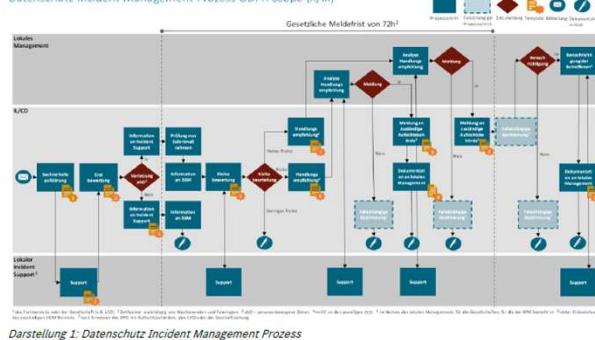
1. Datenschutz Incident Management.....
2. Prozessbeschreibung.....
3. Zentrale Meldung und Weiterleitung an den Konzerndatenschutz.....
4. Anwendungsbereich dieses Prozesses.....
 - Beeinträchtigung der Datenverfügbarkeit.....
 - Beeinträchtigung der Datenintegrität.....
 - Beeinträchtigung der Datenvertraulichkeit.....
5. Anlage 1: Weitere Beispiele zur zweistufigen Meldepflicht.....¹1

5. Anlage 1: Weitere Beispiele zur zweistufigen Meldepflicht

Sachverhalt	Datenschutz- vorfall? (Ja/Nein)	Begründung	Meldung an Aufsichtsbehörde? (Ja/Nein)	Begründung	Benachrichtigung Betroffene? (Ja/Nein)	Begründung	Empfohlene Abhilfemaßnahmen
Auf dem Heimweg ist einem Mitarbeiter dessen verschlüsselter Arbeitslaptop in der S-Bahn abhandengekommen.	Nein.	Da der BitLocker aktiv war, ist ein State of the Art Sicherheitsniveau der Datensicherheit gewährleistet.	Nein.	Kein Datenschutzvorfall.	Nein.	Kein Datenschutzvorfall.	k.A.
Ca. 50 Werksausweise wurden mit einem falschen Foto bedruckt und an Mitarbeiter ausgehändigt. Der Fehler ist schnell aufgefallen und der Werkschutz sammelt die fehlerhaften Werksausweise derzeit ein.	Ja.	Verletzung der Integrität aufgrund der Änderung personenbezogener Daten durch die falsche Zuordnung von Bild und Name.	Nein.	Da der Fehler umgehend erkannt und behoben wurde, liegen keine Anzeichen für ein Missbrauchsrisiko vor. Es ist kein Risiko für die Rechte und Freiheiten der betroffenen Personen erkennbar.	Nein.	Keine Meldepflicht gegenüber der Aufsichtsbehörde, daher auch keine datenschutzrechtliche Meldepflicht gegenüber den Betroffenen (Zweistufigkeit der Meldepflicht).	Sensibilisierung der Mitarbeiter in Form einer abteilungsinternen Kommunikation.



Datenschutz Incident Management Prozess GDPR Scope (II/III)



4. Wann besteht eine Verletzung des Schutzes personenbezogener Daten?

Unter „Verletzung des Schutzes personenbezogener Daten“ sind Fälle zu verstehen, bei denen die Sicherheit der Verarbeitung bei einem Group Unternehmen verletzt wurde. Dies kann auch unbeabsichtigt passiert sein. Eine Verletzung der Sicherheit liegt vor, wenn in Bezug auf personenbezogene Daten

- Vernichtung
- Verlust
- Veränderung eintreten
- unbefugte Offenlegung oder
- unbefugter Zugang

Handreichung Datenschutz Incident Management - Beschäftigte

Version 5, 30.07.2024



Dieses Dokument beruht auf den Vorschriften der Datenschutz-Grundverordnung (EU-DSGVO) und beinhaltet verbindliche Vorgaben sowie Empfehlungen zur Umsetzung datenschutzrechtlicher Anforderungen für eine standardisierte Verwendung im Konzern.

Kurzzusammenfassung:

Diese Handreichung gibt eine Übersicht über die gesetzlichen Anforderungen der Datenschutz-Grundverordnung (EU-DSGVO) hinsichtlich der Meldepflichten gegenüber den Datenschutzaufsichtsbehörden und den Betroffenen, die bei Bekanntwerden von Verletzungen des Schutzes personenbezogener Daten eingehalten werden müssen. Zur Einhaltung der Meldepflicht an die Aufsichtsbehörde ist ein spezieller Meldeprozess innerhalb von 72 Stunden erforderlich.

Die Handreichung verfolgt zweierlei Ziele. Zum einen hat sie das Ziel, ein einheitliches Verständnis von Verletzungen des Schutzes personenbezogener Daten zu schaffen. Zum anderen zeigt die Handreichung auf, welche Schritte die Mitarbeiter der gesamten Mercedes-Benz Group durchführen müssen, wenn sie eine Verletzung des Schutzes personenbezogener Daten feststellen.

Adressatenkreis:

Diese Unterlage gilt für alle Beschäftigten der gesamten (Group) Gesellschaften.

6. Was muss ich bei einem Verdacht tun?

Grundsätzlich sind Mitarbeiterinnen und Mitarbeiter dazu angehalten, einen Verdacht über eine Verletzung des Schutzes personenbezogener Daten zu melden. Bevor Mitarbeiter einen Vorfall jedoch melden, sollten sie den Verdacht mit Kollegen oder Vorgesetzten besprechen, um weitere Meinungen einzuhören und den Arbeitsaufwand bei der Meldestelle zu reduzieren.

Die folgenden Beispiele verdeutlichen, dass nicht jeder Vorfall eine Verletzung des Schutzes personenbezogener Daten darstellen muss. Der Vorfall ist unbedingt im Kontext zu betrachten.

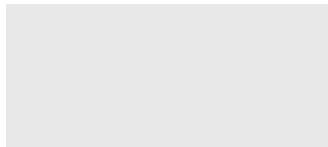
Beispiel	Verletzung?	Folge
Ein Mitarbeiter vergisst ein ausgedrucktes Papier mit personenbezogenen Daten im Drucker. Ein anderer Mitarbeiter findet das Papier im Drucker.	Hierbei handelt es sich nicht um eine Verletzung des Schutzes personenbezogener Daten.	Der Mitarbeiter sollte den Fall deshalb nicht melden.
Das Sicherheitsnetz eines Netzwerkdruckers im Büro wird geknackt und Fremde haben Zugriff auf alle sensiblen Dokumente, die an diesen Drucker gesendet werden.	Hierbei handelt es sich um eine Verletzung des Schutzes personenbezogener Daten.	In diesem Fall muss der Fall unverzüglich gemeldet werden.

Inhaltsverzeichnis

1. Hintergrundinformationen	4
1.1 EU- Datenschutz-Grundverordnung	4
1.2 Datenschutz Incident Management.....	4
2. Reichweite und Ziel der Handreichung Datenschutz Incident Management.....	4
2.1 Reichweite.....	4
2.2 Ziel.....	4
3. Was sind personenbezogene Daten?...	5
4. Wann besteht eine Verletzung des Schutzes personenbezogener Daten?.....	5
4.1 Beeinträchtigung der Datenverfügbarkeit.....	5
4.2 Beeinträchtigung der Datenintegrität.....	6
4.3 Beeinträchtigung der Datenvertraulichkeit.....	6
5. Melde- und Benachrichtigungspflicht.....	6
6. Was muss ich bei einem Verdacht tun?.....	8
7. Was passiert mit meiner Meldung?	9
8. Warum sollte ich Verletzungen melden?.....	10
9. Anlage 1: Weitere Beispiele zur zweistufigen Meldepflicht.....	11



I



Verletzung des Schutzes personenbezogener Daten (Datenschutzvorfälle) – Beschreibung des Vorfalls

Nutzen Sie dieses Dokument, um den Datenschutzvorfall zu beschreiben und für die Meldung an das Information Security Management.

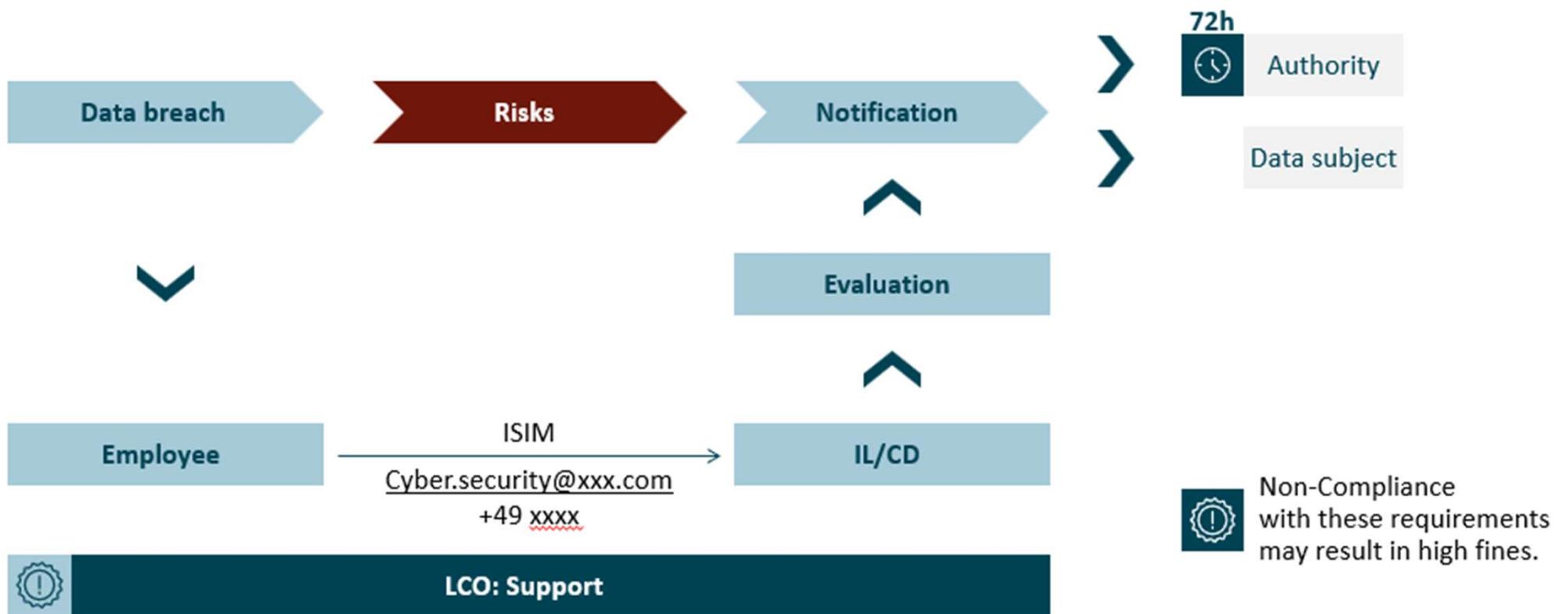
Beschreibung

Name der betroffenen MB (Group) Gesellschaft	(Nennen Sie bitte die korrekte Bezeichnung der Gesellschaft, die für den Vorfall verantwortlich ist.)
Name und Kontaktdaten des ISIM Supports (i.d.R. LCO/LCR)	(Nennen Sie den Ansprechpartner, welcher die Aufklärung lokal koordiniert und weitere Informationen zum Vorfall geben kann.)
Beschreibung der Art der Verletzung des Schutzes von personenbezogenen Daten	(Beschreiben Sie den Vorfall möglichst präzise. Worin liegt die potentielle Verletzung? Wo ist der Vorfall passiert? Wer war beteiligt? Wie haben Sie diesen erfahren? Wie war die zeitliche Abfolge? Nennen Sie alle Beteiligten und wie die Verletzung bekannt wurde.)
Zeitpunkt des Vorfalls (Datum und Uhrzeit)	(Wann hat sich der Vorfall ereignet?)
Bekanntwerden des Vorfalls (Datum und Uhrzeit)	(Wann haben Sie als Meldender vom Vorfall erfahren?)

Betroffene Datenkategorien:	(Nennen Sie die von dem Vorfall betroffenen Datenkategorien (z. B. Kundendaten, Fahrzeugdaten, Beschäftigtendaten). Weisen Sie ausdrücklich darauf hin, wenn besondere Kategorien personenbezogener Daten betroffen sind.)
Anzahl an betroffenen Personen:	(Geben Sie eine Einschätzung zu der ungefähren Anzahl an betroffenen Personen. Nennen Sie die betroffenen Gruppen. Beispiele: Kunden, Altarbeiter, Lieferanten, Kinder oder andere schutzwürdige Personengruppen)
Ungefähr Anzahl der betroffenen personenbezogenen Datensätze:	(Geben Sie eine Einschätzung zu der ungefähren Anzahl an betroffenen personenbezogenen Datensätzen)
Ursache der Verletzung des Schutzes personenbezogener Daten:	(Beschreiben Sie die Ursache. Beispiele: Unabsichtlich, Technische Fehler/Defizite, Fremdangriffen eines Lieferanten, Prozessdefizit, Softwarefehler)
Risikoabschätzung:	(Beschreiben Sie die wahrscheinlichen Folgen auf Basis der aktuellen Tatsachengrundlagen. Beispiele: Übermittlung an unbefugte Dritte, finanzieller Verlust, Reputationsschaden)
Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten:	(Beschreiben Sie die vor der Verletzung der Verletzung des Schutzes personenbezogener Daten getroffenen Maßnahmen. Beispiele: Weiterer offizieller Personenkreis, Sicherstellung, Auflösungsmaßnahme, Sensibilisierung der Mitarbeiter oder Dienstleister)
Gegebenenfalls Maßnahmen zur Abmilderung möglicher nachteiligen Auswirkungen:	(Beschreiben Sie die zur Eindämmung der negativen Auswirkungen getroffenen Maßnahmen.)
Unterlagen, die den Vorgang erläutern:	(Stellen Sie im erforderlichen Umfang Unterlagen bereit, die den Vorgang erklären. Beispiele: E-Mail oder Schrifturkarte, Prozessbeschreibung, betreffende Verträge, Screenshots, Bespielbelebemits)
Erst wenn festzustellt, dass eine Meldepflicht an die zuständige Aufsichtsbehörde erfolgen muss, ist dieses Feld zu befüllen. Benachrichtigungspflicht gegenüber den Betroffenen:	(Bestätigen Sie Ihre Einschätzung für Sie obpflicht, die Betroffenen zu benachrichtigen (Art. 34 DS-GVO? Ja / Nein) Falls nein: Bitte begründen Sie Ihre Entscheidung. Falls ja: Wann und wann wurden (wurden) die Betroffenen benachrichtigt und welche Gegenmaßnahmen haben Sie Ihnen empfohlen?)

A	B	C	D	E	F	G	H	I
Entity ID	"Bereichs ID" (sofern vorhanden)	Wer hat gemeldet? (Konkrete Person aus Fachbereich)	Was ist passiert?	Wann ist es passiert? (Datum Bekanntwerden des Vorfalls)	Wann wurde der Vorfall gemeldet?		SIR Nummer (von ISIM)	Inquiry ID (von IL/CD)
					An ISIM	An LCO		





Handreichung Sicherheit der Verarbeitung

Version 3, 14.11.2022

 Dieses Dokument beruht auf den Vorschriften der Datenschutz-Grundverordnung (EU-DSGVO) und beinhaltet verbindliche Vorgaben sowie Empfehlungen zur Umsetzung datenschutzrechtlicher Anforderungen für eine standardisierte Verwendung im Konzern.

Kurzzusammenfassung:
Durch die Regulations for Information Security (RISE) werden die Anforderungen an den Schutz von Group-Informationen festgelegt. Diese Anforderungen gelten damit auch für personenbezogene Daten, für die die Mercedes-Benz Group die Verantwortung trägt. Ihre konsequente Umsetzung ist die Basis, um die datenschutzrechtlichen Anforderungen an die Sicherheit der Verarbeitung zu erfüllen. Es muss bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau durch geeignete technische und organisatorische Maßnahmen gewährleistet werden. Die Wirksamkeit der Maßnahmen ist regelmäßig zu überprüfen.

Sowohl der für die Verarbeitung der personenbezogenen Daten Verantwortliche als auch der Auftragsverarbeiter haben die Pflicht die Sicherheit der Verarbeitung zu gewährleisten.

Adressatenkreis:
Verantwortlich für die Einhaltung der Vorschriften zum Datenschutz ist das geschäftsführende Organ der jeweiligen Konzerngesellschaft bzw. Zentraleinheit im Anwendungsbereich der EU sowie betroffener Gesellschaften in Drittstaaten.

Diese Unterlage richtet sich an das jeweilige lokale Management und den zugeordneten Local Compliance Officer (LCO) bzw. Local Compliance Responsible (LCR) und Supports, welche personenbezogene Daten verarbeiten oder deren Verarbeitung steuern und Aufgaben für den Datenschutz ausüben.

Inhaltsverzeichnis

1. Implementierung technischer und organisatorischer Maßnahmen
2. Risikoorientiertes Vorgehen
3. Weitere Empfehlungen
4. Dokumentation
5. Regelmäßige Überprüfung der getroffenen Maßnahmen

1. Implementierung technischer und organisatorischer Maßnahmen

Anforderungen zu technisch organisatorischen Maßnahmen (TOMs) waren bereits in der EU-Richtlinie zum Datenschutz enthalten und finden sich heute auch in der EU-DSGVO wieder. Daher enthält auch die [Group Konzernrichtlinie Datenschutz](#) (EU) (A 17) seit jeher entsprechende Vorgaben zur Sicherheit in der Verarbeitung von personenbezogenen Daten. Die technischen und organisatorischen Maßnahmen müssen für die Verarbeitung von personenbezogenen Daten auf ein für das Risiko angemessenes Schutzniveau abzielen. Die Maßnahmen müssen sowohl vor Angriffen von außen schützen, als auch verhindern, dass es intern zu unzulässigen Datenverarbeitungen oder Missbrauch z.B. durch Mitarbeiter kommt.

1. Vertraulichkeit

!!! Auch Bestandteil bei
Auftragsverarbeitungsvereinbarungen
mit Dienstleistern



MS Compliance Update & Awareness 2023

MS...

März 2023

Zwei Richtlinien legen die internen Anforderungen für Daten und Informationen in der xxx Group fest

Gesamtüberblick



Meldepflicht ignoriert oder verpasst – Und dann?

Warum es dazu kommen kann:



Konsequenzen für das Unternehmen:

- **Bußgelder** nach Art. 83 DSGVO
 - meldepflichtige Datenpanne nicht oder zu spät gemeldet: bis zu 10 Mio € bzw. 2 % des Jahresumsatzes
 - Betroffene nicht informiert: bis zu 20 Mio € bzw. 4% des Jahresumsatzes
- **Vertrauensverlust** bei Kunden, Partnern und Öffentlichkeit
- **Aufsichtsmaßnahmen** (Überwachung, Prüfungen, Nachbesserungsauflagen)
- **Zivilrechtliche Ansprüche** Betroffener (Schadensersatz nach Art. 82 DSGVO)
- **Reputationsschaden** durch öffentliche Bekanntmachung oder Medienberichte
- **Haftung des Beschäftigten im Einzelfall möglich**, wenn grobe Fahrlässigkeit oder Vorsatz vorliegt

Fazit





Time for a
QUIZ

<https://quizacademy.io>

Key-Code

U - L W Q J Z E



Noch Fragen

