

# MELDUNG VON DATENSCHUTZVORFÄLLEN

STAND: FEBRUAR 2020



ERLEBEN, WAS VERBINDET.

# INHALT

- 
- 01** Was ist ein Datenschutzvorfall?

---

  - 02** Beispiele für Datenschutzvorfälle

---

  - 03** Wie können Datenschutzvorfälle gemeldet werden - Leitplanken?

---

  - 04** Was passiert nach einer erfolgten Meldung beim Konzerndatenschutz?

---

  - 05** Was passiert, wenn Vorfälle nicht (rechtzeitig) gemeldet werden?

---

  - 06** Weitere Materialien
-

# **01 - WAS IST EIN DATENSCHUTZVORFALL?**

# WAS IST EIN DATENSCHUTZVORFALL?

## ALLGEMEINE DEFINITION



Ein Datenschutzvorfall ist z. B. ...

... ein Verstoß gegen **Datensicherheit**, der zu einer Verletzung des **Schutzes personenbezogener Daten** führt.



# WAS IST EIN DATENSCHUTZVORFALL?

## GESETZLICHE DEFINITION



Datenschutz-Grundverordnung Artikel 4 (12)\*:

„Verletzung des Schutzes personenbezogener Daten“ ist eine Verletzung der Sicherheit, die zur **Vernichtung**, zum **Verlust** oder zur **Veränderung**, ob unbeabsichtigt oder unrechtmäßig, oder zur **unbefugten Offenlegung** von beziehungsweise zum **unbefugten Zugang** zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“

Ein **Datenschutzvorfall** ist demnach z. B. ...

... die **Verletzung der Verfügbarkeit**

- Bsp.: Löschung, Vernichtung, Verlust etc. von pb-Daten

... und/oder **Verletzung der Integrität**

- Bsp.: Veränderung (unbeabsichtigt oder unrechtmäßig) von pb-Daten

... und/oder **Verletzung der Vertraulichkeit**

- Bsp.: unbefugte Offenlegung Verwendung, unbefugter Zugang von/zu pb-Daten



# 02 - BEISPIELE FÜR DATENSCHUTZVORFÄLLE

# BEISPIEL DATENSCHUTZVORFALL: VERLETZUNG DER VERFÜGBARKEIT



## BEISPIELE:

- Daten\* wurden (unrechtmäßig / unbeabsichtigt) gelöscht oder vernichtet.
- Daten\* wurden verschlüsselt und können nicht mehr entschlüsselt werden, da z. B. der Schlüssel unwiderruflich gelöscht wurde
- Daten\* wurden auf einem Backup (z. B. auf einer externen Festplatte) gespeichert. Der Zugriff auf das Backup ist nicht möglich.
- Ein (verschlüsselter) USB-Stick mit Daten\* wurde verloren.



Egal ob unbeabsichtigt oder unrechtmäßig - es kommt nicht auf die Umstände der Datenschutzverletzung an.



ERLEBEN, WAS VERBINDET.

\* gemeint sind personenbezogene Daten

# BEISPIEL DATENSCHUTZVORFALL: VERLETZUNG DER INTEGRITÄT



## BEISPIELE:

- Aufgrund eines fehlerhaften Berechtigungskonzepts wurden Daten\* inhaltlich verändert.
- Ein Callcenter Mitarbeiter ordnet aufgrund eines Arbeitsfehlers die Kontonummer von Kunde A Kunde B zu.
- Falsche, gefälschte oder verfälschte Daten führen zu Fehlbuchungen, falschen Lieferungen oder fehlerhaften Produkten, da sie einer falschen Person zugeordnet werden.
- Nach einem Hackerangriff auf das Kundencenter wird zeitnah bei einer ungewöhnlich hohen Anzahl von Kunden die Lieferadresse geändert.
- Ein Kunde wird mit der Androhung von Telefonterror erpresst. Es wurden tatsächlich Anrufweiterrichtungen von 100 anderen Kunden auf den Anschluss des betroffenen Kunden über das Kundencenter eingerichtet.



Egal ob unbeabsichtigt oder unrechtmäßig - es kommt nicht auf die Umstände der Datenschutzverletzung an.



ERLEBEN, WAS VERBINDET.

\* gemeint sind personenbezogene Daten



# BEISPIEL DATENSCHUTZVORFALL: VERLETZUNG DER VERTRAULICHKEIT



## BEISPIELE:

- Falschversand von Rechnungen per Email bei RechnungOnline, z.B. Kunde A erhält Rechnung von Kunde B.
- Falschversand von Auftragsbestätigungen per Email, z.B. Nichtkunde erhält eine Auftragsbestätigung, die für einen Kunden bestimmt ist.
- Ein Dienstleister hat versehentlich eine Variable für die Vertragsnummer in einer Werbemail falsch programmiert, wodurch diese nicht auf den jeweiligen Kunden individuell angepasst wurde. Stattdessen wurden die statischen Vertragsnummern zweier Kunden in allen Werbemails verwendet.



Egal ob unbeabsichtigt oder unrechtmäßig - es kommt nicht auf die Umstände der Datenschutzverletzung an.



ERLEBEN, WAS VERBINDET.

\* gemeint sind personenbezogene Daten

**SONDERFALL  
TELEKOM ALS  
AUFTRAGSVERARBEITER**

# BEISPIEL DATENSCHUTZVORFALL

## SONDERFALL: DT ALS AUFTRAGSVERARBEITER / PROCESSOR

### BEISPIEL-SITUATION:

- Die Telekom Deutschland GmbH (TDG) verarbeitet personenbezogene Daten eines Kunden auf Basis einer Auftragsverarbeitung (z. B. Cloud-Dienstleistung). Hierfür wurde eine entsprechende Vereinbarung mit den Kunden unterzeichnet. In diesem Fall ist die Telekom Deutschland GmbH „Auftragsverarbeiter“ und der Kunde „Verantwortlicher“ im Sinne der DSGVO.
- Wenn es im Zusammenhang mit der Vereinbarung auf Seiten der TDG zu einem Datenschutzvorfall kommt (siehe Folien 7 - 9), ist die TDG verpflichtet den Kunden („Verantwortlicher“) umgehend zu informieren.
- Die Information muss durch die entsprechende Fachabteilung (Vertragspartner) erfolgen. Group Privacy ist dabei nur nachrichtlich zu informieren.
- Der Kunde prüft den Vorfall und meldet ggf. an die entsprechenden Aufsichtsbehörden. Die TDG unterstützt ggf. dabei.



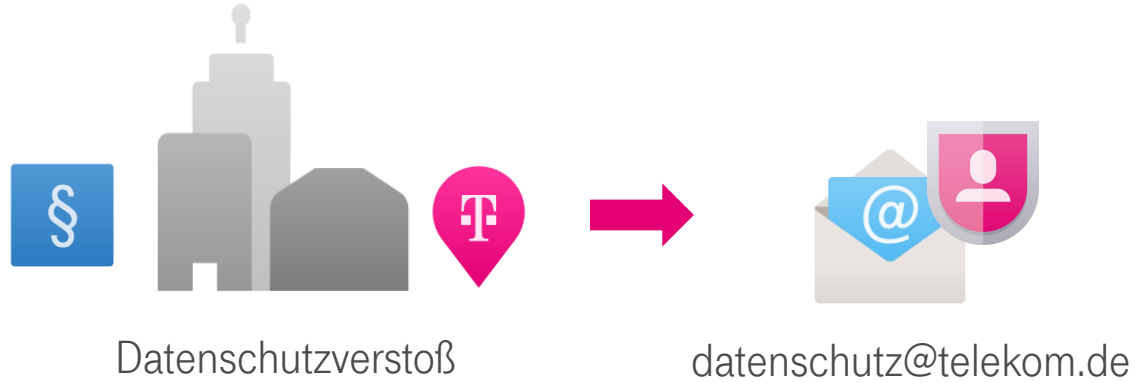
Egal ob unbeabsichtigt oder unrechtmäßig - es kommt nicht auf die Umstände der Datenschutzverletzung an.



LIFE IS FOR SHARING.

# **03 - WIE KÖNNEN DATENSCHUTZVORFÄLLE GEMELDET WERDEN?**

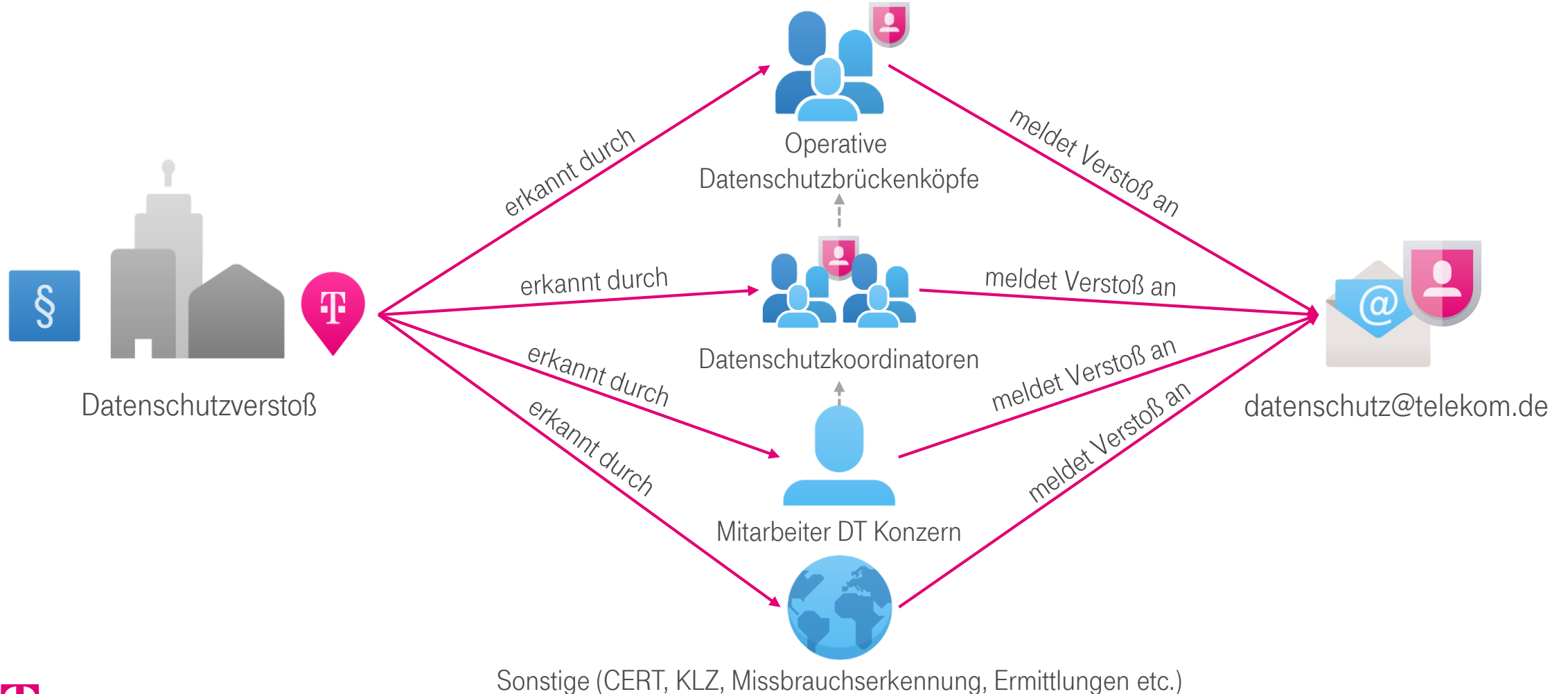
# MELDEWEG BEI DATENSCHUTZVORFÄLLEN



**Datenschutzvorfälle** können  
über unser Funktionspostfach [datenschutz@telekom.de](mailto:datenschutz@telekom.de)  
jederzeit melden.

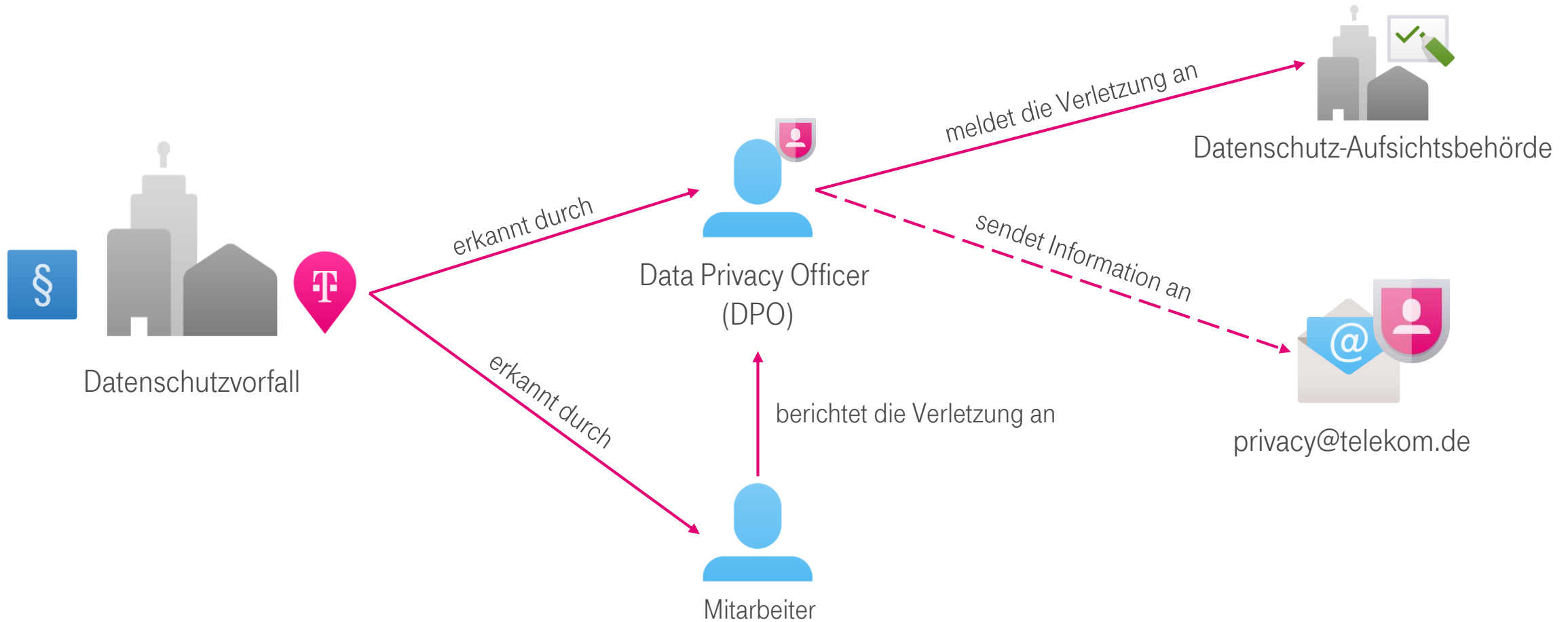
# WIE SIEHT DER MELDEPROZESS AUS?

## ÜBERSICHT- NATIONALER PROZESS



# SONDERFALL: UNTERNEHMEN AUßERHALB DEUTSCHLANDS

## PROZESS ZUR MELDUNG VON DATENSCHUTZVORFÄLLEN



# INHALT DER MELDUNG AN DATENSCHUTZ@TELEKOM.DE

- **Meldendes DT Unternehmen:**
  - Name Konzerneinheit / Ansprechpartner auf Führungsebene / E-Mail / Telefonnummer ...
- **Genaue Darstellung des Sachverhaltes:**
  - Wann / Wie / Wo / unbeabsichtigt oder zielgerichtet / Betroffener Personenkreis...
- **Speichermedium:**
  - Arbeitsplatzrechner / IT-System / mobiles Endgerät / USB-Stick ...
- **Welche personenbezogenen Daten sind betroffen:**
  - Kontaktdaten / Zugangs- / Identifikationsdaten / Bank- / Zahlungs- / Finanzdaten / andere personenbezogene Daten / besondere Arten personenbezogener Daten / Telekommunikationsverkehrsdaten / Standortinformationen...
- **Durch welche technischen Vorkehrungen wurden die personenbezogene Daten gesichert:**
  - Sicherheitskonzept / Verschlüsselungsverfahren...
- **Wurden Sofortmaßnahmen zur Schadensbegrenzung / Eingrenzung der Risiken für die Betroffenen ergriffen?**  
**Achtung:** Der Datenschutzvorfall muss gemeldet werden, nicht aber welche konkreten Personen davon betroffen sind.








# **04 – WAS PASSIERT NACH EINER ERFOLGTEN MELDUNG BEIM KONZERNDATENSCHUTZ?**

# VORGEHEN BEI EINGETROFFENEN MELDUNGEN

## MELDUNG VON DATENSCHUTZVORFÄLLEN

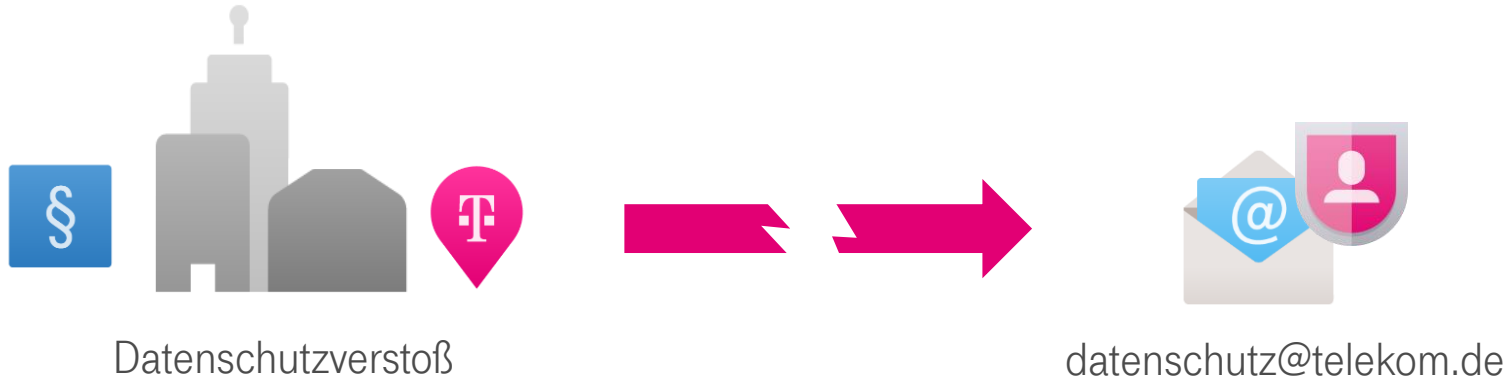
- (1)  Nachdem eine Meldung beim Konzerndatenschutz (Group Privacy) eingetroffen ist, prüfen Experten des Konzerndatenschutzes Ihre Meldung unverzüglich und leiten alle weiteren Schritte ein.
- (2)  Dabei wird zunächst bewertet, ob es sich tatsächlich um einen Datenschutzvorfall handelt und wie hoch das Ausmaß des Schadens ist. Anschließend werden umgehend entsprechende Maßnahmen zur Abwendung besprochen und eingeleitet.
- (3)  Wenn es sich um einen Datenschutzvorfall handelt, wird dieser anschließend an die Aufsichtsbehörden gemeldet und es erfolgt, falls notwendig, eine Benachrichtigung an die betroffenen Personen.

Alle Datenschutzvorfälle müssen nach § 109a Abs. 3 TKG / Artikel 33 (5) DSGVO bis zu 5 Jahren dokumentiert werden.

**05 – WAS PASSIERT WENN NICHT  
GEMELDET WURDE?**

# WAS PASSIERT, WENN VORFÄLLE NICHT GEMELDET WERDEN?

## MELDUNG VON DATENSCHUTZVORFÄLLEN



- Offenheit und Transparenz sind entscheidend für das Vertrauen unserer Kunden in unser Unternehmen und unsere Produkte.
- Die Verheimlichung eines Datenschutzvorfalls würde für das Unternehmen einen viel größeren Schaden mit sich bringen, als die Offenlegung des Vorfalls.
- Ein Datenschutzvorfall muss **innerhalb von 24 (Telekommunikation) / 72 Stunden (DSGVO)** an die zuständige Datenschutzaufsichtsbehörde gemeldet werden. Dies ist auch in Form von „Vorfeld-Meldungen“ möglich. Ein Verstoß gegen die Meldepflicht ist ein Bußgeldtatbestand und kann mit einem hohen Bußgeld geahndet werden.





# RECHTS GRUNDLAGEN

Artikel 33 DS-GVO:

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Artikel 34 DS-GVO:

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

Artikel 4 (12) DS-GVO:

Verletzung des Schutzes personenbezogener Daten

§109a TKG: Daten- und Informationssicherheit

§23 und §30 BCRP: Informationspflicht bei Verstößen

**ERLEBEN, WAS VERBINDET.**

# UNSERE MISSION



## VERTRAUENSÄÄUME SCHAFFEN

MIT UNSEREN PRODUKTEN UND SERVICES WOLLEN WIR DAS VERTRAUEN  
IN DIE MARKEN DES KONZERNES DEUTSCHE TELEKOM STÄRKEN.



**VIELEN DANK FÜR IHRE  
AUFMERKSAMKEIT**