Umgang mit Datenschutz-verletzungen

Hilfestellung zu wichtigen Fragen:

- **Wann** handelt es sich um eine Datenschutzverletzung?
- **Was** ist zu tun und **wer** muss handeln?
- **Wie** gelingt es?
- **Was** kann passieren?

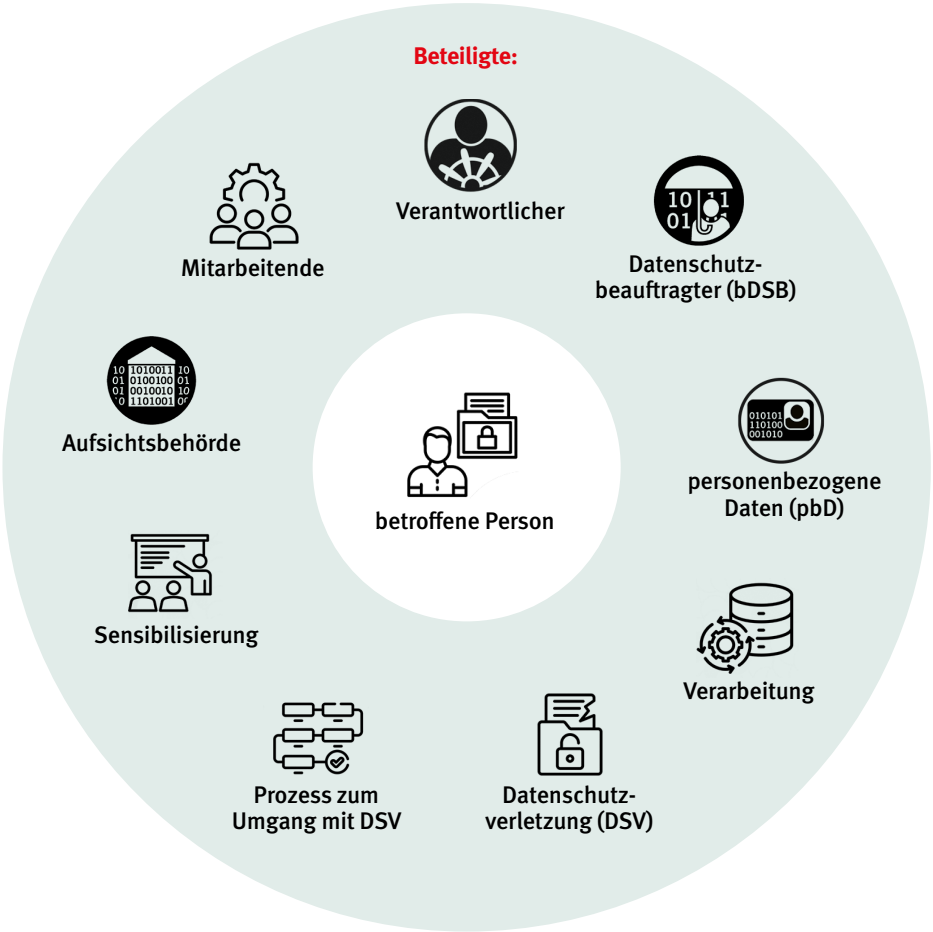
Katholische Datenschutzaufsicht Nord

Kath. Datenschutz-zentrum Frankfurt/M. KdöR

Wann handelt es sich um eine Datenschutzverletzung?

Die Verletzung des Schutzes personenbezogener Daten bedeutet

- eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig,
- zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung der Daten
- beziehungsweise zum unbefugten Zugang zu den Daten führt,
- die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.



Was ist zu tun und wer muss handeln?

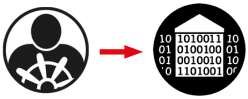
Erkennen einer Datenschutzverletzung durch Mitarbeitende/die Leitung oder einen Hinweis von außen

Prozess zum Umgang mit Datenschutzverletzungen in Gang setzen

Meldung an die Ansprechperson der Einrichtung (Koordinator, bDSB oder Verantwortlicher)

Bewertung des Vorfalls (Verantwortlicher, ggf. mit Unterstützung des Datenschutzbeauftragten)

Bei Gefahr für die Rechte und Freiheiten der betroffenen Person: Meldung an die Datenschutzaufsicht (Frist: 72 Stunden)



Bei hohem Risiko für die Rechte und Freiheiten: unverzügliche Information der betroffenen Person

Maßnahmen zur Abmilderung und Schadens-begrenzung – Vermeidung in der Zukunft

Schlussfolgerung und Sensibilisierung

- Ursachenanalyse durchführen
- Dienstbesprechungen, Teamsitzungen u. ä. für Datenschutzthemen nutzen und gegebenenfalls im Protokoll schriftlich festhalten
- Erkenntnisse aus Datenschutzverletzungen an Mitarbeitende weitergeben
- Durchführung einrichtungsspezifischer Sensibilisierungsmaßnahmen

Wie gelingt es?

Prozess zum Umgang mit Datenschutzverletzungen

- definieren, bekanntmachen und als zentrale Information speichern
- regelmäßig evaluieren
- funktionsbezogen gestalten, unabhängig von natürlichen Personen

Vorhandene Expertise in der Einrichtung nutzen

- bDSBs und ihre Erreichbarkeit bekanntmachen
- Arbeitshilfen der bDSBs nutzen
- ggf. Datenschutzkoordinatoren benennen

Sensibilisierung für den Datenschutz

- Schulungen im Onboarding-Prozess und danach regelmäßig durchführen
- zentrale Verfügbarkeit von Informationen zum Datenschutz (eigene Regelungen, Gesetzestexte, QM-Handbuch o. ä.) sicherstellen
- Arbeitsprozesse und Datenschutz gemeinsam denken und entwickeln

Informiert sein und handeln

- innerbetrieblichen Prozess zum Umgang mit Datenschutzverletzungen kennen
- bei Rückfragen zum Prozess an bDSB oder Datenschutzkoordinator wenden
- Datenschutzhinweise und -vorgaben (z. B. im QM-Handbuch) kennen und anwenden

Datenschutz leben und frühzeitig in die Arbeitsprozesse integrieren!

Was kann passieren?

Beispiele für Datenschutzverletzungen

Generell

- Hackerangriff auf IT-System mit personenbezogenen Daten (pbD)
- unsachgemäße Entsorgung von pbD (z. B. Entsorgung von Akten im Hausmüll oder Altpapier)
- Phishing-Angriff
- Falschversand von E-Mails (Nichtnutzung von BCC, falscher Adressat, fehlerhafte E-Mail-Adresse)
- Diebstahl oder Verlust von Geräten (Laptop, Kamera, Handy), Speichermedien oder Akten
- unverschlüsselter Versand von sensiblen pbD

Gesundheitsbereich

- Falschversand eines Arztbriefes (Brief oder Fax)
- unbefugte Foto- oder Videoaufnahmen von Patienten oder Mitarbeitenden mit dem Handy
- eigenmächtige Veröffentlichungen von Inhalten über Patienten, Klienten oder Mitarbeitende auf privaten Social-Media-Kanälen
- Zugriff auf Behandlungsdaten durch unberechtigte Mitarbeitende des Krankenhauses
- unbefugte Auskunft am Empfang

Kirchengemeinden

- unbefugter Zugriff auf Meldedaten
- (telefonische) Auskünfte über Gemeindemitglieder an unberechtigte Dritte
- Videoüberwachung in Kirchen mit Überwachung von Beichtstühlen

Vereine und Verbände

- Foto- und Videoaufnahmen durch Mitarbeitende oder Ehrenamtliche ohne entsprechende Einwilligungen und deren Veröffentlichung oder Weitergabe an Dritte (z. B. bei Veranstaltungen)
- unsachgemäßer Umgang mit Mitgliedsdaten

Kinder- und Jugendeinrichtungen

- Weitergabe von pbD an Nicht-Sorgeberechtigte
- fehlende Regelungen des Verantwortlichen zu Foto- und Videoaufnahmen durch Eltern (z. B. bei Veranstaltungen)
- Übermittlung von pbD an öffentliche Träger über nicht gesicherte Übertragungswege
- eigenmächtige Veröffentlichungen von Inhalten über Schutzbefohlene auf privaten Social-Media-Kanälen

Altenhilfe

- versehentliche Mitteilung von Gesundheitsdaten an Angehörige eines anderen Pflegeheimbewohners
- unberechtigter Zutritt von Bewohnern eines Pflegeheims oder von Besuchern ins Dienstzimmer
- Verbreitung von Inhalten über Bewohner oder Mitarbeitende über Social-Media-Kanäle (z. B. Fotos oder Videos)

Beschäftigten- und Bewerberdaten

- Falschversand von Arbeitsverträgen
- Verwechslungen von Gehaltsmitteilungen
- Offenlegung von pbD durch Zugriff auf falsch abgelegte Dateien

Katholische Datenschutzaufsicht Nord
Unser Lieben Frauen Kirchhof 20,
28195 Bremen

Meldeportal:

zuständig für die (Erz-)Bistümer
Hamburg, Hildesheim, Osnabrück
und das Bischöflich Münstersche
Offizialat in Vechta i.O.

Kath. Datenschutzzentrum
Frankfurt/M. KdöR
Roßmarkt 23, 60311 Frankfurt/M.

Meldeportal:

zuständig für die (Erz-)Bistümer
Freiburg, Fulda, Limburg,
Mainz, Rottenburg-Stuttgart,
Speyer und Trier