Richtlinie zum Vorgehen bei Datenpannen

1. Einleitung

Bei der Verarbeitung personenbezogener Daten können Fehler passieren. Das Gesetz spricht hier von Datenpannen.

Bei einer Datenpanne sind verschiedene Maßnahmen zu ergreifen. Diese werden in dieser Richtlinie beschrieben. **Sie gilt für alle Beschäftigten und Ehrenamtlichen.**

Was ist eine Datenpanne?

Eine Datenpanne liegt vor, **wenn personenbezogene Daten** oder andere vertrauliche Informationen unrechtmäßig verarbeitet oder übermittelt werden oder auf sonstige Weise **für unbefugte Personen zugänglich sind** (Verletzung der Vertraulichkeit).

Beispiele: Verlust oder Diebstahl von Datenträgern wie Laptop, USB-Stick oder Kamera, Brief an falschen Empfänger, offener E-Mail-Verteiler (Verwendung Cc-Feld statt Bcc-Feld).

Eine Datenpanne kann auch vorliegen, wenn personenbezogene Daten versehentlich **unwiederbringlich gelöscht** wurden, obwohl diese noch benötigt werden (Verletzung der Verfügbarkeit).

Beispiel: Zerstörung des Servers durch Brand oder Wasserschaden ohne Vorliegen von Sicherungskopien.

Eine Datenpanne kann auch vorliegen, wenn personenbezogene Daten versehentlich so **verändert** wurden, dass unklar ist, ob diese noch richtig sind (Verletzung der Integrität).

Datenpannen sind regelmäßig der Datenschutzaufsichtsbehörde (die Kirchliche Datenschutzaufsicht der ostdeutschen Bistümer und des Katholischen Militärbischofs) zu melden.

Es gelten kurze und strenge Fristen:

Ist die Datenpanne meldepflichtig, ist sie **spätestens nach 72 Stunden** zu melden. **Wird die Frist nicht eingehalten, sind Sanktionen möglich. Daher sind die beschriebenen Prozessschritte schnell und unverzüglich durchzuführen!** Es ist nicht zu warten, bis alle Informationen vollständig vorliegen. Diese können auch nachgereicht werden.

2. Beteiligte

Neben demjenigen, der die Datenpanne entdeckt, sind folgende Personen zu beteiligen:

INTERNER KOORDINATOR FÜR DATENSCHUTZ

Name:	Birgitt Korbmacher	E-Mail: birgitt.korbmacher@erzbistumberlin.de
Telefon (Büro):	030-32684179	recht@erzbistumberlin.de
Telefon (Mobil):	<[Telefonnummer]>	

IT-VERANTWORTLICHER			
Name:	Robert Arnold	E-Mail:	robert.arnold@erzbistumberlin.de
Telefon (Büro):	030-32684230		
Telefon (Mobil):	<[Telefonnummer]>		

ABTEILUNGSLEITUNG			
Name:	laut Ornigramm	E-Mail:	<[E-Mail-Adresse]>
Telefon (Büro):	<[Telefonnummer]>		
Telefon (Mobil):	<[Telefonnummer]>		

3. Ablauf

Schritt 0: Feststellung einer Datenpanne

Verantwortlich: Derjenige, der die Datenpanne bemerkt

Wird eine Datenpanne festgestellt oder besteht der Verdacht einer Datenpanne, erlangt ein Beschäftigter Kenntnis von einer Datenpanne oder von Umständen, die den Verdacht einer Datenpanne begründen, stößt er unverzüglich den nachfolgenden Prozess an.

Schritt 1: Benachrichtigung der zuständigen Personen

Verantwortlich: Derjenige, der die Datenpanne bemerkt

Als erstes sind nachfolgende Personen unverzüglich (per Telefon und E-Mail) zu benachrichtigen:

- Interner Koordinator für Datenschutz,
- IT-Verantwortlicher und
- Abteilungsleitung.

Jede der oben genannten Personen ist zu informieren.

Die **Prozessschritte 2.1 und 2.2** werden aufgrund der kurzen Fristen und einer möglicherweise weiterhin bestehenden Gefahr nach Möglichkeit **zeitgleich durchgeführt**.

Schritt 2.1: Prüfung, ob die Datenpanne noch akut oder beendet ist

Verantwortlich: interner Koordinator für Datenschutz und IT-Verantwortlicher

Im zweiten Schritt wird vom internen Koordinator für Datenschutz und dem IT-Verantwortlichen geprüft, ob die Datenpanne noch akut ist.

Wann ist die Datenpanne noch akut?

Die Datenpanne ist noch akut, wenn

- die Daten weiterhin unbefugten Personen zugänglich sind oder
- weiterhin Daten gelöscht oder geändert werden.

Ist die Datenpanne noch akut oder ist ihr Status unbekannt, stimmen die oben genannten Personen Maßnahmen ab, um die Datenpanne schnellstmöglich zu beenden oder einzudämmen. Ist die Datenpanne offensichtlich beendet, müssen keine Notfallmaßnahmen getroffen werden.

Schritt 2.2: Prüfung von Benachrichtigungspflichten

Verantwortlich: interner Koordinator für Datenschutz, Abteilungsleitung

Spätestens jetzt ist der Datenschutzbeauftragte einzubeziehen

Der interne Koordinator für den Datenschutz und die Abteilungsleitung prüfen mit dem Datenschutzbeauftragten, ob eine Meldung gegenüber der Kirchlichen Datenschutzaufsicht und eine Information gegenüber den betroffenen Personen erfolgen muss.

Muss eine Meldung an den Kirchlichen Datenschutzaufsicht und gegebenenfalls eine Information an die betroffenen Personen erfolgen, ist mit **Schritt 3** fortzufahren. Andernfalls folgt **Schritt 4**.

An die **Kirchliche Datenschutzaufsicht** ist zu melden, wenn nach einer ersten Bewertung voraussichtlich ein **Risiko für die Rechte und Freiheiten der betroffenen Person** besteht.

Die **betroffene Person** ist zusätzlich zu informieren, wenn die Datenpanne zu einem **hohen Risiko für die persönlichen Rechte und Freiheiten der betroffenen Person** führt.

Bei der Bewertung sind folgende Punkte zu berücksichtigen:

- Welche und wie viele Daten sind betroffen?
- Sind die Daten verschlüsselt oder anderweitig geschützt?
- Welche Schäden drohen (materielle und immaterielle Schäden)?
- Wie hoch ist der Schaden?
- Kann die betroffene Person selbst nach der Information noch Schutzmaßnahmen ergreifen?
- Angaben zu den technischen Umständen der Datenpanne und Motivlage des unrechtmäßigen Datenempfängers (zufälliger oder vorsätzlicher Zugriff).

Achtung: Ergibt die Bewertung, dass eine Meldepflicht besteht, muss die Meldung **spätestens nach 72 Stunden** bei der Kirchlichen Datenschutzaufsicht eingehen. **Wochenenden und gesetzliche Feiertage sind vom Fristlauf nicht ausgenommen.**

Schritt 3: Inhalt der Meldung

Verantwortlich: Interner Koordinator für Datenschutz, IT-Verantwortlicher, Abteilungsleitung und Datenschutzbeauftragter

Die Verantwortlichen tragen alle für eine Meldung erforderlichen Informationen zusammen. Dies umfasst zumindest folgende Daten:

- Beschreibung, was passiert ist, mit Angaben, welche Art von Daten betroffen sind, welche und wie viele Personen und Datensätze betroffen sind,
- Namen und die Kontaktdaten des internen Koordinators für Datenschutz sowie des Datenschutzbeauftragten,
- eine Beschreibung der möglichen Folgen der Datenpanne und
- eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenpanne und gegebenenfalls Maßnahmen zur Verringerung ihrer Folgen.

Die Meldung an die Kirchliche Datenschutzaufsicht hat **innerhalb der 72 Stunden** zu erfolgen:

Kirchliche Datenschutzaufsicht der ostdeutschen Bistümer und des Katholischen Militärbischofs

Matthias Ullrich

Badepark 4
39218 Schönebeck

Telefon: 03928 7179018
Telefax: 03928 7179019

Email: kontakt@kdsa-ost.de

Die Meldung sollte über das Meldeformular erfolgen:
https://www.kdsa-ost.de/meldestelle/datenschutzverletzung.html

Schritt 4: Ursachenforschung und Dokumentation

Verantwortlich: Interner Koordinator für Datenschutz und IT-Verantwortlicher

In jedem Fall sind die Ursachen der Datenpanne zu ermitteln. Die Ergebnisse der Ursachenforschung sind zu dokumentieren. Dokumentiert werden sollte auch:

- Wer hat wann an wen gemeldet,
- welche Maßnahmen wurden ergriffen,
- welche Erwägungsgründe waren maßgeblich für die Risikobewertung,
- welche Meldungen sind erfolgt oder unterblieben,
- welche Maßnahmen wurden getroffen, um eine erneute Datenpanne zu verhindern,
- besteht Optimierungsbedarf am hier beschriebenen Meldeprozess.

Das Protokoll ist aufzubewahren und auf Nachfrage der Kirchlichen Datenschutzaufsicht zur Verfügung zu stellen.

Kontaktdaten des betrieblichen Datenschutzbeauftragten:

Der Datenschutzbeauftragte bzw. dessen Mitarbeitende beraten Sie während des Prozesses. Diese sind bei einer Datenpanne **vor** einer Meldung an die Kirchliche Datenschutzaufsicht zu informieren:

ANSPRECHPARTNER	
Konstantin Kawerau, Volljurist,	Tel.: +49 (0) 30 3087749-22 E-Mail: kkawerau@datenschutz-nord.de
Jan-Christoph Thode Justiziar	Tel.: +49 (0) 421 3087749-21 E-Mail: jthode@datenschutz-nord.de
datenschutz nord GmbH Konsul-Smidt-Straße 88 28217 Bremen	office@datenschutz-nord.de

BETRIEBLICHER DATENSCHUTZBEAUFTRAGTER	
Dr. Uwe Schläger datenschutz nord GmbH Konsul-Smidt-Straße 88 28217 Bremen	E-Mail: office@datenschutz-nord.de www.datenschutz-nord-gruppe.de

Stand: Oktober 2022