72 Std.-Notfallplan im Falle einer Datenpanne (Ziel und Prozessbeschreibung)

1. **Schnelle Kenntniserlangung von Datenpannen nach Bekanntwerden der Datenschutzverletzung**
   - Revisionsfähige Dokumentation: Zeitpunkt des Bekanntwerdens der Datenpanne (Aktenvermerk, E-Mail o.ä.) durch den/die fachverantwortliche/n Mitarbeiter (bzw. Auftragsverarbeiter) und/oder die Leitung der Einrichtung bzw. Dienststelle. (Beginn der 72 Stunden Frist)
   - Sofern nicht schon bekannt, unverzügliche Meldung an die Leitung der Einrichtung/Dienststelle durch die Mitarbeiterinnen und Mitarbeiter bzw. den Auftragsverarbeiter. Dabei ist es wichtig festzustellen, welcher Datenschutzklasse (vgl. Hinweise s.u.) die verlorenen personenbezogenen Daten zugeordnet sind, um welche Datenkategorien es sich handelt (Adressdaten, Bankdaten, Gesundheitsdaten etc.) und wie viele Datensätze bzw. Personen von der Datenschutzverletzung betroffen sind.
   - Die Leitung der Einrichtung/Dienststelle meldet die Datenpanne direkt nach Bekanntwerden an den zuständigen Betrieblichen Datenschutzbeauftragten (BDSB) oder die Stabstelle Betrieblicher Datenschutz.

2. **Risikoanalyse/Bewertung der Datenpanne**
   - Durch die verantwortliche Dienststellenleitung in Zusammenarbeit mit dem zuständigen BDSB oder der Stabsstelle
   - Entwicklung objektiver Kriterien (Eintrittswahrscheinlichkeit, Schwere des Schadens für die betroffene Person, etc.) und Beschreibung der möglichen Folgen der Datenschutzverletzung

3. **Gegenmaßnahmen durch die verantwortliche Stelle**
   - Reflexion des Ablaufs (Bearbeitungsverfahren)
   - Abwendung und/oder zumindest Eindämmung der möglichen nachteiligen Auswirkungen, die durch missbräuchliche Verwendung der Daten für die betroffenen Personen entstehen könnten

4. **Entscheidung ob eine Meldung an die überdiözesane Datenschutzaufsicht erfolgen muss**
   - Durch die verantwortliche Dienststellenleitung in enger Zusammenarbeit mit dem/der zuständigen BDSB oder der Stabsstelle
   - Ggfls. Meldung an die überdiözesane Datenschutzaufsicht nach § 33 KDG durch die verantwortliche Stelle (https://www.bistum-trier.de/datenschutz/ oder unter https://meldungen.katholisches-datenschutzzentrum.de/?post_type=dsverletzung&mandant=sw)
   - Ggfls. Information der von der Datenschutzverletzung betroffenen Personen durch die verantwortliche Stelle nach § 34 KDG

Hinweise zu personenbezogenen und besonderen personenbezogenen Daten und ihre Zuteilung zu Datenschutzklassen:

Personenbezogene Daten sind nach § 4 Nr. 1 KDG:

alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

Besondere Kategorien personenbezogener Daten sind nach § 4 Nr. 2 KDG:

Personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Die Zugehörigkeit zu einer Kirche oder Religionsgemeinschaft ist keine besondere Kategorie personenbezogener Daten.

Die Zuordnung zu einer Datenschutzklasse erfolgt im Hinblick auf die im Dokument enthaltenen Daten mit dem höchsten Schutzbedarf. Die jeweiligen Schutzmaßnahmen sind kumulativ zu verstehen, d.h. um den erhöhten Schutzbedarf zu gewährleisten müssen zusätzliche, weitere Schutzmaßnahmen ergriffen werden. Entsprechend gelten für die Datenschutzklasse (DSK) III selbstverständlich auch die Maßnahmen der DSK I und II.

Datenschutzklasse I (Schutzniveau I vgl. § 11 KDG-DVO)

(Eine missbräuchliche Verarbeitung lässt keine besonders schwer wiegende Beeinträchtigung des Betroffenen erwarten): z.B. Namens- und Adressangaben ohne Sperrvermerke, Berufs-, Branchen- oder Geschäftsbezeichnungen

Datenschutzklasse II (Schutzniveau II vgl. § 12 KDG-DVO)

(Eine missbräuchliche Verarbeitung kann den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen): z.B. Daten über Mietverhältnisse, Geschäftsbeziehungen sowie Geburts- und Jubiläumsdaten

Achtung ab DSK II: Kennwort/Authentifizierungsverfahren/elektronischer Versand nach außerhalb des geschlossenen und gesicherten BGV-Netzwerkes grundsätzlich verschlüsselt!

Datenschutzklasse III (Schutzniveau III vgl. § 13 KDG-DVO)

(Eine missbräuchliche Verarbeitung kann die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen. z.B. Gesundheitsdaten, rassische und ethnische Herkunft, politische Meinungen, Daten zum Sexualleben oder zur sexuellen Orientierung, strafbare Handlungen, religiöse oder weltanschauliche bzw. philosophische Überzeugungen, Gewerkschaftszugehörigkeit, genetische oder biometrische Daten zur eindeutigen Identifizierung, arbeitsrechtliche Rechtsverhältnisse, Disziplinarentscheidungen, Namens- und Adressangaben mit Sperrvermerken, usw.

Achtung ab DSK III: auf mobilen Geräten nur wenn zwingend erforderlich und nur noch verschlüsselt, nach dem aktuellen Stand der Technik, abspeichern. Langfristige Lesbarkeit!