72 Stunden-Notfallplan im Fall einer Datenpanne
(Ziel- und Prozessbeschreibung)

1. **Schnelle Dokumentation von und Kommunikation über Datenpannen nach Bekanntwerden der Datenschutzverletzung**
   - Revisionsfähige Dokumentation: Zeitpunkt, zu dem die Datenpanne bekannt geworden ist (Aktenvermerk, E-Mail o.ä.) durch den/die fachverantwortliche/n Mitarbeiter/in (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 Mitarbeiterin(nen) und Mitarbeiter bzw. den Auftragsverarbeiter. Dabei ist es wichtig, festzustellen, zu welcher Datenschutzklasse (vgl. Hinweise unten) die verlorenen personenbezogenen Daten gehören, 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 Datenpannedirekt nach Bekanntwerden an die / den zuständige/n Betriebliche/n Datenschutzbeauftragte/n (BDSB) oder die Stabstelle Betrieblicher Datenschutz.

2. **Risikoanalyse / Bewertung der Datenpanne**
   - Durch die verantwortliche Dienststellenleitung in Zusammenarbeit mit dem zuständigen BDSB oder der Stabsstelle
   - Bewertung der Datenpanne nach objektiven Kriterien durch die verantwortliche Dienststellenleitung (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 betroffene(n) Person(en) 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 (www.bistum-trier.de/datenschutz/ oder unter http://bit.ly/meldung-schutz)
   - Ggfls. Information der von der Datenschutzverletzung betroffenen Person(en) durch die nach § 34 KDG verantwortliche Stelle

Hinweise zur Einteilung der personenbezogenen Daten in Datenschutzklassen:

Datenschutzklasse I

(Eine missbräuchliche Verarbeitung lässt keine besonders schwer wiegende Beeinträchtigung der / des Betroffenen erwarten.)

Dazu gehören z.B. Adressangaben ohne Sperrvermerke, Berufs-, Branchen- oder Geschäftsbezeichnungen

Datenschutzklasse II

Eine missbräuchliche Verarbeitung kann den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen.)

Zum Beispiel Daten über Mietverhältnisse, Geschäftsbeziehungen sowie Geburts- und Jubiläumsdaten

Datenschutzklasse III

Eine missbräuchliche Verarbeitung kann die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen.)

Zum Beispiel Daten über gesundheitliche Verhältnisse, strafbare Handlungen, religiöse oder politische Anschauungen, arbeitsrechtliche Rechtsverhältnisse, Disziplinarentscheidungen usw. sowie Adressangaben mit Sperrvermerken.

Bischöfliches Generalvikariat
Stabsstelle Betrieblicher Datenschutz
Mustorstraße 2
54290 Trier
Tel. 0651 7105-468
E-Mail: datenschutz@bgv-trier.de