**Verfahrensanweisung „Datenpanne“**

|  |
| --- |
| 1. **Ziel und Zweck des Verfahrens** |
| Ziel: Einhaltung der gesetzlichen Bestimmung aus der Datenschutzgrundverordnung (DS-GVO) und Abwendung oder Minimierung von Schäden für den Verantwortlichen für die Datenverarbeitung und den / die Betroffenen.  Handreichung für den DSB für die Durchführung des Verfahrens.  Koordinierte Durchführung des Verfahrens durch den DSB ggf. mit der Meldepflicht an die zuständige Aufsichtsbehörde und ggf. die Benachrichtigung der betroffenen, natürlichen Personen. |

|  |  |
| --- | --- |
| 1. **Geltungsbereich und Befugnisse:** | |
| **Geltungsbereich** | Alle Einrichtungen des DRK |
| **Mitarbeit und Befugnisse** | Der Datenschutzbeauftragte (DSB) koordiniert das Verfahren.  Die Mitarbeiter aller betroffenen Fachbereiche unterstützen den DSB bei der Durchführung. |

|  |  |
| --- | --- |
| 1. **Eingaben und strukturelle Voraussetzungen:** | |
| **Eingaben** | Eine Schutzverletzung personenbezogener Daten (pbD) liegt vor und wurde erkannt. |
| **Strukturelle Voraussetzungen** | Softwarepanne, Hackerangriff oder organisatorisches oder menschliches Versagen liegt vor. |

|  |
| --- |
| 1. **Beschreibung:** |
| **Gesetzliche Grundlage**  Die gesetzliche Grundlage für die Durchführung des Verfahrens bei einer Schutzverletzung von personenbezogenen Daten (pbD) ist in Art. 33 und 34, sowie ErwG (Erwägungsgrund) 85-88 DS-GVO verankert.  **Meldepflichtige Vorfälle**  Im weitesten Sinne liegt bei der Schutzverletzung von pbD eine Verletzung der Sicherheit der Datenverarbeitung vor. Nach Art. 4 Nr. 12 DS-GVO handelt es sich um folgende Verletzungssituationen:   * Vernichtung pbD (z.B. Datenlöschung) * Verlust (z.B. Diebstahl oder Zerstörung von Speichermedien) * Veränderung (z.B. von Datensatzinhalten) * Unbefugte Offenlegung (z.B. unbefugte Dritte erhalten Daten ohne Erlaubnistatbestand) * Unbefugter Zugang (z.B. durch falsche Berechtigungskonzepte)   Die Meldepflicht tritt ein, wenn Schutzmaßnahmen nicht wirkungsvoll waren und dadurch die Schutzvorgaben der DS-GVO verletzt wurden. Für die Meldepflicht ist es unerheblich, ob eine Softwarepanne zur Schutzverletzung geführt hat oder ein Hackerangriff dafür verantwortlich ist. Die frühere Beschränkung auf bestimmte Datenkategorien besteht nicht mehr – alle pbD sind in die Meldepflicht eingeschlossen, unabhängig davon, ob die Schutzverletzung verschuldet, unabsichtlich oder widerrechtlich erfolgt ist.  Nur eine infrastrukturelle Verletzung der IT-Sicherheit ohne Personenbezug ist von der DS-GVO nicht erfasst.  Eine Meldung an die Aufsichtsbehörde erfolgt nur dann, wenn es gesichert zu einer Schutzverletzung pbD gekommen ist. Eine vage Vermutung oder der bloße Verdacht reichen nicht aus.  Auch der Auftragsverarbeiter ist in der Pflicht, dem Verantwortlichen eine Schutzverletzung pbD unverzüglich zu melden (Art. 33 Abs. 2 DS-GVO). Der Auftragsverarbeiter unterstützt den Verantwortlichen. Da der Umfang der Unterstützungsleistung nicht in der DS-GVO geregelt ist empfiehlt sich eine Konkretisierung im Auftragsverarbeitungsvertrag. Regelungsgegenstände sollten sein:   * Umfang der Unterstützungspflicht * Bereitzustellende Informationen * Zeitpunkt und Frist für die Mitteilung * Verschwiegenheitsvereinbarung   **Beurteilung des Vorfalls**  Für eine Meldung der Schutzverletzung an die Aufsichtsbehörde und zusätzlich an den / die Betroffenen ist nicht notwendig, wenn die Schutzverletzung „nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt“ (Art. 33 Abs. 1 und ErwG 75 DS-GVO zu den Risiken für die Rechte und Freiheiten natürlicher Personen); Zur Beurteilung des Risikos nach der DS-GVO beachten Sie bitte das Vorgehen in der entsprechenden Handlungsanleitung.  **Meldung gegenüber der Aufsichtsbehörde**  Für die Meldung einer Schutzverletzung pbD müssen nicht sofort alle Informationen bereitstehen. Art. 33 Abs. 3 DS-GVO gestattet ein schrittweises Vorgehen. Nach der ersten Meldung erfolgen die weiteren Meldungen bezogen auf die Erstmeldung zum Zeitpunkt, wenn neue Informationen bekannt sind bis schließlich alle zu meldenden Informationen gemäß Art. 33 Abs. 3 lit. a bis d beisammen sind.  Die Meldung an die Aufsichtsbehörde hat „**unverzüglich und möglichst binnen 72 Stunden“ nach bekannt werden der Schutzverletzung zu erfolgen** (Art. 33 Abs. 1 Satz 1 und ErwG 85 und 87 DS-GVO). Dies gilt auch für etwaige Folgemeldungen. Eine Überschreitung der Frist ist nur in begründeten Fällen möglich.  „Unverzüglich“ bedeutet nach der Legaldefinition in § 121 Abs. 1 Satz 1 BGB „ohne schuldhaftes Zögern“, also innerhalb einer angemessenen Prüfungs- und Überlegungszeit.  **Inhalt der Meldung an die Aufsichtsbehörde**  Hat die Risikobeurteilung ergeben, dass eine Meldung an die Aufsichtsbehörde erfolgt (es reicht ein „normales“ Risiko), orientiert man sich an dem Kriterienkatalog (Minimalanforderung) aus Art. 33 Abs. 3 lit. a bis d DS-GVO:   * Beschreibung der Art der Schutzverletzung (z.B. Datenverlust) * Angabe der Kategorien von betroffenen Personen (z.B. Mitarbeiter, Kunden) * Angabe der ungefähren Zahl der betroffenen Personen, der betroffenen Datenkategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze * Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle * Beschreibung der wahrscheinlichen Folgen der Schutzverletzung (z.B. finanzieller Schaden durch Offenlegung von Bank- und Kreditkartenkonten) * Eine Beschreibung ergriffener oder vorgeschlagener Maßnahmen zur Behebung der Schutzverletzung und gegebenenfalls Maßnahmen zur Abmilderung der Folgen. * Ebenfalls welche Maßnahmen aus welchen Gründen noch nicht erfolgt sind.   Eine besondere Form schreibt die DS-GVO nicht vor (zu Format und Verfahren der Meldung siehe auch ErwG 88 DS-GVO). Liegt ein hohes Risiko für die Betroffenen vor oder andere Dringlichkeiten, empfiehlt sich vorab eine telefonische Kontaktaufnahme mit der Aufsichtsbehörde, der dann ein Brief, eine E-Mail oder ein Fax folgt.  **Information der betroffenen Personen**  Betroffene müssen - im Gegensatz zur Aufsichtsbehörde - erst dann benachrichtigt werden, wenn durch die Schutzverletzung ein hohes Risiko für ihre Rechte und Freiheiten besteht (Art. 34 Abs. 1 und ErwG 86 DS-GVO). In jedem Fall erfolgt die Benachrichtigung der Betroffenen separat und nicht mit der gleichen Information, wie die an die Aufsichtsbehörden. Es empfiehlt sich, 2 unterschiedliche Vorlagen für die Benachrichtigung der Aufsichtsbehörde und der Betroffenen zu erstellen.  **Art und Weise und Inhalt der Information Betroffener**  Die Benachrichtigung betroffener Personen hat in klarer, verständlicher Sprache zu erfolgen. Sie beschreibt die Art der Schutzverletzung und enthält die Informationen aus Art. 33 Abs. 3 lit b bis d DS-GVO (Art. 34 Abs. 2 DS-GVO):   * Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle * Beschreibung der wahrscheinlichen Folgen der Schutzverletzung * Eine Beschreibung ergriffener oder vorgeschlagener Maßnahmen zur Behebung der Schutzverletzung und gegebenenfalls Maßnahmen zur Abmilderung der Folgen.   **Ausnahmen von der Benachrichtigungspflicht Betroffener**  In 2 Fällen muss der Verantwortliche die Betroffenen nicht benachrichtigen (Art. 34 Abs. 3 DS-GVO):   1. Im Vorfeld wurden technische und organisatorische Maßnahmen ergriffen, die unbefugten Zugang zu den Daten nunmehr verhindern und 2. Maßnahmen im Nachgang stellen sicher, dass ein hohes Risiko für die Betroffenen nicht mehr besteht. Beispielsweise durch eine Risikominimierung für gelöschte Daten durch Wiederherstellung oder eine Fernlöschung verlorener Speichermedien.   Auf die Ausnahmen kann sich der Verantwortliche nur berufen, wenn eine neuerliche Bewertung des Restrisikos sicherstellt, dass es unter die Schwelle für Meldung oder Benachrichtigung fällt.  Ist die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden, kann an ihre Stelle eine öffentliche Benachrichtigung / Bekanntmachung treten (Art. 34 Abs. 3 lit c DS-GVO), beispielsweise, wenn veraltete Kontaktdaten von Kunden vorliegen und neue erst ermittelt werden müssen. Die Maßnahme muss unbedingt „vergleichbar wirksam“ informieren.  § 29 Abs. BDSG-neu beschreibt den Sonderfall in dem keine Pflicht zur Benachrichtigung Betroffener vorliegt, „soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen“.  Dies trifft dann zu, wenn beispielsweise personenbezogene Daten offenbart werden müssten, die der ärztlichen Schweigepflicht nach § 203 StGB unterliegen und wegen des überwiegenden berechtigten Interesses eines Dritten geheim gehalten werden müssen.  **Dokumentationspflicht**  Die Dokumentation dient nicht nur der Aufsichtsbehörde zur Prüfung, sondern auch dem Verantwortlichen selbst.  In Anlehnung an Art. 33 DS-GVO enthält die Dokumentation alle Fakten, die in Zusammenhang mit der Schutzverletzung stehen, die Auswirkungen und die Abhilfemaßnahmen. Sie kann über die Mindestanforderung hinausgehen und alles enthalten, was bei einer Aufarbeitung der Vorfälle nützlich ist und hilft, das Risiko für Schutzverletzungen künftig zu minimieren.  **Bußgelder**  Aufsichtsbehörden können bei Verstößen gegen Art. 33 und 34 DS-GVO Geldbußen bis zu 2 Mio € verhängen oder 2% des Jahresumsatzes (Art. 83 Abs. 4 lit a DS-GVO).  Darüber hinaus können betroffene Personen Schadensersatzansprüche geltend machen (§ 823 BGB). |