Arbeitshilfe zur Meldung von Datenpannen

Allgemeiner Teil

Was ist eine Datenpanne?

Unter einer Datenpanne werden Verletzungen des Schutzes personenbezogener Daten im Sinne von § 4 Nr. 1 DSG-EKD verstanden. Eine Verletzung des Schutzes personenbezogener Daten ist gemäß § 4 Nr. 14 DSG-EKD eine Verletzung der Sicherheit, die

- zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von personenbezogenen Daten oder
- zum unbefugten Zugang zu personenbezogenen Daten

führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Hierzu zählen z. B. der Verlust von Datenträgern oder Geräten, auf denen Daten unverschlüsselt gespeichert sind, das Bekanntwerden von Passworten und der unberechtigte Zugriff auf Daten oder Datenabflüsse durch Softwarefehler. Daraus kann sich eine Meldepflicht nach §§ 32, 33 DSG-EKD ergeben.

Wer ist zur Meldung verpflichtet?

Die Meldepflicht wird von der verantwortlichen Stelle ausgeführt (§ 32 Abs. 1 Satz 1 DSG-EKD). Wer verantwortliche Stelle ist, ergibt sich aus § 4 Nr. 9 DSG-EKD. Innerhalb der verantwortlichen Stelle trifft diese Pflicht die Leitung.

Außerdem sind Auftragsverarbeiter gemäß § 32 Abs. 2 DSG-EKD verpflichtet Daten- pannen unverzüglich an die verantwortliche Stelle (Auftraggeber) zu melden.

Meldung an die Aufsichtsbehörde

Wann muss die Aufsichtsbehörde informiert werden?

Die verantwortliche Stelle muss eine Datenpanne unverzüglich, das heißt ohne schuldhaftes Zögern, an die Aufsichtsbehörde nach § 39 DSG-EKD melden. Die Meldung ist nicht erforderlich, wenn die Datenpanne voraussichtlich nur zu einem unerheblichen Risiko für die Rechte betroffener natürlicher Personen führt. Die Meldepflicht entsteht mit Kenntnis der betroffenen Stelle von der Datenpanne (z. B. unrechtmäßige Datenübermittlung oder Kenntnisnahme). Für die Meldung an die Aufsichtsbehörde ist unerheblich, ob die Sicherheitslücke bereits geschlossen ist oder ob z. B. Ermittlungen der Strafverfolgungsbehörde noch nicht abgeschlossen sind. Maßgeblich ist ausschließlich, ob ein nicht unerhebliches Risiko für die Rechte betroffener Personen besteht.

Auftragsverarbeiter müssen eine Datenpanne unverzüglich der beauftragenden Stelle melden (§ 32 Abs. 2 DSG-EKD). Deshalb muss die Meldepflicht des Auftragsverarbeiters gegenüber der beauftragenden Stelle ausdrücklich im Vertrag zur Auftragsverarbeitung geregelt sein (siehe auch § 30 Abs. 3 Nr. 8 DSG-EKD). Die beauftragende Stelle entscheidet dann, ob eine Meldung an die Aufsichtsbehörde und ggf. auch eine Benachrichtigung an betroffene Personen notwendig ist.

Wann liegt ein „voraussichtlich nicht unerhebliches Risiko“ für die persönlichen Rechte natürlicher Personen vor?

Eine Meldung hat grundsätzlich immer dann zu erfolgen, wenn personenbezogene Daten unberechtigt abgeflossen sind. Diese Verpflichtung besteht nur dann nicht, wenn für die Rechte betroffener Personen lediglich ein unerhebliches Risiko besteht.

Bei der Feststellung, ob ein „voraussichtlich nicht unerhebliches Risiko“ besteht, sind die Eintrittswahrscheinlichkeit und Schwere der Datenpanne und der drohenden Rechtsverletzung zu berücksichtigen. Dabei sind Art, Umfang und Umstände der zugrundliegenden Verarbeitung zu beachten.

Worüber muss die Aufsichtsbehörde informiert werden?

Die Datenpanne muss im Rahmen der Meldung gemäß § 32 Abs. 3 Nr. 1 - 4 DSG-EKD detailliert beschrieben werden. Alle relevanten Informationen sind hierbei der Aufsichtsbehörde mitzuteilen. Im Einzelnen müssen insbesondere folgende Informationen enthalten sein:

§ 32 Abs. 3 Nr. 1 DSG-EKD

Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der

- Kategorien und der ungefähren Zahl der betroffenen Personen;
- Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

Wichtige Kontrollfragen in diesem Zusammenhang sind:

- Was hat zu der Datenpanne geführt (z. B. Fehlverhalten, Einwirkungen von außen, organisatorische Mängel, technische Probleme)?
- Was ist mit den Daten geschehen (z. B. Verlust, Löschung, Diebstahl, unbefugte Kenntnisnahme)?
- Um welche Kategorien von betroffenen Personen handelt es sich (z. B. Beschäftigte, Gemeindeglieder, Patienten, Klienten)?
- Um welche Kategorien personenbezogener Datensätze handelt es sich (z. B. Beschäftigtendaten, Meldedaten, Gesundheitsdaten)?
- Um welche Einzelangaben handelt es sich (z. B. Name, Straße, Alter, Diagnose)?
- Wann ist die Datenpanne geschehen? Wann wurde dies von der verantwortlichen Stelle bemerkt?

§ 32 Abs. 3 Nr. 2 DSG-EKD

Den Namen und die Kontaktdaten der örtlich Beauftragten für den Datenschutz oder einer sonstigen Anlaufstelle für weitere Informationen.

Hinweis: Sind keine örtlich Beauftragten für den Datenschutz bestellt, so ist die Person zu benennen, die verbindlich Auskunft zur Datenpanne geben kann.

§ 32 Abs. 3 Nr. 3 DSG-EKD

Eine Beschreibung der wahrscheinlichen Folgen der Datenpanne. Wichtige Kontrollfragen in diesem Zusammenhang sind:

- Welche Nachteile und Folgen sind für die Betroffenen zu befürchten (z. B. Diskriminierung, Rufschädigung, wirtschaftliche oder gesellschaftliche Nachteile, Identitätsdiebstahl)?
- Wie wahrscheinlich ist deren Eintritt?

§ 32 Abs. 3 Nr. 4 DSG-EKD

Eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenpanne und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Hinweis: Die Maßnahmen sind gegenüber der Aufsichtsbehörde so zu beschreiben, dass diese feststellen kann, ob eine ggf. bestehende Sicherheitslücke nunmehr geschlossen ist. Mögliche Beispiele sind der Austausch von Passwörtern, die Tatsache, dass ein Server vom Netz genommen worden ist, die Verbreitung einer Publikation einschränken, Mitarbeitersensibilisierung, Inhalt aus dem Internet entfernen oder Pseudonymisierung wiederherstellen.

In welcher Form muss die Aufsichtsbehörde informiert werden?

Grundsätzlich ist hierfür keine Form vorgeschrieben. Aus Nachweisgründen hinsichtlich der Anforderungen aus § 32 DSG-EKD sollte die Benachrichtigung der Aufsichtsbehörde schriftlich oder in elektronischer Form erfolgen.

Welche Folgen kann eine unterlassene Meldung haben?

Die Benachrichtigung der Aufsichtsbehörde ist eine Pflicht nach § 32 Abs. 1 DSG- EKD. Soweit diese fahrlässig oder vorsätzlich unterbleibt, liegt eine Pflichtverletzung der verantwortlichen Stelle vor. Mögliche Folgen sind die allgemeinen Aufsichtsmittel nach § 44 Abs. 2 und 3 DSG-EKD und die Geldbuße nach § 45 Abs. 1 DSG-EKD.

Benachrichtigung an die betroffene Person

Wann muss die betroffene Person informiert werden?

Die betroffene Person ist gemäß § 33 Abs. 1 DSG-EKD unverzüglich zu benachrichtigen, wenn die Datenpanne voraussichtlich ein hohes Risiko für die persönlichen Rechte betroffener Personen zur Folge hat.

Von einer Benachrichtigung kann gemäß § 33 Abs. 3 DSG-EKD abgesehen werden, wenn:

- die verantwortliche Stelle durch nachträgliche Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht, oder
- die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine im kirchlichen Bereich übliche öffentliche Bekanntmachung (z. B. Amtsblatt, Gemeindebrief, Aushang) oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

Als Maßnahmen, die eine Benachrichtigung entbehrlich machen können, kommen z. B. in Frage: Löschen veröffentlichter Daten, Einschränkung von Zugriffs- und Nutzungsrechten, Behebung von Sicherheitslücken in Software, Verschlüsselung.

Worüber muss die betroffene Person benachrichtigt werden?

Sinn und Zweck der Benachrichtigung über die Datenpanne ist es, die betroffene Person in die Lage zu versetzen, geeignete Schutzmaßnahmen treffen zu können und somit Schaden von ihr abzuwenden. Deshalb sollte die betroffene Person in transparenter und verständlicher Art und Weise darüber informiert werden, was geschehen ist und welche Gefahren (z. B. Missbrauch oder Reputationsschaden) ihr durch die Datenpanne drohen.

Zunächst sollte die betroffene Person über die Art der Datenpanne informiert werden. Außerdem ist es erforderlich, konkret zu benennen, welche personenbezogenen Daten von der Datenpanne betroffen sind. Weiterhin muss die Information an die betroffene Person gemäß § 33 Abs. 2 i. V. m. § 32 Abs. 3

DSG-EKD folgende Punkte umfassen:

- den Namen und die Kontaktdaten der örtlich Beauftragten für den Datenschutz oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Datenpanne;
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenpanne und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Zur Schadensminderung sollte die verantwortliche Stelle neben der Beschreibung bereits ergriffener oder geplanter Maßnahmen konkrete Handlungsempfehlungen an die betroffene Person geben. Beispiele können die Änderung von Passwörtern oder Kundennummern sein.

Besonderheiten ergeben sich bei Personen, die unter Betreuung stehen oder bei Minderjährigen: Hier sind ggf. die Betreuer oder die Personensorgeberechtigten zu informieren. Ist die Einsichtsfähigkeit der betroffenen Personen gegeben, dann sind diese zusätzlich zu benachrichtigen.

In welcher Form ist die betroffene Person zu benachrichtigen?

Grundsätzlich muss jede betroffene Person einzeln über die Datenpanne informiert werden. Zur besseren Nachweisbarkeit für die verantwortliche Stelle sollte die Benachrichtigung mittels einer verschlüsselten E-Mail oder per Post erfolgen. Die Benachrichtigung muss in klarer und einfacher Sprache formuliert sein.

Soweit von einer Benachrichtigung gemäß § 33 Abs. 3 Nr. 2 DSG-EKD abgesehen werden kann, hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen. Diese muss in einer im kirchlichen Bereich üblichen Art und Weise erfolgen. Die betroffenen Personen müssen auf diesem Wege vergleichbar wirksam informiert werden. Es muss hierbei immer der konkrete Einzelfall betrachtet werden. So kann eine Veröffentlichung im Gemeindebrief bzw. in Schaukästen der Gemeinde ausreichen, wenn die Datenpanne lediglich gemeindeinterne Auswirkungen hat. Falls Personen außerhalb der Gemeinde betroffen sind, muss eine Veröffentlichung in einer anderen Art und Weise erfolgen, z. B. in einer Tageszeitung.

Welche Folgen kann eine unterlassene Benachrichtigung nach sich ziehen?

Die Benachrichtigung der betroffenen Person ist eine Pflicht nach § 33 Abs. 1 DSG- EKD. Soweit diese fahrlässig oder vorsätzlich unterbleibt, liegt eine Pflichtverletzung der verantwortlichen Stelle vor. Mögliche Folgen sind die allgemeinen Aufsichtsmittel nach § 44 Abs. 2 und 3 DSG-EKD und die Geldbuße nach § 45 Abs. 1 DSG-EKD. Soweit der Person aufgrund der unterlassenen Benachrichtigung die Möglichkeit genommen wird, eigene Maßnahmen zu ergreifen, können sich weitere Schadensersatzansprüche ergeben.

Dokumentation der Datenpanne

Der Vorfall sowie die getroffenen Maßnahmen sind nach § 32 Abs. 5 DSG-EKD zu dokumentieren. Die Dokumentation muss alle mit dem Vorfall zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen umfassen. Die Maßnahmen sind so detailliert zu beschreiben, dass die Aufsichtsbehörde feststellen kann, ob die Sicherheitslücke geschlossen wurde bzw. wie die festgestellte unrechtmäßige Kenntnisnahme für die Zukunft ausgeschlossen ist.

Meldepflicht des Auftragsverarbeiters

Wird einem Auftragsverarbeiter eine Datenpanne bekannt, so hat er dies der verantwortlichen Stelle nach § 32 Abs. 2 DSG-EKD unverzüglich mitzuteilen. Daraufhin kann diese ihrer Meldepflicht nach § 32 Abs. 1 DSG-EKD an die Aufsichtsbehörde nachkommen. Die Verpflichtungen des Auftragsverarbeiters sollen im Rahmen des AV-Vertrages zwischen die Parteien geregelt werden (vgl. § 8 Informations- und Unterstützungspflichten des Auftragsverarbeiters der AV- Mustervereinbarung).

Anforderungen an die interne Organisation der verantwortlichen Stelle

Es muss sichergestellt sein, dass der Sachverhalt, der eine Meldepflicht auslösen kann, der Leitung bzw. dem Vorstand unverzüglich zur Kenntnis gebracht wird. Diese internen Meldungen (Alarmkette) können im Rahmen einer Dienstanweisung geregelt werden. Mitarbeitende sind diesbezüglich zu sensibilisieren. Es soll eine zentrale Anlaufstelle für mögliche Datenpannen geschaffen werden, die weitere notwendige Schritte einleitet. Hierfür können die örtlich Beauftragten für den Datenschutz bestimmt werden.