Was ist zu tun bei Datenpannen?

(Jupp Joachimski, Datenschutzbeauftragter der bayerischen (Erz-) Diözesen)

Was ist eine Datenpanne?

Der Begriff „Datenpanne“ existiert so nicht im kirchlichen Datenschutzgesetz. Vielmehr findet man dort den Begriff der Datenschutzverletzung. Eine Datenschutzverletzung liegt immer dann vor, wenn der Datenverkehr infolge eines Verstoßes gegen Datenschutzgesetze Fehler aufweist, die dazu führen können, dass dem Inhaber der personenbezogenen Daten ein Schaden erwächst. Bei der Feststellung eines irregulären Datenvorgangs ist allerdings noch völlig unklar, ob wirklich gegen Datenschutzbestimmunen verstoßen wurde und ob dies gegebenenfalls schuldhaft geschah – und wie es mit einem Schaden aussieht. Deswegen gebrauchen wir häufig den nicht wirklich im Gesetz verwendeten Begriff „Datenpanne“.

Was kann alles eine Datenpanne sein?

Die Liste möglicher Datenpannen ist nahezu unendlich. Ich werde deswegen in der Reihenfolge ihrer Häufigkeit nur die allerwichtigsten Datenpannen darstellen.

1. *Verwendung der AN- oder CC-E-Mail-Adressierung statt BCC:*
   E-Mail-Adressen, die Sie in den Feldern **AN** oder **CC** des Programms Outlook angeben, werden allen Empfängern mitgeteilt. Damit erfahren regelmäßig Personen E-Mail-Adressen (=personenbezogene Daten), die sie nichts angehen.
   Abhilfe: Schicken Sie Kopien grundsätzlich in BCC!

2. *Versendung normaler Post an die falsche Adresse:*
   Der Krankenhausbrief wird an Dr. Hubert Meier statt an Dr. Herbert Meier geschickt.
   Abhilfe: Jeden Brief mit besonders sensiblen Daten vor dem Absenden auf richtigen Adressaten auf den Briefumschlag prüfen.

3. *Datenträger mit personenbezogenen Daten geht z.B. auf dem Postweg verloren.*
   Abhilfe: Legen Sie bei einem europäischen Anbieter ein Speicherkonto an (z.B. Magenta, Ionos, Web.de, Strato), speichern Sie die Daten in einem Ordner und geben Sie dem Empfänger Zugangsberechtigung (= „Teilen“).

4. *Ein Hacker- oder Phishingangriff führt zu Datenverlust oder Datenweiterleitung an Unbefugte.* Bei dieser Situation ist anfangs meist die Reichweite des Schadens und sein Ausmaß gar nicht recht abschätzbar. Auch diese Situation geht auf regelmäßig auf eine Fehlleistung eines Benutzers zurück. Abhilfe:
   Öffnen Sie nie Anhänge von Emails oder Links in Emails, wenn Ihnen der Absender unbekannt ist oder das Mail Besonderheiten aufweist wie verlockende Angebote, Entscheidungsdruck erzeugende Umstände oder wenn Sie sonst – z.B. der

Aufmachung wegen – Zweifel an der Daseinsberechtigung des E-Mails haben. Wenn Sie nicht telefonisch beim Absender zurückfragen können, lassen Sie das E-Mail unangetastet und fragen Sie in Ihrer IT-Abteilung nach. Die kann Ihnen z.B. dadurch helfen, dass sie die verdächtige Datei bei einer darauf spezialisierten Webseite, z.B. **virustotal.com**, prüfen lässt.

Und wenn es doch passiert ist?

Jetzt ist Ihre Prognose bzw. Beurteilung des Sachverhalts gefragt:

1. *Kann aus der Datenpanne jemandem ein Schaden entstehen?*
   Diese Frage ist häufig nicht sehr einfach zu beantworten. Zunächst einmal kann der Schaden ein vermögensrechtlicher oder auch nur ein körperlicher bzw. psychischer sein. Jeder körperliche Schaden, auch der psychische, verpflichtet nach dem Bürgerlichen Gesetzbuch zum Schadensersatz. Deswegen kann zum Beispiel eine Rufschädigung durchaus ein Schaden in diesem Sinne sein. Ein Schaden kann zum Beispiel auch darin bestehen, dass der Betroffene mit Reklame-E-Mails überschüttet wird. Besonders nahe liegt ein Schaden, wenn besondere personenbezogene Daten Gesundheit, die sexuelle Orientierung o. ä. betroffen sind.

   Für das weitere Verfahren können Sie einfach davon ausgehen, dass die Schadensmöglichkeit immer dann anzunehmen ist, wenn ein Schaden nicht ausgeschlossen werden kann. Nur wenn das der Fall wäre, können Sie die weitere Prüfung hier beenden, sonst geht es weiter mit 2.

2. *Ist eine Handlung der kirchlichen Dienststelle ursächlich für die eingetretene Gefahr gewesen?*
   Bitte beachten Sie, hier kommt es nicht auf das Verschulden an. Entscheidend ist zunächst nur, ob die Gefahr auch eingetreten wäre, wenn es keinerlei Handlung der kirchlichen Dienststelle gegeben hätte. Kommen Sie nach gewissenhafter Prüfung zu exakt diesem Schluss, können Sie hier aufhören.

3. *Wie geht es weiter bei Zweifelsfällen?*
   Es liegt in der Natur von Beurteilungen und Prognosen, dass sie unzutreffend sein können. Ich empfehle Ihnen ganz heiß, im Zweifelsfall mit der Abarbeitung dieser Hilfestellung fortzufahren. Warum?

   - Zum einen vermeiden Sie den Vorwurf, Sie hätten aus Angst vor den unangenehmen Konsequenzen eine gesetzlich vorgeschriebene Handlung unterlassen.
   - Zum andern setzen Sie sich durch eine ordnungsgemäße Meldung nicht im besonderen Maße Nachteilen aus. Warum dies so ist, erläutere ich am Ende dieser Hilfestellung.

Was muss bei Bejahung der Voraussetzungen getan werden?

Hier lasse ich das Gesetz antworten. § 33 Abs.1 S.1 KDG bestimmt:

> Der Verantwortliche meldet der Datenschutzaufsicht unverzüglich die Verletzung des Schutzes personenbezogener Daten, wenn diese Verletzung eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt.

Zu den Einzelheiten:

1. *Wer ist der „Verantwortliche"?*
   In der Regel der Leiter der kirchlichen Einrichtung, also z. B. bei Kirchenstiftungen der Pfarrer oder Kirchenverwaltungsvorstand. Er gibt die Meldung aber auch für Kindergärten oder sonstige kirchliche Einrichtungen seiner Pfarrgemeinde ab. Bei kirchlichen Krankenhäusern ist der Klinikvorstand gefragt – immer derjenige, der auch sonst die Geschicke der Einrichtung bestimmt.

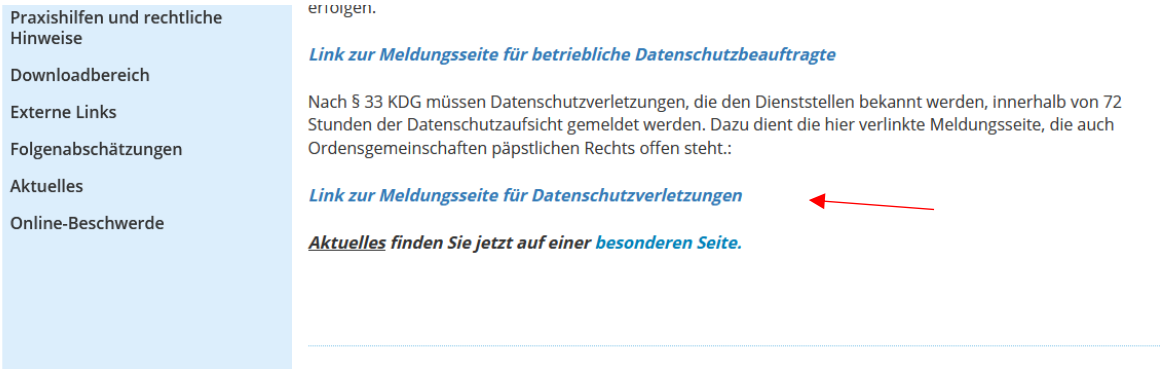
2. *Wann muss die Meldung erfolgen?*
   § 33 Abs.1 S. 2 KDG sagt:
   Erfolgt die Meldung nicht binnen 72 Stunden, nachdem die Verletzung des Schutzes personenbezogener Daten bekannt wurde, so ist ihr eine Begründung für die Verzögerung beizufügen.
   Es empfiehlt sich also wirklich, die Meldung frühzeitig abzusetzen. Eine verspätete Meldung kann böse Folgen nach sich ziehen.

3. *Wie wird gemeldet?*
   Individualisten stellen ihre Meldung nach § 33 Abs.3 KDG[1] selbst zusammen und versenden sie per E-Mail (die Schneckenpost könnte die 72-Stunden-Grenze knacken). Wer es arbeitssparender will, nützt den Meldungslink auf allen Webseiten der deutschen Diözesandatenschutzbeauftragten, so auch auf meiner (am Ende der Startseite).

---

(3)[1] Die Meldung gemäß Absatz 1 enthält insbesondere folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
b) den Namen und die Kontaktdaten des betrieblichen Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
c) eine Beschreibung der möglichen Folgen der Verletzung des Schutzes personenbezogener Daten;
d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.



Hier gibt es den Link noch einmal in aktiver Ausführung:
https://meldungen.katholisches-datenschutzzentrum.de/?post_type=dsverletzung&mandant=sued

Bitte warten Sie ab, bis Ihre Meldungsbestätigung eintrifft!

Kann mir etwas passieren?

Natürlich löst die Meldung an die Datenschutzaufsicht deren Kenntnis von dem Vorfall aus. Damit geht aber gleichzeitig die Verantwortung für das weitere Vorgehen auf sie über. Da die Datenschutzaufsicht täglich mit diesen Fragen zu tun hat, kann sie routinierter reagieren.

In den allermeisten Fällen erfolgt seitens der Datenschutzaufsicht auch keine weitere Aktion gegenüber der kirchlichen Dienststelle. Es ist insbesondere ganz selten, dass gegen den Urheber einer Datenpanne eine Geldbuße verhängt wird. Das hängt mit der besonderen Fassung des § 51 KDG zusammen:

> (1) Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter vorsätzlich oder fahrlässig gegen Bestimmungen dieses Gesetzes, so kann die Datenschutzaufsicht eine Geldbuße verhängen.

Nach Absatz 1 setzt also die Verhängung einer Geldbuße voraus, dass **der Verantwortliche vorsätzlich oder fahrlässig gehandelt hat**[2]. Daran fehlt es regelmäßig bei Handlungen eines Mitarbeiters, es sei denn,

- er sei nicht ausreichend geschult oder eingewiesen worden oder
- der Verantwortliche habe ihn überlastet.

In beiden Fällen lässt sich ein Verschulden des Verantwortlichen begründen.

Wer sich in diese Frage näher einlesen will, den lade ich zur Lektüre dieses Aufsatzes ein. Auch hier gibt es noch Lesenswertes dazu.

[2] Hier ist darauf hinzuweisen, dass nicht alle deutschen Diözesandatenschutzbeauftragten und vor allem nicht das Interdiözesane Datenschutzgericht von der Existenz dieser Vorschrift ausgehen. Außerdem besteht eine Ausnahme beim sog. „Mitarbeiterexzess“, wenn der Mitarbeiter ausschließlich im Eigeninteresse tätig wird.