Evangelische Hochschule Berlin

Richtlinie zum Vorgehen bei Datenpannen

Diese Richtlinie beschreibt das gebotene Vorgehen bei Datenpannen. Sie gilt verbindliche für alle Beschäftigten und alle Geschäftsbereiche.

Datenpannen lösen Meldepflichten aus, für die strenge Fristen gelten:

Vorgeschrieben ist eine unverzügliche Meldung gegenüber der Datenschutzaufsicht. Erfolgt eine Meldung zu spät, drohen hohe Bußgelder. Aus diesem Grund sind die beschriebenen Prozessschritte schnell und unverzüglich durchzuführen! Es sollte nicht gewartet werden, bis alle Informationen vollständig vorliegen. Diese können auch nachgereicht werden.

Neben dem Beschäftigten, der die Datenpanne entdeckt, sind folgende Personen am Prozess beteiligt:

INTERNER KOORDINATOR FÜR DATENSCHUTZ	
Prof. Dr. phil. Michael Komorek	
Telefon (Büro): +49 30 84582-200 Telefon (Mobil): +49 176 66557889	E-Mail: komorek@eh-berlin.de
Vertreter/in: Andreas Flegl E-Mail: flegl@eh-berlin.de	Telefon (Büro): +49 30 84582-400 Telefon (Mobil): +49 176 70023481

LEITER IT	
Wolfgang Aridas	
Telefon (Büro): +49 30 84582-444 Telefon (Mobil): +49 174 3106672	E-Mail: aridas@eh-berlin.de
Vertreter/in: Marco Menzel E-Mail: menzel@eh-berlin.de	Telefon (Büro): +49 30 84582-505 Telefon (Mobil): ---

HOCHSCHULLEITUNG	
Prof. Dr. Sebastian Schröer-Werner (Rektor)	
Telefon (Büro): +49 30 84582-100 Telefon (Mobil): ---	E-Mail: schröer-werner@eh-berlin.de
Vertreter/in: Prof. Dr. Michael Komorek E-Mail: komorek@eh-berlin.de	Telefon (Büro): +49 30 84582-200 Telefon (Mobil): +49 176 66557889

Prozessablauf

Schritt 1: Feststellung einer Datenpanne

Verantwortlich: Beschäftigter

Erlangt ein Beschäftigter Kenntnis von einer Datenpanne oder von Umständen, die den Verdacht einer Datenpanne begründen, stößt er unverzüglich den nachfolgenden Prozess an.

Was ist eine Datenpanne?

Eine Datenpanne liegt vor, wenn personenbezogene Daten[1] oder andere vertrauliche Informationen,

a. die die Hochschule für sich oder für andere im Auftrag verarbeitet oder
b. die externe Stellen im Auftrag der Hochschule verarbeiten,

unrechtmäßig übermittelt werden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind (Verletzung der Vertraulichkeit).

Eine Datenpanne kann auch vorliegen, wenn personenbezogene Daten versehentlich unwiederbringlich gelöscht wurden und eigentlich noch erforderlich wären (Verletzung der Verfügbarkeit).

Schließlich kann eine Datenpanne vorliegen, wenn personenbezogene Daten versehentlich so verändert wurden, dass ihre Richtigkeit nicht mehr sichergestellt werden kann (Verletzung der Integrität).

Schritt 2: Benachrichtigung der zuständigen Personen

Verantwortlich: Beschäftigter bzw. jede Person, die Kenntnis vom Verstoß erlangt

Im ersten Schritt benachrichtigt der Beschäftigte unverzüglich (per Telefon und E-Mail):

- den internen Koordinator für Datenschutz
- den Leiter IT
- die Hochschulleitung

Jede der oben genannten Personen ist zu informieren. Sind die oben genannten Personen nicht zu erreichen, sind die Vertreter zu kontaktieren.

Die nachfolgenden Prozessschritte 2.1 und 2.2 werden aufgrund der geltenden Fristen und einer eventuellen Gefahr im Verzug nach Möglichkeit zeitgleich durchgeführt.

[1] Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Schritt 2.1: Prüfung, ob die Datenpanne noch akut oder beendet ist

Verantwortlich: Der interne Koordinator für Datenschutz und der Leiter IT

Im zweiten Schritt wird von den Verantwortlichen geprüft, ob die Datenpanne noch akut ist. Die Prüfung wird von den vorgenannten Personen gemeinsam durchgeführt. Bei Bedarf werden Spezialisten aus den Fachabteilungen als Sachverständige hinzugezogen.

Wann ist die Datenpanne noch akut?

Die Datenpanne ist noch akut, wenn ihre Ursache fortbesteht und weitere unrechtmäßige Übermittlungen oder Kenntnisnahmen von personenbezogenen Daten drohen bzw. die Verfügbarkeit und Integrität der Daten weiter beeinträchtigt ist.

Ist die Datenpanne noch akut oder ist ihr Status unbekannt, stimmen die oben genannten Personen Notfallmaßnahmen ab, um die Datenpanne schnellstmöglich zu beenden oder einzudämmen.

Ist die Datenpanne offensichtlich beendet, müssen keine Notfallmaßnahmen getroffen werden.

Schritt 2.2: Prüfung von Benachrichtigungspflichten

Verantwortlich: Der interne Koordinator für Datenschutz und die Hochschulleitung

Der interne Koordinator für den Datenschutz und die Hochschulleitung prüfen, ob Informationspflichten nach §§ 32, 33 DSG-EKD bestehen. Kommen sie zu dem Schluss, dass die Datenschutzaufsicht und die Betroffenen nach §§ 32, 33 DSG-EKDzu benachrichtigen sind, wird eine Meldung nach Schritt 3 durchgeführt. Sofern keine Meldung zu erfolgen hat, folgt Schritt 4.

Die Datenschutzaufsicht ist nach § 32 DSG-EKD zu informieren, wenn im Rahmen einer Risikoprognose hinsichtlich der Verletzung des Schutzes personenbezogener Daten voraussichtlich ein Risiko für die Rechte und Freiheiten der betroffenen Person besteht.

Die betroffene Person (z.B. Mitarbeiter oder Student) ist zusätzlich nach § 33 DSG-EKD zu informieren, sofern die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Person führt.

In der Risikoabwägung sind alle Umstände des Einzelfalls aus der Sicht der betroffenen Person zu berücksichtigen, z.B.:

- Welche und wie viele Daten sind betroffen?
- Sind die Daten verschlüsselt oder anderweitig geschützt?
- Welche Schäden drohen (materielle und immaterielle Schäden)?
- Wie hoch ist der Schaden?
- Kann die betroffene Person selbst nach der Information noch Schutzmaßnahmen ergreifen?
- technische Umstände der Datenpanne und Motivlage des unrechtmäßigen Datenempfängers (zufälliger oder vorsätzlicher Zugriff)

Achtung: Wird festgestellt, dass die Datenpanne voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, muss die Datenschutzaufsicht unverzüglich informiert werden. Wochenenden und gesetzliche Feiertage sind vom Fristlauf nicht ausgenommen. Eine entsprechende Bereitschaft der Verantwortlichen ist sicherzustellen.

Sofern die Datenpanne nicht die „eigenen" Daten betrifft, sondern im Rahmen eines Auftragsverhältnisses eine andere verantwortliche Stelle (Auftragsverarbeitung), ist die Datenpanne nicht der Datenschutzaufsicht zu melden, sondern nach § 32 Abs. 2 DSG-EKD unverzüglich dem Auftraggeber der Auftragsverarbeitung.

Schritt 3: Inhalt der Meldung

Verantwortlich: Der interne Koordinator für Datenschutz, Leiter IT und die Hochschulleitung

Die Verantwortlichen tragen die für eine Meldung erforderlichen Informationen zusammen. Dies umfasst mindestens folgende Daten:

- 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
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
- 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

Die Information an die Datenschutzaufsicht sollte an folgende Stelle erfolgen:

Der Beauftragte für den Datenschutz der
Evangelischen Kirche in Deutschland
Außenstelle Berlin

Invalidenstraße 29
10115 Berlin

E-Mail: ost@datenschutz.ekd.de

Für die Fristwahrung ist der Eingang der Meldung bei der Datenschutzaufsicht maßgeblich. Es sollte daher als Erstkontakt ein Fax, eine verschlüsselte E-Mail oder das Online-Meldeformular auf der Webseite der Datenschutzaufsicht genutzt werden. Der Postweg kann im Nachgang genutzt werden. In Zweifelsfällen sollte die Datenschutzaufsicht telefonisch kontaktiert werden.

Sofern neben der Datenschutzaufsicht auch die betroffene Person informiert werden muss, da ein hohes Risiko für diese besteht, ist ein durchführbares Verfahren auf Grundlage der

Anzahl der betroffenen Personen und den Umständen der Meldung zu entwickeln (z.B. welche Kontaktdaten sind vorhanden, wieviele Personen sind betroffen).

Nach Abschluss der Meldung erfolgt eine weitere Ursachenforschung und Dokumentation nach Schritt 4.

Schritt 4: Ursachenforschung und Dokumentation

Verantwortlich: Interner Koordinator für Datenschutz und Leiter IT

Unabhängig davon, ob eine Meldung an die Datenschutzaufsicht oder die betroffenen Personen erfolgt, erforschen anschließend der interne Koordinator für Datenschutz und der Leiter IT die Ursachen der Datenpanne. Steht die Datenpanne im Zusammenhang mit einer automatisierten Datenverarbeitung, wird die Ursachenforschung gemeinsam mit den Fachabteilungen durchgeführt. Die Ergebnisse der Ursachenforschung werden in einem Protokoll festgehalten.

Das Protokoll hat die von Schritt 1 bis Schritt 3 durchgeführten Maßnahmen zu enthalten:

- Wer hat wann an wen gemeldet?
- Welche IT-Sicherheitsmaßnahmen wurden ergriffen?
- Welche Erwägungsgründe waren maßgeblich für die Risikobewertung?
- Welche Meldungen sind erfolgt oder unterblieben?
- Welche Maßnahmen wurden getroffen, um eine erneute Datenpanne zu verhindern?
- Besteht Optimierungsbedarf am hier beschriebenen Meldeprozess?

Das Protokoll ist Bestandteil des Datenpannen-Registers in privacy port, in dem alle Datenschutzvorfälle gesammelt werden und auf Nachfrage der Datenschutzaufsicht zur Verfügung gestellt werden können.

Kontakt zum betrieblichen Datenschutzbeauftragten

Sollten im Prozess Fragen auftauchen, kann jederzeit der Datenschutzbeauftragte einbezogen werden. Dies gilt unabhängig vom oben beschriebenen Verfahren. Der Datenschutzbeauftragte steht während des Prozesses beratend zur Verfügung und ist über die Datenpanne und eine etwaige Meldung an die Datenschutzaufsicht zu informieren:

ANSPRECHPARTNER	
Jan-Christoph Thode Seniorberater Datenschutz	Tel.: +49 (0) 30 3087749-21 E-Mail: jthode@datenschutz-nord.de
Dr. Sanela Kühn Seniorberaterin Datenschutz	Tel.: +49 (0) 30 3087749-23 E-Mail: skuehn@datenschutz-nord.de
datenschutz nord GmbH Niederlassung Berlin Kurfürstendamm 212 10719 Berlin	

EVANGELISCHE HOCHSCHULE BERLIN

BETRIEBLICHER DATENSCHUTZBEAUFTRAGTER	
Oliver Stutz datenschutz nord GmbH Konsul-Smidt-Straße 88 28217 Bremen	E-Mail: office@datenschutz-nord.de www.datenschutz-nord-gruppe.de