Umgang mit Datenpannen

Mitarbeiterrichtlinie zum Umgang mit Datenpannen nach Artikel 33, 34 Europäische Datenschutz-Grundverordnung (EU-DSGVO)

OA1001-01

Group24 AG (group24)

INHALTSVERZEICHNIS

STAMMDATEN

Referenz-Nummer:	OA1001-01
Dokumententitel:	Umgang mit Datenpannen
Fachlich Verantwortlicher:	Datenschutzbeauftragter der group24 AG
Zuständiger Bereich:	Datenschutzmanagement
Geltungsbereich:	group24 AG
Gültig von:	01.11.2022
Gültig bis:	31.12.2024
Verantwortlicher Prüfer:	Marc Eismann / Christian Hornhues
Wiedervorlage Datum:	01.10.2024
Dokumentenkategorie	intern

ÄNDERUNGSVERZEICHNIS

Version	Datum	Autor	Inhalte der Änderung
1.0	25.10.2022	Marcel Konrads	Initiale Erstellung
1.1	01.11.2023	Cihat Dokumaci	Anpassung Formatierung Abschnitt 4.2

REVIEWNACHWEIS UND FREIGABE

Version	Datum	Teilnehmer	Inhalte des Reviews
V1.0	31.10.2022	Marc Eismann / Christian Hornhues	
V1.1	15.11.2023	Marc Eismann / Christian Hornhues	Review 2023

1 EINLEITUNG

Bei der group24 werden personenbezogene Daten verarbeitet. Diese bedürfen des besonderen Schutzes. Im Falle einer Datenpanne ist die group24 verpflichtet, die zuständige Datenschutzaufsichtsbehörde und in bestimmten Fällen die Betroffenen unverzüglich zu informieren. Ziel der Regelung ist es u.a. bei Datenverlusten Folgeschäden für den/die Betroffenen in Form von finanziellen Einbußen oder sozialen Nachteilen zu vermeiden.

1.1 Begriffe

Personenbezogene Daten sind gemäß *„VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)“*: *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“* (Art. 4 Nr. 1 EU-DSGVO).

Eine Datenpanne im Sinne der Europäischen Datenschutzgrundverordnung (EU-DSGVO) ist die *„Verletzung des Schutzes personenbezogener Daten“* und ist definiert als *„eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“* (Art. 4 Nr. 12 EU-DSGVO).

2 MELDUNG DATENPANNE

Sollten Sie bemerken oder den Verdacht haben, dass personenbezogene Daten unrechtmäßig Dritten zugänglich gemacht wurden, sich Dritte solche Daten unrechtmäßig verschafft haben oder entsprechende Informationen abhandengekommen sind, informieren Sie bitte unverzüglich:

Geschäftsführung / Vorstand

Marc Eismann, +49254220080649, m.eismann@group.de

Christian Hornhues, +49 211 749586902, c.hornhues@group24.de

Datenschutzbeauftragter

Marcel Konrads, +49 2542 20080689, datenschutz@group24.de

Interne IT

Jens Niehues, +49 2542 20080616, j.niehues@group24.de

Aus dieser Meldung entstehen Ihnen als Mitarbeiter/in keinerlei berufliche oder persönliche Nachteile. Die Namensangabe erfolgt freiwillig.

3 NOTWENDIGE INFORMATIONEN

1.) Wann und wo ist die Datenpanne aufgetreten?

_____

_____

_____

2.) Beschreibung des konkreten Vorfalls

Z. B. Verlust oder Diebstahl von Datenträgern, unrechtmäßige/irrtümliche Übermittlung, unrechtmäßige Einsichtnahme durch einen Mitarbeiter, Angriff auf Computersysteme

_____

_____

_____

_____

_____

3.) Welche Datenarten sind betroffen?

- ☐ Angaben über die rassische oder ethnische Herkunft
- ☐ politische Meinungen
- ☐ religiöse oder philosophische Überzeugungen
- ☐ Gewerkschaftszugehörigkeit
- ☐ Gesundheitsdaten
- ☐ Sexualleben
- ☐ Daten, die einem Berufsgeheimnis unterliegen
- ☐ Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen
- ☐ personenbezogene Daten zu Bank- oder Kreditkartenkonten
- ☐ genetische Daten
- ☐ biometrische Daten

☐ Sonstige/bspw. persönliche Kontaktdaten/Unbekannt (sofern bekannt, bitte nähere Bezeichnung der Datenarten):

_____

_____

_____

4.) Wie viele Datensätze sind [ungefähr] betroffen?

_____

5.) Besteht aus Ihrer Sicht das Risiko des Datenmissbrauchs?

☐ Ja ☐ Nein

Wenn nein, warum?

_____

6.) Drohen aus Ihrer Sicht schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen (z. B. Identitätsbetrug, unberechtigte Abbuchungen, soziale Nachteile)?

☐ Ja ☐ Nein

Wenn nein, warum?

_____

7.) Sind Maßnahmen zur Sicherung der Daten ergriffen worden?

☐ Ja ☐ Nein

Wenn ja, welche?

_____

8.) Sonstige Mitteilungen:

_____

_____

_____ _____

Name (optional) Datum

4 SCHRITTWEISES VORGEHEN BEI DATENPANNEN

Datenpannen lösen Meldepflichten aus, für die strenge Fristen gelten. Laut Art. 33 Abs. 1 DSGVO hat die Meldung nach dem Bekanntwerden über die Verletzung des Schutzes personenbezogener Daten unverzüglich durch den Verantwortlichen zu erfolgen. Bei verspäteter Meldung drohen hohe Bußgelder. Daher sollen die folgenden Schritte schnell und unverzüglich durchgeführt werden.

Sollten notwendige Informationen noch nicht vollständig vorliegen, können diese nach Meldung immer nachgereicht werden!

Neben dem Beschäftigten, der die Datenpanne entdeckt, sind die unter Nr. 2 genannten Personen am Meldeprozess beteiligt.

4.1 Schritt 1: Feststellen einer Datenpanne

Beteiligt: Beschäftigter

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

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

- die von der group24 für sich oder für andere im Auftrag verarbeitet oder
- die Unterauftragnehmer im Auftrag der group24 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 normalerweise noch erforderlich sind (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).

4.2 Schritt 2: Benachrichtigung der zuständigen Personen

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

Der Beschäftigte benachrichtigt nach dem Feststellen einer Datenpanne unverzüglich die unter Punkt 2 genannten Personen (Vorstand bzw. Geschäftsführung, Datenschutzbeauftragter sowie die interne IT).

Jede der genannten Personen ist über die Datenpanne zu informieren. Sind die unter Punkt 2 genannten Personen nicht erreichbar, so sind ggfs. ihre Vertreter zu kontaktieren.

HINWEIS: Die nachfolgenden Schritte 3.1 und 3.2 werden aufgrund geltender Fristen und einer potenziellen Gefahr im Verzug nach Möglichkeit gleichzeitig ausgeführt!

4.3 Schritt 3.1: Prüfung der Datenpanne

Beteiligt: Datenschutzbeauftragter und interne IT

Nachdem Kenntnis über die Datenpanne erlangt wurde, muss geprüft werden, ob diese noch akut ist. Die Prüfung wird von den verantwortlichen Beteiligten durchgeführt. Bei Bedarf können Spezialisten aus den Fachabteilungen als Sachverständige hinzugezogen werden.

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

Sofern die Datenpanne noch akut oder ihr Status unbekannt ist, müssen durch die oben genannten Beteiligten Notfallmaßnahmen abgestimmt werden, um die Datenpanne schnellstmöglich zu beenden oder einzudämmen.

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

4.4 Schritt 3.2: Prüfung von Meldungspflichten

Beteiligt: Datenschutzbeauftragter und Vorstand bzw. Geschäftsführung

Der interne Datenschutzbeauftragte und der Vorstand prüfen, ob Informationspflichten gemäß Art. 33 und Art. 34 DSGVO bestehen. Sollten die zuständige Aufsichtsbehörde und die Betroffenen nach den genannten Artikeln zu benachrichtigen sein, erfolgt die Meldung analog Schritt 4. Sofern keine Meldung zu erfolgen hat, folgt Schritt 5.

Die zuständige Aufsichtsbehörde ist laut Art. 33 DSGVO unverzüglich zu informieren, wenn im Rahmen einer Risikoabschätzung bezogen auf die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein Risiko für die Rechte und Freiheiten der betroffenen Person besteht. (Wochenenden und gesetzliche Feiertage sind vom Fristlauf nicht ausgenommen!)

Die betroffene Person (z.B. Mitarbeitende oder Kunden) ist zusätzlich gemäß Art. 34 DSGVO zu informieren, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Person führt.

Im Rahmen der Risikoabschätzung 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?

- Drohen materielle oder immaterielle Schäden?
- Wie hoch ist der Schaden?
- Kann die betroffenen Person selbst nach der Information noch Schutzmaßnahmen ergreifen?
- Technische Umstände der Datenpanne und Motivlage des unrechtmäßigen Datenempfängers (zufälliger oder vorsätzlicher Zugriff)

Sofern die Datenpanne nicht die „eigenen" Daten betrifft, sondern im Rahmen einer Verarbeitung von Daten im Auftrag eine andere verantwortliche Stelle, ist die Datenpanne nicht der Aufsichtsbehörde zu melden, sondern nach Art. 33 Abs. 2 DSGVO unverzüglich dem Auftraggeber der Auftragsverarbeitung.

4.5 Schritt 4: Inhalt der Meldung

Beteiligt: Vorstand bzw. Geschäftsführung, interne IT und Datenschutzbeauftragter

Im Falle einer Meldung an die zuständige Aufsichtsbehörde tragen die genannten Beteiligten alle notwendigen Informationen gemäß Art. 33 Abs. 3 DSGVO zusammen, mindestens aber:

- 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 zuständige Aufsichtsbehörde sollte an folgende Stelle erfolgen:

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
Kavalleriestr. 2-4
40213 Düsseldorf
Telefon: 0211/38424-0
Fax: 0211/38424-999
E-Mail: poststelle@ldi.nrw.de

Für die Wahrung der Frist ist der Eingang der Meldung bei der Aufsichtsbehörde maßgeblich. Daher sollte für den Erstkontakt das Webformular des LDI NRW genutzt werden (abrufbar unter https://ldi-fms.nrw.de/lip/action/invoke.do?id=Datenschutzverletzung).
In Zweifelsfällen sollte die Aufsichtsbehörde telefonisch kontaktiert werden.

Sofern neben der Aufsichtsbehörde auch die betroffene Person benachrichtigt 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 (beispielsweise welche Kontaktdaten sind vorhanden und wie viele Personen sind betroffen).

4.6 Schritt 5: Ursachenforschung und Dokumentation

Beteiligt: Interne IT und Datenschutzbeauftragter

Unabhängig davon, ob eine Meldung an die zuständige Aufsichtsbehörde oder betroffene Personen erfolgt, suchen die Beteiligten die Ursachen der Datenpanne. Steht die Datenpanne im Zusammenhang mit einer automatisierten Datenverarbeitung, wird die Suche nach der Ursache zusammen mit den Fachabteilungen durchgeführt. Die Ergebnisse werden in einem Protokoll festgehalten.

Als Vorlage kann das unter Punkt 3 verwendete Informationsprotokoll verwendet werden.

Das Protokoll ist Bestandteil des Datenpannen-Registers und wird bei der group24 im gemeinsam genutzten Datenschutzmanagement abgelegt und muss auf Nachfrage der Aufsichtsbehörde zur Verfügung gestellt werden können.

5 VERBINDLICHKEIT DER REGELUNGEN

5.1 Verbindlichkeit der Regelungen

Die im Anhang aufgeführten, veröffentlichten und in Kraft gesetzten Dokumente gelten als Anlage zu dieser OA und sind für alle Mitarbeiter verbindlich.

Sie sind insoweit Bestandteil dieser Organisationsanweisung.

5.2 Ausnahmeregelung

Sollte eine gültige Regelung für einzelne Systeme oder Prozesse, aus welchen Gründen auch immer, nicht umsetzbar sein, so kann der IT Security Manager für dieses System bzw. diesen Prozess eine Ausnahme von den Regeln genehmigen. Die Entscheidung des IT Security Manager erfolgt risikobasiert.

6 VERSTÖßE UND SANKTIONEN

Bei schweren Verstößen oder Missbrauchsfällen bei der Nutzung der IT-Services und bereitgestellter Hardware können neben der Sperre des Zugangs weitere disziplinäre und arbeitsrechtliche Maßnahmen eingeleitet werden.