Mitarbeiterrichtlinie zum Umgang mit Datenschutzverstößen, -ereignissen und -vorfällen nach Art. 33,34 DS-GVO

Muster (Dr. Eberhard Kiesche, Version 2.0 vom 09.07.2021, wird fortlaufend überarbeitet)

Erläuterung der gesetzlichen Vorgaben

In unserem Unternehmen werden personenbezogene Daten verarbeitet. Diese bedürfen des besonderen Schutzes. Im Falle von Datenschutzverstößen ist das Unternehmen als Verantwortlicher nach Art. 33, 34 DS-GVO (siehe auch Erwägungsgründe 85, 86,87, 88) verpflichtet, ggf. bei einem hohen Risiko die betroffenen Personen und die zuständige Aufsichtsbehörde bei einem Risiko für natürliche Personen *unverzüglich* zu informieren.

Ziel dieser Regelung ist u.a., bei Datenschutzverletzungen Schäden für die Betroffenen in Form von finanziellen Einbußen oder sozialen Nachteilen und für das Unternehmen (z.B. Imageverlust) zu vermeiden und alle kritischen Datenschutzvorfälle (Datenpannen) zu dokumentieren und zu bewerten.

Die Fähigkeit, zügig auf Datenpannen zu reagieren, ist von zentraler Bedeutung (Einhaltung der 72 Stunden-Frist). Im Vordergrund steht der Schutz natürlicher Personen, die von den Datenschutzverletzungen betroffen sind.

„Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen (Art. 4 Nr. 1 DS-GVO). „Verletzung des Schutzes personenbezogener Daten“ ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (Art. 4 Nr. 12 DS-GVO).

Eine Datenschutzverletzung im Sinne der Datenschutz-Grundverordnung liegt u.a. vor, wenn personenbezogene Daten und Informationen unrechtmäßig an unberechtigte Dritte übermittelt werden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangen und dabei Beeinträchtigungen der Rechte oder schutzwürdiger Interessen der Betroffenen drohen. Ein Datenschutzverstoß liegt auch vor, wenn Daten gestohlen werden, Geräte oder Speichermedien mit unverschlüsselten Daten verloren gehen oder intern im Unternehmen das Vier-Augen-Prinzip für betrügerische oder unzulässige Zwecke genutzt wird. Auch das unrechtmäßige Erheben personenbezogener Daten, Verstoß gegen Datenschutzgesetze, eine versehentliche Löschung oder Vernichtung, auftragswidriges Verhalten des Auftragsverarbeiters oder dessen fehlerhafte Datenverarbeitung zählen zu den Datenschutzverstößen. Auch Erpressungs-Schadsoftware (Ransom-Software) muss unverzüglich der zuständigen Stelle im Unternehmen gemeldet werden.

Sollten Sie bemerken oder den Verdacht haben, dass personenbezogene Daten unrechtmäßig verarbeitet worden sind, Dritten ohne Rechtsgrundlage zugänglich gemacht wurden, sich Dritte solche personenbezogenen Daten unrechtmäßig verschafft haben (Hacking) oder entsprechende Informationen und Daten abhandengekommen sind, informieren Sie bitte umgehend die zuständige Person:

_____ [Zimmer/Durchwahl]

Achtung: Aus dieser Meldung entstehen Ihnen als Mitarbeiter/in **keinerlei berufliche oder persönliche unmittelbare oder mittelbare Nachteile. Die Namensangabe erfolgt freiwillig**. **Sie sind auch nicht in der Arbeitnehmerhaftung**.[1]

[1] Diese Klarstellung sollte möglichst mit dem Betriebsrat, soweit vorhanden, in einer Betriebsvereinbarung zu Datenpannen nach Art. 33 DSGVO vorgenommen oder vertraglich zugesichert werden.

Meldebogen: Datenschutzverletzung, Datenschutzereignis, Datenschutzvorfall (für Meldung nach Art. 33, 34 DS-GVO)

1.) Wann und wo ist die Datenschutzverletzung/der Datenschutzvorfall aufgetreten? Wie ist er bekanntgeworden?

_____

_____

_____

2.) Beschreibung des konkreten Vorfalls bzw. Ereignisses, Risikobezug zum Unternehmen und mögliche Fehlerursachen:

- z.B. Hackerzugriff auf zentrale Verarbeitungssysteme;
- Diebstahl von Passwörtern;
- unbefugte Einsichtnahme;
- Missbrauch von Nichtzugriffsberechtigten (z.B. durch Mitarbeiter);
- Offenlegung von personenbezogenen Daten durch Hacker;
- Verfälschung von Daten;
- Verlust oder Diebstahl von Daten und Datenträgern/Geräten;
- unrechtmäßige/irrtümliche Übermittlung von personenbezogenen Daten wie z.B. Fehlversand von Unterlagen an falsche Empfänger;
- unrechtmäßige Weitergabe an einen nicht befugten Mitarbeiter;
- Angriffe auf Computersysteme/Netzwerke (z.B. durch infizierte Webseiten, Schadsoftware, Phishing oder Ransom-Software);
- unverschlüsselter E-Mail-Versand;
- Unterlagen mit personenbezogenen Daten verloren, gestohlen oder an einem unsicheren Platz gelagert;
- nicht datenschutzgerechte Entsorgung von Datenträgern (z.B. Festplatten);

_____

_____

_____

_____

3.) Welche Datenarten (Kategorien) sind betroffen?

- □ politische Meinungen
- □ religiöse oder weltanschauliche Überzeugungen
- □ Gewerkschaftszugehörigkeit
- □ Gesundheitsdaten
- □ biometrische oder genetische Daten
- □ Daten zum Sexualleben
- □ Daten, die einem Berufsgeheimnis unterliegen
- □ Daten, die einem Sozialgeheimnis unterliegen
- □ Daten, die einem Steuergeheimnis unterliegen
- □ Daten, die einem besonderen Amtsgeheimnis unterliegen
- □ Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen
- □ personenbezogene Daten zu Bank- oder Kreditkartenkonten
- □ Eigene Beschäftigte
- □ Kundendaten
- □ Daten von Minderjährigen
- □ Lokalisierungsdaten
- □ Noch nicht bekannt
- □ Weitere personenbezogene Daten: _____

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

Minimal und maximal geschätzte Anzahl:

_____

_____

5.) Besteht aus Ihrer Sicht das (einfache) Risiko eines Datenmissbrauchs?

- □ Ja
- □ Nein

Wenn nein, warum?

_____

6.) Beschreibung der wahrscheinlichen Folgen: Drohen aus Ihrer Sicht ein Risiko für die Rechte, Freiheiten oder schutzwürdigen Interessen der Betroffenen (Schäden wie z.B. Diskriminierung, Identitätsdiebstahl, unbefugte Zugriffe auf personenbezogene Daten, soziale und finanzielle Nachteile) ?

□ Ja

□ Nein

Wenn nein, warum?_____

_____

7.) Sind korrektive Maßnahmen zur Schadensminimierung, Sicherung der Daten bzw. zur Abwehr weiterer Angriffe bzw. zur Beseitigung der Ursachen des Datenschutzvorfalls unverzüglich ergriffen bzw. vorgeschlagen worden (genaue Beschreibung)?

□ Ja

□ Nein

Wenn nein, warum?

_____

8.) Sonstige Mitteilungen:

_____

_____

_____

_____

_____

Namen (freiwillig) Datum