D_10c Vorgehen bei Datenschutzverletzungen

Folgender Ablauf basiert auf Artikel 33 und 34 der DSGVO (siehe nächste Seite)

Aufrechterhaltung der Datensicherheit

Daten müssen vor Missbrauch, Änderung, Verlust, sowie unerlaubten Zugriff geschützt werden. Um dies sicherzustellen sollten folgende Punkte bedacht werden:

- Wie sensibel sind meine verarbeiteten Daten?
- Welcher Schaden kann durch eine Datenschutzverletzung entstehen?
- Welche Compliance wird benötigt, um das Unternehmen davor zu schützen?

Eine Datenschutzverletzung

Sensible Daten gehen verloren oder werden von nicht berechtigten Personen zugegriffen, verändert, verwendet oder anderswertig missbräuchlich verwendet.

Reaktion auf eine Datenschutzverletzung

Schritt 1	**Die Verletzung eindämmen und eine vorläufige Einschätzung durchführen**	• Sofort Schritte einleiten um die Verletzung einzudämmen • Person für Koordinierung festlegen
Schritt 2	**Evaluierung des Risikos für Betroffene**	• Prüfen welche sensiblen Daten betroffen sind • Identifikation von möglichen Risiken • Umfang der Datenschutzverletzung identifizieren
Schritt 3	**Benachrichtigung über Datenschutzverletzung innerhalb von 72 Stunden**	• Risikoanalyse auf Einzelfallbasis • Nicht jede Datenschutzverletzung muss gemeldet werden

Müssen betroffene benachrichtigt werden?

Sollte ein reales Risiko mit der Möglichkeit von ernsten Schäden bestehen, sollten Betroffene benachrichtigt werden um sich selbstständig vor Schäden zu schützen.

Außerdem können rechtliche/vertragliche Pflichten bestehen, die zu einer Benachrichtigung verpflichtet.

Ablauf der Benachrichtigung

- **Wann?** So bald wie möglich
- **Wie?** Durch direkten Kontakt (Mail, Anruf)
- **Wen?** Den direkt betroffenen
- **Was?** Beschreibung der Datenschutzverletzung, Information über

Weitere Schritte

- **Aufarbeitung des Vorfalls/Dokumentation**
- **Setzen von Maßnahmen zur zukünftigen Prävention**
- **Sicherheitsvorkehrungen verschärfen**
- **Mitarbeiter für das Thema sensibilisieren**

Artikel 33 DSGVO

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

(2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

(3) Die Meldung gemäß Absatz 1 enthält zumindest 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 Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen 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.

(4) Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(5) Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.

Artikel 34 DSGVO

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

(2) Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Maßnahmen.

(3) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

a) der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;

b) der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;

c) dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

(4) Wenn der Verantwortliche die betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die Aufsichtsbehörde unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.

Bei einem Data-Breach in meinem Unternehmen wichtige Personen:

Verantwortliche/r in der Geschäftsführung: _____

Rechtsabteilung: _____

EDV-Verantwortlicher: _____

Rechtsanwalt: _____

Sonstige Stellen/Personen die informiert werden müssen bzw unterstützen können:

_____

_____

Hinweis: Dieses Muster dient der beispielsweisen Umsetzung der Regelungen der DSGVO in Bezug auf Data-Breach im Unternehmen. Dieses ist an die Bedürfnisse des jeweiligen Unternehmens individuell anzupassen.

Dieses Muster wurde mit größter Sorgfalt erstellt, für die Richtigkeit, Vollständigkeit, Aktualität oder Qualität des bereitgestellten Musters können wir jedoch keine Gewähr übernehmen. Haftungsansprüche gegen Personen, welche dieses Muster erstellt haben, sind daher ausgeschlossen.