Krisenplan im Falle von Datenschutzverstößen

Datenschutzrichtlinien (nachfolgend „Richtlinien“ genannt) der Organisation _____

Generelles:

- Bewahren Sie bei Datenschutzverstößen, selbst wenn Sie diese selbst verursacht haben, die Ruhe. Panik hilft keinem.
- Haben Sie keine Angst davor, Verstöße zu melden. Richtige Probleme entstehen meist erst dadurch, dass Verstöße verheimlicht werden.
- Handeln Sie schnell. Bei Verstößen mit mittlerem und hohem Risiko ist das Unternehmen verpflichtet, den Verstoß innerhalb von 72 Stunden der Aufsichtsbehörde anzuzeigen. Schon ein Verstoß gegen diese zeitliche Vorgabe kann zu einem Bußgeld führen.
  Meldung hier: https://www.datenschutz-bayern.de/service/data_breach.html

A: Handlungsanweisung

1. Datenschutzverstoß erkennen	
1.1 Was ist geschehen?	
1.2 Welche personenbezogenen Daten sind betroffen?	
1.3 Wie viele Personen sind betroffen?	
1.4 Dauert der Verstoß noch an?	
1.5 Was ist der Grund für den Verstoß (wenn feststellbar)?	
1.6 Ist eine Zusammenfassung der wesentlichen Informationen für eine Weiterleitung erfolgt (Mindestinformationen: Art des Datenschutzverstoßes, die ungefähre Anzahl der Betroffenen und Datensätze sowie die Datenkategorien)?	

2. Eskalation	
2.1 Ist der Vorgesetzte informiert?	
2.2 Ist der Datenschutzbeauftragte informiert?	
2.3 Sind Kooperationspartner, die mit den personenbezogenen Daten in Verbindung stehen, informiert?	
2.4 Ist der IT-Dienstleister informiert?	
3. Maßnahmen	
3.1 Welche technischen oder sonstigen Maßnahmen zur Behebung oder Beseitigung des Verstoßes sind ergriffen worden?	
3.2 Ist der Verstoß verschuldet (menschliches Versagen oder Organisationsverschulden)?	
4. Dokumentation	
4.1 Ist der Verstoß ausreichend dokumentiert?	
4.2 Sind die ergriffenen Maßnahmen ausreichend dokumentiert?	

5. Risikobewertung	
5.1 Welches Risiko für Rechte und Freiheiten von natürlichen Personen ergeben sich aus dem Verstoß? (Die Risikobewertung sollte durch den Datenschutzbeauftragten erfolgen)	
5.2 Die Kriterien für die Risikobewertung sind: • Art und Schutzbedürftigkeit der betroffenen Datensätze (z.B. Kreditkartendaten höher schutzbedürftig als E-Mailadressen) • Anzahl der betroffenen Datensätze; • Maß der Identifizierbarkeit von Personen anhand der Datensätze; • Anzahl und ggfs. Schutzbedürftigkeit der betroffenen Menschen • Wahrscheinlichkeit der unbefugten Kenntnisnahme durch Dritte; • Anzahl der Personen, die unbefugt Kenntnis nehmen könnten; • Schwere der Folgen für die Betroffenen • Technische und/oder organisatorische Einflussmöglichkeiten zur Reduzierung des Kreises der Personen, die unbefugt Kenntnis nehmen könnten. • Hohes Risiko z.B. bei Diskriminierung, Identitätsdiebstahl, Betrug, Vermögensschäden oder Reputationsschäden.	
6. Folgen der Risikobewertung	
a) Kein Risiko	• nur interne Maßnahmen

b) Mittleres Risiko	• Interne Maßnahmen • Benachrichtigungen der Aufsichtsbehörde innerhalb von 72 Stunden
c) Hohes Risiko	• Interne Maßnahmen • Benachrichtigungen der Aufsichtsbehörde innerhalb von 72 Stunden • sofortige Benachrichtigung der Betroffenen • ggf. Benachrichtigungen über Veröffentlichung in den Medien (in Absprache mit der Aufsichtsbehörde)

Beispiel	Meldung an Aufsichtsbehörde?	Meldung an die Betroffenen?
Diebstahl einer CD mit archivierten und nach Stand der Technik verschlüsselten Datensätze	*Eher nein, jedoch abhängig von Art der Daten*	*Nein*
Datenabzug von sicherer Website durch Cyberattacke	*Ja*	*Ja*
Vorübergehender Stromausfall im Call-Center	*Nein*	*Nein*

Beispiel	Meldung an Aufsichtsbehörde?	Meldung an die Betroffenen?
Cyberattacke, durch die Datensätze verschlüsselt werden, ohne dass Backups vorhanden sind und die Daten entschlüsselt werden können	*Ja*	*Ja*
Jemand ruft an und meldet einen Datenschutzverstoß. Die interne Analyse ergibt, dass dieser Datenschutzverstoß vorliegt und auch andere betroffen sein könnten.	*Ja*	*Ja*
Ein Hacker zieht Zugangsdaten (Benutzername, Passwort) und Kursbuchungshistorie ab und veröffentlicht sie im Internet	*Ja*	*Ja*
Ein externer Websitebetreiber stellt einen Fehler im Code fest, der die Benutzerautorisierung kontrolliert	*Ja*, nachdem der Websitebetreiber das Unternehmen benachrichtigt hat	*Ja/Nein* (abhängig von Dauer des Fehlers und der betroffenen Daten)
Datensätze von 5000 Kursteil-	*Ja*	*Ja/Nein (abhängig von Art der*

nehmern wurden an falsche Empfänger (etwa 1000) versendet		*Daten und drohender Konsequenzen)*
Newsletter werden mit E-Mailadressen von weiteren Newsletter-Abonnenten verschickt (z.B. in „Cc“)	*Ja/Nein* (abhängig davon, ob es ein Einzelfall war und der Art der betroffenen Daten)	*Ja/Nein (abhängig davon, ob es ein Einzelfall war und der Art der betroffenen Daten)*