Einleitung (Art.33 DS-GVO):

„(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 55 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.“

i. Dokumentation / Meldung / Information

Eine kurze Übersicht gibt die Website der LfDI-NRW zu den Pflichten bei einer Verletzung[1].

- Interne Dokumentationspflicht: kein bis geringes Risiko (also immer)
- Meldepflicht an Aufsichtsbehörde: mittleres Risiko
- Betroffenen – Information: hohes Risiko

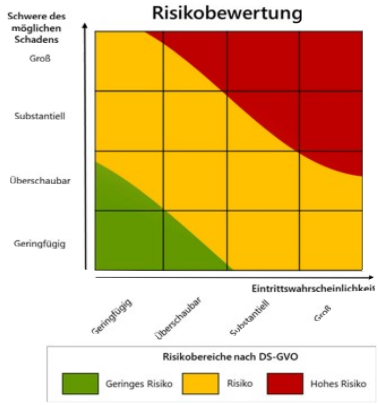
Oft genannte Beispiele für kein bis geringes Risiko sind der Verlust einer nach dem Stand der Technik verschlüsselten Festplatte, zu der ein Backup besteht, oder veröffentlichte (z.B. Telefonbuch, Website), bekannte E-Mail- oder Adressdaten u. ä.

ii. Risikoanalyse

Grundsätzlich hat eine Risikoanalyse aus Eintrittswahrscheinlichkeit und möglicher Schwere eines Schadens zu erfolgen, wie hier rechts im Bild gezeigt. Hinweis (übrigens):

„Es ist NICHT ZULÄSSIG auf Anforderungen der Grundsätze nach Art. 5 DS-GVO zu verzichten und Risiken daraus in Kauf zu nehmen. RISIKO - AKZEPTANZ oder RISIKO - TRANSFER (z. B. bekannt aus der Informationssicherheit) stehen den Verantwortlichen im Datenschutz NICHT ZUR VERFÜGUNG.“

Nach Art der Daten (Adressen, E-Mail, Fotos, Benutzername, Passwort, Biometrie, Berufsgeheimnis, Standort, Bank/Kreditdaten, Gesundheit, Religion, Sexualität, Politik u. ä.) ist der mögliche Schaden für die Betroffenen einzuschätzen (Finanzieller Art, Identitätsdiebstahl, Ruf- / Imageschaden, Bloßstellung, Geheimnisoffenbarung, Existenzgefährdung u. ä.).



Bildquelle: Datenschutzkonferenz (DSK) Kurpapier Nr. 18, Schaubild Seite 5

iii. Was ist zu tun?

(a) Im Vorfeld sollte neben den Schulungen zur Sensibilisierung die Meldekette festgelegt sein, die Zusammensetzung des Notfallteams incl. Datenschutzverantwortliche, -berater und mögliche, notwendige, externe Spezialisten, sowie Kommunikationsverantwortliche.

(b) Durch technische und organisatorische Maßnahmen den Schaden analysieren, eingrenzen, abschätzen und das Risiko möglichst mindern.

(c) Geeignete Information der Mitarbeiter (einheitliches Außenbild), der Aufsichtsbehörde, der Cybereinheit der Polizei und der Betroffenen. *(Wenn die Möglichkeit besteht, dass Daten in die falschen Hände geraten könnten, sollten m. E. auch bei geringem Risiko die Betroffenen informiert werden, allein um möglich Risiken besser einzuschätzen und bevor Betroffene es aus dritter Hand erfahren.)*

iv. Checkliste Schadensmeldung zur Dokumentation und ggf. Meldung (schriftlich / Online)

Natürlich verweisen die meisten Websites der Datenschutzbeauftragten auf ihr Meldung im Online-Portal. Welche Informationen sie sich zurechtlegen sollten finden Sie in der nachfolgenden Checkliste oder zur Nutzung als schriftliche Meldung.

Link zur Checkliste & Meldung

1 Quelle: LfDI-NRW: „Meldepflicht für Verantwortliche – Verletzung des Schutzes personenbezogener Daten“

CC BY SA