Neue Leitlinien zur Meldung von Verletzungen des Schutzes personenbezogener Daten

von Carmen Lupşan, Rechtsanwältin

Der Europäische Datenschutzausschuss (**EDSA**) hat am 29. März 2023 Leitlinien zur Meldung von Verletzungen des Schutzes personenbezogener Daten (die „**Leitlinien**“) beschlossen. Hierbei handelt es sich eigentlich um eine aktualisierte Fassung der von der Artikel-29-Datenschutzgruppe verabschiedeten und vom EDSA bestätigten Leitlinien.

Ausgangspunkt

Bei der Erstellung der Leitlinien geht der EDSA davon aus, dass grundlegende Anforderungen der DSGVO, wie die geeigneten technischen und organisatorischen Sicherheitsvorkehrungen zur Gewährleistung eines zum Schutz der verarbeiteten Daten geeigneten Sicherheitsniveaus, erfüllt sind. Dadurch soll untern anderem sichergestellt werden, dass Datenschutzverletzungen mithilfe dieser Sicherheitsvorkehrungen unverzüglich festgestellt werden können.

Die internen Datenschutzlichtlinien des Verantwortlichen müssen hierfür die kurzfristige Reaktionskette im Falle der Verletzung enthalten. Somit ist nicht nur die Vorbereitung, sondern auch die Implementierung der Datenschutzrichtlinien wesentlich, um eine kurzfristige Risikobewertung und ggf. Meldung zu gewährleisten.

Was ist eine Datenschutzverletzung?

Die DSGVO definiert diese als eine Verletzung der Sicherheit, die unbeabsichtigt oder unrechtmäßig zu Vernichtung, Verlust, Veränderung, unbefugter Offenlegung von oder unbefugtem Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Datenschutzverletzungen lassen sich nach drei Grundsätzen der Informationssicherheit in Verletzung der Vertraulichkeit, der Integrität und der Verfügbarkeit unterteilen. Somit kann beispielsweise auch ein Stromausfall zu einer Verletzung der Verfügbarkeit führen, allerdings muss immer fallbezogen geprüft werden, inwieweit dadurch die Rechte und Freiheiten der betroffenen Personen gefährdet wurden.

Wann soll gemeldet werden?

Eine Datenschutzverletzung muss unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, der zuständigen Aufsichtsbehörde gemeldet werden, es sei denn, dass die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Bei der Festlegung des Zeitpunktes der Kenntnisnahme kann sich der Verantwortliche nicht darauf berufen, dass er keine geeigneten technischen und organisatorischen Sicherheitsvorkehrungen umgesetzt und somit verspätet Kenntnis erlangt hat. Dasselbe gilt auch für die Frist, die er einhalten muss.

Die Mitteilung ist lediglich erforderlich, wenn aufgrund der Prüfung festgestellt wurde, dass die Datenschutzverletzung voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Wie ist an die Aufsichtsbehörde zu melden?

Die DSGVO sieht einige Mindestinformationen der Meldung vor:

- Beschreibung der Art der Datenschutzverletzung, soweit möglich mit Angabe u.a. der Kategorien und der ungefähren Zahl der betroffenen Personen,
- Namen und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen zuständigen Person für zusätzliche Informationsanfragen;
- Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung;
- Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Die Meldung kann auch schrittweise vorgenommen werden (falls z.B. eine abschließende Prüfung innerhalb von 72 Stunden nicht möglich ist).

Wie ist die betroffene Person zu informieren?

Birgt die Datenschutzverletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung. Die Mindestinformationen entsprechen den oben ausgeführten Grundsätzen.

Die Leitlinien sehen einige Kriterien vor, wonach das Risiko bewertet werden kann, wie z.B. Art, Sensibilität und Umfang personenbezogener Daten, Schwere der Folgen, Anzahl der betroffenen Personen, besondere Eigenschaft der betroffenen Personen oder des Verantwortlichen etc.

Fazit

Die Leitlinie fasst die wesentlichen Schritte, die ein Verantwortlicher im Falle einer Datenschutzverletzung vornehmen muss, wie folgt zusammen:

- Unverzügliche Informierung der zuständigen Person des Verantwortlichen über sicherheitsrelevante Ereignisse,
- Bewertung des Risikos für die Rechte und Freiheiten der betroffenen Person im Einzelfall;
- Eventuell Mitteilung an die zuständige Behörde und/ oder Informierung der betroffenen Person(en);
- Währenddessen Treffen von Maßnahmen zur Minimisierung des Risikos;
- Dokumentierung der Datenschutzverletzung und der Maßnahmen, unabhängig davon. ob die Mitteilung an die Aufsichtsbehörde bzw die Informierung der betroffenen Person erfolgt.

Kontakt und weitere Informationen:

Stalfort
Legal. Tax. Audit.
25 Jahre

STALFORT Legal. Tax. Audit.
Bukarest – Bistrița – Sibiu

Büro Bukarest:
T.: +40 – 21 – 301 03 53
F: +40 – 21 – 315 78 36
M: bukarest@stalfort.ro
www.stalfort.ro