Wann und wie sind Datenschutzverletzungen zu melden?

von Carmen Lupsan, Rechtsanwältin

Mitte Dezember hat der Europäische Datenschutzausschuss (**EDSA**) die Leitlinien 01/ 2021 zu Beispielen für die Meldung von Datenschutzverletzungen (die „**Leitlinien**") angenommen.

Die Leitlinien dienen als Stütze dafür, wie Datenschutzverantwortliche und Auftragsverarbeiter Datenschutzverletzungen handhaben müssen, bzw. was im Rahmen der Datenschutz-Folgenabschätzung berücksichtigt werden muss. Sie umfassen 18 Beispiele, die nach unterschiedlichen Angriffsarten aufgeteilt sind. Die Leitlinien sind als praxisbezogene Ergänzung zu den Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679 der Artikel-29-Datenschutzgruppe (WP 29) gedacht.

Was ist eine Datenschutzverletzung?

Die Datenschutzverletzung ist in der Datenschutz- Grundverordnung (**DSGVO**) definiert und bedeutet eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zu Vernichtung, Verlust, Veränderung, oder unbefugter Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Datenschutzverletzungen lassen sich gemäß der Stellungnahme 03/2014 über die Meldung von Verletzungen des Schutzes personenbezogener Daten der WP29 wie folgt unterteilen:

- **Vertraulichkeitsverletzung:** bedeutet die unbefugte oder unbeabsichtigte Preisgabe von oder Einsichtnahme in personenbezogene Daten,
- **Integritätsverletzung:** bedeutet die unbefugte oder unbeabsichtigte Änderung personenbezogener Daten und
- **Verfügbarkeitsverletzung:** bedeutet den unbefugten oder unbeabsichtigten Verlust des Zugangs zu personenbezogenen Daten oder die unbeabsichtigte oder unrechtmäßige Vernichtung personenbezogener Daten.

Was muss im Falle einer Datenschutzverletzung vorgenommen werden?

Gemäß Art 33 der **DSGVO** muss der Verantwortliche im Fall einer Datenschutzverletzung unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde melden, es sei denn, dass die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Ferner besteht bei einer Datenschutzverletzung, die voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat, die Pflicht, die betroffene Person unverzüglich über die Verletzung zu benachrichtigen (Art. 34 DSGVO). Ausgehend von diesen Pflichten wurden die Leitlinien erstellt.

Fallbeispiele

Die Beispiele sind in 5 Hauptarten eingeteilt (Ransomware, Datenexfiltration, interne menschliche Risikoquelle, verlorene oder gestohlene Geräte oder Papierdokumente, falsche Versendung) und enthalten jeweils eine Beschreibung der ersten Maßnahmen, die ergriffen werden müssen, eine

detaillierte Risikoanalyse im Einzelfall, Maßnahmen zur Eindämmung der Risiken sowie sich für den Verantwortlichen ergebende Pflichten.

Ransomware-Angriffe

Bei Angriffen durch Ransomware, d.h. Schadprogrammen, die die Daten des Verantwortlichen bis zur Zahlung eines Lösegelds verschlüsseln, wird darauf abgestellt, ob es einen Back-up gibt bzw. ob eine Datenexfiltration stattgefunden hat. Ferner ist u.a. auch relevant, um welches Volumen an betroffenen Daten es sich handelt, und ob besondere Kategorien von Daten betroffen sind. Abhängig davon kann im Einzelfall das Ergebnis für ähnliche Ransomware-Angriffe unterschiedlich ausfallen.

Angriffe zur Datenexfiltration

Hierbei handelt es sich um unautorisierte Übertragungen von/ Zugriffe auf Daten. Wichtig ist bei der Risikoanalyse, inwieweit die Angreifer Zugang zu den entsprechenden Daten hatten (z.B. ob nur Passwörter, die mit einem starken Hash-Algorithmus abgesichert wurden, übermittelt wurden). Selbstverständlich wird ein solcher Angriff gegenüber besonderen Verantwortlichen (z.B. Banken) anders gehandhabt als gegenüber Verantwortlichen, die keine solche vertraulichen Daten halten.

Verlorene oder gestohlene Geräte und Papierdokumente

In solchen Fällen müssen u.a. die Art der betroffenen personenbezogenen Daten, die angewendeten Sicherheitsmaßnahmen des Gerätes, das abhandengekommen ist etc. analysiert werden. Es ist in der Risikoanalyse danach zu unterscheiden, ob die Daten z.B. verschlüsselt sind oder es sich um besondere Kategorien von personenbezogenen Daten handelt.

Fazit

Die Leitlinien sind ein wichtiges Hilfsmittel im Falle eines Datenschutzverstoßes. Dennoch muss jeder Verstoß im Einzelfall betrachtet und eine entsprechende Datenschutz-Folgenabschätzung vorbereitet werden. Meistens weisen Datenschutzverstöße zudem auf Schwächen des Systems hin; eine Prüfung ist sowohl bzgl. der Notwendigkeit der Meldung an die Datenschutzbehörde als auch im Hinblick auf die angewandten technischen und organisatorischen Maßnahmen des Verantwortlichen geboten.

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