derStandard.at

20.4.2018

Wo im Datenschutz die größten Risiken lauern

Axel Anderl, Anja Cervenka

20. April 2018, 13:00

Die neue DSGVO verlangt eine Datenschutz-Folgenabschätzung

Wien – Die Datenschutz-Folgenabschätzung ist ein zentraler Dreh- und Angelpunkt der Datenschutz-Grundverordnung (DSGVO): Sie erfolgt für als besonders kritisch und riskant identifizierte Datenverarbeitungen.

Ziel ist es, die tatsächlichen Risiken einer konkreten Verarbeitung von personenbezogenen Daten zu identifizieren (wie zum Beispiel potenzielle Hackerangriffe, technische Schwachstellen wegen der eingesetzten Technologie, unachtsame Mitarbeiter), zu bewerten, risikominimierende Maßnahmen festzulegen und diese systematisch zu beschreiben (zum Beispiel Firewall, Begrenzung der Zugriffsberechtigungen, Mitarbeiterschulung). Die Abschätzung dient nicht dem Selbstzweck, sondern ist die Basis für die Frage, ob und in welchem Umfang eine Datenverarbeitung überhaupt zulässig ist.

Zugleich ist die Datenschutz-Folgenabschätzung gemeinsam mit dem Verarbeitungsverzeichnis die Basis für etwaige Meldungen bei Datenschutzverstößen: Nur wer die Verarbeitungen sauber dokumentiert hat und die Risiken kennt, kann der Behörde im Anlassfall innerhalb der knappen 72-Stunden-Frist die erforderliche detaillierte Auskunft geben.

Hohes Risiko

Datenschutz-Folgenabschätzungen sind dann erforderlich, wenn die Datenverarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Betroffenen zur Folge hat. Das ist jedenfalls der Fall, wenn

- eine Bewertung von Personen durch eine automatisierte Entscheidung stattfindet (Profiling),
- umfangreich sensible (Gesundheitsdaten!) oder strafrechtliche Daten (Whistleblowing-Hotline) verarbeitet werden oder
- bei systematischer Überwachung öffentlich zugänglicher Bereiche.

Eine gewisse Hilfestellung bieten die von der Datenschutzbehörde zu erlassenden Listen von Anwendungen, für die eine Abschätzung jedenfalls ("black list") oder nicht ("white list") notwendig ist.

In einem ersten Behördenentwurf der "white list" werden die bisherigen Standardverarbeitungen, die etwa die praktisch relevanten Bereiche Kundenverwaltung, Rechnungswesen, Logistik, Buchführung und Personalverwaltung umfassen, ausgenommen. Gleiches gilt für Verarbeitungen, die nach dem alten Regime einer Vorabkontrolle der Datenschutzbehörde unterzogen wurden und im Wesentlichen unverändert weiterbetrieben werden.

Systematische Beschreibung

Mindestinhalt einer Folgenabschätzung ist die systematische Beschreibung der Verarbeitung und ihrer Zwecke, die Bewertung der Notwendigkeit und Verhältnismäßigkeit sowie der Risiken. Als letzter Schritt müssen die aufgrund des Risikos getroffenen Abwehrmaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren dokumentiert und implementiert werden.

Auf technischer Ebene bietet die ISO/IEC-29134:2017-Leitlinie eine Hilfestellung. Gibt es einen Datenschutzbeauftragten im Unternehmen, ist dieser beratend hinzuziehen; die Pflicht zur Durchführung bleibt beim Verantwortlichen. Wichtig ist auch, die Datenschutz-Folgenabschätzungen laufend zu prüfen und an geänderte Umstände (neue Risiken, eingetretene Incidents) anzupassen. (Axel Anderl, Anja Cervenka, 20.4.2018)

Axel Anderl ist Managing Partner bei Dorda Rechtsanwälte, leitet das IT/IP-Team und ist Koleiter der Datenschutzgruppe. **Anja Cervenka** ist Rechtsanwaltsanwärterin bei Dorda und auf Datenschutzrecht spezialisiert.