Elisabeth Niekrenz

Die neuen Leitlinien des EDSA zum Umgang mit Verletzungen des Schutzes personenbezogener Daten

Der Europäische Datenschutzausschuss (EDSA) hat am 14.01.2021 einen Entwurf für neue Leitlinien zum Umgang mit Verletzungen des Schutzes personenbezogener Daten zur Konsultation veröffentlicht (EDSA, Guidelines 1/2021, v. 1.0). Die Leitlinien illustrieren anhand von Fallbeispielen, wie Datenschutzvorfällen vorgebeugt werden kann, welche Maßnahmen zur Risikoeindämmung getroffen werden sollten und wie im Ernstfall zu reagieren ist. Ein Fokus liegt auf der Bewertung der Risiken für die Betroffenen, deren Abschätzung entscheidend für das Bestehen von Melde- und Benachrichtigungspflichten ist. Bis zum 02.03.2021 konnten Stellungnahmen zu dem Entwurf abgegeben werden.

Hintergrund

Die möglichen Szenarien eines Datenschutzvorfalls reichen von der Versendung eines Briefes an den falschen Adressaten über den Diebstahl verschlüsselter Tablets bis zum Abfluss von Bankdaten Hunderttausender Betroffener. Eine Verletzung des Schutzes personenbezogener Daten liegt gemäß Art. 4 Nr. 12 DSGVO bei Verletzungen der Sicherheit vor, die zu ihrer Vernichtung, ihrem Verlust, ihrer Veränderung, zur unbefugten Offenlegung oder dem unbefugten Zugriff zu denselben führen.

Verantwortliche sind unter Umständen verpflichtet, solche Vorfälle an die zuständigen Aufsichtsbehörden zu melden und die Betroffenen zu benachrichtigen, Art. 33 Abs. 1 bzw. 34 Abs. 1 DSGVO. Dreh- und Angelpunkt für das Bestehen dieser Pflichten ist das Risiko für die Rechte und Freiheiten der Betroffenen. Die Meldung an die Aufsichtsbehörden ist die Regel: Sie ist immer erforderlich, es sei denn, die Verletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen, Art. 33 Abs. 1 Satz 1 DSGVO. Die Benachrichtigung der Betroffenen muss hingegen nur erfolgen, wenn der Vorfall voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

Zuletzt gaben die Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/670, WP 250 rev. 01 (Stand: 2018) umfassende Hinweise zur Auslegung dieser Vorschriften.

Struktur der Leitlinie

Die neuen Leitlinien illustrieren anhand von 18 Fallbeispielen ausführlich, wie mit Datenschutzvorfällen umzugehen ist. Der Schwerpunkt liegt auf der durchzuführenden Risikoanalyse sowie auf Maßnahmen, die zur Vorbeugung von Datenschutzvorfällen und zur Eindämmung der Risiken ergriffen werden sollten. Die vorgestellten Fälle sind fiktiv, beruhen aber auf typischen Fällen aus dem Erfahrungsschatz der Aufsichtsbehörden (Rn. 14).

Das Papier ist in sechs verschiedene Typen von Datenschutzvorfällen unterteilt: Ransomware-Angriffe, Angriffe mit Datenabfluss, Risiken durch internes Personal, Verlust oder Diebstahl von Geräten oder Dokumenten, Datenschutzverletzungen in Zusammenhang mit postalischen Versendungen und „Social Engineering"-Attacken. Für jedes Fallbeispiel stellen die Leitlinien zunächst dar, welche Kategorien von personenbezogenen Daten betroffen sind und in welchem Ausmaß eine Verletzung ihres Schutzes stattfand. Auch die Sicherheitsvorkehrungen, die im Voraus getroffen wurden, sowie Maßnahmen, die die Verantwortlichen unmittelbar nach dem Vorfall ergriffen, werden aufgeführt. Im Anschluss analysieren die Leitlinien, welche Risiken für die Betroffenen bestehen und ordnen ein, ob es sich um ein geringes bzw. kein Risiko, ein Risiko oder ein hohes Risiko handelt. Davon wird abgeleitet, ob eine Melde- bzw. Benachrichtigungspflicht besteht. Schließlich stellt das Papier dar, welche Maßnahmen die Verantwortlichen zur Minimierung der Risiken der jeweiligen Vorfälle treffen können.

In allen dargestellten Fällen liegt eine Verletzung des Schutzes personenbezogener Daten vor. Demnach ist in jedem Fall eine interne Dokumentation notwendig, wie sich aus Art. 33 Abs. 5 DSGVO ergibt. Der EDSA rekurriert auf die bekannte Unterteilung von Verletzungen des Schutzes personenbezogener Daten: Verletzungen der Vertraulichkeit, der Integrität und der Verfügbarkeit (Rn. 5). Am häufigsten treten in den Leitlinien Verletzungen der Vertraulichkeit auf.

Risikobewertung

Das Risiko für die Rechte und Freiheiten natürlicher Personen ergibt sich aus der Schwere möglicher negativer Folgen des Datenschutzvorfalls sowie deren Eintrittswahrscheinlichkeit (Erwägungsgrund 75 DSGVO). Hinsichtlich der negativen Folgen werden vom EDSA körperliche, materielle und immaterielle Schäden unterschieden (Rn. 6). Bei der Bewertung komme es auf eine Zusammenschau der relevanten Umstände an, nämlich der Art der betroffenen Daten, ihres Umfangs sowie der Anzahl der betroffenen Personen und der Art der Verletzung.

Zur Einstufung als hohes Risiko kommt es nach Ansicht des EDSA in Fällen, in denen Daten abgeflossen sind, denen ein hohes Missbrauchspotenzial innewohnt, z. B. Kopien von Ausweisdokumenten oder Zahlungsdaten, die für Identitätsdiebstahl oder Phishing verwendet werden können und so materielle oder immaterielle Schäden auslösen (Rn. 45). Eine hohe Zahl von betroffenen Personen erhöhe das Risiko (Rn. 43, 95). Auch ein Fall, in dem Telefonrechnungen eines einzelnen Betroffenen aufgrund einer gezielten Attacke abgeflossen sind, wird als hohes Risiko eingestuft: Sie böten Aufschluss über das Privatleben und könnten zu Stalking und Schäden für die körperliche Integrität führen (Rn. 124).

Insgesamt resultieren hohe Risiken meist aus Verletzungen der Vertraulichkeit von Daten. Am Beispiel eines Krankenhauses, das wegen einer Ransomwareattacke Krankendaten zwei Tage lang aus Backups wiederherstellen muss, wird jedoch deutlich, dass auch aus Verletzungen der Verfügbarkeit ein hohes Risiko für die Betroffenen resultieren kann: Hier müssen laut EDSA medizinische Behandlungen verschoben werden, bis die notwendigen Daten wiederhergestellt sind (Rn. 38). Dagegen ist stets eine umfassende Betrachtung aller Faktoren nötig: So führen die Leitlinien auch ein Beispiel auf, in dem trotz abgeflossener Gesundheitsdaten (über Laktoseintoleranz) nur ein geringes Risiko besteht, weil nur zwei Personen betroffen und die Daten kaum in schädigender Weise nutzbar sind (Rn. 115).

Ein einfaches Risiko soll etwa vorliegen, wenn Daten einiger Dutzend Personen, die durch einen Ransomwareangriff verschlüsselt wurden, aus analogen Aufzeichnungen wiederhergestellt werden müssen und es dadurch zu kleineren Verzögerungen bei der Lieferung an Kunden kommt (Rn. 31).

Dass durch adäquate IT-Sicherheitsmaßnahmen Melde- und Benachrichtigungspflichten abgewendet werden können, zeigt ein Fall, in dem 1200 gehashte Passwörter von Nutzenden einer Kochwebseite an Dritte abgeflossen sind. Hier betrachten die Leitlinien den Vorfall als nur mit geringem Risiko verbunden, obgleich die Zahl der Betroffenen groß ist (Rn. 58). Die Verfügbarkeit eines Backups und zuverlässige Verschlüsselung bewahre ein Unternehmen, das zum Opfer eines Ransomwareangriffs wird, vor Melde- und Benachrichtigungspflichten, weil keine Risiken entstanden seien (Rn. 22).

Maßnahmen zur Vorbeugung und Eindämmung

Im Kern erfordert das Management von Verletzungen des Schutzes personenbezogener Daten nach Ansicht des EDSA die Entwicklung und Testung von Prozessen, die im Falle eines IT-Sicherheitsvorfalls durchlaufen werden (Rn. 11). Dazu gehöre die Benennung zuständiger Ansprechpartner und die Festlegung von Dokumentationswegen. Das Personal sei sowohl über IT-Sicherheitsmaßnahmen als auch über das Erkennen von Cyber-Vorfällen und die zu ergreifenden Maßnahmen und Unternehmensprozesse im Ernstfall zu schulen (Rn. 12). Nimmt der Verantwortliche Notiz von einem Zwischenfall, muss er laut EDSA sofort ermitteln, welche Auswirkungen auf Betroffene wahrscheinlich sind und auf dieser Basis die Risikobewertung durchführen (Rn. 9).

Alle geeigneten und angemessenen Schutzmaßnahmen müssten ergriffen werden. Schließlich sei zu untersuchen, welche Schwachstellen im System den Vorfall ermöglicht haben, damit sie beseitigt werden könnten. Auch in Situationen, in denen kein hohes Risiko vorliegt und daher keine Pflicht zur Benachrichtigung der Betroffenen besteht, schlagen die Leitlinien vor, die Betroffenen zu informieren, wenn dadurch Risiken minimiert werden können (Rn. 62).

Zu jedem Typus von Datenschutzvorfall werden zudem umfangreiche Hinweise für die Vorsorge und Schadensbegrenzung gegeben. Diese erheben keinen Anspruch auf Vollständigkeit – im Hinblick auf die Verschiedenartigkeit von Verarbeitungsvorgängen sollen sie weniger als Checkliste, als vielmehr zur Ideenanregung gelesen werden (Rn. 70).

Bei vielen Vorschlägen handelt es sich um grundlegende Maßnahmen zur Gewährleistung der IT-Sicherheit. Dazu gehören laut EDSA die Einrichtung zuverlässiger Verfahren zur Erstellung von Backups, die Segmentierung technischer Systeme, um die Verbreitung von Malware so gut wie möglich zu verhindern, Verschlüsselung sowie die Verwendung sicherer Passwörter und multifaktorieller Authentifizierungsverfahren (R. 70). Zur Verminderung von Risiken, die von Personen innerhalb der eigenen Organisation ausgehen, werden unter anderem strenge Regeln über Zugangsrechte von Mitarbeitenden zu personenbezogenen Daten und technische Kontrollen des Zugangs empfohlen (Rn. 84).

Fazit

Neben aufsehenerregenden Cyberangriffen kann es auch durch triviale Vorgänge wie die Versendung eines Briefs an den falschen Empfänger oder den Verlust eines USB-Sticks zu einem Datenschutzvorfall kommen. Die Leitlinie ist aufgrund der Anknüpfung an Fallbeispiele recht anschaulich, sodass sich die Lektüre für Datenschutzberater lohnt und zur Überprüfung der eigenen Prozesse und Vorbeugemaßnahmen anregen kann.

Autorin: **Elisabeth Niekrenz ist Rechtsanwältin bei Spirit Legal Fuhrmann Hense Partnerschaft von Rechtsanwälten in Leipzig. Zuvor war sie als Policy Officer bei der NGO Digitale Gesellschaft e.V. tätig.**