Melden oder nicht melden? Die EDSA-Leitlinien zur Einstufung von Datenschutzverstößen

Categories : Datenschutzrecht

Tagged as : Benachrichtungspflicht, Daten-Exfiltration, Datenschutzverstöße, EDSA-Leitlinien, Gesundheitsdaten, Meldepflicht, personenbezogene Daten, Ransomware-Erpressungsfälle, Risikobewertung, Sozialdaten

Date : 29. April 2021

Datenpannen sind und bleiben ein heikles Thema. Das beweist nicht zuletzt das am Osterwochenende bekannt gewordene Datenleck bei Facebook, durch das Daten von über 533 Mio. Nutzerinnen und Nutzern im Netz veröffentlicht worden sind. Eine solche Datenpanne dürfte gegenüber der Aufsichtsbehörde zweifellos meldepflichtig sein. Doch nicht immer ist die Rechtslage so eindeutig. Häufig ist die Frage, wann genau ein Datenschutzvorfall meldepflichtig ist und wann Betroffene informiert werden müssen, nicht ohne Weiteres zu beantworten.

Gesetzliche Vorgaben und Leitlinien

Nach Art. 33 Abs. 1 DS-GVO müssen Verletzungen des Schutzes personenbezogener Daten der Aufsichtsbehörde grundsätzlich gemeldet werden. Diese Pflicht besteht allerdings nicht, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Besteht hingegen voraussichtlich sogar ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen, ist der Verantwortliche regelmäßig zusätzlich verpflichtet, die betroffenen Personen über die Verletzung zu benachrichtigen. Weil die Einordnung des Risikos in der Praxis immer wieder zu Schwierigkeiten führt, hat der Europäische Datenschutzausschuss (EDSA) Leitlinien dazu veröffentlicht. An Beispielen wird aufgezeigt, wann eine Datenpanne meldepflichtig und wann eine Verletzung darüber hinaus benachrichtigungspflichtig sein kann.

Die Beispiele betreffen alle Branchen, auch den Energiemarkt. Genannt werden z.B. der Umgang mit sog. Ransomware-Erpressungsfällen, Daten-Exfiltration (unautorisierter Transfer von Daten) sowie auch nur fehlerhaft versandte digitale und analoge Post. Bei der Bewertung, ob ein Vorfall melde- und benachrichtigungspflichtig ist, ist nach Ansicht des EDSA insbesondere zu prüfen, ob sensible Daten enthalten sind und welches Ausmaß die Verletzung hat.

Keine Melde- und Benachrichtigungspflicht: Der „Fall Laktoseintoleranz“

Weder eine Melde- noch eine Benachrichtigungspflicht sieht der EDSA beispielsweise in einem Fall, in dem eine Kursteilnehmerliste versehentlich an die 15 Teilnehmer des Kurses statt an das Hotel, in dem der Kurs stattfinden sollte, geschickt wurde. Die Liste enthielt Namen, E-Mail-Adressen und Essensvorlieben der 15 Teilnehmer. Zwei Teilnehmer hatten angegeben, dass sie laktoseintolerant sind.

Die Informationen bergen nach Ansicht des EDSA hinsichtlich der Art, der Sensibilität, des Umfangs und des Kontextes der personenbezogenen Daten nur ein geringes Risiko für die Rechte und Freiheiten betroffener Personen. Zwar handelt es sich bei dem Hinweis auf die Laktoseintoleranz um Gesundheitsdaten, bei denen in der Regel davon auszugehen ist, dass deren Weitergabe zu einem hohen Risiko führen kann; in diesem speziellen Fall gebe es jedoch keine Anhaltspunkte für drohende physische, materielle oder immaterielle Schäden durch die unbefugte Offenlegung der Informationen. Im Gegensatz zu Lebensmittelpräferenzen könne eine Laktoseintoleranz normalerweise nicht mit religiösen oder philosophischen Überzeugungen in Verbindung gebracht werden.

Melde- aber keine Benachrichtigungspflicht: Wenn Versicherungspolicen in die falschen Hände gelangen…

Eine Meldung gegenüber der Aufsichtsbehörde sei hingegen notwendig, wenn ein Versicherungsunternehmen angepasste Beitragspolicen per Post verschickt und zwei Briefe für unterschiedliche Versicherungsnehmer in einem Umschlag versandt werden. Das Risiko sei aber in diesem Fall nicht als hoch einzustufen, sondern liege vielmehr zwischen einem geringen und mittleren Risiko für die betroffenen Personen. Eine Benachrichtigung sei daher nicht notwendig.

Melde- und Benachrichtigungspflicht – Wenn Kontakt- und Sozialdaten auf Reisen gehen

Sowohl eine Melde- als auch eine Benachrichtigungspflicht sieht der EDSA in einem Fall, in dem ein Jobcenter in einer E-Mail über bevorstehende Schulungen versehentlich ein Dokument anhängte, das alle persönlichen Daten der Arbeitssuchenden (Name, E-Mail-Adresse, Postanschrift, Sozialversicherungsnummer) enthielt. Die Zahl der betroffenen Personen betrug mehr als 60.000. Das voraussichtlich hohe Risiko resultiert nach den Ausführungen des EDSA daraus, dass es sich um Daten einer beträchtlichen Anzahl von Personen handelte und um eine Offenlegung der Sozialversicherungsnummern mit anderen grundlegenden persönlichen Daten.

Was tun bei einem eigenen Verstoß?

Unternehmen, die personenbezogene Daten verarbeiten, müssen im Falle eines Datenschutzverstoßes unverzüglich eine eingehende Risikobewertung über die Folgen des Verstoßes für die betroffenen natürlichen Personen durchführen und darüber entscheiden, wie sie weiter vorgehen. Die Meldefrist für einen Datenschutzverstoß beträgt grundsätzlich maximal 72 Stunden ab Kenntnis über die Verletzung. Bei der Risikobewertung können die Leitlinien des EDSA helfen. Eine interne Dokumentation sollte jedoch unabhängig vom Ergebnis der Risikobewertung erfolgen.

Ansprechpartner*innen sind: Dr. Jost Eder/Thomas Schmeding/Dr. Maximilian Festl-Wietek/Xaver-Moritz Müller-Hübers