Handwerkskammer Lübeck

Informationsschreiben an Fotografenbetriebe

Datenschutzvorfall bei der Portraitbox GmbH (Paderborn) – dringender Handlungsbedarf für Fotografenbetriebe

1. Worum es geht

Nach der Information von Portraitbox wurde über einen kompromittierten API Schlüssel am Wochenende 16./17. Mai 2026 ein Zugriff auf die AWS Infrastruktur des Anbieters erlangt. Bei dem Angriff sollen

sämtliche Foto- und Kundendaten heruntergeladen
und diese Daten im Anschluss gelöscht worden seien.

Nach Mitteilung wird der Firma Portraitbox mit der Veröffentlichung der Daten gedroht.

2. Welche Daten sind (voraussichtlich) betroffen?

Nach derzeitigem Kenntnisstand sind betroffen:

alle Galerien und Fotos

Namen, E-Mail-Adressen, Lieferadressen, Bestellhistorien sowie Galerie-Zugangsdaten der Endkunden.

Mit hoher Wahrscheinlichkeit sind auch Aufnahmen Minderjähriger betroffen.

3. Sie sind Verantwortlicher – nicht Portraitbox

Datenschutzrechtlich ist die Rollenverteilung eindeutig: Das Fotostudio ist Verantwortlicher nach Art. 4 Nr. 7 DSGVO, Portraitbox lediglich Auftragsverarbeiter nach Art. 28 DSGVO. Die E-Mail von Portraitbox erfüllt ausschließlich dessen Informationspflicht aus Art. 33 Abs. 2 DSGVO.

Die Melde- und Benachrichtigungspflichten treffen Sie selbst – ebenso die Haftung gegenüber den betroffenen Personen nach Art. 82 DSGVO.

4. Pflicht 1: Meldung an die Aufsichtsbehörde (Art. 33 DSGVO)

Sofern eine meldepflichtige Verletzung des Schutzes personenbezogener Daten vorliegt, muss die Meldung an die zuständige Landesdatenschutzbehörde (maßgeblich ist in der Regel der Sitz Ihres Studios) binnen 72 Stunden erfolgen. Für Betriebe mit Sitz in Schleswig-Holstein ist dies das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD).

- ▪ Anschrift: Holstenstraße 98, 24103 Kiel
- ▪ Postanschrift: Postfach 71 16, 24171 Kiel
- ▪ Telefon: 0431 988-1200
- ▪ Fax: 0431 988-1223
- ▪ E-Mail: mail@datenschutzzentrum.de

- ▪ Webseite: www.datenschutzzentrum.de

Inhaltliche Mindestangaben nach Art. 33 Abs. 3 DSGVO sind insbesondere:

- ▪ Art der Verletzung (was ist passiert?),
- ▪ Kategorien und ungefähre Zahl betroffener Personen,
- ▪ Kategorien und ungefähre Zahl betroffener Datensätze,
- ▪ wahrscheinliche Folgen,
- ▪ ergriffene bzw. vorgeschlagene Maßnahmen.

Informationsschreiben an Fotografenbetriebe

5. Pflicht 2: Benachrichtigung der Betroffenen (Art. 34 DSGVO)

Zudem ist eine Benachrichtigung der Endkunden erforderlich, wenn voraussichtlich ein hohes Risiko für deren Rechte und Freiheiten besteht. Hier sprechen mehrere Umstände deutlich dafür:

- ▪ die Veröffentlichungsdrohung,
- ▪ die typische Betroffenheit sensibler Aufnahmen (z. B. Hochzeit, Schwangerschaft, Erotik),
- ▪ die voraussichtliche Betroffenheit Minderjähriger,
- ▪ die Kombination aus E-Mail-Adresse und Galerie-Zugangsdaten (Risiko von Phishing und Credential-Stuffing).

Die Ausnahmen des Art. 34 Abs. 3 DSGVO (insbesondere wirksame Verschlüsselung) greifen nach derzeitigem Kenntnisstand nicht ersichtlich.

Der Benachrichtigungstext muss klar, transparent und rechtssicher formuliert sein. Beschönigungen können als Transparenzverstoß ausgelegt werden, übermäßige Alarmierung erhöht das Risiko von Schadensersatzklagen und beschädigt das Vertrauen Ihrer Kundschaft nachhaltig.

6. Pflicht 3: Eigene Position sichern (parallel zur Pflichterfüllung)

Unabhängig von Melde-/Benachrichtigungspflichten sollten Sie Ihre Rechtsposition gegenüber Portraitbox sichern. Dazu sollten Sie folgende Punkte beachten:

- ▪ Auftragsverarbeitungsvertrag (AVV) prüfen: Welche Technisch- Organisatorischen-Maßnahmen (TOMs) wurden in dem AVV zugesichert? Wurden diese auch eingehalten? Nach dem Stand der Technik sollte ein einzelner kompromittierter API-Schlüssel keinen vollständigen Datenabfluss ermöglichen.
- ▪ Beweise sichern: Sämtliche Korrespondenz, Verträge, Screenshots und – soweit vorhanden – Logs/Protokolle sollten gesichert aufbewahrt werden.
- ▪ Regress prüfen: Ansprüche können je nach Lage aus dem AVV gemäß § 280 BGB sowie Art. 82 Abs. 2 Satz 2 DSGVO in Betracht kommen. Ggf. sollte ein Rechtsanwalt die Prüfung übernehmen.

7. Vorsorge: Eigene Datenschutz-Organisation überprüfen

Aufsichtsbehörden prüfen im Rahmen von Datenpannenuntersuchungen häufig auch das übrige Compliance-Niveau. Wir empfehlen daher, zeitnah folgende Punkte zu überprüfen:

- ▪ Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO),
- ▪ Auswahl und Kontrolle von Auftragsverarbeitern (Art. 28 Abs. 1 DSGVO),
- ▪ eigene TOMs (Art. 32 DSGVO),
- ▪ unabhängige Backups Ihrer Bilddaten,
- ▪ Zwei-Faktor-Authentisierung für relevante Systeme,
- ▪ tragfähige Einwilligungen insbesondere bei sensiblen Aufnahmen,
- ▪ Aktualität und Vollständigkeit Ihrer Datenschutzerklärung.

Ansprechpartner

Handwerkskammer Lübeck
Rechtsabteilung
Telefon: 0451 1506-195
rechtsauskunft@hwk-luebeck.de