

EDOEB Presse_101247 vom 4. Juni 2024

EDÖB, 2024-06-04, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/edoeb_Presse_101247

FR: EDOEB Presse_101247 du 4 juin 2024

IT: EDOEB Presse_101247 del 4 giugno 2024

Regeste

Xplain: Abschluss der drei Verfahren mit Annahme aller Empfehlungen | Die Bundesämter fedpol und BAZG sowie das Unternehmen Xplain haben per Ende Mai 2024 die Empfehlungen des EDÖB im Zusammenhang mit dem Ransomware-Vorfall bei Xplain vollumfänglich angenommen. Der EDÖB hatte im zweiten Semester 2023 drei Untersuchungen eröffnet und am 1. Mai 2024 zu jeder Untersuchung einen Schlussbericht mit datenschutzrechtlichen Empfehlungen publiziert (s. Medienmitteilung vom 01.05.2024), die das fedpol, das BAZG und Xplain nun angenommen haben. Die Bundesverwaltung und deren private Auftragsbearbeiter sind angehalten, ihre Zusammenarbeit in Bezug auf die Erkenntnisse der drei Untersuchungen zu überprüfen. Der EDÖB behält sich vor, in der ganzen Bundesverwaltung diesbezügliche Kontrollen durchzuführen.

Volltext

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) Medienmitteilungen 04.06.2024 Presse_101247 Préposé fédéral à la protection des données et à la transparence (PF PDT) Communiqués de presse 04.06.2024 Presse_101247 Incaricato fedele della protezione dei dati e della trasparenza Comunicati stampa 04.06.2024 Presse_101247

Xplain: Abschluss der drei Verfahren mit Annahme aller Empfehlungen | Die Bundesämter fedpol und BAZG sowie das Unternehmen Xplain haben per Ende Mai 2024 die Empfehlungen des EDÖB im Zusammenhang mit dem Ransomware-Vorfall bei Xplain vollumfänglich angenommen. Der EDÖB hatte im zweiten Semester 2023 drei Untersuchungen eröffnet und am 1. Mai 2024 zu jeder Untersuchung einen Schlussbericht mit datenschutzrechtlichen Empfehlungen publiziert (s. Medienmitteilung vom 01.05.2024), die das fedpol, das BAZG und Xplain nun angenommen haben. Die Bundesverwaltung und deren private Auftragsbearbeiter sind angehalten, ihre Zusammenarbeit in Bezug auf die Erkenntnisse der drei Untersuchungen zu überprüfen. Der EDÖB behält sich vor, in der ganzen Bundesverwaltung diesbezügliche Kontrollen durchzuführen.

Xplain: Abschluss der drei Verfahren mit Annahme aller Empfehlungen Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter Bern, 04.06.2024 - Die Bundesämter fedpol und BAZG sowie das Unternehmen Xplain haben per Ende Mai 2024 die Empfehlungen des EDÖB im Zusammenhang mit dem Ransomware-Vorfall bei Xplain vollumfänglich angenommen. Der EDÖB hatte im zweiten Semester 2023 drei Untersuchungen eröffnet und am 1. Mai 2024 zu jeder Untersuchung einen Schlussbericht mit datenschutzrechtlichen Empfehlungen publiziert (s. Medienmitteilung vom 01.05.2024), die das fedpol, das BAZG und Xplain nun angenommen haben. Die Bundesverwaltung und deren private Auftragsbearbeiter sind angehalten, ihre Zusammenarbeit in Bezug auf die Erkenntnisse der

drei Untersuchungen zu überprüfen. Der EDÖB behält sich vor, in der ganzen Bundesverwaltung diesbezügliche Kontrollen durchzuführen. Beim Betrieb und der Weiterentwicklung ihrer digitalen Applikationen arbeitet die Bundesverwaltung mit privaten Unternehmen zusammen, in deren Zug die Bearbeitung von Personendaten übertragen wird. Die aufsichtsrechtliche Aufarbeitung des Ransomware-Vorfalles bei Xplain zeigt exemplarisch die hohen Risiken und Schadenspotenziale auf, die mit solchen Datenübertragungen einhergehen. Nach Annahme der Empfehlungen durch die Parteien stehen die Bundesverwaltung und ihre privaten Auftragsbearbeiter in ihrer Gesamtheit in der Pflicht, diese hohen Risiken zu analysieren und rechtzeitig durch angemessene Massnahmen auf ein vertretbares Mass zu senken. Gemäss den Erkenntnissen der drei Untersuchungen haben sie dabei folgende zentralen Vorgaben der Datenschutzgesetzgebung des Bundes zu beachten: Bundesorgane müssen als datenschutzrechtlich «Verantwortliche» bei der Zusammenarbeit mit privaten Unternehmen als Auftragsbearbeiter (so z.B. für die Erbringung von Supportdienstleistungen) prüfen, ob es erforderlich ist, dass Personendaten die geschützte IKT-Infrastruktur der Bundesverwaltung verlassen, oder ob es erforderlich ist, dass beauftragte Private Zugang zu dieser Infrastruktur erlangen. Auch ist zu prüfen, ob Personendaten vor ihrer Übermittlung anonymisiert werden können und welche übrigen technischen Massnahmen oder organisatorischen Vorkehren zur Verhinderung von Datenschutzverletzungen zu treffen sind. Nach Analyse der datenschutzrelevanten Risiken und Bestimmung der zu deren Minimierung geeigneten Massnahmen müssen die Bundesorgane und die privaten Unternehmen ihre Umsetzungsprozesse - wie Datenflüsse, Anonymisierung oder Zugriffsmodalitäten - vollständig und verständlich dokumentieren. Auch müssen Bundesorgane die erforderlichen technischen und organisatorischen Massnahmen in den mit den Privaten abgeschlossenen Verträgen gegebenenfalls unter Vereinbarung von Konventionalstrafen festhalten. Private Auftragsbearbeiter haben sich bei der Bearbeitung von Personendaten hinsichtlich deren Umfangs, Intensität und Dauer an den Rahmen der vertraglichen Pflichten und Vorgaben zu halten. Geeignete Massnahmen zur Einhaltung dieser Vorgaben sind Konzepte zur rechtzeitigen Datenlöschung, die Sensibilisierung und Schulung der Mitarbeitenden sowie periodische interne oder externe Audits. Adresse für Rückfragen Information Feldeggweg 1 3003 Bern Links Links Medienmitteilung vom 01.05.2024 - EDÖB schliesst Untersuchungen gegen das Unternehmen Xplain und die Bundesämter fedpol und BAZG ab Herausgeber Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter <http://www.edoeb.admin.ch/>

Export aus OpenCaseLaw (CC0). Verbindlich ist allein der vom erlassenden Gericht veröffentlichte Originaltext. Quellen-URL siehe oben.