EDOEB Presse_100884 vom 1. Mai 2024

EDÖB, 2024-05-01, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/edoeb_Presse_100884

FR: EDOEB Presse_100884 du 1 mai 2024

IT: EDOEB Presse_100884 del 1 maggio 2024

Regeste

EDÖB schliesst Untersuchungen gegen das Unternehmen Xplain und die Bundesämter fedpol und BAZG ab | Der EDÖB hat bei den drei Untersuchungen Verletzungen des Datenschutzgesetzes festgestellt, die auf Fehler im Supportprozess zurückzuführen sind. Die Ergebnisse der Untersuchungen zeigen auf, dass Personendaten vom fedpol und BAZG einerseits ohne die notwendigen Datenschutzvorkehrungen an Xplain gelangten und diese andererseits anschliessend datenschutz- und teilweise vertragswidrig von Xplain aufbewahrt wurden.

Volltext

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) Medienmitteilungen 01.05.2024 Presse_100884 Préposé fédéral à la protection des données et à la transparence (PFPDT) Communiqués de presse 01.05.2024 Presse_100884 Incaricato fedeale della protezione dei dati e della trasparenza Communicati stampa 01.05.2024 Presse_100884

EDÖB schliesst Untersuchungen gegen das Unternehmen Xplain und die Bundesämter fedpol und BAZG ab | Der EDÖB hat bei den drei Untersuchungen Verletzungen des Datenschutzgesetzes festgestellt, die auf Fehler im Supportprozess zurückzuführen sind. Die Ergebnisse der Untersuchungen zeigen auf, dass Personendaten vom fedpol und BAZG einerseits ohne die notwendigen Datenschutzvorkehrungen an Xplain gelangten und diese andererseits anschliessend datenschutz- und teilweise vertragswidrig von Xplain aufbewahrt wurden.

EDÖB schliesst Untersuchungen gegen das Unternehmen Xplain und die Bundesämter fedpol und BAZG ab Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter Bern, 01.05.2024 - Der EDÖB hat bei den drei Untersuchungen Verletzungen des Datenschutzgesetzes festgestellt, die auf Fehler im Supportprozess zurückzuführen sind. Die Ergebnisse der Untersuchungen zeigen auf, dass Personendaten vom fedpol und BAZG einerseits ohne die notwendigen Datenschutzvorkehrungen an Xplain gelangten und diese andererseits anschliessend datenschutz- und teilweise vertragswidrig von Xplain aufbewahrt wurden. Nach dem Ransomware-Vorfall auf das Unternehmen Xplain im Mai 2023 wurden zahlreiche Personendaten der Bundesverwaltung, darunter auch besonders schützenswerte Personendaten, im Darknet publiziert. Diese Daten waren auf einem Server von Xplain gespeichert. Der EDÖB hat daraufhin am 20.06.23 gegen die Bundesämter für Polizei (fedpol) und Zoll und Grenzsicherheit (BAZG) und am 13.07.23 gegen das Unternehmen Xplain je eine Untersuchung eröffnet. Er hat insbesondere untersucht, unter welchen Umständen die Daten von den untersuchten Bundesämtern an Xplain übermittelt und auf den Server von Xplain gespeichert wurden. In seinen Berichten kommt der EDÖB zum Schluss, dass weder das fedpol noch das BAZG mit Xplain klar vereinbart hatten, ob bzw. unter welchen Voraussetzungen Personendaten im Rahmen von Supportleistungen

durch Xplain auf deren Server gespeichert werden dürfen. Es hätte ausdrücklich festgehalten werden müssen, in welchem Umfang Personendaten an Xplain übermittelt und von Xplain gespeichert werden dürfen. Der tatsächliche Prozess war so ausgestaltet, dass Personendaten im Rahmen von Supportfällen an Xplain gelangten, ohne dass genaue Anforderungen für die Übermittlung und die Erfüllung der Datensicherheit bei Xplain definiert wurden. Dadurch entstand auf dem Server von Xplain eine Sammlung von unstrukturierten Daten aus den Bundesämtern. Der EDÖB stellte zudem fest, dass die Menge an Personendaten, die im Rahmen dieses Prozesses übertragen wurden, unverhältnismässig war. Xplain hatte keine Zugriffsmöglichkeiten auf die Datenbanken des fedpols oder des BAZG. Das Unternehmen hätte jedoch wissen müssen, dass die von ihr programmierten Supportfunktionen auch Personendaten enthalten können und diese damit im Rahmen der Supportprozesse auf ihrem Server bearbeitet werden. Für diese Bearbeitungen hat Xplain als Auftragsbearbeiterin keine angemessenen Massnahmen zur Gewährleistung der Datensicherheit oder des Informationsschutzes gemäss Best Practice getroffen. Was die Aufbewahrung von Personendaten der Bundesverwaltung betrifft, verletzte Xplain die datenschutzrechtlichen Grundsätze der Zweckbindung und der Verhältnismässigkeit. Zudem hat Xplain, trotz vereinzelt vorhandener vertraglicher Löschpflichten, diese Personendaten vertragswidrig aufbewahrt. Der EDÖB hat gegenüber dem BAZG, fedpol und Xplain Empfehlungen ausgesprochen, deren Umsetzung die Risiken weiterer Datenschutzverletzungen nachhaltig minimieren sollen. Die drei Adressaten haben eine dreissigtägige Frist, um dem EDÖB mitzuteilen, ob sie die Empfehlungen annehmen. Hinweis: Parallel zu der vom EDÖB als unabhängige Untersuchungsbehörde nach Massgabe des DSG durchgeführten Untersuchung führte der Bundesrat in Anwendung des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG) eine Administrativuntersuchung durch, die sich ebenfalls mit dem Datenabfluss bei der Xplain AG befasste und deren Schlussbericht ebenfalls am 01.05.2024 publiziert wird. Die beiden Untersuchungen wurden voneinander unabhängig durchgeführt. Adresse für Rückfragen Information Feldeggweg 1 3003 Bern Dokumente Dokumente Schlussbericht Xplain vom 25. April 2024 (PDF, 1 MB) Schlussbericht fedpol vom 25. April 2024 (PDF, 2 MB) Schlussbericht BAZG vom 25. April 2024 (PDF, 1 MB) Herausgeber Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter http://www.edoeb.admin.ch/