EDOEB schlussbericht-und-empfehlungen-vom-25-april-2024-des-eidgenoessischen-datenschu-2024-04-25 vom 25. April 2024

EDÖB, 2024-04-25, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/edoeb_schlussbericht-und-empfehlungen-vom-25-april-2024-des-eidgenoessischen-datenschu-2024-04-25

FR: EDOEB schlussbericht-und-empfehlungen-vom-25-april-2024-des-eidgenoessischen-datenschu-2024-04-25 du 25 avril 2024

IT: EDOEB schlussbericht-und-empfehlungen-vom-25-april-2024-des-eidgenoessischen-datenschu-2024-04-25 del 25 aprile 2024

Erwägungen

E. 7

Xplain ist ein privates Unternehmen (AG) mit Sitz in Interlaken und zwei Entwicklungspartnerschaf- ten mit Niederlassungen in Deutschland und Spanien im Besitz von zwei Verwaltungsräten der Xplain und je einen Mitarbeitenden. Zusammen mit den Niederlassungen beschäftigt das Unterneh- men rund 70 Mitarbeitende.

E. 8

Gemäss eigener Beschreibung ist das Unternehmen seit der Gründung im Jahr 2000 fast aus- schliesslich als Lieferantin von Standard-Software für die Innere Sicherheit tätig und arbeitet für Behörden und Organisationen mit Sicherheits-, Migrations-, Strafverfolgungs- und Strafvollzugsauf- gaben. Für diese Behörden und Organisationen bietet Xplain «innovative-Softwareprodukte mit ei- ner vollständigen Abdeckung der Arbeitsprozesse von der Erstaufnahme bis zur Archivierung an. Der Fokus der Lösungen liegt auf der hohen Automatisierung der «Kilowäsche» und der Einhaltung der gesetzlichen Vorgaben, insbesondere auch der Formvorschriften der Strafprozessordnung so- wie dem schnellen und nachvollziehbaren Austausch der Informationen zwischen allen Beteiligten – auch mobil. In den letzten 22 Jahren haben sich über 30 Organisationen unter anderem aus Polizei, Strafverfolgung, Justiz, Vollzug und Migration für eine Lösung von Xplain entschieden.»

E. 9

Das BAZG hat Xplain für die Entwicklung von eneXs-stationär und eneXs-mobile beauftragt. 2.2. IT- Infrastruktur von Xplain

E. 10

Im Mai 2023 bezog Xplain vom Hostanbieter Dienstleistungen wie Host Services – (Hyper-V-Server), Dedicated Services – (eigenständige physische Server) und Cloud Services – (Da- tenablagen). Nach Bekanntwerden des Ransomware-Vorfalls wurde die weitere Zusammenarbeit mit sistiert.

2.3. Personendaten auf dem Fileserver von Xplain

E. 14

Das BAZG hat eine Analyse der im Darknet publizierten Daten durchgeführt, die einen Bezug zum BAZG aufweisen. Folglich betrifft die Analyse vom BAZG einen Teil der im Darknet publizierten Daten. Diese Daten waren auf dem Fileserver von Xplain gespeichert.

E. 15

Das BAZG hat sich für die Datenanalyse an die Vorgehensweise von fedpol angelehnt. Daraus resultierte der Entscheid für eine risikobasierte Vorgehensweise, da die im Darknet veröffentlichten Daten nicht zweifelsfrei einzelnen Betroffenen zugeordnet werden konnten. Dem BAZG ist dafür durch das NCSC und fedpol ein Datenrepository (400 GB) mit mutmasslich BAZG-bezogenen Da- teien zugewiesen worden. Des Weiteren stellte Xplain ihrerseits einen «Datendump» (26 GB) zur Verfügung.

E. 16

Das Datenpaket stammte aus einem Backup von Xplain mit mutmasslich BAZG bezogenen Da- teien, die potenziell im Darknet veröffentlicht werden könnten. Ein Vergleich mit den veröffentlichten Daten im Darknet hat ergeben, dass von 30'757 Dateien 7067 Dateien bzw. 23% veröffentlicht wur- den.

E. 17

In der Folge konnte das zugewiesene Datenpaket von 400 GB vom BAZG vertieft auf personenbe- zogene Daten geprüft werden. Dabei hat die Analyse ergeben, dass es sich bei den personenbe- zogenen Daten um Test- oder Fehlerberichte sowie Logfiles handelte.

E. 18

Die Datenmenge von ca. 420 GB bezeichnet die Grösse des Leaks und bedeutet damit nicht un- mittelbar Datensätze mit personenbezogenen Daten.

E. 19

Das Ergebnis der Analyse ergab zudem, dass in 61 Fällen (Stand: 11. August 2023) besonders schützenswerte Personendaten, die einen BAZG-Bezug aufweisen, im Darknet veröffentlicht wur- den. Dabei handelt es sich zum einen um biometrische Daten, die eine natürliche Person eindeutig identifizieren, zum anderen um Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen.

E. 20

In der Schlussanalyse wurden unter den geleakten Daten mit BAZG-Bezug gesamthaft 133 Einträge mit mutmasslich betroffenen Personen identifiziert. In sechs Einträgen waren Mitarbeitende des BAZG betroffen, während von 127 Einträgen mit mutmasslich betroffenen Personen 67 Einträge mit besonders schützenswerten Personendaten entdeckt wurden. Das Kriterium zur Einstufung in er- höhtes Risiko entspricht der Tatsache, dass es sich um besonders schützenswerten Personendaten handelt.

E. 21

Aufgrund des risikobasierten Ansatzes der im Darknet festgestellten Daten erfolgte keine Analyse ob Personendaten im Sinne des Schengen-Datenschutzgesetz (SR.235.3) betroffen waren.

E. 22

Für weitere Details zu den publizierten Daten im Darknet wird auf den Bericht des NCSC verwie- sen.1

E. 23
Gemäss der letzten Prüfung des BAZG am 26. Januar 2024 sind die Daten immer noch im Darknet zu finden und somit nicht gelöscht. Dadurch besteht die Datensicherheitsverletzung bis dato. 2.4. Xplain als Dienstleister vom BAZG

E. 24
Die Dienstleistungen von Xplain für das BAZG umfassen gemäss vertraglicher Vereinbarung die Lieferung der Software, Pflege und Support sowie die Weiterentwicklung von eneXs. Das Produkt eneXs ist eine kundenspezifische Entwicklung, welches die Anforderungen einer Grenzkontrolllö- sung an der Schengen-Aussengrenze, an den Binnengrenzen und im Inland abdeckt. Die Anwen- dung eneXs stationär wurde im Herbst 2023 durch ein neues Grenzkontrollsystem, welches durch einen Drittanbieter entwickelt wurde, abgelöst. Die mobile Lösung eneXs-mobile ist derzeit noch im

1 Bericht zu den Datenanalysen nach dem Cyberangriff auf die Firma Xplain vom 07.03.2024.

Einsatz. Dessen Nachfolgelösung (GKS mobile) wird laut BAZG voraussichtlich im Q2 2024 in Be- trieb genommen.

E. 25
Die Datenbearbeitungen in diesem Zusammenhang werden in Bezug auf eneXs-mobile näher ge- prüft. 2.4.1. Bearbeitung von Fehlerbehebungen durch Xplain im Allgemeinen

E. 26
Der Programmcode für diese Anwendungen ist durch Xplain bereitgestellt und durch das BIT auf deren Umgebung implementiert worden. Eine systematische Datenweitergabe sei gemäss BAZG nie Gegenstand der Zusammenarbeit zwischen dem BAZG und Xplain gewesen.

E. 27
Xplain hält fest, dass sie nicht beauftragt waren, Kundendaten zu hosten oder zu bearbeiten. Es bestünden zwar Verträge zu Unterhalt, Support und Wartung der Applikationen, diese würden aber nicht Hosting und Bearbeitung von Personendaten beinhalten. Datenhosting und Datenbearbeitung bilde schlicht nicht Servicebestandteil von Xplain als Softwareentwicklerin. Das Geschäftsmodell von Xplain bestehe nicht darin, im Auftrag von Kunden Personendaten zu bearbeiten, sondern in der Entwicklung von Software, welche anschliessend auf den Systemen der Kunden betrieben und verwaltet werden.

E. 28
Bei eneXs-mobile erfolgte der 1st und 2nd Level Support beim BAZG, der 3rd Level Support bei Xplain.

E. 29
Xplain erfüllte für das BAZG den 3rd Level Support, namentlich für die Anwendung eneXs-mobile. Für die Erfüllung des 3rd Level Supports muss ein systembedingter Fehler

in der Software vorliegen. Der ordentliche Ablauf gestaltete sich wie folgt: das Problem wurde, wenn möglich, auf der Testum- gebung der Bundesstellen durch die dort zuständigen Fachdienste nachgespielt. Jene Person, die das Problem bearbeitet hat (TAV oder FAV), hat das Logfile auf dem T-Laufwerk Xplain zur Verfü- gung gestellt. Die Avisierung von Xplain erfolgte mittels E-Mail oder Telefonanruf. Xplain hat da- raufhin das Logfile vom T-Laufwerk in ihre Umgebung kopiert und das Logfile auf dem T-Laufwerk gelöscht.

E. 30

Xplain hält fest, dass sie, wo es für sie überhaupt ersichtlich war, keine sensitiven Daten wollten. Generell seien sie nicht vom BAZG geschult und instruiert worden. 2.4.2. Datenübertragungen durch eneXs-mobile

E. 31

Die Software eneXs-stationär und eneXs-mobile sind Anwendungen, mit welchen Dokumente ein- gelesen und Fahndungsabfragen durchgeführt werden können. Weiter werden die daran ange- schlossenen Geräte wie bspw. Passleser, Fingerabdruckscanner, Kamera etc. gesteuert. Die Soft- ware eneXs selbst enthält keine Datenbank, jedoch wird ein Teil der biometrischen Indikatoren und Prozess-Daten für eine begrenzte Zeit, alleinig für Kontrollprozesse, zwischengespeichert und da- rauf automatisch gelöscht.

E. 32

Genutzt werden kann eneXs sowohl von FAT-Clients, aus der Virtual Desktop Infrastructure (VDI) sowie von mobilen Geräten. Dabei ermöglich eneXs das Lesen von Daten und initialisiert basierend darauf eine automatische Abfrage in Fahndungs- und Administrativ-Datenbanken wie bspw. RIPOL. Der eneXs-Server selbst befindet sich in der Shared Services Zone (SSZ) des BIT. Die SSZ unter- liegt den Betriebsauflagen der Bundesverwaltung und wird bezüglich Sicherheitsauflagen analog aller Anwendungen in den BIT Rechenzentren betrieben. Der Zugriff zur SSZ wird mittels Firewall geschützt. Damit wurden die Auflagen des ISC-EJPD für den eneXs-Server sichergestellt.

E. 33

Wie bei der Verwendung von Software üblich, können auch bei eneXs Fehler auftreten. Denkbare Fehlerarten beziehen sich dabei insbesondere auf die elektronische Dokumentenüberprüfung, feh- lende, unvollständige Treffer oder False Positives. In der Folge kann dieses Verhalten zu fehlerhaf- ten Detailanzeigen führen, oder die Performance der Anwendung, wie Verbindungsprobleme oder Latenz, kann Anomalien aufweisen. Der Fehler muss reproduzierbar sein, damit Xplain

infolgedessen in die Lage versetzt wird, den Fehler zu beheben. Von einem aufgetretenen Fehler werden durch eine Funktion in der Anwendung eneXs-mobile die benötigten Logfiles erstellt. Xplain analysiert daraufhin die generierten Reports auf Ihrer Infrastruktur mit dem Ziel zur Fehlerbehebung.

E. 34

Für die Anwendung eneXs-mobile wird das LogFile gesichert, das anschliessend per E-Mail an die eigene BAZG-E-Mail-Adresse des BAZG-Mitarbeitenden geschickt wird. Danach sendet der BAZG- Mitarbeitende das LogFile an das interne 2nd- Level

Supportteam des BAZG. Das BAZG Support- team sichtet seinerseits den Fehler, u.a. auch zum Sicherstellen, dass gleiche Fehler nicht mehrfach an Xplain gemeldet werden. Fehler, welche durch das BAZG-Supportteam im Rahmen des 2nd Level Supports gelöst werden können, werden BAZG intern erledigt und nicht an Xplain gesendet. Handelt es sich jedoch um einen systembedingten Fehler, wird das Logfile nach vorheriger Rück- sprache mit Xplain auf dem sogenannten T-Laufwerk, einem zentralen Fileshare der Bundesver- waltung, abgelegt.

E. 35

Im Anschluss erfolgt eine Vollzugsmeldung mittels E-Mail oder Telefon an Xplain, dass der ange- meldete Fehlerbricht (bei eneXs-stationär) oder das Logfile (bei eneXs-mobile) zur Analyse auf dem T-Laufwerk bereit liegt. Damit Xplain auf das T-Laufwerk zugreifen kann, wird via BAB-Client-BAZG ein Remotezugriff ermöglicht. Daraufhin kann der Fehlerbericht oder das Logfile von Xplain vom T- Laufwerk zwecks Analyse, auf ihre eigene Infrastruktur kopiert werden. Im Anschluss an den Ko- piervorgang werden die auf dem T-Laufwerk des BAZG abgelegten Fehlerberichte oder des Logfiles dort von Xplain gelöscht.

E. 36

Die Software eneXs-mobile verfügt zudem seit Beginn über eine Funktion, durch welche die Benut- zerin oder der Benutzer aktiv eine Fehlermeldung inklusive Log-Dateien an einen FTP-Server ver- senden kann. Die Zugangsdaten zu dem FTP-Server waren im Programmcode fest (hard coded) hinterlegt. Dies war und ist bei der Bundesverwaltung bzw. beim BAZG nicht möglich, weil die Netz- werke der Bundesverwaltung einen Versand auf einen externen FTP-Server nicht zulassen. Daher wurden bei BAZG keine Fehlermeldungen über einen FTP-Server an Xplain übermittelt.

E. 37

Wie im ISDS-Konzept für eneXs-mobile bemerkt wird,2 ist eine Prüfung des Programmcodes von eneXs-mobile nicht möglich. Damit bestand fortlaufend das Risiko, dass sich darin unentdeckte Schwachstellen befanden, die auch zu unerlaubtem Abfluss von Daten im Allgemeinen und zu per- sonenbezogenen Daten im Einzelnen hätten führen können. 2.4.3. Daten für die Anwendungsentwicklung

E. 38

Bei BAZG stehen für die Entwicklung und Wartung im Allgemeinen Testdaten des jeweils betroffe- nen Informationssystems zur Verfügung. Einzelne externe Informationssysteme enthalten aber in ihrer Integrationsumgebung auch produktive Daten (reelle bzw. «scharfe» Daten). Das heisst, dass je nach Informationssystem Xplain entweder nur Testdaten oder aber auch produktive Daten zur Vertragserfüllung zur Verfügung standen. 2.5. Datenübertragungen aus Sicht Xplain

E. 39

Gemäss Xplain sind Personendaten aus der Bundesverwaltung wie folgt übermittelt worden: ■ Angaben im Rahmen von Projektdaten (z.B. Kontaktangaben, involvierte Mitarbei- tende/Stellen, Ansprechpartner etc.); ■ Angaben im Rahmen von Fehlerbehebungen, ■ In Einzelfällen wurden Daten übermittelt, die in zugriffsgeschützten Laufwerken abgelegt oder nur auf dedizierten Geräten weiter analysiert und bearbeitet wurden.

2 Informations- und Datenschutzkonzept (ISDS-Konzept), Template vom 19. Dezember 2019, Stand 01.01.2016, Druckdatum 10.04.2019.

2.6. Vertragssituation zwischen BAZG und Xplain

E. 40

Das BAZG hat seit 2009 Geschäftsbeziehungen mit Xplain. Sie betreffen drei verschiedenen An- wendungen, die Xplain für das BAZG entwickelt, weiterentwickelt und zusätzlich für diese Wartungs- und Support-Dienstleistungen erfüllt. Es bestehen zahlreiche Verträge zwischen dem BAZG und Xplain. Typischerweise wurde als erstes ein Entwicklungsvertrag abgeschlossen, worauf mehrere Weiterentwicklungsverträge mit Support und Wartung sowie Lizenzverträge vereinbart wurden. Diese Verträge wurden in einem Intervall von ca. fünf Jahren jeweils erneuert. So kamen zahlreiche Verträge zustande.

E. 41

Festzuhalten ist, dass die mobile Lösung eneXs-mobile derzeit noch im Einsatz ist. Dessen Nach- folgelösung (GKS mobile) wird laut BAZG voraussichtlich im Q2 2024 in Betrieb genommen. Die neue Anwendung GKS-mobile wurde ebenfalls durch Xplain entwickelt. Im Weiteren wurde die An- wendung eneXs-stationär im Herbst 2023 durch «bocoa» abgelöst. Die Anwendung «bocoa» stammt jedoch nicht von Xplain, sondern wurde durch einen anderen Anbieter entwickelt.

E. 42

Die Verträge wurden auf Grundlage der Vorlagen des BBL erstellt. 2.6.1. eneXs-mobile

E. 43

Bei eneXs handelt es sich um ein kundenspezifisches Produkt, das die Bedürfnisse nach einer Grenzkontrolllösung an der Schengen-Aussengrenze, an den Binnengrenzen und im Inland ab- deckt. Das GWK hat für den Betrieb des MAPP (Multifunktionales Abfragegerät für Personen- und Passkontrollen) auf die Anwendung eneXs-stationär aufgebaut und benötigte zusätzlich eine dazu angepasste mobile Version. Dazu wurde Xplain im Jahr 2010 mit der Entwicklung einer entspre- chenden mobilen Version beauftragt.

E. 44

Das BAZG und das BBL haben für die Weiterentwicklung, Pflege und Support der Anwendung en- eXs-mobile für den Zeitraum vom 01. Mai 2019 bis 30. Juni 2023 (verlängert bis 30. Juni 2024) mit Xplain einen Vertrag abgeschlossen.3 Neben dem Vertrag wurden die folgenden Dokumente als Vertragsbestandteile integriert: Offertanfrage vom 21.02.2019, AGB für Werkverträge im Informa- tikbereich und die Pflege von Individualsoftware (Ausgabe 20. Oktober 2010) und das Angebot der Lieferantin OF-190304 vom 04. März 2019 eneXs-mobile. 2.7. Personensicherheitsüberprüfung

E. 45

Die Mitarbeitenden von Xplain, die direkt mit der Bundesverwaltung zusammenarbeiten, wurden einer Personensicherheitsüberprüfung unterzogen. Eine Verpflichtung hierzu wurde in einzelnen Verträgen festgehalten. 2.8. Ransomware-Vorfall auf Xplain

E. 46

Die Angreifer der Hackergruppe PLAY haben sich im Mai 2023 unbefugt Zugang zu einem von der Firma gehosteten Server verschafft und sich mittels «Lateral Movement» durch das Netz- werk der Xplain bewegt. Die Systeme beim externen Hoster umfassten einerseits Entwicklungs- und Testserver sowie andererseits bestimmte Administrations- und Build-Umgebungen der Xplain.

E. 47

In der Folge hat sich die Hackergruppe durch das Netzwerk der Xplain vorgearbeitet. Vielfach drin- gen Angreifer mittels nicht privilegierter Zugangsdaten in ein Netzwerk und starten von dort eine Erkundung der Systemumgebung zum Zweck der Orientierung als auch der Privileg-Erweiterung. Anschliessend erfolgte der Zugriff auf den Fileserver von Xplain am Standort in Interlaken, mit einem

3 Vertrag für die Erbringung von werkvertraglichen Leistungen im Informatikbereich, die Pflege und den Support von Individualsoftware für die Fachanwendung eneXs-mobile, 2019-2023, Vertrags-Nr.: 530047786, Referenz-Nr.: 530115732.

Personen direkt und aktiv informiert. Von den 127 Einträgen mit mutmasslich betroffenen Personen hatten 72 Personen eine EU-Staatsangehörigkeit. Bei 33 Personen (von 72) wurde die Persönlich- keitsverletzung jeweils «mit erhöhtem Risiko» bewertet. Allerdings konnten lediglich die Anschriften von 16 betroffenen Personen mit EU-Staatsangehörigkeit ausfindig gemacht werden. Die restlichen 18 Personen, die aktiv informiert wurden, waren entweder Schweizer Staatsangehörige oder Dritt- staatsangehörige.

E. 50

Die öffentliche Information wurde am 24. August 2023 publiziert, zusammen mit einem «Brenn- punktteaser», das heisst mit einem Internetauftritt auf der Startseite des BAZG. Die betroffenen Personen und Mitarbeitenden wurden am 11. Oktober 2023 per Brief informiert. 2.9.2. Umgesetzte technische und organisatorische Massnahmen 51. Entsprechend der Data Breach-Meldung vom 19.06.2023, wurden unmittelbar nach Bekanntwerden des Vorfalls das NCSC und fedpol kontaktiert, um die Aufarbeitung zu koordinieren. Dadurch sollte eine enge Zusammenarbeit sowie eine kongruente Abstimmung sichergestellt werden. Infolgedes- sen wurden unmittelbare Massnahmen wie bspw. die Sperrung aller Xplain-Accounts, Revozierung und ersetzen der geleakten Zertifikate eingeleitet und durchgeführt. Ebenso wurde der Vorfall bei der Bundesanwaltschaft angezeigt. Als Sofortmassnahme wurde die Zusammenarbeit mit Xplain unmittelbar nach Bekanntwerden des Datenabflusses gestoppt. Dies betraf insbesondere die Ab- nahme- und Testarbeiten zum neuen mobilen Grenzkontrollsystem. Auf konzeptioneller Ebene lie- fen die Projektarbeiten derweil weiter. 52. Umgehend nach Bekanntwerden des Datendiebstahls wurde vom BAZG eine Taskforce gebildet, welche u. a. die Aufarbeitung, Massnahmenprüfung und Koordination des weiteren Vorgehens zur Aufgabe hatte. Dazu wurde die Taskforce mit Spezialisten, Mitgliedern aus GL, DSBO, ISBO, Rechtsdienst, Kommunikation sowie dem politischen Stab besetzt. 53. Neben der Aufstellung eines Analyseteams durch die Taskforce wurden durch das BAZG alle an Xplain zur Verfügung gestellte Hardware des BAZG wie Notebooks und Mobilphones zurückver- langt. Weiter hat das BAZG von Xplain den Sourcecode der eingesetzten Anwendungen zur Ana- lyse einverlangt, wobei das BAZG schliesslich nur den Sourcecode von eneXs stationär erhalten hat. 54. Der erhaltene Sourcecode ist anschliessend durch das

BAZG einer risikobasierten Prüfung unter- zogen worden. Dazu wurde der Sourcecode nach Schadsoftware durchsucht sowie nach Code, der allenfalls eingeschleust wurde, um automatisch Reports mit Daten zu generieren und diese an- schliessend auf die Systeme von Xplain zu senden. Allerdings konnten die dazu eingesetzten BAZG-Spezialisten nichts Verdächtiges feststellen. Der Sourcecode wurde anschliessend durch das BAZG zerstört und Xplain entsprechend bestätigt. 55. Später wurde zusammen mit dem NCSC die Software eneXs mobile geprüft. Hierbei stand eine dynamische Analyse mittels Sandbox im Vordergrund, bei welcher geprüft wurde, ob eneXs mobile darüber hinaus heimlich Verbindungen zu Xplain aufbaut. Es konnte jedoch nichts Derartiges ent- deckt werden. 56. Das BAZG legt zudem dar, dass die gefundenen Datensätze nicht nach BAZG / fedpol getrennt werden können. Begründet wird dies damit, weil Xplain keine Datentrennung gewährleistet. Daher konnten in der Folge die Datensätze auch nicht eindeutig zugeordnet werden.

58. Der EDÖB geht davon aus, dass die in diesem Bericht festgestellten Sachverhalte bei anderen Bundesbehörden und Applikationen gleich oder ähnlich stattgefunden haben. 3. Stellungnahme zum Sachverhalt 59. Mit Schreiben vom 22. März 2024 hat das BAZG zum Sachverhalt Stellung genommen. Die Ergän- zungen und Anmerkungen wurden übernommen, soweit sie für die datenschutzrechtliche Beurtei- lung relevant waren.

4. Datenschutzrechtliche Beurteilung 4.1. Vorbemerkungen 60. Gestützt auf Art. 70 Bundesgesetz über den Datenschutz vom 25. September 2020 (DSG) erfolgt die datenschutzrechtliche Beurteilung nach dem Bundesgesetz über den Datenschutz vom 19. Juni 1992 (aDSG). Gewisse Begrifflichkeiten und materiellrechtliche Konkretisierungen werden jedoch vom DSG übernommen, soweit sie eine identische Bedeutung haben und der Klarheit die- nen.4 61. Die nachfolgenden rechtlichen Beurteilungen nach aDSG gelten grundsätzlich auch bei der Anwen- dung des revidierten DSG, weil in diesen Bereichen keine materiellen Unterschiede bestehen. Wo materielle Unterschiede zwischen altem DSG und revidiertem DSG vorhanden sind, wird auf die Unterschiede hingewiesen. 62. Ob für die im Rahmen dieser Sachverhaltsabklärung untersuchten Personendatenbearbeitungen hinreichende gesetzliche Grundlagen bestehen, ist nicht Gegenstand dieser Untersuchung. 63. Der EDÖB eröffnete ursprünglich ein Vorverfahren betreffend RIPOL-Zugriffe und anschliessend ein formelles Verfahren betreffend RIPOL-Zugriffe und Datenschutzverletzungen im Zusammen- hang mit Xplain gestützt auf Art. 22 SDSG und Art. 27 Abs. 2 aDSG. Das Verfahren betreffend RIPOL-Zugriffe wurde sistiert (siehe Ziffer 6), und das vorliegende Verfahren wurde gestützt auf Art. 27 aDSG weitergeführt, da erste Erkenntnisse der Abklärung rasch den Schluss zuliessen, dass schwerpunktmässig kaum Personendaten im Sinne des SDSG betroffen sind. 64. Die Datenbearbeitungen vom BAZG im Zusammenhang mit den Anwendungen eneXs-mobile ste- hen im Vordergrund (siehe Ziffer 5). Der EDÖB hat seine Untersuchung auf diese Anwendung ein- geschränkt: Die Anwendung eneXs-mobile führte zahlenmässig zu den meisten Personendaten- übermittlungen von Behörden zu Xplain. Dabei ist festzuhalten, dass neben dem BAZG zahlreiche weitere Behörden die Anwendung eneXs-mobile verwenden, insbesondere zahlreiche kantonale Polizeibehörden, aber auch andere Bundesbehörden. Andere Anwendungen, die Xplain für die Bun- desverwaltung entwickelt und implementiert hat, führten gemäss Erkenntnissen des EDÖB zu kei- nen systematischen Datenflüssen von

Behörden zu Xplain, weshalb auf die Untersuchung der rest- lichen Anwendungen verzichtet wurde. Die Reaktionen vom BAZG nach dem Vorfall werden kurz beurteilt. Die datenschutzrechtliche Beurteilung des Ransomware-Vorfalls durch Play ist nicht Gegenstand der Untersuchung. 4.2. Vertragliche Vereinbarungen mit Xplain 65. Das BAZG hat seit 2009 Geschäftsbeziehungen mit Xplain betreffend drei verschiedenen Anwendungen, die Xplain entwickelt, weiterentwickelt und zusätzlich für diese Wartungs- und Support- Dienstleistungen erfüllt (siehe Ziffer 40). Im Rahmen der Vertragsbeziehung zu eneXs-mobile er- folgte die Übertragung von Personendaten an Xplain. 66. Es spielt keine Rolle, dass die Übertragung von Personendaten nur ein Nebeneffekt bei der gesam- tem Vertragserfüllung darstellt. Insbesondere der Support- und Wartungsprozess (siehe insb. Zif- fer 28 ff. und 33 ff.) ist auf die Übertragung von Personendaten hin angelegt, auch wenn sie einen geringen Umfang im Vergleich zu den Kerntätigkeiten von Xplain ausmachen. In Bezug auf diese Datenbearbeitungen liegt ein Auftragsbearbeitungsverhältnis gemäss Art. 10a aDSG vor. Art. 10a aDSG formuliert die Anforderungen an die Auftragsdatenbearbeitung. Die Qualifikation der

4 So wird nicht vom «Inhaber der Datensammlung» (Art. 3 lit. i aDSG) gesprochen, sondern vom Verantwortlichen (Art. 5 lit. j DSG) und statt vom Dritten, dem eine Datenbearbeitung übertragen wird (Art. 10a aDSG), vom Auftragsbearbeiter (Art. 9 DSG).

Datenübertragungen an Xplain als Auftragsdatenbearbeitung und die Anforderungen an diese wer- den nachfolgend in Bezug auf eneXs-mobile näher begründet. 4.3. Datenübermittlung durch eneXs-mobile 67. In Art. 22 Abs. 2 VDSG wird festgehalten, dass das Bundesorgan, das Personendaten durch Dritte bearbeiten lässt, für den Datenschutz verantwortlich bleibt und dafür sorgt, dass die Daten auftrags- gemäss bearbeitet werden, insbesondere was deren Verwendung und Bekanntgabe betrifft. Die Voraussetzungen, damit ein Bundesorgan Personendaten durch Dritte bearbeiten lassen kann, wird in Art. 10a Abs. 1 aDSG geregelt. Diese Bestimmung entspricht materiell im Wesentlichen dem neuen DSG (Art. 9 DSG). Gemäss Art. 16 Abs. 1 aDSG bleibt das Bundesorgan, das Personendaten durch Dritte bearbeiten lässt, für den Datenschutz verantwortlich. 4.3.1. Datenbearbeitung durch Xplain 68. «Nach Art. 10a Abs. 1 (a)DSG kann die Bearbeitung von Personendaten durch Vereinbarung oder Gesetz Dritten übertragen werden. Voraussetzung für die (teilweise) Übertragung der Datenbear- beitung an Dritte ist, dass die Daten nur so bearbeitet werden, wie der Auftraggeber den Dritten hierzu ermächtigt. Zudem dürfen keine gesetzlichen oder vertraglichen Geheimhaltungsinteressen die Übertragung verbieten und eine Bearbeitung der Personendaten zu eigenen Zwecken durch den Dritten muss ausgeschlossen sein; würden die Personendaten (auch) für Zwecke des Dritten bearbeitet, ginge die Datenbearbeitung über eine «Datenbearbeitung durch Dritte» im Sinne von Art. 10a (a)DSG hinaus und bedürfte eines eigenen Rechtfertigungsgrundes bzw. der Einhaltung der Voraussetzungen von Art. 19 (a)DSG.»5 Für eine Auslagerung gemäss Art. 10a Abs. 1 aDSG wird somit eine Übertragung durch Vereinbarung oder Gesetz, keine Bearbeitung zu eigenen Zwe- cken des Auftragnehmers sowie keine widersprechenden Geheimhaltungsverpflichtungen voraus- gesetzt. 4.3.2. Vereinbarung oder Gesetz 69. Eine gesetzliche Grundlage, wonach Xplain zur fraglichen Bearbeitung legitimiert wird, ist nicht er- sichtlich. Es ist deshalb zu prüfen, ob zwischen dem BAZG und Xplain eine Vereinbarung bestand, welche die Bearbeitung von Personendaten beinhaltet. 70. Weder die vom BAZG vorgebrachten Argumente (siehe Ziffer 26), noch die Ausführungen von Xplain

(siehe Ziffer 27), die darauf abzielen, das Bestehen einer Vereinbarung über eine Datenbearbeitung zu verneinen, vermögen zu überzeugen. Die Vorbringen dürften aus unterschiedlichen Gründen motiviert sein, sie verkennen jedoch die datenschutzrechtliche Situation. 71. Gemäss Art. 3 lit. e aDSG bedeutet «bearbeiten» im Sinne des DSG jeder Umgang mit Personen- daten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten. Der Begriff des Bearbeitens wird weit gefasst und beinhaltet auch die Kenntnisnahme oder das Einsicht- gewähren (Art. Art. 3 lit. f aDSG). 72. Das tatsächliche Bearbeiten von Personendaten wird durch den Ransomware-Vorfall im Mai 2023 belegt. Aufgrund des Zugriffs auf den Fileserver von Xplain am Standort Interlaken wurde ein Teil der Daten, die auf dem erwähnten Fileserver gespeichert waren, im Juni 2023 im Darknet publiziert. Somit bearbeitete bzw. hatte Xplain mindestens diejenigen Personendaten vom BAZG gespeichert, die im Darknet publiziert wurden. Xplain verfügte über 26 GB Daten vom BAZG auf ihrem Fileserver, wovon 23% bzw. 7067 Dateien veröffentlicht wurden. In den im Darknet publizierten Daten wurden viele Logs von eneXs-mobile mit Personendaten festgestellt. Folglich hat Xplain im Mai 2023

5 Zum Ganzen BVerGer A-4941/2014, Urteil vom 09.11.2016, Ziff. 12.7.3.

Personendaten vom BAZG auf ihrem Fileserver in Interlaken gespeichert bzw. im Sinne von Art. 3 lit. e aDSG bearbeitet. 73. Das BAZG und das BBL hat mit Xplain einen Vertrag betreffend Leistungen im Informatikbereich, die Pflege und den Support von Individualsoftware für die Fachanwendung eneXs-mobile abge- schlossen.6 Gemäss dem Vertragsgegenstand regelt der Vertrag «[…] die Pflege und Support der mobilen eneXs Lösung inkl. der Schnittstellen und eneXs Komponenten (eneXs Server, eneXs Fachapplikationen etc.) […]». Der Vertrag mit dem BAZG7 bezieht sich auf die Zeitperiode vom 1. Mai 2019 bis zum 30. Juni 2023. Er sieht in Bezug auf den Support von eneXs-mobile vor, dass das BAZG Ausnahmezustände und Fehlermeldungen zu dokumentieren hat (Vertrag Ziffer 5). Xplain stellt eine qualifizierte Fehler-Annahme und ein Fehlermanagement zur Verfügung, das die Off-Site Fehleridentifikation und die Off-Site Korrektur von Fehlern vorsieht. Der Kontakt für Pflege und Sup- port hat über Telefon oder eMail zu erfolgen (Vertrag Buchstabe B). BAZG stellt Xplain für die Wartung und Pflege eine Umgebungskonfiguration in den Räumen von Xplain zur Verfügung. 74. Zwar wurden verschiedene Regelungen zu Pflege und Support getroffen, aus dem Wortlaut des Vertrags bleibt jedoch unklar, ob das BAZG davon ausging, dass Xplain im Rahmen von Support und Wartung nur Kenntnis von Personendaten erhält oder ob der Support und Wartungsprozess - insbesondere die Organisation des 2nd und 3rd Levels - so ausgestaltet wurde, dass dieser die Spei- cherung von Personendaten auf dem Fileserver von Xplain beinhaltet (zur Beurteilung des 2nd und 3rd Level-Prozesses siehe nachfolgende Ziffer 93 ff.). Der Vertrag ist jedoch zusammen mit dem tatsächlich durchgeführten Support-Prozess (siehe Ziffer 34 f.) zu betrachten, weshalb die Parteien Wissen mussten, dass Personendaten übertragen werden. Von einem aufgetretenen Fehler wurden durch eine Funktion in der Anwendung eneXs-mobile Screenshots oder Fehler-Reports erstellt. Da keine technischen oder organisatorische Massnahmen ergriffen wurden, um die Personendaten in den Screenshots oder Fehler-Reports zu anonymisieren, musste sowohl für das BAZG als auch für Xplain erkennbar sein, dass Personendaten an Xplain übertragen werden. 75. Auch wenn Xplain nicht regelmässig Personendaten vom BAZG übermittelt

worden wären, handelt Xplain als Auftragsbearbeiterin gemäss Art. 10a aDSG, solange sie regelmässig im Rahmen von Pflege und Support Kenntnis von Personendaten erhält. In diesem Fall ist es notwendig, mit Xplain zu vereinbaren, welchen Anforderungen und Voraussetzungen diese Kenntnisnahmen unterliegen. Festzuhalten wäre etwa, dass die Personendaten nicht in anderen Systemen abgespeichert werden dürfen oder welche Anforderungen bei einer Kenntnisnahme gelten. 76. Unter Berücksichtigung der gesamten Umstände ist davon auszugehen, dass mit dem erwähnten Vertrag betreffend eneXs-mobile die Vertragsparteien eine Vereinbarung gemäss Art. 10a aDSG getroffen haben. Gegenstand und Umfang der Datenbearbeitungen wird im Vertrag zwar nicht kon- kret geregelt. Das ist aber so möglich, weil die Vereinbarung an keine Form gebunden ist. Das Risiko einer unklaren Regelung trägt das BAZG als Verantwortliche. 4.3.3. Keine Bearbeitung zu eigenen Zwecken 77. In Ziffer 23.2 der im Vertrag integrierten AGB8 wir die Bearbeitung von Personendaten für andere Zwecke ausgeschlossen.

6 Siehe vorangehende Ziffer 44. 7 Vertrag für die Erbringung von werkvertraglichen Leistungen im Informat kbereich, die Pflege und den Support von Individualsoftware für die Fachanwendung eneXs-mobile, 2019-2023, Vertrags-Nr.: 530047786, Referenz-Nr.: 530115732. 8 Allgemeine Geschäftsbedingungen für Werkverträge im Informatikbereich und die Pflege von Individualsoftware, Ausgabe 20.10. 2010.

4.3.4. Keine widersprechenden Geheimhaltungsinteressen 78. Bei der Erfüllung des Vertrages musste davon ausgegangen werden, dass Xplain Kenntnis von Amtsgeheimnissen erhält. Das Amtsgeheimnis steht grundsätzlich einer Auslagerung nicht entge- gen, sofern die Dritten als Hilfspersonen i.S.v. Art. 321 Abs. 1 StGB zu qualifizieren sind.9 Dies ist bei den Mitarbeitenden von Xplain erfüllt. Zusätzlich muss sichergestellt werden, dass die Geheim- haltungsverpflichtung dem Auftragnehmer überbunden wird. Dies wird mit Art. 22 der AGB erfüllt. 79. Zudem stellt der IKT-Grundschutz Anforderungen angesichts des Risikos der Amtsgeheimnisver- letzung. Die zu berücksichtigen Massnahmen werden aufgelistet und auf das Dokument «Anforde- rungen angesichts des Risikos von Amtsgeheimnisverletzungen» hingewiesen.10 4.3.5. Fazit 80. Somit bestätigen die vorangehenden Erläuterungen, dass ein Auftragsbearbeitungsverhältnis vor- liegt und der Auslagerung von Personendaten im Zusammenhang mit eneXs-mobile gestützt auf Art. 10a Abs. 1 aDSG grundsätzlich nichts entgegenstand, obwohl Gegenstand und Umfang der Datenbearbeitung vertraglich nur rudimentär geregelt wurden. Insbesondere wurde nicht transpa- rent festgehalten, ob und wie bei Supportleistungen Personendaten an Xplain übertragen werden und somit das Prinzip der Verhältnismässigkeit eingehalten werden kann. Da es sich nicht um eine Datenbekanntgabe im Sinne von Art. 3 lit. f aDSG handelt, bleibt das BAZG für die Datenbearbei- tungen von Xplain verantwortlich, solange Xplain die Personendaten nicht über die Vereinbarung hinaus bearbeitet. Nicht geprüft wurde, ob die Anforderungen gemäss dem IKT-Grundschutz um- gesetzt wurden. 4.3.6. Gewährleistung der Datensicherheit 81. Gemäss Art. 10a Abs. 2 aDSG muss sich der Auftraggeber insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet. Im Gesetz zwar nicht ausdrücklich erwähnt, aber mitum- fasst, ist die Pflicht des Auftraggebers, sich um die Einhaltung des Datenschutzes und damit auch der anderen allgemeinen Datenschutzgrundsätze aktiv zu bemühen. Die Umsetzung der eigenen Verpflichtungen hinsichtlich Datensicherheit ist dem Dritten zu überbinden.11 82. Der Verantwortliche hat dem Auftragnehmer klare Vorgaben für Sicherheitsmassnahmen zu

ma- chen und deren Umsetzung und Einhaltung zu kontrollieren. Sofern der Auftragnehmer selbst dem aDSG untersteht, kann der Verantwortliche davon ausgehen, dass die technischen und organisa- torischen Massnahmen der Datensicherheit (Art. 7 aDSG) angemessen erfüllt sind (Art. 22 Abs. 3 VDSG e contrario). Der Verantwortliche ist deshalb verpflichtet, den Auftragsbear- beiter sorgfältig auszuwählen, zu instruieren und soweit nötig zu überwachen.12 83. Zudem hält auch der IKT-Grundschutz der Bundesverwaltung als minimale Sicherheitsanforderung fest, dass bei Dienstleistungen durch Dritte die IKT-Sicherheitsvorgaben des Bundes verbindlich und vertraglich zu regeln sind.13 4.3.7. Auswahl 84. Dem EDÖB ist nicht bekannt, nach welchen Kriterien das BAZG für die Umsetzung einer mobilen App zur Abfrage auf polizeiliche Datenbanken Xplain vor rund 15 Jahren ausgewählt hat, weshalb diesbezüglich keine Beurteilung erfolgen kann. Typischerweise wurde die Vertragsbeziehung mit

9 Botschaft zur Totalrevision des DSG, 2017, S. 7031 f., wonach dies sowohl nach aDSG wie auch nach DSG gilt. 10 IKT-Grundschutz in der Bundesverwaltung, Version 4.6, Stand 01.04.2021, Kap. 2 Ziff. 15.2. 11 Zum Ganzen BVerGer A-4941/2014, Urteil vom 09.11.2016, Ziff. 12.7.3 12 Botschaft DSG 1988, 463; Botschaft DSG 2017, 7032. 13 IKT-Grundschutz in der Bundesverwaltung, Version 4.6, Stand 01.04.2021, Kap. 2 Ziff. 15.1.

Xplain jeweils für eine Zeitperiode von rund vier Jahren abgeschlossen. Bei jedem Entscheid für eine neue Zeitperiode ist die Auswahl objektiv neu zu beurteilen. Solange Xplain Daten im Bereich der inneren Sicherheit bearbeitet und dabei besonders schützenswerte Daten oder vertrauliche und geheime Informationen bearbeitet, müssen datenschutzrechtliche Kriterien berücksichtigt werden; etwa ob Xplain über ein Informationssicherheitsmanagementsystem verfügt und ob dazu eine Zer- tifizierung nach einem international anerkannten Standard vorliegt. Diese hohen Anforderungen sind gerechtfertigt, wenn eine Zusammenarbeit mit Xplain im Bereich der inneren Sicherheit einge- gangen werden soll. 4.3.8. Instruktion 85. Zu prüfen ist, inwieweit die Vergewisserungspflicht des Verantwortlichen geht, dass der Auftrags- bearbeiter die Datensicherheit gewährleistet. Nach Art. 7 Abs. 1 aDSG wird die Datensicherheit gewährleistet, sofern die Personendaten durch angemessene technische und organisatorische Mas- snahmen geschützt werden. Die verantwortlichen Bundesorgane treffen die nach den Artikeln 8-10 VDSG erforderlichen technischen und organisatorischen Massnahmen zum Schutz der Persönlich- keit und der Grundrechte der Personen, über die Daten bearbeitet werden. Bei der automatisierten Datenbearbeitung arbeiten die Bundesorgane mit dem Informatikstrategieorgan Bund (ISB; heute BACS) zusammen (Art. 20 Abs. 1 VDSG). 86. Grundsätzlich kann das BAZG davon ausgehen, dass Xplain die angemessenen technischen und organisatorischen Massnahmen umgesetzt hat, da Xplain selbst als Verantwortlicher dem aDSG untersteht und Art. 7 aDSG einzuhalten hat. In Art. 8 DSG wird dies neu konkretisiert, indem auch der Auftragsbearbeiter explizit erwähnt wird. Soweit indessen spezifische Sicherheitsmassnahmen des Auftraggebers bestehen – hier der Bundesverwaltung – sind diese dem Auftragsbearbeiter spe- zifisch zu überbinden. 87. Gemäss dem Vertrag erbringt Xplain als Spezialistin und in Kenntnis des Vertragszwecks Pflege und Support als «Basisleistung», Erweiterungen und Weiterentwicklungen sowie Pflege und Sup- port von Systemteilen und Weiterentwicklungen. Der Vertrag enthält keine spezifischen daten- schutzrechtlichen Instruktionen. In den integrierten AGB wird in Ziffer

23.1 festgehalten, dass die Parteien sich verpflichten, «die wirtschaftlich zumutbaren sowie technisch und organisatorisch mög- lichen Vorkehrungen zu treffen, damit die im Rahmen der Vertragsabwicklung anfallenden Daten gegen unbefugte Kenntnisnahme Dritter wirksam geschützt sind». Andere Vereinbarungen, worin das BAZG Xplain über die Anforderungen der Datensicherheit genauer instruiert, bestanden ge- mäss den Feststellungen des EÖDB nicht. 88. Um beurteilen zu können, welche technischen und organisatorischen Massnahmen erforderlich sind zum Schutz der Persönlichkeit und Grundrechte der Personen, über die Daten bearbeitet werden, bildet der Gegenstand und der Umfang der Bearbeitung die Ausgangslage. Dies wurde indessen nicht klar geregelt und stellt ein grundlegendes Problem für die angemessene Erfüllung der Anfor- derungen der Datensicherheit eines Auftragsbearbeiters dar. Der Programmcode von eneXs-mobile ist durch Xplain bereitgestellt und durch das BIT auf deren Umgebung implementiert worden. Ge- mäss dem BAZG sei eine systematische Datenweitergabe nie Gegenstand der Zusammenarbeit zwischen dem BAZG und Xplain gewesen. Der Wartungs- und Supportprozess war allerdings durch die von Xplain in der Software programmierte Funktion vorgegeben. Bei einem aufgetretenen Fehler werden in eneXs-mobile Screenshots oder Fehler-Reports mit produktiven Daten, die auch Perso- nendaten enthalten, erstellt und aus der IT-Bundesinfrastruktur in die IT-Infrastruktur von Xplain übertragen (siehe Ziffer 33 ff.). Die Parteien hätten erkennen müssen, dass dieser Support- und Wartung bzw. die Fehlerbehebungsprozesse Personendaten beinhaltet und der genaue Umgang mit diesen Personendaten wäre konkret zu regeln gewesen. 89. Möglich gewesen wären grundsätzlich zwei Varianten: das BAZG hätte Xplain ausdrücklich vertrag- lich verpflichten können, dass Personendaten nur auf der Bundesinfrastruktur des Bundes bearbei- tet werden dürfen bzw. die Speicherung von Personendaten ausserhalb der Bundesverwaltung

strikt verboten wäre. Dazu hätte das BAZG Xplain alle notwendigen Voraussetzungen dazu zur Verfügung stellen müssen und prüfen, ob dies in der Praxis auch konsequent umgesetzt wird. In der zweiten Variante werden Personendaten ausserhalb der Bundesinfrastruktur bearbeitet. Dazu müssen alle datenschutzrechtlichen Anforderungen beachtetet werden, insbesondre eine Bearbei- tung im Sinne der Verhältnismässigkeit und der Risikominimierung indem Regeln bzw. Prozesse befolgt werden, damit so wenig Personendaten wie möglich die Bundesinfrastruktur verlassen. Wo möglich sind Personendaten zu anonymisieren. Personendaten, die ausserhalb der Bundesinfra- struktur bearbeitet werden, müssen gemäss ihrem Schutzbedürfnis mit den erforderlichen techni- schen und organisatorischen Massnahmen geschützt werden, insbesondere durch die Einhaltung von Löschregeln. 4.3.9. Überwachung 90. Bei Xplain wurden keine regelmässigen Prüfungen im Hinblick auf die Einhaltung der Datensicher- heit, etwa in Form von Audits, durchgeführt. Im ISDS-Konzept zu eneXs werden als Restrisiken die fehlenden personellen Ressourcen des TAV und FAV als Restrisiken festgehalten. Aus operativer Sicht steht das Funktionieren der Systeme mit möglichst wenig Fehlern und Störungen im Vorder- grund, sodass konzeptionelle Datenschutzrisiken nicht erkannt oder zwar erkannt werden, aber keine Ressourcen für die Korrektur vorhanden sind. Folglich wurde zwar erkannt, dass mehr Res- sourcen notwendig wären, diese wurden aber nicht hinreichend zur Verfügung gestellt. 91. Neben der Kontrolle und Einhaltung der Prozesse durch eigene Ressourcen kann diese Aufgaben auch Dritten übertragen werden, z.B. privaten Auditunternehmen. Dies kann im Einzelfall ein geeig- netes Mittel sein, um die

eigenen Prozesse und deren Einhaltung aus datenschutzrechtlicher Sicht zu prüfen. Dies kann aber auch durch interne Stellen umgesetzt werden, da es oft nicht zielführend ist, wenn diese Verantwortung an Stellen ausserhalb der Bundesverwaltung delegiert wird. Eine geeignete Kontrolle kann im Einzelfall bereits dadurch erfüllt werden, dass durch Xplain die Kon- trolle und Einhaltung vereinbarter datenschutzrechtlicher Anforderungen mit Nachweisen bestätigt wird. 4.3.10. Fazit 92. Aus den obigen Darlegungen geht hervor, dass das BAZG die Gewährleistung der Datensicherheit gemäss Art. 10a Abs. 2 aDSG nicht ausreichend erfüllt hat. Das BAZG hätte die Übertragung von Personendaten im Rahmen von Wartung und Support ausdrücklich regeln und besser instruieren müssen, insbesondere unter welchen datenschutzrechtlichen Anforderungen im Rahmen von War- tung und Support Personendaten die IT-Bundesinfrastruktur verlassen oder nicht. Je nach Variante hätten dann die angemessenen technischen und organisatorischen Massnahmen geregelt werden müssen, um die Gewährleistung der Datensicherheit erfüllen zu können. Schliesslich hätten diese Prozesse angemessen kontrolliert werden müssen. 4.4. Support und Wartung 93. Kern der datenschutzrechtlichen Problematik ist die Übermittlung von Personendaten aus der Bun- desinfrastruktur in die IT-Infrastruktur von Xplain im Rahmen der Wartungs- und Supportprozesse (siehe Ziffer 33 ff.). Solange die Personendaten in der Bundesinfrastruktur bleiben, sind diese ge- mäss den Vorgaben des Bundes bzw. mindestens vom IKT-Grundschutz geschützt. Dem EDÖB sind keine Anhaltspunkte bekannt, dass das BAZG zusammen mit den bundesinternen Leistungs- erbringen den IKT-Grundschutz sowie den erhöhten Schutzbedarf bei erhöhtem Schutzbedürfnis für die Bundesinfrastruktur nicht erfüllt hat. Das Problem war, das nicht geprüft und beurteilt wurde, ob bzw. welche Personendaten beim Wechsel vom 2nd Level Support zum 3rd Level Support die Bundesinfrastruktur verlassen müssen.

4.4.1. Verhältnismässigkeit 94. Das Bundesgericht hält zum Grundsatz der Verhältnismässigkeit fest, dass «eine Massnahme für das Erreichen des im öffentlichen oder privaten Interesse liegenden Zieles geeignet und erforderlich ist und sich für die Betroffenen in Anbetracht der Schwere der Grundrechtseinschränkung als zu- mutbar erweist. Es muss eine vernünftige Zweck-Mittel-Relation vorliegen […]. Erforderlich ist eine Massnahme, wenn der angestrebte Erfolg nicht durch gleich geeignete, aber mildere Massnahmen erreicht werden kann […]. Im Bereich des Datenschutzes heisst dies unter anderem, dass Daten nur dann und nur soweit bearbeitet werden dürfen, als es für den Zweck der Datenbearbeitung notwendig ist (Prinzip der Datenvermeidung und Datensparsamkeit […])».14 95. Damit Xplain ihre Aufgaben des 3rd Level Support umsetzten kann, muss der Fehler oder der Auftrag für eine Weiterentwicklung verständlich und nachvollziehbar sein. Dafür werden in der Praxis häufig – weil es schnell und einfach umsetzbar ist – konkrete Beispiele verwendet, die oft eben auch be- sonders schützenswerte Personendaten enthalten können. Der Inhalt der Fehlerberichte muss aber erforderlich im Sinne der Verhältnismässigkeit sein. Auf die Fehlerberichte angewendet heisst das, dass Personendaten gelöscht oder anonymisiert werden müssen. Nur wenn die Personendaten wirklich notwendig sind, um den 3rd Level Support umzusetzen, wird die Erforderlichkeit erfüllt. Das Prinzip der Datenvermeidung und Datensparsamkeit ist somit zentral. 96. Folglich verletzt die Funktion, mit welcher Screenshots und Log-Files mit Personendaten für die Behebung von Support und Wartung erstellt werden (siehe Ziffer 33), das Prinzip der Verhältnis- mässigkeit, soweit nicht erforderliche Personendaten übertragen wurden.

4.4.2. Datensicherheit 97. Nach Art. 7 aDSG müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. In Art. 20 VDSG werden die Min- destanforderungen festgehalten. Wer Personendaten bearbeitet, sorgt für die Vertraulichkeit, Ver- fügbarkeit und Integrität der Daten, um einen angemessenen Datenschutz zu gewährleisten (Art. 20 Abs. 1 i.V.m. Art. 8 Abs. 1 VDSG). Insbesondere sind die Daten gegen die Risiken von unbefugtem Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen zu schützen (Art. 1 lit. e VDSG). 98. Der IKT-Grundschutz legt die minimalen organisatorischen, personellen und technischen Anforde- rungen an die Informatiksicherheit der Bundesverwaltung bzw. deren Informatikschutzobjekte (Schutzobjekte) fest. Der IKT-Grundschutz und die Datensicherheit gemäss DSG verfolgen unter- schiedliche Schutzziele. Während der IKT-Grundschutz die Schutzobjekte schützt, dient das DSG dem Schutz der Persönlichkeit von Personen. Der EDÖB beurteilt deshalb die Datensicherheit ge- mäss Art. 7 aDSG und nicht den IKT-Grundschutz. 99. Die Informationsweitergabe zwischen dem 2nd und 3rd Level Support bzw. zwischen dem BAZG und Xplain hätte so organsiert werden müssen, dass das Risiko von potentiellen Persönlichkeitsverlet- zungen angemessen minimiert wird. Ein organisatorischer Fehler lag insbesondere bei der Verwen- dung der dezidierten Endgeräte, welche Xplain Mitarbeitende erhielten. Solange die Xplain Mitar- beitenden nur mit den erhaltenen BAZG Notebooks auf der Bundesinfrastruktur arbeiten, bleiben alle Daten im geschützten Perimeter der Bundesverwaltung. Offensichtlich bestand seitens BAZG und Xplain kein Bewusstsein darüber, welche Anforderungen aus datenschutzrechtlicher Sicht gel- ten müssen, sobald Personendaten den Perimeter der Bundesverwaltung verlassen. Solange näm- lich Xplain mit den erhaltenen BAZG Notebooks arbeitet, wird das datenschutzrechtliche Risiko nicht erheblich erhöht, weil die Daten im geschützten Perimeter der Bundesverwaltung bleiben. Ob- wohl Mitarbeitende von Xplain die BAZG Notebooks für die Unterstützung im 2nd Level Support

14 BGE 147 I 346, E. 5.5.

erhielten, wurden die Laptops auch dazu verwendet, um Daten von der Bundesinfrastruktur auf den Fileserver von Xplain weiterzuleiten, zu bearbeiten und zu speichern. 100. Zusammenfassend kann festgehalten werden, dass der Grundsatz der Datensicherheit insbeson- dere deshalb verletzt wurde, weil keine organisatorischen Massnahmen bei der Überschneidung von 2nd und 3rd Level Support getroffen wurden, um entweder Personendatenflüsse zu Xplain zu verhindern oder die Voraussetzungen hierfür zu regeln und einzuhalten. 4.4.3. Zweckbindung 101. Gemäss Art. 4 Abs. 3 aDSG dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Bei der Umsetzung des 3rd Level Support entspricht der Zweck die Lösung des konkreten Problems oder die Umsetzung einer Weiterentwicklung. Eine Ablage bzw. ein Archiv von behandelten Anfra- gen macht aus betriebsökonomischer Sicht zwar Sinn, ist aber aus datenschutzrechtlicher Sicht ein anderer Zweck und müsste im Sinne der Verhältnismässigkeit mit anonymisierten Daten erfolgen. Folglich müssen die Personendaten nach Abschluss der Anfrage gelöscht werden. Dies ergibt sich bereits aus der erwähnten Gesetzesbestimmung, wurde aber auch in den AGB festgelegt (siehe Ziffer 77) 102. Folglich wurde durch die Nichtlöschung der 3rd Level Arbeiten der Grundsatz der Zweckbindung sowie die Vertragspflicht durch Xplain verletzt. Das BAZG bleibt jedoch für diese Verletzung gestützt auf Art. 16 Abs. 1

aDSG verantwortlich. 4.5. Daten für Anwendungsentwicklung 103. Je nach Informationssystem können auch produktive Daten in der Integrationsumgebung vorhanden sein (siehe Ziffer 38). 104. Für die Entwicklung sind keine produktiven Daten erforderlich, weshalb bei der nicht stringenten Trennung von Test- und Produktivdaten der Verhältnismässigkeitsgrundsatz verletzt wird. 4.6. IT-Infrastruktur von BAZG 105. Dem EDÖB liegen keine Anhaltspunkte vor, dass die IT-Infrastruktur im Rahmen des Ransomware- Vorfalls die Datensicherheit oder andere Anforderungen des DSG nicht erfüllt hätte, weshalb dies nicht Gegenstand der Untersuchung bildet. 4.7. Reaktionen von BAZG auf Ransomware-Vorfall 4.7.1. Information an Dritte 106. Im aDSG bestand keine ausdrückliche Bestimmung betreffend Meldung von Verletzungen der Da- tensicherheit, im Gegensatz zu Art. 24 DSG. Weil das BAZG den EDÖB über den Ransomware- Vorfall informiert hat, kann offenbleiben, ob sich eine solche Meldepflicht nach Treu und Glauben und der allgemeinen Informationspflicht ergeben hätte. 107. Nach dem Ransomware-Vorfall hat das BAZG involvierte Stellen und betroffene Personen informiert und ein Kontaktformular für Rückfragen auf der Webseite publiziert (siehe Ziffer 49). Mit diesen Massnahmen hat das BAZG seine Informationspflichten nach Treu und Glauben wahrgenommen. 4.7.2. Technische und organisatorische Massnahmen 108. Gemäss Art. 4 Abs. 1 aDSG hat die Bearbeitung von Personendaten nach Treu und Glauben zu erfolgen. Werden nach einem Vorfall dem Verantwortlichen Mängel in der Datensicherheit bekannt, sind diese Mängel nach Treu und Glauben und in Erfüllung der Datensicherheit (Art. 7 aDSG),

sofern zumutbar, so schnell wie möglich zu korrigieren. Das heisst notwendige technische und or- ganisatorische Massnahmen zur Behebung oder Vermeidung weiterer möglicher Persönlichkeits- verletzungen sind schnellstmöglich umzusetzen. 109. Zur Bewältigung des Ransomware-Vorfalls bei Xplain hat das BAZG das NCSC und fedpol kontak- tiert und die Aufarbeitung koordiniert. Die Zusammenarbeit und Koordination mit anderen involvierten Stellen, insbesondere mit Xplain, dem NCSC und dem fedpol erfolgte, soweit der EDÖB dies beurteilen kann, professionell und zielgerichtet. Infolgedessen wurden zahlreiche technische und organisatorische Massnahmen umgesetzt (siehe Ziffer 51 ff.) 110. Durch die Einleitung der erwähnten Massnahmen wurde der Vorfall durch das BAZG gewissenhaft aufgearbeitet. 4.8. Abschliessende Bemerkungen 111. Die auf dem Fileserver von Xplain gespeicherten Daten bzw. die im Darknet publizierten Daten stammen zu einem Grossenteil aus Log-Files der Anwendung eneXs-mobile und eneX-stationär. Die Anwendungen eneXs-stationär und eneXs-mobile wurde von verschiedenen Bundesbehörden und insbesondere auch von zahlreichen kantonalen Polizeibehörden verwendet. Die Anwendungen ermöglichen die Abfrage auf zahlreiche Datenbanken, die vom BAZG aber insbesondere auch von anderen Behörden geführt werden. Die Anwendungen von eneXs wurde zwar vom BAZG bei Xplain in Auftrag gegeben, die Anwendungen wurden aber von anderen Bundes- und Kantonsbehörden auch verwendet. 112. Der EDÖB stellte fest, dass ein anderes Bundesamt die offensichtlich datenschutzwidrige Support- funktion der Standardanwendung (wie in ORMA) im Jahr 2020 feststellte und Xplain mitteilte. Spä- testens zu diesem Zeitpunkt hätte Xplain bzw. die Bundesverwaltung das Risikopotential bei der Übermittlung von Personendaten im Rahmen des 3rd Level Supports erkennen und entsprechende Massnahmen für die gesamte Bundesverwaltung umsetzen müssen, etwa die Löschung aller pro- duktiven Daten bei

Xplain oder die Sicherung der Daten durch angemessene organisatorische und technische Massnahmen.

21/27

5. Empfehlungen 113. Gestützt auf Art. 29 Abs. 3 aDSG erlässt der EDÖB gegenüber dem BAZG die nachfolgenden Emp- fehlungen. 114. Die Auftragsdatenbearbeitung wurde nicht klar geregelt. Die datenschutzrechtlichen Risiken in der Zusammenarbeit mit Xplain werden erheblich minimiert, indem sich die Parteien die Datenübertra- gungen bewusst machen, ob bzw. unter welchen Voraussetzungen Personendaten die IKT-Sys- teme des Bundes verlassen dürfen (siehe insb. Ziffer 70, 74 f., 80). In diesem Sinne ist die Auftrags- datenbearbeitung zu konkretisieren. Empfehlungen:

115. Bei der Entscheidung zur weiteren Zusammenarbeit im Bereich der inneren Sicherheit sind daten- schutzrechtliche Kriterien zu berücksichtigen (siehe Ziffer 84). Die datenschutzrechtlichen Prozesse und deren Einhaltung sind regelmässig zu kontrollieren (siehe Ziffer 90 f.) Empfehlungen:

1. Unter Beachtung datenschutzrechtlicher Risiken wird geprüft, ob bzw. unter welchen Voraussetzungen es erforderlich ist, dass Personendaten im Rahmen von Support- prozessen die IKT-Systeme des Bundes verlassen und in den IKT-Systemen von Xplain gespeichert werden müssen.

1a) Ist es nicht erforderlich, dass im Rahmen von Supportprozessen Personen- daten die IKT-Systeme des Bundes verlassen und in den IKT-Systemen von Xplain gespeichert werden, sind die dazu notwendigen technischen und or- ganisatorischen Massnahmen zu bestimmen.

1b) Ist es erforderlich, dass im Rahmen von Supportprozessen vereinzelt Perso- nendaten die IKT-Systeme des Bundes verlassen und in den IKT-Systemen von Xplain gespeichert werden, sind die dazu notwendigen technischen und organisatorischen Massnahmen zu bestimmen. Dabei sind insbesondere die Grundsätze der Datenminimierung und Datensicherheit konsequent umzu- setzen. 2. Die Datenübertragungen gemäss vorangehender Ziffer sind in klaren vertraglichen Vereinbarungen festzuhalten.

3. Bei der nächsten Entscheidung zur weiteren Zusammenarbeit wird kontrolliert, ob ein Informationssicherheitsmanagement (ISMS) besteht und ob das ISMS mit einer Zertifizierung nach einem internationalen Standard nachgewiesen werden kann. 4. Die datenschutzrechtlichen Prozesse und deren Einhaltung werden regelmässig kontrolliert, indem interne oder externe Kontrollen durchgeführt werden oder ein Nachweis zur Einhaltung eingefordert wird.

22/27

116. In Bezug auf den Support und Wartung (siehe Ziffer 94 ff). Empfehlung:

5. Die Mitarbeitenden werden kontinuierlich auf die datenschutzrechtlichen Risiken sensibilisiert.

6. Die Verträge werden im Bereich Datensicherheit präzisiert und wo notwendig ver- einheitlicht.

23/27

6. Verfahren 6.1. Rechtliches Gehör und weiteres Vorgehen 117. Dem BAZG wurde die Möglichkeit gegeben, den Sachverhalt zu prüfen und dazu Stellung zu neh- men. Mit Schreiben vom 22. März 2024 hat das BAZG davon Gebrauch gemacht. 118. Der vorliegende Schlussbericht weist aufgrund des Sachverhalts einen engen Zusammenhang zu den beiden Schlussberichten des EDÖB in Bezug auf das fedpol und Xplain auf. Der EDÖB hat sich deshalb entschieden, die drei Schlussberichte und Empfehlungen den drei Parteien gleichzeitig und mit der gleichen Rechtsbelehrung zu eröffnen. 119. Dem BAZG wird eine Frist von 30 Tagen ab Erhalt des Schlussberichts angesetzt, um sich darüber zu äussern, ob sie die Empfehlungen gemäss vorangehender Ziffer 113 ff. annehmen oder ableh- nen. 6.2. Veröffentlichung des Schlussberichts mit Empfehlungen 120. In Fällen von allgemeinem Interesse kann der EDÖB die Öffentlichkeit über seine Feststellungen und Empfehlungen informieren (Art. 30 Abs. 2 aDSG). Der Ransomware-Vorfall vom Mai 2023 hat ein breites öffentliches Interesse gefunden. Die Information über die Ursachen der widerrechtlichen Publikation von besonders schützenswerten Personendaten im Darknet und die getroffenen und zu treffenden Massnahmen und die entsprechenden Empfehlungen des EDÖB sind von allgemeinem Interesse, da sowohl die öffentliche Verwaltung als auch ein privates Unternehmen betroffen sind. Aus datenschutzrechtlicher Sicht ist diese Konstellation mit besonderen Risken verbunden, denen das Datenschutzgesetz auch eine spezifische Aufmerksamkeit schenkt. Der Schlussbericht und die Empfehlungen des EDÖB im vorliegenden Zusammenhang sind deshalb auch aus diesem Grund von allgemeinem Interesse. 121. Der Schlussbericht vom BAZG wird deshalb zusammen mit den Schlussberichten vom fedpol und Xplain auf der Webseite des EDÖB veröffentlicht (www.edoeb.admin.ch). 122. Dem BAZG wurde die Gelegenheit gegeben, Schwärzungen des Sachverhalts zu beantragen, um eigene Interessen zu schützen. Mit Eingabe vom 12. April 2024 teilte das BAZG mit, dass keine Schwärzungen beantragt werden.

die stellvertretende Beauftragte: der zuständige Jurist:

Florence Henguely

Nicolas Winkelmann

der zuständige Informations- und Sicherheitsspezialist:

der beigezogene Experte: Michael Burger Bruno Baeriswyl