

Schlussbericht und Empfehlungen

vom 25. April 2024

des

Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)

in Sachen fedpol

aufgrund Ransomware-Vorfall

gemäss

Artikel 27 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (aDSG) in Verbindung mit Artikel 70 Bundesgesetz vom 25. September 2020 über den Datenschutz (DSG)



Inhaltsverzeichnis

_	ingslage	1
	ınlass	
	Chronologie der wesentlichen Verfahrensschritte	
1.3. L	Jmfang der Sachverhaltsabklärung	<i>^</i>
2. Sachv	erhalt	2
2.1. E	inleitung	2
2.2. I	T- Infrastruktur von Xplain	2
	Personendaten auf dem Fileserver von Xplain	
2.4. X	(plain als Dienstleister von fedpol	6
2.4.1.	Bearbeitung von Fehlerbehebungen durch Xplain im Allgemeinen	6
2.4.1.1	Datenübertragungen durch eneXs-mobile	7
2.4.1.2	2. Datenübertragung durch ORMA	8
2.4.2.	Datenübertragung im Projekt HOOGAN	9
2.4.3.	Daten für die Anwendungsentwicklung	9
2.5. D	Oatenübertragungen aus Sicht Xplain	9
2.6. V	ertragssituation zwischen fedpol und Xplain	
2.6.1.	eneXs-mobile	
2.6.2.	ORMA	
2.6.3.	Projekt Zugriff HOOGAN-Datenbank für Zutrittskontrolle in Stadion	
2.7. F	Personensicherheitsüberprüfung	10
	Ransomware-Vorfall auf Xplain	
2.9. F	Reaktionen von fedpol auf Ransomware- Vorfall	1′
2.9.1.	Information an Dritte	
2.9.2.	Umgesetzte technische und organisatorische Massnahmen	
2.10. V	Veitere betroffene Bundesämter	13
3. Stellui	ngnahme zum Sachverhalt	14
o. Otoma		
	schutzrechtliche Beurteilung	
	/orbemerkungen	
	/ertragliche Vereinbarungen mit Xplain	
	Oatenübertragung durch eneXs-mobile	
4.3.1.	3	
	Vereinbarung oder Gesetz	
4.3.1.2	3 3	
4.3.1.3	1 31	
4.3.1.4		
4.3.2.	Gewährleistung der Datensicherheit	
4.3.2.1		
4.3.2.2	_	
4.3.2.3	•	
4.3.2.4		
	Datenübertragung durch ORMA	
4.4.1.	Auslagerung	
4.4.1.1	3	
4.4.1.2	5 5	
4.4.1.3	1 - 31	
4.4.1.4		
4.4.2.	Gewährleistung der Datensicherheit	
	Support- und Wartungsprozesse	
4.5.1.	eneXs-mobile	



	Verhältnismässigkeit
4.5.1.2.	Datensicherheit
4.5.1.3.	Zweckbindung
4.5.2.	ORMA
4.6. Da	tenübertragung durch ein HOOGAN-Zugriffs Projekt27
4.7. Da	ten für die Anwendungsentwicklung27
4.8. IT-	nfrastruktur von fedpol
4.9. Re	aktionen von fedpol auf Ransomware-Vorfall28
4.9.1.	Information an Dritte
4.9.2.	Technische und organisatorische Massnahmen
4.10. Ab:	schliessende Bemerkungen
5. Empfeh	ungen
6. Verfahre	en
	chtliches Gehör und weiteres Vorgehen
	öffentlichung des Schlussberichts mit Empfehlungen
7. Anhang	4. Wish Costs Delawarets
1. Alliany	1: Wichtigste Dokumente
_	1: Wichtigste Dokumente
_	•
_	•
8. Anhang	2: Glossar
8. Anhang	•
8. Anhang Abbildung	2: Glossar
8. Anhang Abbildung Abbildung 1	2: Glossar
8. Anhang Abbildung Abbildung 1	2: Glossar
8. Anhang Abbildung Abbildung 1 Abbildung 2	2: Glossar
8. Anhang Abbildung Abbildung 1	2: Glossar
Abbildung Abbildung 1 Abbildung 2 Tabellenve	2: Glossar
Abbildung Abbildung 1 Abbildung 2 Tabellenve	2: Glossar
Abbildung Abbildung 1 Abbildung 2 Tabellenve	2: Glossar



1. Ausgangslage

1.1. Anlass

- Im Mai 2023 ereignete sich ein Ransomware-Vorfall auf das Unternehmen Xplain AG (nachfolgend: Xplain). Xplain ist ein Informatik-Dienstleister verschiedener Bundesorgane und Kantone im Bereich der öffentlichen Sicherheit. Der Vorfall hat zum Abfluss erheblicher Datenmengen geführt, die auf den Systemen von Xplain gespeichert waren. Die Daten wurden in der Folge in Tranchen im Darknet veröffentlicht: Am 1. Juni 2023 wurde eine erste Tranche von 5 GB veröffentlicht, am 14. Juni 2023 folgte eine zweite Tranche von ca. 424 GB, welche auch die zuvor publizierte Tranche umfasste. Betroffen davon waren auch personenbezogene und damit datenschutzrelevante Daten.
- Am 6. Juni 2023 erfolgte eine telefonische und am 16. Juni 2023 eine schriftliche Meldung der Datenschutzverletzung durch das Bundesamt für Polizei fedpol (nachfolgend: fedpol) an den EDÖB. Am 20. Juni 2023 hat der EDÖB eine Sachverhaltsabklärung gegen fedpol eröffnet.
- ^{3.} Parallel eröffnete der EDÖB auch Sachverhaltsabklärungen gegen das Bundesamt für Zoll und Grenzsicherheit BAZG (nachfolgend: BAZG) sowie gegen das Unternehmen Xplain AG.

1.2. Chronologie der wesentlichen Verfahrensschritte

4. Nachfolgend werden die wesentlichen Verfahrensschritte aufgeführt:

06.06.2023	Telefonische Information über den Vorfall der Datensicherheitsverletzung.
16.06.2023	Meldung Datenschutzverletzung via Meldeportal.
20.06.2023	Eröffnung formelle Untersuchung.
04.08.2023	Zustellung Fragenkatalog an fedpol.
28.09.2023	Erhalt Antworten Fragenkataloges.
08.01.2024	Beantragung weitere Akten und Auskünfte.
29.01.2024	Erhalt weitere Rückmeldung Akten und Auskünfte.
31.01.2024	Besprechung mit fedpol zur Klärung des Sachverhalts.
08.03.2024	Sachverhaltsfeststellung an fedpol.
22.03.2024	Erhalt Stellungnahme Sachverhaltsfeststellung.
04.04.2024	Sachverhaltsfeststellung an fedpol zur Beantragung von Schwärzungen.

1.3. Umfang der Sachverhaltsabklärung

- Mit dieser Sachverhaltsabklärung prüft der EDÖB einerseits, ob die Datenbearbeitungen vom fedpol bei der Zusammenarbeit mit Xplain den Anforderungen des Datenschutzgesetzes (DSG) genügen, und andererseits gibt er bei der Feststellung von Mängeln Empfehlungen ab. Im Fokus stehen die Datenbearbeitungen vom fedpol im Zusammenhang mit Xplain zum Zeitpunkt des Ransomware-Vorfalls. Dabei werden die Datenbearbeitungen des fedpol durch die Anwendungen eneXs-mobile und ORMA sowie in Bezug auf ein Zugriffsprojekt auf die Datenbank HOOGAN durch ein Stadion näher geprüft.
- Die Sachverhaltsabklärungen gegen das BAZG und fedpol zur Frage der Rechtmässigkeit von Zugriffen von Mitarbeitenden des BAZG auf das von fedpol betriebene Fahndungsregister RIPOL wurden von den Verfahren betreffend Xplain getrennt und bis zu deren Abschlüsse sistiert.



2. Sachverhalt

2.1. Einleitung

- 7. Xplain ist ein privates Unternehmen (AG) mit Sitz in Interlaken und zwei Entwicklungspartnerschaften mit Niederlassungen in Deutschland und Spanien im Besitz von zwei Verwaltungsräten der Xplain und je einen Mitarbeitenden. Zusammen mit den Niederlassungen beschäftigt das Unternehmen rund 70 Mitarbeitende.
- 8. Gemäss eigener Beschreibung ist das Unternehmen seit der Gründung im Jahr 2000 fast ausschliesslich als Lieferantin von Standard-Software für die Innere Sicherheit tätig und arbeitet für Behörden und Organisationen mit Sicherheits-, Migrations-, Strafverfolgungs- und Strafvollzugsaufgaben. Für diese Behörden und Organisationen bietet Xplain «innovative-Softwareprodukte mit einer 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 sowie 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».
- Das fedpol hat Xplain f
 ür mehrere IT-Projekte beauftragt.

2.2. IT- Infrastruktur von Xplain

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



Auf den von AG bereitgestellten Systemen befanden sich im Mai 2023 Referenzinstallationen, Entwicklungsserver, Testserver sowie einige Administrations- und Build-Umgebungen von Xplain. Abbildung 1 illustriert den allgemeinen Systemaufbau und gibt einen Überblick zu den Verbindungen zwischen AG und Xplain.



Abbildung 1: Überblick zum allgemeinen Systemaufbau von Xplain.

- 12. Der Systemaufbau basiert auf einem VPN-Netzwerk, über welches die verschiedenen Standorte miteinander verbunden waren. Remote Arbeitsplätze ihrerseits waren mit einer P2S-VPN-Verbindung via Office-Firewalls verbunden. Alle Daten von Kundenprojekten befanden sich auf Infrastrukturen in der Schweiz vorwiegend auf Servern in Interlaken. Am Standort Interlaken wurden die File-Server mit den Daten und Dokumenten betrieben und verschiedene Server der Build-Pipeline sowie das NAS für Backups. An den Standorten in Spanien (Madrid und Ciudad Real) waren gemäss Xplain keine «relevanten» Daten der Xplain und deren Kunden abgelegt. Der EDÖB geht davon aus, dass mit relevanten Daten Personendaten im Sinne des DSG verstanden werden.
- 13. Entsprechend den Informationen, die der EDÖB erhalten hat, verfügte der betroffene Fileserver im Mai 2023 nicht über den aktuellen Patchlevel und wies zudem unnötig geöffnete Ports auf. Im Weiteren lief auf dem Server kein aktives Monitoring, was u. a. dazu beigetragen hat, dass ungewöhnliche Aktivitäten oder Anomalien nicht zeitnah identifiziert werden konnten.



2.3. Personendaten auf dem Fileserver von Xplain

- Fedpol hat eine Analyse der im Darknet publizierten Daten durchgeführt, welche sich auf von fedpol bearbeitete Daten bezog. Folglich betrifft die Analyse von fedpol nur einen Teil der im Darknet publizierten Daten. Diese Daten waren auf dem Fileserver von Xplain gespeichert.
- Das fedpol hat dem EDÖB am 29.01.2024, in Form von zusätzlichen Unterlagen und Auskünften, eine ausführliche Beschreibung ihrer eigenen Datenanalyse zur Verfügung gestellt. Darin wird unter anderem erläutert, wie mittels einer Analyse der Hashwerte ermittelt werden konnte, dass sämtliche Daten des fünf GB grossen «PARTIAL DUMP» im «FULL DUMP» (907 GB resp. 600 GB; Zahl wurde im Februar 2024 von 907 auf 600 geändert) enthalten sind. Demnach wurden die Daten im Darknet in der Form von 646 komprimierten Dateien des Typs .RAR veröffentlicht. Nach deren Veröffentlichung stellte Xplain am 07.06.2023 fedpol weitere 70 GB Daten als sogenannte «XPLAIN EDITION» zur Verfügung. Demzufolge handelt es sich um Backups der gestohlenen Daten, deren Erstellungsdatum Xplain allerdings nicht kommuniziert habe. Der Vergleich des PARTIAL DUMPS mit dem FULL DUMP offenbarte, dass Daten mit einem eindeutigen fedpol-Bezug demnach nur teilweise im Darknet publiziert wurden. Anhand des Abgleichs des eindeutigen Hash- Wertes von jeder Datei der 70 GB Daten von der «XPLAIN EDITION» zum veröffentlichten Datensatz im Darknet konnte fedpol feststellen, dass 39% (52'368 Files) der fedpol Daten veröffentlicht wurden. Daraus zieht fedpol für sich den Schluss, dass PLAY die übrigen Daten mit fedpol-Bezug nicht «gestohlen» oder zumindest nicht veröffentlicht hat. Bei der Analyse der Ordnerstruktur von Xplain zeigte sich ausserdem, dass zwar aus jedem Verzeichnis Daten veröffentlicht wurden, aber jeweils nicht der gesamte Inhalt daraus. Die gefundenen 646 .RAR-Archive wurden durch fedpol extrahiert und wiederum in 52 Stammordner aufgeteilt. Daraus wurden 19'816 Unterordner und 147'546 Dateien ermittelt, mit einer Gesamtgrösse von 395 GB. Zwei dieser Dateien sind sogenannte «.tibx-Dateien», mit einer Gesamtgrösse von 242 GB. Hierbei referenziert fedpol auf Xplain, welche angibt, dass es sich dabei um Images von Windows-Servern ohne Kundendaten handelt. Die verbleibenden 147'544 Dateien haben ein Datenvolumen von 153 GB. Einige Dateien sind weitere Archivdateien bzw. komprimierte Dateien (bspw. .ZIP). Diese wurden beim Import in die, durch fedpol, genutzte Forensik-Software entpackt. Daraus resultierten ungefähr 3.9 Mio. Dateien aus dem FULL DUMP.
- offengelegt wurden. Im weiteren Verlauf flossen Personendaten aus ORMA mitsamt den allozierten Strafdaten aus dem Jahr 2018 an die Hackergruppe PLAY. Ebenso sind Täterpersonalien mit terroristischem Hintergrund, als auch ORMA-Interpolmeldungen zu Verbrechen im Zusammenhang mit Terrorismus aus dem Jahr 2020 betroffen. Weiter wurden Personendaten einer PAX (Interpol) sowie Suchergebnisse aus RIPOL mit sensiblen Daten geleakt.
- 17. Bei den geleakten Dokumenten wurden viele Logs von eneXs gefunden mitsamt einer gewissen Menge an Personendaten pro einzelnem Log. Mit der Anwendung eneXs-mobile kann fedpol Abfragen durchführen von RIPOL, SIS, HOOGAN, C-VIS, ISA, ISR, ZEMIS, AS (INTERPOL), FABER, MOFIS und ORBIS. Die stichprobeweise Prüfung der Logs zeigten im Ergebnis einerseits produktive Klardaten und andererseits teilweise anonymisierte Daten. In der von fedpol durchgeführten Analyse wurden Personendaten von RIPOL, SIS, INTERPOL und ISA gefunden.
- Ein zusätzlicher Abfluss von Personendaten wurde aus der HOOGAN-Datenbank, mit Personendaten aus einer Liste vom 02. September 2015 eruiert. Auf der geleakten Liste waren total 766 Personen aufgelistet, welche alle von fedpol per Brief informiert wurden. Von den 766 Personen waren 690 am 07. Juli 2023 nicht mehr in HOOGAN registriert, 76 waren am 07. Juli 2023 noch in HOOGAN registriert.
- ^{19.} Die vorgängig beschriebenen Daten wurden in verschiedenen Formaten im Darknet publiziert. Eine grosse Mehrheit wurde in BASE64 codiert. Bspw. sind das Scans von Pässen mitsamt Passbildern



- und den dazu gehörenden Unterschriften, Interpol Alert-Listen mit Namen von international gesuchten Personen, Tatortbilder etc., abgeflossen.
- 20. In der Folge wurden diverse technische Logfiles von eneXs in dem 900 GB Leak mit operativen Daten gefunden. Aus diesen Logfiles konnten in der Folge u. a. datenschutzrelevante Daten extrahiert werden, welche teilweise auch besonders schützenswerte Personendaten enthalten, unterschiedliche Zeitspannen abdecken und wiederum aus verschiedenen Quellsystemen wie bspw. ISA, ZEMIS, RIPOL, HOOGAN, INTERPOL etc. stammten. Alle betroffene Personen wurden gemäss den Vorgaben des DSG persönlich angeschrieben und über den Vorfall informiert.
- ^{21.} Die Quellsysteme sind nachfolgend aufgeführt.

System	Verantwortliche Behörde	Beschreibung
ASF (Interpol)	fedpol	Fahndungssystem von Interpol für Personen und Sachen.
SIS	fedpol	Schengen-Informationssystem zu Schengen- Fahndungen für Personen und Sachen.
C-VIS	SEM	Schengen-Visa-System
RIPOL	fedpol	Nationales automatisiertes Fahndungssystem.
ZEMIS	SEM	Zentrales Migrationssystem.
ORBIS	SEM	Nationaler Teil des Visa-Systems.
HOOGAN	fedpol	System zur Verwaltung von Hooliganismus und Massnahmen.
ISR	SEM	Informationssystem zur Verwaltung von Reisedokumenten für ausländische Personen.
ISA	fedpol	System zur Ausstellung und Verwaltung der Schweizer Reisepässe.
MOFIS	ASTRA	Automatisiertes Motorfahrzeug-Informations- system.
RUMACA	BAZG	Rapportierungssystem des BAZG.
FABER	ASTRA	Informationssystem für Führerzulassungen.

Tabelle 1: Quellsysteme



23. Analyseerkenntnisse des fedpol betreffend das Architekturdesign hinsichtlich des Error-Handlings zeigen weiter, dass bei ORMA jeweils Fehlerreporte durch die Erstellung von Print-Screens aller offenen Anwendungen generiert wurden. Weiter enthielten die Log-Files der Anwendung eneXs neben den Anfragen auch die Resultate der Produktivsysteme.



^{24.} Aufgrund der Datenanalyse kommt fedpol zum Schluss, dass die Hackergruppe PLAY Daten der administrativen Ablage von Xplain entwendet hat. Dabei handelt es sich um Daten organisatorischer Art wie bspw. Offerten, Rechnungen, Verträge, Stundenrapporte, aber auch projektbezogene Unterlagen wie Konzepte, Projekt- und Phasendokumente, Testdaten sowie technische Dokumentationen. Im Weiteren um supportbezogene Unterlagen mit teilweise produktiv-operativen Datensätzen, wie bspw. Printscreens, Logfiles, etc.

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

2.4. Xplain als Dienstleister von fedpol

- Die Zusammenarbeit von fedpol mit Xplain besteht aus IT-Projektbegleitung, Softwareentwicklung und -Weiterentwicklung sowie der Wartung und dem Support der von Xplain an fedpol gelieferten Anwendungen ORMA, und eneXs-mobile. Die von fedpol genutzten Anwendungen selbst werden beim bundesinternen Leistungserbringer ISC-EJPD betrieben. Ausnahmen bilden die Anwendungen eneXs-mobile und erfolgte durch das BIT im Auftrag des BAZG, und ist eine lokale Anwendung.
- Die Datenbearbeitungen in diesem Zusammenhang werden in Bezug auf eneXs-mobile und ORMA geprüft. Auch wird der Einzelfall der HOOGAN-Daten analysiert.

2.4.1. Bearbeitung von Fehlerbehebungen durch Xplain im Allgemeinen

- 28. Gemäss Angaben von fedpol hätten Mitarbeitende von Xplain zu keinem Zeitpunkt Zugriff auf die Serverinfrastruktur beim ISC-EJPD. Der Programmcode für diese Anwendungen sei durch Xplain bereitgestellt und durch das ISC-EJPD auf deren Umgebung implementiert worden.
- ^{29.} 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.
- 30. Sowohl bei eneXs-mobile als auch bei ORMA erfolgt der 1st und 2nd Level Support beim EJPD, der 3rd Level Support bei Xplain.
- 31. Aufgrund von Ressourcenknappheit im internen 2nd Level Support bei fedpol hat Xplain den 2nd Level Support personell unterstützt. Dazu nahmen drei Personen von Xplain für fedpol Aufgaben in den Bereichen Betrieb, Wartung, Support und Weiterentwicklung wahr. Diese Arbeiten von Xplain erfolgten über die Infrastruktur von fedpol und auf von fedpol zur Verfügung gestellten dedizierten Endgeräten, gemäss dem Berechtigungs- und Zugriffskonzept von fedpol. Die Personen verfügten jeweils über ein fedpol Notebook mitsamt einem so genannten X-Account für externe Dienstleister. Damit verbunden verfügten diese Mitarbeitende über eine fedpol-Mailbox, über welche E-Mails mit anderen fedpol Mitarbeitenden über die Bundesinfrastruktur ausgetauscht werden konnten. Damit war auch eine Verschlüsselung sensibler Inhalte möglich. Weiter verfügten diese drei

_

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



Mitarbeitenden auf der Produktions- und der Integrationsumgebung über einen Zugang zum Single Sign on Portal (SSO-Portal) des ISC-EJPD und zur Anwendung ORMA.

- 32. Xplain erfüllte für fedpol den 3rd Level Support für die Anwendungen ORMA, und und Für die Erfüllung des 3rd Level Supports muss ein Fehler in der Software nicht auf Applikationsebene vorliegen. Der ordentliche Ablauf gestaltete sich wie folgt: das Problem wurde, wenn möglich, auf der Testumgebung der Bundesstellen durch den dort zuständigen Mitarbeitenden nachgespielt. Darauf gestützt wurde durch den Anwendungsverantwortlichen (AV) bei fedpol die Fehlermeldung erstellt, die dieser anschliessend per E-Mail an support@xplain.ch und im Fall von ORMA per JIRA oder einen Sharepoint an Xplain übermittelte.
- Innerhalb ihrer eigenen IT-Infrastruktur betreibt Xplain eine Instanz der Software JIRA. JIRA wird von Xplain als Ticketingsystem genutzt. Aus dem Bereich «PSI-POLS Betrieb und Support» haben fedpol Mitarbeitende Zugriff auf JIRA und können selbst Support-Tickets erstellen und bearbeiten. Der Austausch von schriftlichen Informationen erfolgt mehrheitlich per E-Mail. Hiermit werden Informationen zu Projekten, dem Betrieb und Support sowie der Weiterentwicklung ausgetauscht.

34.

2.4.1.1. Datenübertragungen durch eneXs-mobile

- 35. Im Rahmen des Programms FMÜ «Ausbau und Betrieb des Verarbeitungssystems zur Fernmeldeüberwachung sowie der polizeilichen Informationssysteme des Bundes» setzte fedpol im Projekt IKT-ProgFMÜ-P4-EFMÜ (P4-EFMÜ) die «Kompatibilitätsanpassungen der Systeme von fedpol» um. Im Teilprojekt «zentrale Abfragen» wurde die Notwendigkeit einer mobilen App für fedpol zur Abfrage auf polizeiliche Datenbanken bekräftigt und durch die Direktion fedpol der Auftrag erteilt, eine solche App für das ganze fedpol zu beschaffen. Der Benutzerin und dem Benutzer sollte ermöglicht werden, Abfragen ab einem Smartphone zu Personen, Fahrzeugen, Sachen und Dokumenten auf Informationssystemen wie RIPOL, SIS, ZEMIS, Mofis usw. durchführen zu können. Der Aufbau des Einsatzes eneXs-mobile als App für das fedpol erfolgte über die aufgebauten Infrastrukturen des Grenzwachtkorps EZV (heute BAZG), welches die App bereits im produktiven Einsatz hatte. Die eneXs-mobile App entsprach derjenigen der aktuellen App des GWK und bot im Zeitpunkt der Einführung den folgenden Funktionsumfang:
 - Einmalabfragen von Personen, Dokumenten, Sachen, Fahrzeugen und Nummernschildern aus manuellen Suchmasken über den eneXs Server;
 - Fotografieren der MRZ von Identifikation- und Reisedokumenten und Übernahme der Abfrageparameter in die Abfragemaske;
 - Fotografieren des Nummernschilds und Übernahme der Abfrageparameter in die Fahrzeugmaske.
- Die Software eneXs-mobile ist eine Anwendung, mit der Dokumente eingelesen und Fahndungsabfragen durchgeführt werden können. Weiter werden die daran angeschlossenen Geräte wie bspw. Passleser, Fingerabdruckscanner, Kamera etc. gesteuert. Die Software eneXs selbst enthält keine Datenbank, jedoch wird ein Teil der biometrischen Indikatoren und Prozess-Daten für eine begrenzte Zeit, für Kontrollprozesse, zwischengespeichert und darauf automatisch gelöscht.
- 37. Genutzt werden kann eneXs sowohl von FAT-Clients aus der Virtual Desktop Infrastructure (VDI) sowie von mobilen Geräten. Dabei ermöglicht 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 unterliegt 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.
- Wie bei der Verwendung von Software üblich, können auch bei eneXs Fehler auftreten. Denkbare Fehlerarten beziehen sich dabei insbesondere auf die elektronische Dokumentenüberprüfung, fehlende, unvollständige Treffer oder False Positives. In der Folge kann dieses Verhalten zu fehlerhaften 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 Screenshots oder Fehler-Reports erstellt. Diese werden durch das fedpol in der Folge manuell an Xplain geschickt. Xplain analysiert daraufhin die generierten Reports auf Ihrer Infrastruktur mit dem Ziel zur Fehlerbehebung.
- Für die Anwendung eneXs-mobile wird das LogFile gesichert, das anschliessend per E-Mail an die eigene fedpol-E-Mail-Adresse des fedpol-Mitarbeitenden geschickt wird. Danach sendet der fedpol-Mitarbeitende das LogFile an das interne 2nd- Level Supportteam des fedpol. Das fedpol Supportteam sichtet seinerseits den Fehler, u.a. auch zum Sicherstellen, dass gleiche Fehler nicht mehrfach an Xplain gemeldet werden. Fehler, welche durch das fedpol-Supportteam im Rahmen des 2nd Level Supports gelöst werden können, werden fedpol intern erledigt und nicht an Xplain gesendet. Handelt es sich jedoch um einen systembedingten Fehler, wird der Fehlerbericht nach vorheriger Rücksprache mit Xplain auf dem sogenannten T-Laufwerk, einem zentralen Fileshare der Bundesverwaltung, abgelegt.
- Im Anschluss erfolgt eine Vollzugsmeldung mittels E-Mail oder Telefon an Xplain, dass der angemeldete Fehlerbricht oder das Logfile zur Analyse auf dem T-Laufwerk bereit liegt. Damit Xplain auf das T-Laufwerk zugreifen kann, wird via BAB-Client-fedpol ein Remotezugriff ermöglicht. Daraufhin kann der Fehlerbericht von Xplain vom T-Laufwerk zwecks Analyse, auf ihre eigene Infrastruktur kopiert werden. Im Anschluss an den Kopiervorgang werden die auf dem T-Laufwerk des fedpol abgelegten Fehlerberichte dort von Xplain gelöscht.
- Die Software eneXs-mobile verfügt zudem seit der Einführung über eine Funktion, durch welche die Benutzerin oder der Benutzer aktiv eine Fehlermeldung inklusive Log-Dateien an einen FTP-Server versenden kann. Die Zugangsdaten zu dem FTP-Server waren im Programmcode fest (hard coded) hinterlegt. Die Verwendung dieser Funktion war und ist bei der Bundesverwaltung bzw. bei fedpol nicht möglich, weil die Netzwerke der Bundesverwaltung einen Versand auf einen externen FTP-Server nicht zulassen. Daher konnten bei fedpol keine Fehlermeldungen über einen FTP-Server an Xplain übermittelt werden.

2.4.1.2. Datenübertragung durch ORMA

- Die Anwendung ORMA verfügt ebenfalls über eine integrierte Supportfunktion, welche Fehlerberichte aufzeichnen und auch übermitteln kann. Dazu muss der Benutzer diese Funktion manuell einschalten. Danach werden durch die Supportfunktion die Inhalte aller momentan geöffneten Anwendungen aus dem Zwischenspeicher (Cache) abgegriffen. In der Folge wird daraus eine ZIP-Datei generiert, welche im Anschluss manuell zur Fehleranalyse an Xplain weitergeleitet wurde.
- ^{43.} Der Austausch von schriftlichen Informationen erfolgte mehrheitlich per E-Mail; für die Wartung und den Support für ORMA über JIRA; sowie einen Sharepoint nur für ORMA. Hiermit wurden Informationen zu Projekten, dem Betrieb und Support sowie der Weiterentwicklung ausgetauscht.
- ^{44.} Nach dem Ransomware-Vorfall im Mai 2023 war einer der zahlreichen IT-Sofortmassnahmen die Einstellung des in der vorangehenden Ziffer beschriebenen Prozesses.
- 45. Der in den vorangehenden Ziffern beschriebene Prozess wurde von einem ehemaligen Anwendungsverantwortlichen in einem anderen Bundesamt, dass die gleiche Anwendung von Xplain bezieht, im Jahr 2020 bemerkt. Daraufhin wurde bei Xplain vom Anwendungsverantwortlichen eine



Anforderung zur Behebung spezifiziert. Ab diesem Zeitpunkt wurden produktive Daten vor dem Weiterleiten aus den ErrorReport.zip-Dateien von Personen des entsprechenden Amts vor der Übermittlung an Xplain herausgelöscht.

2.4.2. Datenübertragung im Projekt HOOGAN

- Fedpol beauftragte im Jahr 2012 Xplain mit der Umsetzung einer Zutrittskontrolle durch Abgleiche mit den Einträgen in der HOOGAN-Datenbank für den Zutritt ins Stadion. Als bei der Zutrittskontrolle und dem Abgleich der HOOGAN-Datenbankeinträge Probleme auftraten, wurde Xplain mit der Fehlerbehebung beauftragt. In diesem Zusammenhang hat fedpol einen Auszug aus HOOGAN-Datenbank aus dem Jahr 2015 per E-Mail an einen Xplain Mitarbeitenden gesandt.
- Dieser Auszug wurde vom Xplain Mitarbeiter auf seinem persönlichen Laufwerk gespeichert, worauf nur er und Administratoren Zugriff hatten. Dieser Auszug wurde im Darknet veröffentlicht.

2.4.3. Daten für die Anwendungsentwicklung

^{48.} Bei fedpol stehen gemäss eigener Aussage für die Entwicklung und Wartung Testdaten des jeweils betroffenen Informationssystems zur Verfügung. In der Integrationsumgebung von fedpol waren somit nur Testdaten vorhanden.

2.5. Datenübertragungen aus Sicht Xplain

- ^{49.} Gemäss Xplain sind Personendaten aus der Bundesverwaltung wie folgt übermittelt worden:
 - Angaben im Rahmen von Projektdaten (z.B. Kontaktangaben, involvierte Mitarbeitende/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.

2.6. Vertragssituation zwischen fedpol und Xplain

- 50. Bei fedpol bestehen seit 2003 verschiedenen Anwendungen, die Xplain entwickelt, weiterentwickelt und für diese zusätzlich Wartungs- und Support Dienstleistungen erbringt. Es bestehen daher zahlreiche Verträge zwischen fedpol und Xplain. In der Regel 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 etwas über 100 Verträge zustande.
- ⁵¹ Die Verträge wurden auf Grundlage der Vorlagen des BBL erstellt.
- Da einzelne Dienstleistungsverträge mit Xplain bis ins Jahr 2003 zurückdatieren, stellte der EDÖB unter anderem die Frage, ob fedpol die Xplain-Dienstleistungen vorgängig jeweils einer datenschutzrechtlichen Beurteilung unterzogen hat. Darauf antwortete fedpol, dass man gemäss den IKT-Vorgaben des Bundes vorgegangen sei. Im Weiteren sei in den Verträgen ab Januar 2021 auch eine «Cyberklausel» enthalten. Bei der Zusammenarbeit mit Dritten hält fedpol zudem fest, die IKT-Vorgaben und -Weisungen der Bundesverwaltung einzuhalten.

2.6.1. eneXs-mobile

Die Anwendung eneXs-mobile ist seit 2020 in Betrieb. Fedpol hat mit Xplain einen Vertrag abgeschlossen betreffend die Erbringung von Informatikdienstleitungen im Zusammenhang mit der Aufschaltung von eneXs-mobile.² Neben dem Vertrag wurden die folgenden Dokumente als

² Vertrag für die Erbringung von Informatikdienstleistungen (Auftrag), 0316004366.



Vertragsbestandteile integriert: Verpflichtungserklärung pro Mitarbeitenden, die AGB für Informatikdienstleistungen des Bundes (Ausgabe 20. Oktober 2010) sowie das Angebot der Auftragnehmerin vom 22. März 2019. Der Vertrag wurde bis zum 31. Dezember 2022 abgeschlossen. Die Vertragsverlängerung bis Ende 2023 wurde Mitte 2023 gestoppt.

2.6.2. ORMA

- ORMA ist seit ca. 2004 in Betrieb. Fedpol hat mit Xplain mehrere Verträge abgeschlossen für die Wartung und Pflege sowie Weiterentwicklung der Anwendung ORMA, die im Zeitpunkt des Ransomware- vorfalls im Mai 2023 gültig waren:
 - Vertrag für die Erbringung von Informatikdienstleistungen (Auftrag),
 abgeschlossen für den Zeitraum vom 01. Januar 2015 bis 31. Dezember 2024.³
 - Vertrag für die Erbringung von Informatikdienstleistungen (Auftrag),
 Dienstleistungen ORMA 2018+, Zusatzaufwände 2023,
 abgeschlossen für den Zeitraum 01. Januar 2015 bis 31. Dezember 2023.⁴
 - Vertrag für die Erbringung von Informatikdienstleistungen (Auftrag),
 Dienstleistungen Clean ORMA Phase 2, 2023
 abgeschlossen für den Zeitraum vom 01. Januar 2015 bis 31. Dezember 2023.⁵

In den drei oben aufgeführten Verträgen sind weitere Dokumente als Vertragsbestandteile integriert, insbesondere AGB der Bundesverwaltung.

Für die Anwendung ORMA hat fedpol eine SCHUBAN⁶ und ein ISDS-Konzept⁷ erstellt, für eneXsmobile nicht. Zudem hat fedpol die Umsetzung des IKT-Grundschutzes für die Anwendung ORMA geprüft und in einem Dokument festgehalten.⁸

2.6.3. Projekt Zugriff HOOGAN-Datenbank für Zutrittskontrolle in Stadion

Fedpol hat mit Xplain einen Vertrag abgeschlossen betreffend «Dienstleistungen im Projekt HOO-GAN + Zutrittskontrolle, Pilot ».9

2.7. Personensicherheitsüberprüfung

^{57.} 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

58.	Die Angreit	fer der Hac	kergruppe	e PLAY ha	aben s	ich im Mai	2023 u	nbefug	t Zug	ang zu eine	m von der
	Firma	AG gehos	steten Se	rver versc	hafft u	nd sich mi	ttels «La	ateral M	/lover	nent» durch	das Netz-
	werk der 2	Xplain bew	egt. Die	Systeme	beim	externen	Hoster		AG	umfassten	einerseits

³ Referenz Nr.: 0316000091.

⁴ Referenz Nr.: 0316000091 / 500.

⁵ Referenz Nr.: 0316000091 / 520.

⁶ Schutzbedarfsanalyse (SCHUBAN) vom 29.08.2016.

⁷ Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) vom 03.12.2019.

⁸ Massnahmenumsetzung zum IKT- Grundschutz in der Bundesverwaltung, Version 2.0 vom 19. Dezember 2013 (Stand 01. März 2015).

⁹ Vertragsnummer: 40312071652.



- Entwicklungs- und Testserver sowie andererseits bestimmte Administrations- und Build-Umgebungen der Xplain.
- In der Folge hat sich die Hackergruppe durch das Netzwerk der Xplain vorgearbeitet. Vielfach dringen 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 Nutzdatenbestand von ca. 1.5 TB. Infolgedessen wurden gemäss Angreifer 907 GB Daten (wurde im Februar 2024 auf 600 GB geändert) abgezogen.
- 60. Der genaue Angriffsvektor konnte indes von den mit der Untersuchung beauftragten Sicherheitsfirmen nicht abschliessend ermittelt werden. Das ist u. a. dem Grund geschuldet, dass weder das Testsystem, aufgrund seiner Verschlüsselung noch weitere Datenquellen, wie bspw. eine zentrale Logverwaltung oder ein SIEM, für die Untersuchung zur Verfügung standen.

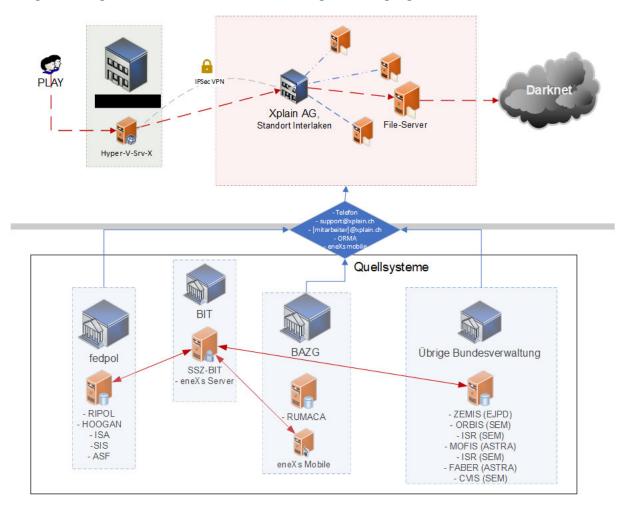


Abbildung 2: Vereinfachte Illustration des Hackervorfalls auf die Xplain AG. (Quelle: Eigene Grafik).

2.9. Reaktionen von fedpol auf Ransomware- Vorfall

2.9.1. Information an Dritte

61. Der EDÖB wurde erstmalig telefonisch durch die Direktorin fedpol am 06. Juni 2023 über den Ransomware-Vorfall informiert. Eine diesbezügliche Strafanzeige wurde am 12. Juni 2023 bei der Bundesanwaltschaft eingereicht. Am 16. Juni 2023 erfolgte die Meldung über den Vorfall über das Databreach-Portal des EDÖB.



- Wurden Personendaten mit einem internationalen Bezug im Darknet gefunden, wurden der betroffene Staat oder betroffene Stellen informiert. Dabei wurde sowohl über den aktuellen Kenntnisstand des Ransomware-Vorfalls informiert als auch über die konkret im Darknet publizierten Daten. In diesem Sinne wurden mit mehreren Schreiben sowohl Europol, INTERPOL und eu-LISA informiert.
- Falls Daten von anderen Behörden in den von fedpol analysierten Daten festgestellt wurden, hat fedpol diese umgehend darüber informiert. So wurden insbesondere verschiedene Kantonspolizeien, die Militärpolizei, das SEM, die Migrationsbehörde Aargau, verschiedene Gerichte, das Bundesamt für Justiz, die Bundesanwaltschaft sowie das BAZG informiert.
- 64. Ab dem 15. Juni 2023 informierte fedpol die Mitarbeitenden auf dem Intranet über den Vorfall. Die Aktualisierungen wurden jeweils mit einer Intranet-News angekündigt und bei Bedarf erläutert. Durch diesen Kanal wurde über den Ablauf und Zuständigkeiten, den verschiedenen Untersuchungen und Kontaktstellen bei Fragen informiert sowie über mögliche Risiken von Social Engineering sensibilisiert.
- 65. Fedpol hat am 12. Juli 2023 auf ihrer Webseite die Öffentlichkeit über den veröffentlichten Auszug der HOOGAN- Datenbank von 2015 informiert. Im genannten Auszug werden 766 Personen aufgeführt, wovon 690 am 07. Juli 2023 nicht mehr in HOOGAN registriert waren. Den möglichen Betroffenen wurde auf der Webseite ein Kontaktformular zur Verfügung gestellt. Daraufhin haben sich 295 Personen bei fedpol gemeldet. Sämtliche Anfragen wurden persönlich beantwortet.

2.9.2. Umgesetzte technische und organisatorische Massnahmen

- ^{66.} Alle User- Accounts (Wartungs- und Supportzugänge) von Xplain wurden umgehend deaktiviert.
- ^{67.} Fedpol hat eine interne Einsatzorganisation gebildet, welche mit der Vorfallanalyse beauftragt wurde. Die Ergebnisse der Untersuchungen, inkl. der Teile der Daten, die im Darknet publizierten wurden, wurden eingangs täglich und danach wöchentlich in den Sitzungen der Einsatzorganisation präsentiert, in den Protokollen festgehalten, und die zu treffenden Massnahmen wurden besprochen.
- ^{68.} Fedpol hat insgesamt 4'792 Files analysiert und beurteilt, wovon 1'892 IT-relevant waren. Bei etwas über 600 Files wurden unter dem Aspekt der IT-Sicherheit kritische Inhalte identifiziert, wodurch 106 IT-Massnahmen eingeleitet wurden. Bei der Definition der einzuleitenden Massnahmen wurde unterschieden, ob die identifizierten Inhalte für externe Partner (Kantone, KAPOs, andere Bundesbehörden) relevant sind. Wenn ja, wurden entsprechende « Informationsmassnahmen » ausgelöst. Die restlichen Massnahmen wurden nach Umsetzungsdringlichkeit (Sofortmassnahme, mittelfristige Massnahme, langfristige Massnahme) kategorisiert.
- In der Folge wurden verschiedene IT-Massnahmen ergriffen, um weitere Datenabflüsse zu verhindern. Dazu gehörten die rasche Änderung von Zugangsdaten und Zertifikaten für Benutzer und Systeme, kontinuierliche Überwachung von Web-Services und Systemen, sowie die Anpassung der nach aussen exponierten IP-Adressen. Es wurden ebenfalls Massnahmen ergriffen, um den Zugriff von Xplain-Mitarbeitenden auf die Bundesinfrastruktur über die zur Verfügung gestellten BAB-Clients zu sperren. Zusätzlich wurden Zertifikate gesperrt und alle eneXs-Zertifikate für die Datenbankabfrage ausgetauscht. Zudem wurde eine detaillierte Softwareanalyse, einschliesslich des Source-Codes, durchgeführt. Um das Bewusstsein der Mitarbeitenden für Datenschutz, den Umgang mit Passwörtern und Handlungsanweisungen zu schärfen, wurden ebenfalls Sensibilisierungsmassnahmen eingeleitet. Zusätzlich wurden verschiedene Aufträge an Xplain erteilt, wie das Herunterfahren von Servern und die Änderung von Passwörtern.
- ^{70.} Zur Einleitung von Präventiv-Massnahmen wurde ein Fokus auf die Zusammenarbeit mit weiteren externen IT-Dienstleistern gelegt. Die wichtigste Massnahme zur Steuerung der Zusammenarbeit mit Drittfirmen war eine Sensibilisierung und eine Forderung zur Darlegung der Einhaltung des IKT-



Grundschutzes. Zu diesem Zweck ist in Zusammenarbeit mit dem GS-EJPD ein Schreiben erstellt worden, welches durch das GS-EJPD an die 36 wichtigsten IT-Lieferanten des EJPD gesendet wurde. Zusätzlich hat fedpol ein Schreiben an 105 weitere IT-Lieferanten verschickt, welche nicht durch das GS-EJPD abgedeckt waren.

2.10. Weitere betroffene Bundesämter

71. Xplain stellt der Bundesverwaltung insgesamt folgende 15 Anwendungen bereit.

Anwendung	Beschreibung	Vertrags- partner
eneXs-mobile VI.x	Grenzkontrolllösung.	BAZG
eneXs mobile 2.0	Nachfolgeprodukt von eneXs-mobile.	BAZG
eneXs Server	Wird zentral in der Bundesverwaltung betrieben und dient zur Abfrage auf Datenbanken wie RI-POL, MOFIS etc.	BAZG
eneXs-stationär	Grenzkontrolllösung.	BAZG
ORMA	Geschäfts- und Aktenverwaltungssystem inkl. Meldungsverarbeitung des nationalen und inter- nationalen Schriftverkehrs (INTERPOL, Euro- pol).	fedpol



Anwendung	Beschreibung	Vertrags- partner

Tabelle 2: Genutzte Xplain-Anwendungen in der Bundesverwaltung.

^{72.} 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

Mit Schreiben vom 21. März 2024 hat fedpol zum Sachverhalt Stellung genommen. Die Ergänzungen und Anmerkungen wurden übernommen, soweit sie für die datenschutzrechtliche Beurteilung relevant waren.



4. Datenschutzrechtliche Beurteilung

4.1. Vorbemerkungen

- 74. 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 dienen. 10
- ^{75.} Die nachfolgenden rechtlichen Beurteilungen nach aDSG gelten grundsätzlich auch bei der Anwendung 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.
- ^{76.} Ob für die im Rahmen dieser Sachverhaltsabklärung untersuchten Personendatenbearbeitungen über hinreichende gesetzliche Grundlagen bestehen, ist nicht Gegenstand dieser Untersuchung.
- Der EDÖB eröffnete ursprünglich ein Vorverfahren betreffend RIPOL-Zugriffe und anschliessend ein formelles Verfahren betreffend RIPOL-Zugriffe und Datenschutzverletzungen im Zusammenhang 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.
- Die Datenbearbeitungen von fedpol im Zusammenhang mit den Anwendungen eneXs-mobile und ORMA sowie in Bezug auf ein Projekt betreffend HOOGAN stehen im Vordergrund (siehe Ziffer 5). Der EDÖB hat seine Untersuchung auf diese Anwendungen eingeschränkt: Die Anwendung eneXs-mobile führte zahlenmässig zu den meisten Personendatenübermittlungen von Behörden zu Xplain. Dabei ist festzuhalten, dass neben fedpol zahlreiche weitere Behörden die Anwendung eneXs-mobile verwenden, insbesondere zahlreiche kantonale Polizeibehörden, aber auch andere Bundesbehörden. Die Anwendung ORMA ist eine Softwarelösung für die Geschäftsverwaltung, die Xplain auch bei anderen Behörden implementiert hat, weshalb auch diese Anwendung untersucht wurde. Andere Anwendungen, die Xplain für die Bundesverwaltung entwickelt und implementiert hat, führten gemäss Erkenntnissen des EDÖB zu keinen systematischen Datenflüssen von Behörden zu Xplain, weshalb auf die Untersuchung der restlichen Anwendungen verzichtet wurde. Das Projekt betreffend die HOOGAN-Datenbank zeigt zudem exemplarisch auf, wie Personendaten in Einzelfällen zu Xplain gelangen konnten. Die Reaktionen von fedpol nach dem Vorfall werden kurz beurteilt. Die datenschutzrechtliche Beurteilung des Ransomware-Vorfalls durch Play ist nicht Gegenstand dieser Untersuchung.

4.2. Vertragliche Vereinbarungen mit Xplain

^{79.} Das fedpol verfügt über langjährige vertragliche Beziehungen mit Xplain (siehe Ziffer 49). Diese betreffen die IT-Projektbegleitung, Softwareentwicklung und -Weiterentwicklung sowie die Wartung und der Support der von Xplain an fedpol gelieferten Anwendungen. Im Rahmen dieser Vertragsbeziehungen erfolgte die Übertragung von Personendaten an Xplain.

^{80.} Es spielt keine Rolle, dass die Übertragung von Personendaten nur ein Nebeneffekt bei der gesamten Vertragserfüllung darstellt. Insbesondere der Support- und Wartungsprozess ist auf die

¹⁰ 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).



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 Datenübertragungen an Xplain als Auftragsdatenbearbeitung und die Anforderungen an diese werden nachfolgend in Bezug auf die betrachteten Anwendungen näher begründet.

4.3. Datenübertragung durch eneXs-mobile

81. In Art. 22 Abs. 2 VDSG¹¹ wird festgehalten, dass das Bundesorgan, das Personendaten durch Dritte bearbeiten lässt, für den Datenschutz verantwortlich bleibt und dafür sorgt, dass die Daten auftragsgemäss 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.¹² Gemäss Art. 16 Abs. 1 aDSG bleibt das Bundesorgan, das Personendaten durch Dritte bearbeiten lässt, für den Datenschutz verantwortlich.

4.3.1. Datenbearbeitung durch Dritte

«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 Datenbearbeitung 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.» ¹³ Für eine Auslagerung gemäss Art. 10a Abs. 1 aDSG wird somit eine Übertragung durch Vereinbarung oder Gesetz, keine Bearbeitung zu eigenen Zwecken des Auftragnehmers sowie keine widersprechenden Geheimhaltungsverpflichtungen vorausgesetzt.

4.3.1.1. Vereinbarung oder Gesetz

- ^{83.} Eine gesetzliche Grundlage, wonach Xplain zur fraglichen Bearbeitung legitimiert wird, ist nicht ersichtlich. Es ist deshalb zu prüfen, ob zwischen fedpol und Xplain eine Vereinbarung bestand, welche die Bearbeitung von Personendaten beinhaltet.
- 84. Weder die von fedpol vorgebrachten Argumente (siehe Ziffer 28), noch die Ausführungen von Xplain (siehe Ziffer 29), 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.
- 85. Gemäss Art. 3 lit. e aDSG bedeutet «bearbeiten» im Sinne des DSG jeder Umgang mit Personendaten, 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 Einsichtgewähren (Art. Art. 3 lit. f aDSG).

¹¹ Verordnung zum Bundesgesetz über den Datenschutz (VDSG) vom 14. Juni 1993; SR 235.11.

¹² Botschaft zur Totalrevision des DSG, 2017, S. 7031.

¹³ Zum Ganzen BVerGer A-4941/2014, Urteil vom 09.11.2016, Ziff. 12.7.3.



- Das tatsächliche Bearbeiten von Personendaten durch Xplain 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 von fedpol gespeichert, die im Darknet publiziert wurden. Xplain verfügte über 70 GB Daten von fedpol auf ihrem Fileserver, wovon 39% bzw. 52'368 Files veröffentlicht wurden (siehe Ziffer 70). In den im Darknet publizierten Daten wurden viele Logs von eneXs-mobile mit Personendaten festgestellt. Folglich hat Xplain im Mai 2023 Personendaten von fedpol auf ihrem Fileserver in Interlaken gespeichert bzw. im Sinne von Art. 3 lit. e aDSG bearbeitet.
- Das fedpol hat mit Xplain einen Vertrag betreffend Erbringung von Informatikdienstleistungen im Zusammenhang mit der Aufschaltung von eneXs-mobile abgeschlossen. 14 Gemäss dem Vertragsgestand regelt der Vertrag «die Lieferung von Lizenzen, die Wartungs- und Support-Leistungen und die Erbringung von Informatik-Dienstleistungen im Zusammenhang mit der Aufschaltung von eneXs mobile (ineXs) für iOS-Smartphones beim fedpol.» Vertraglich wurde betreffend Wartung und Support nur die Vergütung geregelt. Bei Wartung und Support von eneXs-mobile, womit auf unterschiedliche Datenbanken mit besonders schützenswerten Personendaten zugegriffen werden kann, muss davon ausgegangen werden, das Xplain regelmässig mindestens Einblick in Personendaten erhalten kann. Um von einer Übertragung von Personendaten auszugehen, spielt es keine Rolle, dass dies nur eine Nebenleistung der eigentlichen Aufgabe darstellt, was vorliegend zutrifft.
- ^{88.} Die Verpflichtungserklärungen (Beilage 1 und 2) zum Vertrag betreffend Erbringung von Informatikdienstleistungen im Zusammenhang mit der Aufschaltung von eneXs-mobile¹⁵ und die vertraglich
 vereinbarte Möglichkeit für Personensicherheitsprüfungen für Mitarbeitende von Xplain (Ziff. 10.1
 des Vertrages) zeigen auf, dass die Parteien von Personendatenbearbeitungen im Zusammenhang
 mit eneXs-mobile durch Xplain ausgingen. Dies ergibt sich insbesondere dadurch, indem Xplain mit
 der Verpflichtungserklärung auf die berufliche Schweigepflicht nach Massgabe des DSG ausdrücklich hingewiesen wurde. Auch war eine Personensicherheitsprüfung gestützt auf
 Art. 11 Abs. 2 lit. f PSPV¹⁶ notwendig, wenn «Personen regelmässig Zugang zu besonders schützenswerten Personendaten haben, deren Bekanntgabe die Persönlichkeit der Betroffenen schwerwiegend beeinträchtigen kann», was auf Mitarbeitende von Xplain zutreffen kann.
- Aus dem Wortlaut des Vertrages bleibt jedoch unklar, ob fedpol lediglich davon ausging, dass Xplain nur im Rahmen von Support und Wartung Kenntnis von Personendaten erhält und deshalb die Verpflichtungserklärung abgeschlossen hat sowie die Möglichkeit der Personensicherheitsprüfung vereinbarte, oder ob der Support und Wartungsprozess insbesondere die Organisation des 2nd und 3rd Levels so ausgestaltet wurde, dass dieser die Speicherung von Personendaten auf dem Fileserver von Xplain beinhaltet (zur Beurteilung des 2nd und 3rd Level-Prozesses siehe nachfolgende Ziffer 124 ff.). Wird der Vertrag jedoch mit dem tatsächlich durchgeführten Support-Prozess (siehe Ziffer 38 f.) betrachtet, mussten die Parteien Wissen, 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 fedpol als auch für Xplain erkennbar sein, dass Personendaten an Xplain übertragen werden.
- Unter Berücksichtigung der gesamten Umstände ist davon auszugehen, dass mit dem erwähnten Vertrag betreffend eneXs-mobile die Vertragsparteien eine Vereinbarung gemäss Art. 10a aDSG

¹⁴ Siehe vorangehende Ziffer 53.

¹⁵ Vertragsnummer 0316004366.

Verordnung über die Personensicherheitsprüfung, SR 120.4; war im Zeitpunkt der Vertragsschliessung in Kraft, wurde auf 01.01.2024 aufgehoben.



getroffen haben. Gegenstand und Umfang der Datenbearbeitung wird im Vertrag zwar nicht konkret geregelt. Das ist aber so möglich, weil die Vereinbarung an keine Form gebunden ist. Somit kann auch offenbleiben, ob der dem EDÖB nicht bekannte Vertragsbestandteil «Angebot der Auftragnehmerin vom 22. März 2019» den Gegenstand und Umfang der Datenbearbeitung regelt. Das Risiko einer unklaren Regelung trägt das fedpol als Verantwortliche.

4.3.1.2. Keine Bearbeitung zu eigenen Zwecken

^{91.} Sowohl in den erwähnten Verpflichtungserklärungen sowie in Ziff. 17.2 der im Vertrag integrierten AGB¹⁷ wird die Bearbeitung von Personendaten für andere Zwecke ausgeschlossen.

4.3.1.3. Keine widersprechenden Geheimhaltungspflichten

- ^{92.} Bei der Erfüllung des Vertrages musste davon ausgegangen werden, dass Xplain Kenntnis von Amtsgeheimnissen erhält. Das Amtsgeheimnis steht grundsätzlich einer Auslagerung nicht entgegen, sofern die Dritten als Hilfspersonen i.S.v. Art. 321 Abs. 1 StGB zu qualifizieren sind. ¹⁸ Dies ist bei den Mitarbeitenden von Xplain erfüllt. Zusätzlich muss sichergestellt werden, dass die Geheimhaltungsverpflichtung dem Auftragnehmer überbunden wird. Dies wird mit den Verpflichtungserklärungen sowie Art. 16 der AGB erfüllt.
- ^{93.} Zudem stellt der IKT-Grundschutz Anforderungen angesichts des Risikos der Amtsgeheimnisverletzung. Die zu berücksichtigen Massnahmen werden aufgelistet und auf das Dokument «Anforderungen angesichts des Risikos von Amtsgeheimnisverletzungen» hingewiesen. ¹⁹

4.3.1.4. Fazit

Somit bestätigen die vorangehenden Erläuterungen, dass ein Auftragsbearbeitungsverhältnis vorliegt 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 transparent 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 fedpol für die Datenbearbeitungen von Xplain verantwortlich, solange Xplain die Personendaten nicht über die Vereinbarung hinaus bearbeitet. Nicht geprüft wurde, ob die Anforderungen gemäss dem IKT-Grundschutz umgesetzt wurden.

4.3.2. Gewährleistung der Datensicherheit

- ^{95.} 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 mitumfasst, 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.²⁰
- ^{96.} Der Verantwortliche hat dem Auftragnehmer klare Vorgaben für Sicherheitsmassnahmen zu machen und deren Umsetzung und Einhaltung zu kontrollieren. Sofern der Auftragnehmer selbst dem aDSG untersteht, kann der Verantwortliche davon ausgehen, dass die technischen und organisatorischen Massnahmen der Datensicherheit (Art. 7 aDSG) angemessen erfüllt sind

¹⁷ Allgemeine Geschäftsbedingungen für Informatikdienstleistungen, Stand 20.10.2010.

¹⁸ Botschaft zur Totalrevision des DSG, 2017, S. 7031 f.; wonach dies sowohl nach aDSG wie auch nach revidiertem DSG gilt.

¹⁹ IKT-Grundschutz in der Bundesverwaltung, Version 4.6, Stand 01.04.2021, Kap. 2 Ziff. 15.2.

²⁰ Zum Ganzen BVerGer A-4941/2014, Urteil vom 09.11.2016, Ziff. 12.7.3.



- (Art. 22 Abs. 3 VDSG e contrario). Der Verantwortliche ist deshalb verpflichtet, den Auftragsbearbeiter sorgfältig auszuwählen, zu instruieren und soweit nötig zu überwachen.²¹
- ^{97.} 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.²²

4.3.2.1. Auswahl

Dem EDÖB ist nicht bekannt, nach welchen Kriterien fedpol im Jahr 2019 für die Umsetzung einer mobilen App zur Abfrage auf polizeiliche Datenbanken Xplain ausgewählt hat. Bekannt ist jedoch, dass der Einsatz von eneXs-mobile über die bereits aufgebauten Infrastrukturlösungen des Grenzwachtkorps EZV erfolgte, welche die Anwendung bereits im produktiven Einsatz hatte. Typischerweise wurden die Vertragsbeziehung mit 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 auch datenschutzrechtliche Kriterien berücksichtigt werden; etwa ob Xplain über ein Informationssicherheitsmanagementsystem verfügt und ob dazu eine Zertifizierung nach einem international anerkannten Standard vorliegt. Diese hohen Anforderungen sind gerechtfertigt, wenn eine Zusammenarbeit mit Xplain im Bereich der inneren Sicherheit eingegangen werden soll.

4.3.2.2. Instruktion

- ^{99.} Zu prüfen ist, inwieweit die Vergewisserungspflicht des Verantwortlichen geht, dass der Auftragsbearbeiter die Datensicherheit gewährleistet. Nach Art. 7 Abs. 1 aDSG wird die Datensicherheit gewährleistet, sofern die Personendaten durch angemessene technische und organisatorische Massnahmen geschützt werden. Die verantwortlichen Bundesorgane treffen die nach den Artikeln 8-10 VDSG erforderlichen technischen und organisatorischen Massnahmen zum Schutz der Persönlichkeit 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).
- 100. Grundsätzlich kann fedpol 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 spezifisch zu überbinden.
- 101. Gemäss dem Vertrag erbringt Xplain als Spezialistin und in Kenntnis des Vertragszwecks die Lieferung von Lizenzen zur Nutzung der eneXs-mobile App, Anpassung und Erweiterung auf dem eneXs-Server sowie Wartungs- und Support-Leistungen.
- 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 Anforderungen der Datensicherheit eines Auftragsbearbeiters dar. Fedpol hat Xplain keine direkten Zugriffe auf die Serviceinfrastruktur beim ISC-EJPD bzw. auf diejenigen Datenbanken ermöglicht, für welche fedpol verantwortlich ist. Der Wartungs- und Supportprozess war allerdings durch die von

²¹ Botschaft DSG 1988, 463; Botschaft DSG 2017, 7032.

²² IKT-Grundschutz in der Bundesverwaltung, Version 4.6, Stand 01.04.2021, Kap. 2 Ziff. 15.1.



Xplain in der Software programmierte Funktion vorgegeben. Bei einem aufgetretenen Fehler werden in eneXs-mobile Screenshots oder Fehler-Reports mit produktiven Daten, die auch Personendaten enthalten, erstellt und aus der IT-Bundesinfrastruktur in die IT-Infrastruktur von Xplain übertragen (siehe Ziffer 38 f.). 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.

- 103. Der Vertrag betreffend die Aufschaltung von eneXs-mobile zwischen fedpol und Xplain enthält keine spezifischen datenschutzrechtlichen Instruktionen. In den integrierten AGB Informatikdienstleistungen wird in Ziffer 17 festgehalten, dass die Parteien sich verpflichten, «die wirtschaftlich zumutbaren sowie technisch und organisatorisch möglichen Vorkehrungen zu treffen, damit die im Rahmen der Vertragsabwicklung anfallenden Daten gegen unbefugte Kenntnisnahme Dritter wirksam geschützt sind». Andere Vereinbarungen, worin fedpol Xplain über die Anforderungen der Datensicherheit genauer instruiert, bestanden gemäss den Feststellungen des EÖDB nicht.
- In der erwähnten Verpflichtungserklärung wird festgehalten: «[...] Nach Rück-/Übergabe an den Besteller sind die Daten auf den Anlagen der Auftragnehmerin unverzüglich physisch zu löschen. Die Ausführung der Löschung ist dem Besteller unaufgefordert schriftlich zu bestätigen. [...]». Daraus folgt, dass Xplain nach Erhalt von Personendaten diese nach fertiger Bearbeitung des Supportoder Wartungsauftrages hätte löschen müssen. Diese Löschpflicht ergibt sich bereits gestützt auf den allgemeinen Verhältnismässigkeitsgrundsatz gemäss Art. 4 Abs. 2 aDSG, weshalb die Bestimmung keine weitergehende Verpflichtung als das DSG mit sich bringt.
- Möglich gewesen wären grundsätzlich zwei Varianten: Fedpol hätte Xplain ausdrücklich vertraglich verpflichten können, dass Personendaten nur auf der Bundesinfrastruktur des Bundes bearbeitet werden dürfen bzw. die Speicherung von Personendaten ausserhalb der Bundesverwaltung strikt verboten wäre. Dazu hätte fedpol 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 Bearbeitung 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 Bundesinfrastruktur bearbeitet werden, müssen gemäss ihrem Schutzbedürfnis mit den erforderlichen technischen und organisatorischen Massnahmen geschützt werden, insbesondere durch die Einhaltung von Löschregeln.
- Dem EDÖB liegt keine SCHUBAN und kein ISDS-Konzept vor. Daraus liegt der Schluss nahe, dass fedpol die Anwendung eneXs-mobile bei der eigenen Implementierung nicht mehr näher geprüft hat, weil darauf vertraut wurde, dass dies das BAZG bereits richtig vorgenommen hat und die Anwendung alle datenschutzrechtlichen Anforderungen erfüllt. Das fedpol hätte aber vor der Implementierung von eneXs-mobile mindestens eine eigene SCHUBAN und gegebenenfalls ein ISDS-Konzept erstellen müssen, allenfalls auf Grundlage der bereits vorhandenen. Dabei hätten die Risiken des Support- und Fehlerbehebungsprozesses erkannt und entsprechende Vereinbarung zur datenschutzkonformen Umsetzung abgeschlossen werden müssen.

4.3.2.3. Überwachung

107. Fedpol macht geltend, dass aufgrund von fehlenden personellen und finanziellen Ressourcen keine regelmässigen Prüfungen bei Xplain im Hinblick auf die Einhaltung der Datensicherheit, etwa in Form von regelmässigen Audits, vorgenommen werden konnten. Aus operativer Sicht steht das Funktionieren der Systeme mit möglichst wenig Fehlern und Störungen im Vordergrund, sodass konzeptionelle Datenschutzrisiken nicht erkannt oder zwar erkannt werden, aber keine Ressourcen für die Korrektur vorhanden sind. Folglich wurde zwar erkannt, dass mehr Ressourcen notwendig wären, diese wurden aber nicht hinreichend zur Verfügung gestellt.



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 geeignetes 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 Kontrolle und Einhaltung vereinbarter datenschutzrechtlicher Anforderungen mit Nachweisen bestätigt wird.

4.3.2.4. Fazit

Aus den obigen Darlegungen geht hervor, dass fedpol die Gewährleistung der Datensicherheit gemäss Art. 10a Abs. 2 aDSG nicht ausreichend erfüllt hat. Fedpol 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 Wartung 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. Datenübertragung durch ORMA

4.4.1. Auslagerung

Die Ausführungen zur Auslagerung (Art. 10a Abs. 1 aDSG) durch eneXs-mobile (siehe Ziff.81 ff.) gelten für ORMA analog. Im Unterschied zu eneXs-mobile bestehen für ORMA jedoch mehrere und detailliertere Verträge, weshalb nachfolgend auf die diesbezüglichen Unterschiede eingegangen wird.

4.4.1.1. Vereinbarung oder Gesetz

- Aus dem Vertrag «Erbringung von werkvertraglichen Leistungen im Informatikbereich und die Pflege von Individualsoftware»²³ werden bei Wartung und Support die Personendatenbearbeitungen durch Xplain nicht geregelt. Im Folgevertrag wird jedoch wieder auf die berufliche Schweigepflicht gemäss DSG verwiesen.²⁴
- Als Grundauftrag wird «Wartung und Pflege der Software (wiederkehrende Kosten) gemäss bestehendem Wartungsvertrag. (AGB Lizenzen). Vgl. Absatz C dieses Vertrages.» definiert. In Absatz C des Vertrages wird festgehalten, dass die Pflege und der Support von ORMA im Rahmenvertrag 403.000.-1, Spezifikationsblatt Nr. 1 / 30.01.2014 geregelt wird. Im genannten Dokument finden sich namentlich folgende Bestimmungen:

«

3) Umfang der Pflege

Der Lieferant erbringt die folgenden Leistungen:

Hotline

Bereitschaftsdienst während der Bereitschaftszeit

²³ Vertragsnummer: 0316004363, siehe auch Ziffer 54 hiervor.

Vertrag über die Erbringung von Informat kdienstleistungen (Auftrag), Dienstleistungen ORMA 2018+, Zusatzaufwände 2023, Vertragsnummer 0316000091 / 500, Ziff. 13.1; siehe auch nachfolgende Ausführungen in Ziffer 116.



Qualifizierte Fehler-Annahme Fehler-Management und Benennung eines individuellen Kundenansprechpartners der die Leistungen koordiniert

Wartung

Off-Site Fehleridentifikation
Off-Site Korrektur von Fehlern / Mängeln
Software-Updates / -Patches
Remote-Diagnose
Dokumentationsservice

4) Bereitschafts- und Reaktionszeit

4.1) Pflegebereitschaftszeit Montag - Freitag 08.00 - 12.00 Uhr und 14.00 - 17.00 Uhr (ausgenommen offizielle Feiertage)

4.2) Reaktionszeit (Interventionszeit)

Reaktionszeit 4 Stunden

»

- Unter Berücksichtigung der zitierten Bestimmung bleibt unklar, ob die Parteien lediglich davon ausgingen, dass Xplain im Rahmen von Support und Wartung Personendaten zur Kenntnisnahme erhält oder, ob der Support und Wartungsprozess insbesondere die Organisation des 2nd und 3rd Levels so ausgestaltet wurde, dass dieser das Bearbeiten von Personendaten auf dem Fileserver von Xplain beinhaltet (zur Beurteilung des 2nd und 3rd Level-Prozesses siehe nachfolgende Ziffer 124 ff.). In beiden Fällen handelt es sich um ein Bearbeiten im Sinne von Art. 3 lit. e und f aDSG. Eine entsprechende Verpflichtungserklärung wurde abgeschlossen und die Möglichkeit der Personensicherheitsprüfung wurde vereinbarte. Fedpol hat mit Xplain keine ausreichende vertragliche Vereinbarung betreffend den Support und die Wartungsprozesse und die damit verbundenen Datenübertragungen getroffen.
- 114. Fedpol musste davon ausgehen, dass mit den von Xplain zur Verfügung gestellten Fehlerbehebungs- und Wartungsprozessen (siehe Ziffer 42 f.) ein Bearbeiten von Personendaten erfolgt, weshalb unter Berücksichtigung der gesamten Umstände auch bei ORMA eine Vereinbarung gemäss Art. 10a Abs. 1 aDSG vorliegt. Der Umfang der Datenbearbeitung wird im Vertrag nicht klar geregelt und somit auch der Grundsatz der Verhältnismässigkeit nicht berücksichtigt. Es kann offenbleiben, ob der dem EDÖB nicht bekannte Vertragsbestandteil «Angebot der Auftragnehmerin vom 22. März 2019» den Gegenstand und Umfang der Datenbearbeitung regelt. Das Risiko einer unklaren Regelung trägt das fedpol als Verantwortliche.

4.4.1.2. Keine Bearbeitung zu eigenen Zwecken

In Ziff. 17.2 der im Vertrag integrierten AGB²⁵ wird die Bearbeitung von Personendaten für andere Zwecke ausgeschlossen. Die analoge Verpflichtungserklärung wie bei eneXs-mobile wurde in diesem Vertrag nicht als Vertragsbestandteil integriert.

4.4.1.3. Keine widersprechenden Geheimhaltungspflichten

^{116.} Die Geheimhaltungspflicht wird mit Art. 16 der AGB überbunden. Im Übrigen gelten die Ausführungen in Ziffer 92 f. analog.

²⁵ Allgemeine Geschäftsbedingungen für Informatikdienstleistungen, Stand 20.10.2010.



4.4.1.4. Fazit

Mit den erwähnten Verträgen betreffend ORMA haben die Parteien eine Vereinbarung für die Auslagerung im Sinne von Art. 10a aDSG getroffen. Faktisch war der Wartungs- und Supportprozess durch die entsprechende Programmierung der Software vorgegeben (siehe Ziffer 42 f.) und die Übertragung an Xplain ständige Praxis. Die Datenübertragung wird zwar vertraglich grob umschrieben, jedoch finden sich keine ausdrücklichen Bestimmungen, welche datenschutzrechtlichen Anforderungen gelten, damit Personendaten die IT-Bundesinfrastruktur verlassen bzw. auf der IT-Infrastruktur von Xplain gespeichert werden können. Das Risiko einer unklaren Regelung trägt fedpol als Verantwortliche, sofern Xplain die Personendaten nicht über die Vereinbarung hinaus bearbeitet. Nicht geprüft wurde, ob alle Anforderungen gemäss dem IKT-Grundschutz umgesetzt wurden.

4.4.2. Gewährleistung der Datensicherheit

- Die Ausführungen zur Gewährleistung der Datensicherheit (Art. 10a Abs. 2 aDSG; Ziff. 95 ff.) durch eneXs-mobile gelten für ORMA analog. Im Unterschied zu eneXs-mobile bestehen für ORMA jedoch mehre und detailliertere Verträge, weshalb nachfolgend wiederum auf die diesbezüglichen Unterschiede eingegangen wird.
- ^{119.} Im Zeitpunkt des Ransomware-Vorfalls waren drei Verträge zwischen fedpol und Xplain betreffend ORMA in Kraft.²⁶ Im Vertrag «ORMA 2018+, Zusatzaufwände 2023»²⁷ wurde betreffend Datensicherheit folgendes vereinbart (Hervorhebungen hinzugefügt):

Ziffer 13.7 Schutz der Informatik- und Telekommunikationssysteme vor Angriffen und Meldepflicht

«

- 1. Die Auftragnehmerin ist verpflichtet, für die und bei der Vertragsabwicklung ihre Informatik- und Telekommunikationssysteme (umfassend insbesondere Infrastruktursysteme, Netzwerke, Geräte und Anwendungen sowie Daten und Informationen) im Folgenden bezeichnet als «Systeme» in ihrem Verantwortungsbereich nach dem jeweils aktuellen Stand der Technik mittels technisch und organisatorisch möglichen sowie wirtschaftlich zumutbaren Vorkehrungen vor Angriffen zu schützen.
- Als «Angriffe» (äquivalente Begriffe: «Cyberattacken» oder «Cyberangriffe») gelten insbesondere der unbefugte Zugang, die Störung, die Manipulation oder der Missbrauch der Systeme von innen oder aussen. Weiter gehören insbesondere der Diebstahl, die unrechtmässige Verarbeitung oder die Vernichtung von Informationen oder Daten sowie sonstige rechtswidrige Eingriffe in die Systeme dazu (vgl. insbesondere Art. 143, 143bis,144bis, 147,179novies, 272-274 des Strafgesetzbuches (StGB)).
- 3. Die Auftragnehmerin verpflichtet sich insbesondere, ihr und ihren beigezogenen Dritten¹ (z.B. Sub-unternehmer und Zulieferer) für die korrekte Vertragserfüllung verfügbar gemachte oder bei ihnen entstandene Daten und Informationen entsprechend den Bestimmungen dieser Ziffer zu schützen. Das gilt insbesondere, wenn es sich um sicherheitsrelevante Angaben oder um Personendaten handelt. Es sind dabei die Anforderungen und Vorgaben des Bundesgesetzes über den Datenschutz (DSG), der Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CybRV; SR 120.73) und der Informationsschutzverordnung (IS-chV; SR 510.411) zu beachten und einzuhalten.
- 4. Die Auftragnehmerin meldet der Auftraggeberin unaufgefordert jedes erkannte Ereignis, welches die Einhaltung ihrer Pflichten beeinträchtigen könnte, unverzüglich nach Auftreten bzw. Kenntnisnahme, spätestens innerhalb einer Frist von 24 Stunden. Sie meldet insbesondere versuchte oder erfolgreiche Angriffe sowie andere befürchtete oder erfolgte technische Kompromittierungen von Systemen, Daten und/oder Informationen und allenfalls

²⁶ Siehe Ziffer 54 hiervor.

²⁷ Vertragsnummer: 0316000091 / 500.



entstandene Schäden. Dabei wird auch über die geplanten und getroffenen Massnahmen zu deren Behebung informiert. Zur Vermeidung von Schäden oder weiteren Angriffen gewährt die Auftragnehmerin der Auftraggeberin oder durch sie beauftragten Dritten auf erstmalige Aufforderung unverzüglich den vollen und umfassenden Zugang zu Analysen, Untersuchungsberichten und anderen Feststellungen (Dokumente, Daten, Log-Daten, Gegenstände etc.), die es erlauben, das Ereignis zu analysieren. Die Auftragnehmerin stellt sicher, dass mit der Auftragnehmerin vordefinierte Aktivitäten aufgezeichnet (Logging) und ausgewertet werden, um Angriffe zu erkennen und zu vermeiden. Entdeckte Sicherheitslücken müssen zeitnah behoben werden.

- 5. Die Auftraggeberin (oder ein Dritter in ihrem Auftrag) kann nach Bedarf höchstens zwei Mal jährlich bei der Auftragnehmerin Audits durchführen. Solche werden 7 Arbeitstage vorangekündigt. Jede Partei trägt ihre Kosten des Audits selbst. Sollten jedoch im Rahmen eines Audits wesentliche Mängel im Sinne dieser Bestimmung festgestellt werden, trägt die Auftragnehmerin zusätzlich die Kosten zur Behebung dieser Mängel aber auch die Kosten, die der Auftraggeberin aus dem Audit entstehen. Die Auftragnehmerin ist verpflichtet, festgestellte Mängel innert einer Frist von 1 seit der Meldung zu beheben und der Auftraggeberin den Vollzug zu melden.
- 6. Die Auftragnehmerin schuldet eine Konventionalstrafe, sofern sie die verlangten Vorkehrungen gemäss der vorliegenden Klausel nicht getroffen hat. Diese beträgt je Verletzungsfall 10% der gesamten Vergütung, mindestens jedoch CHF 3'000.-- je Fall. Die Bezahlung der Konventionalstrafe befreit die Auftragnehmerin nicht von der Einhaltung ihrer vertraglichen Pflichten. Die Konventional-strafe wird auf einen allfälligen Schadenersatz angerechnet.
- 7. Die Auftragnehmerin. haftet für den Schaden, welcher der Auftraggeberin entsteht, sofern sie nicht beweist, dass sie kein Verschulden trifft.

Bei wesentlichen Verletzungen dieser Klausel oder mangelnder Mitwirkung in obengenannten Fällen behält sich die Auftraggeberin vor, keine weiteren Leistungen zu beziehen und die Vertragsbeziehung zu beenden.

"

- ^{120.} Im dritten Vertrag «Dienstleistungen Clean ORMA Phase 2 2023»²⁸ werden die gleichen Bestimmungen zur Datensicherheit geregelt.
- Im Vertrag wird weitgehend auf die Einhaltung der gesetzlichen Grundlagen hingewiesen. Da Xplain ein langjähriger Vertragspartner von fedpol ist und spezialisierte Dienstleistungen anbietet, kann fedpol auch davon ausgehen, dass Xplain bei diesbezüglichen Unklarheiten Rücksprache nimmt.
- Regelmässige Prüfungen bei Xplain im Hinblick auf die Einhaltung der Datensicherheit, etwa in Form von regelmässigen Audits, fanden nicht statt, was fedpol mit fehlenden personellen und finanziellen Ressourcen begründet.
- 123. Fedpol ist den Anforderungen von Art. 10a Abs. 2 aDSG nur ungenügend nachgekommen. Bereits aufgrund der unklaren vertraglichen Regelung betreffend die Art und Weise der Datenbearbeitung war es nicht möglich, sich spezifisch zu vergewissern, ob Xplain die Datensicherheit nach den Vorgaben des aDSG und den weiteren Anforderungen der Bundesverwaltung gewährleistet. Zwar konnte sich fedpol grundsätzlich auf die vertragskonforme Erfüllung durch Xplain verlassen, aber eine Prüfung hätte die Schwachstellen bei Xplain ohne weiteres aufdecken können.

¹ In Frage kommen alle in der Liefer- und Produktionskette eingebundenen Parteien, namentlich auch Rechteinhaber und Hersteller.

²⁸ Vertragsnummer: 0316000091 / 520.



4.5. Support- und Wartungsprozesse

Kern der datenschutzrechtlichen Problematik ist die Übermittlung von Personendaten aus der Bundesinfrastruktur in die IT-Infrastruktur von Xplain im Rahmen der Wartungs- und Supportprozesse (siehe Ziffer 38 ff. und 42 ff.). Solange die Personendaten in der Bundesinfrastruktur bleiben, sind diese gemäss den Vorgaben des Bundes bzw. mindestens vom IKT-Grundschutz geschützt. Dem EDÖB sind keine Anhaltspunkte bekannt, dass fedpol zusammen mit den bundesinternen Leistungserbringen 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.

4.5.1. eneXs-mobile

Der Support- und Wartungsprozess für eneXs-mobile verletzt den Grundsatz der Verhältnismässigkeit, der Datensicherheit und der Zweckbindung.

4.5.1.1. Verhältnismässigkeit

- 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 zumutbar 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 [...])».²⁹
- 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 besonders 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.
- ^{128.} Folglich verletzt die Funktion, mit welcher Screenshots und Log-Files mit Personendaten für die Behebung von Support und Wartung erstellt werden (siehe Ziffer 38), das Prinzip der Verhältnismässigkeit, soweit nicht erforderliche Personendaten übertragen wurden.

4.5.1.2. Datensicherheit

- Nach Art. 7 aDSG müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. In Art. 20 VDSG werden die Mindestanforderungen festgehalten. Wer Personendaten bearbeitet, sorgt für die Vertraulichkeit, Verfügbarkeit 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).
- Der IKT-Grundschutz legt die minimalen organisatorischen, personellen und technischen Anforderungen an die Informatiksicherheit der Bundesverwaltung bzw. deren Informatikschutzobjekte

²⁹ BGE 147 I 346, E. 5.5.



- (Schutzobjekte) fest. Der IKT-Grundschutz und die Datensicherheit gemäss DSG verfolgen unterschiedliche Schutzziele. Während der IKT-Grundschutz die Schutzobjekte schützt, dient das DSG dem Schutz der Persönlichkeit von Personen. Der EDÖB beurteilt deshalb die Datensicherheit gemäss Art. 7 aDSG und nicht den IKT-Grundschutz.
- Die Informationsweitergabe zwischen dem 2nd und 3rd Level Support bzw. zwischen dem fedpol und Xplain hätte so organsiert werden müssen, dass das Risiko von potentiellen Persönlichkeitsverletzungen angemessen minimiert wird. Ein organisatorischer Fehler lag insbesondere bei der Verwendung der dezidierten Endgeräte, welche Xplain Mitarbeitende erhielten. Solange die Xplain Mitarbeitenden nur mit den erhaltenen fedpol Notebooks auf der Bundesinfrastruktur arbeiten, bleiben alle Daten im geschützten Perimeter der Bundesverwaltung. Offensichtlich bestand seitens fedpol und Xplain kein Bewusstsein darüber, welche Anforderungen aus datenschutzrechtlicher Sicht gelten müssen, sobald Personendaten den Perimeter der Bundesverwaltung verlassen. Solange nämlich Xplain mit den erhaltenen fedpol Notebooks arbeitet, wird das datenschutzrechtliche Risiko nicht erheblich erhöht, weil die Daten im geschützten Perimeter der Bundesverwaltung bleiben. Obwohl Mitarbeitende von Xplain die fedpol Notebooks für die Unterstützung im 2nd Level Support erhielten, wurden die Laptops auch dazu verwendet, um Daten von der Bundesinfrastruktur auf den Fileserver von Xplain weiterzuleiten, zu bearbeiten und zu speichern.
- ^{132.} Zusammenfassend kann festgehalten werden, dass der Grundsatz der Datensicherheit insbesondere 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.

4.5.1.3. Zweckbindung

- 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 Anfragen 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 ausdrücklich in der Verpflichtungserklärung vertraglich festgelegt (siehe Ziffer 91).
- ^{134.} Folglich wurde durch die Nichtlöschung der 3rd Level Arbeiten der Grundsatz der Zweckbindung sowie die Vertragspflicht durch Xplain verletzt. Das fedpol bleibt jedoch für diese Verletzung gestützt auf Art. 16 Abs. 1 aDSG verantwortlich.

4.5.2. ORMA

Die rechtlichen Ausführungen zum Support- und Wartungsprozess von eneXs-mobile (siehe Ziffer 125 ff.) gelten für ORMA analog. Im Unterschied zur Funktion in eneXs-mobile musste die Benutzerin oder der Benutzer die Funktion für die Aufzeichnung der Fehlerberichte manuell einschalten. Die Supportfunktion war so programmiert, dass die Inhalte aller momentan geöffneten Anwendungen aus dem Zwischenspeicher (Cache) abgegriffen wurden. (siehe Ziffer 42). Das heisst, wurde die Supportfunktion eingeschaltet wegen einer Störung in ORMA und waren gleichzeitig andere Anwendungen geöffnet, etwa ein Bild eines Tatorts und eine E-Mail mit besonders schützenswerten Personendaten, wurden für den Fehlerbericht das Bild des Tatorts und das E-Mail mit besonders schützenswerten Personendaten abgegriffen. Die daraus generierte ZIP-Datei wurde im Anschluss zur Fehleranalyse an Xplain weitergeleitet. Die Integration von gleichzeitig anderen Anwendungen in den Fehlerbericht verletzt offensichtlich und in schwerwiegender Weise das Verhältnismässigkeitsprinzip. Obwohl die Funktion ORMA etwas anders ausgestaltet wurde als in eneXs-



mobile, gelten die Erläuterungen zur Verletzung der Grundsätze der Verhältnismässigkeit (siehe Ziffer 126), der Datensicherheit (siehe Ziffer 129) und der Zweckbindung (siehe Ziffer 133) analog.

4.6. Datenübertragung durch ein HOOGAN-Zugriffs Projekt

- ^{136.} Im Darknet wurde eine Liste der HOOGAN-Datenbank vom 02. September 2015 publiziert, in welcher 766 Personen aufgelistet werden. Diese Daten befanden sich auf dem Fileserver von Xplain (siehe Ziffer 18). Folglich wird geprüft, weshalb die HOOGAN-Liste an Xplain übermittelt, auf dem Fileserver gespeichert und nicht gelöscht wurde.
- Der Vertrag «Erbringung von Informatikdienstleistungen (Auftrag)» betreffend «Dienstleistungen im Projekt Hoogan + Zutrittskontrolle» 30 ist der einzige Vertrag, welcher der EDÖB zwischen fedpol und Xplain im Zusammenhang mit Zutrittskontrollen von Stadien durch Abgleiche mit der HOOGAN-Datenbank in Erfahrung bringen konnte. Die Ablieferung der Leistungsergebnisse wurde auf den 31. Oktober 2012 terminiert. Als Leistungen von Xplain wurden folgende Dienstleistungen definiert:

«

4. Leistungen der Auftragnehmerin

Die Auftragnehmerin erbringt als Spezialistin und in Kenntnis des Vertragszwecks die folgenden Dienstleistungen:

- Teilnahme an 5 Projektsitzungen zu je 3 Stunden inklusive Vor- und Nachbereitung
- Dokumentation Einsatzkonzept
- Dokumentation der Programmänderungen, Anpassungen der Detailspezifikation
- Projektdokumentation mit Reviews und Inputs für Schlussbericht
- Koordination mit dem Stadion [...], Abklärungen zu Installation, Integration in Haustechnik

X

- ^{138.} Aufgrund der Leistungen von Xplain und des Ablieferungstermins am 31. Oktober 2012 und der Tatsache, dass der HOOGAN-Auszug vom 02. September 2015 entspricht und somit rund 3 Jahre danach, besteht kein direkter Zusammenhang zwischen dem versendeten HOOGAN-Auszug und dem erwähnten Vertrag.
- Es ist aber unbestritten, dass der HOOGAN-Auszug an Xplain übermittelt wurde, um im Projekt aufgetretene Fehler zu beheben (siehe Ziffer 46). Die Leistung wurde demnach im Rahmen der übrigen vertraglich vereinbarten Dienstleistungen von Xplain erbracht. Es ist deshalb auch hier grundsätzlich von einem Auftragsbearbeitungsverhältnis auszugehen, das allerdings schriftlich nicht weiter spezifiziert wurde.
- Es ist fraglich, ob die Übermittlung des vollständigen HOOGAN-Auszugs an Xplain verhältnismässig war. Auch ist offen, ob angemessene Massnahmen der Datensicherheit getroffen wurden. Auf jeden Fall verletzt die Aufbewahrung des HOOGAN-Auszuges auf dem Fileserver von Xplain den Grundsatz der Zweckbindung und der Verhältnismässigkeit.

4.7. Daten für die Anwendungsentwicklung

141. Bei fedpol standen für die Entwicklung und Wartung Testdaten des jeweils betroffenen Informationssystems zur Verfügung. In der Integrationsumgebung von fedpol waren somit nur Testdaten vorhanden, weshalb dadurch keine Personendaten an Xplain übermittelt wurden. Somit konnte der EDÖB diesbezüglich bei fedpol keine datenschutzrechtlichen Mängel feststellen.

27/40

³⁰ Vertragsnummer: 40312071652.



4.8. IT-Infrastruktur von fedpol

Dem EDÖB liegen keine Anhaltspunkte vor, dass die IT-Infrastruktur im Rahmen des Ransomware-Vorfalls die Datensicherheit oder andere Anforderungen des DSG nicht erfüllte hätte, weshalb dies nicht Gegenstand der Untersucht bildet.

4.9. Reaktionen von fedpol auf Ransomware-Vorfall

4.9.1. Information an Dritte

- ^{143.} Im aDSG bestand keine ausdrückliche Bestimmung betreffend Meldung von Verletzungen der Datensicherheit, im Gegensatz zu Art. 24 DSG. Weil fedpol 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.
- Nach dem Ransomware-Vorfall hat fedpol involvierte Stellen und betroffene Personen informiert und für Personen, die nicht sicher waren ob sie vom Vorfall betroffen sind, wurde ein Kontaktformular auf der Webseite publiziert (siehe Ziffer 65). Mit diesen Massnahmen hat fedpol seine Informationspflichten nach Treu und Glauben wahrgenommen.

4.9.2. Technische und organisatorische Massnahmen

- 145. 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 organisatorische Massnahmen zur Behebung oder Vermeidung weiterer möglicher Persönlichkeitsverletzungen sind schnellstmöglich umzusetzen.
- ^{146.} Zur Bewältigung des Ransomware-Vorfalls bei Xplain hat fedpol eine Einsatzorganisation gebildet, die zuerst täglich und danach wöchentlich die Aufklärung des Vorfalls, die Erkenntnisse und zu treffenden Massnahmen besprochen, priorisiert und koordiniert hat. Dazu wurde ein hoher Personalaufwand eingesetzt. Die Zusammenarbeit und Koordination mit anderen involvierten Stellen, insbesondere mit Xplain, dem NCSC und dem BAZG erfolgte, soweit der EDÖB dies beurteilen kann, professionell und zielgerichtet. Die Aufklärung des Vorfalls führte dazu, dass das fedpol 106 IT-Massnahmen eingeleitet hat.
- ^{147.} Die Einleitung von 106 IT-Massnahmen zeigt eindrücklich auf, wie gewissenhaft der Vorfall aufgearbeitet wurde, womit die festgestellten M\u00e4ngel im Bereich Datensicherheit nach Treu und Glauben bestm\u00f6glich korrigiert wurden. Die Einleitung von 106 IT-Massnahmen nach dem Vorfall zeigt aber auch auf, dass zahlreiche notwendige technische und organisatorische Massnahmen nicht vorhanden waren.

4.10. Abschliessende Bemerkungen

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, wobei eneX-stationär von fedpol nicht eingesetzt wurde. 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 von fedpol oder anderen Behörden geführt werden. Nicht für alle Personendaten, die aus fedpol Datenbanken in die IT-Infrastruktur von Xplain übermittelt wurden, liegt die datenschutzrechtliche Verantwortung bei fedpol. Hat beispielsweise eine kantonale Polizeibehörde über eneXs-mobile auf eine fedpol Datenbank eine Abfrage durchführen wollen bzw. wurde dabei eine Fehlermeldung generiert und an Xplain übermittelt, hatte fedpol mit dieser Bearbeitung von



- Personendaten keinen direkten Bezug bzw. Einfluss, da fedpol lediglich die Abfrage für die kantonale Polizeibehörde ermöglicht hat. Dabei muss auch festgehalten werden, dass Übermittlung von Fehlermeldungen über den FTP-Server bei der Bundesverwaltung nicht möglich waren und nur von anderen Behörden erfolgen konnten (siehe Ziffer 41).
- Der EDÖB stellte fest, dass ein anderes Bundesamt die offensichtlich datenschutzwidrige Supportfunktion der Standardanwendung (wie in ORMA) im Jahr 2020 feststellte und Xplain mitteilte. Spätestens 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 produktiven Daten bei Xplain oder die Sicherung der Daten durch angemessene organisatorische und technische Massnahmen.



5. Empfehlungen

- 150. Gestützt auf Art. 29 Abs. 3 aDSG erlässt der EDÖB gegenüber dem fedpol die nachfolgenden Empfehlungen.
- Die Auftragsdatenbearbeitung wurde nicht klar geregelt. Die datenschutzrechtlichen Risiken in der Zusammenarbeit mit Xplain werden erheblich minimiert, indem sich die Parteien die Datenübertragungen bewusst machen, ob bzw. unter welchen Voraussetzungen Personendaten die IKT-Systeme des Bundes verlassen dürfen (siehe Ziffer 84 ff.). In diesem Sinne ist die Auftragsdatenbearbeitung zu konkretisieren.

Empfehlungen:

- Unter Beachtung datenschutzrechtlicher Risiken wird geprüft, ob bzw. unter welchen Voraussetzungen es erforderlich ist, dass Personendaten im Rahmen von Supportprozessen 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 Personendaten 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.
 - 1b) Ist es erforderlich, dass im Rahmen von Supportprozessen vereinzelt Personendaten 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 umzusetzen.
- 2. Die Datenübertragungen gemäss vorangehender Ziffer sind in klaren vertraglichen Vereinbarungen festzuhalten.
- Bei der Entscheidung zur weiteren Zusammenarbeit im Bereich der inneren Sicherheit sind datenschutzrechtliche Kriterien zu berücksichtigen (siehe Ziffer 84). Die datenschutzrechtlichen Prozesse und deren Einhaltung sind regelmässig zu überwachen (siehe Ziffer 107 f.)

Empfehlungen:

- 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.
- Die datenschutzrechtlichen Prozesse und deren Einhaltung werden regelmässig kontrolliert, indem interne oder externe Kontrollen durchgeführt werden oder ein Nachweis zur Einhaltung eingefordert wird.



^{153.} In Bezug auf den Support und Wartung (siehe Ziffer 124 ff.) sowie auf die Implementierung einer Anwendung, die bereits von einem anderen Bundesamt verwendet wird (siehe Ziffer 106).

Empfehlung:

- 5. Die Mitarbeitenden werden kontinuierlich auf die datenschutzrechtlichen Risiken sensibilisiert.
- 6. Die Verträge werden im Bereich Datensicherheit präzisiert und wo notwendig vereinheitlicht.
- 7. Wird eine Anwendung implementiert, die bereits von einem anderen Bundesamt verwendet wird, ist mindestens eine eigene SCHUBAN durchzuführen.



6. Verfahren

6.1. Rechtliches Gehör und weiteres Vorgehen

- Dem fedpol wurde die Möglichkeit gegeben, den Sachverhalt zu prüfen und dazu Stellung zu nehmen. Mit Schreiben vom 21. März 2024 hat fedpol davon Gebrauch gemacht.
- Der vorliegende Schlussbericht weist aufgrund des Sachverhalts einen engen Zusammenhang zu den beiden Schlussberichten des EDÖB in Bezug auf das BAZG 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.
- Dem fedpol wird eine Frist von 30 Tagen ab Erhalt des Schlussberichts angesetzt, um sich darüber zu äussern, ob sie die Empfehlungen gemäss vorangehender Ziffer 150 ff. annehmen oder ablehnen.

6.2. Veröffentlichung des Schlussberichts mit Empfehlungen

- 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.
- ^{158.} Der Schlussbericht fedpol wird deshalb zusammen mit den Schlussberichten vom BAZG und Xplain auf der Webseite des EDÖB veröffentlicht (www.edoeb.admin.ch).
- Dem fedpol wurde die Gelegenheit gegeben, Schwärzungen des Sachverhalts zu beantragen, um eigene Interessen zu schützen. Mit Eingabe vom 12. April 2024 machte fedpol davon Gebrauch.

die stellvertretende Beauftragte:	der zuständige Jurist:
Florence Henguely	Nicolas Winkelmann
der zuständige Informations- und Sicherheitsspezialist	der beigezogene Experte
Michael Burger	Bruno Baeriswyl



7. Anhang 1: Wichtigste Dokumente

Die nachfolgende Tabelle enthält eine Übersicht der wichtigsten erhaltenen Dokumente, die geprüft und gegebenenfalls referenziert wurden.

ID	Format	Dateiname
[1]	PDF	20230616. [814437927] Fedpol, Bern.20230616. Databreach. Breachmanager.pdf
[2]	PDF	20230712. MM_Hackerangriff auf die Firma Xplain_ Auszug aus Informationssystem HOOGAN von 2015 im Darknet publiziert - Betroffene werden informiert.pdf
[3]	E-Mail	20240201. fedpol an EDÖB. Foliensätze Präsentation.msg
[4]	PowerPoint	Auswertung Logfiles_eneXs.pptx
[5]	PowerPoint	20240131_EO INTER_FGG2_EDÖB.pptx
[6]	PDF	20240322. fedpol an EDÖB. Stellungnahme Sachverhaltsfeststellung.pdf
[7]	PDF	01 20240129_Antwortschreiben an EDÖB Zusätzliche Unterlagen und Auskünfte.pdf
[8]	PDF	Beilage _1_Nachmeldung Databreach_fedpol_20240129.pdf
[9]	PDF	Beilage_10_euLISA_2023-08-08_Updated_Notification_Ransom-ware_cyberattack_against_the_company_Xplain_in_Switzerland.pdf
[10]	PDF	Beilage_12a_Vorlage_Brief_betroffen_HOOGAN_DE_V4_FINAL.docx
[11]	Word	Beilage_12b_Vorlage_Brief_nicht_betroffen_HOOGAN_DE_V4_FI-NAL.docx
[12]	PDF	Beilage_1a_Schreiben_GS-EJPD_an_ext_IKT-LE (1).pdf
[13]	PDF	Beilage_1b_CLEAN Schreiben fedpol an ext IKT-Leistungserbrin- ger_DE.pdf
[14]	PDF	Beilage_2_Europol_2023-06-16_Ransomware_cyberat-tack_against_the_company_Xplain.pdf
[15]	PDF	Beilage_4_Interpol_2023-06-16_Ransomware_cyberat-tack_against_the_company_Xplain.pdf
[16]	PDF	Beilage_5_Interpol_2023-08-24_Updated_Notification_Ransom-ware_Cyberattack_against_the_Company_Xplain_in_Switzerland.pdf
[17]	PDF	Beilage_7_euLISA_2023-06-27_Ransomware_cyberat-tack_against_the_company_Xplain.pdf
[18]	PDF	Beilage_8_euLISA_2023-07-07_Ransomware_cyberat-tack_against_the_company_Xplain_in_Switzerland.pdf
[19]	PDF	Beilage_9_European_Data_Protection_2023-07-07_Ransom- ware_cyberattack_against_the_company_Xplain.pdf



ID	Format	Dateiname
[20]	PDF	0316000091 500 PSI ORMA 2018+ Zusatzaufwände 2023 Xplain-sig-sig-sig.pdf
[21]	PDF	0316000091 520 PSI DL Clean ORMA Phase 2 Xplain-sig-sig-sig.pdf
[22]	PDF	0316004366 Vertrag Xplain.pdf
[23]	PDF	10780 HSPD-6 - P041-Hi01 Schutzbedarfsanalyse V1.0 2016.08.25.pdf
[24]	PDF	10780 HSPD-6 - P042-Hi02 ISDS-Konzept V1.12 2016.11.10.pdf
[25]	PDF	10780 HSPD-6- Si001-Hi01 IKT-Grundschutz V1.0 2016.11.02.pdf
[26]	PDF	2002-04-26 403.000-1.pdf
[27]	PDF	2003-07-28 Pflichtenheft IPAS-ORMA_1.2.pdf
[28]	PDF	2007-07-03 403.000-2.pdf
[29]	PDF	2007-07-06 403.000-2.1.pdf
[30]	PDF	2011-07-07 VT Xplain fedpol Nr. 40311060850 sw unterschr.pdf
[31]	PDF	2013-02-05 403.000-1.1.pdf
[32]	PDF	2014-02-05 403.000-1.2.pdf
[33]	PDF	2014-11-27 VT ORMA - Xplain fedpol unterschr.pdf
[34]	PDF	20230606 Rapport Nr 0 EO INTER.pdf
[35]	PDF	20230606 Rapport Nr 1 EO INTER.pdf
[36]	PDF	20230607 Rapport Nr 2 EO INTER.pdf
[37]	PDF	20230608 Rapport Nr 3 EO INTER.pdf
[38]	PDF	20230609 Rapport Nr 4 EO INTER.pdf
[39]	PDF	20230610 Rapport Nr 5 EO INTER.pdf
[40]	PDF	20230611 Rapport Nr 6 EO INTER.pdf
[41]	PDF	20230612 Rapport Nr 7 EO INTER.pdf
[42]	PDF	20230613 Rapport Nr 8 EO INTER.pdf
[43]	PDF	20230614 Rapport Nr 9 EO INTER.pdf
[44]	PDF	20230615 Rapport Nr 10 EO INTER.pdf
[45]	PDF	20230616 Rapport Nr 11 EO INTER.pdf
[46]	PDF	20230619_Rapport Nr 12 EO INTER.pdf



ID	Format	Dateiname
[47]	PDF	20230622 Rapport Nr 13 EO INTER.pdf
[48]	PDF	20230626 Rapport Nr 14 EO INTER.pdf
[49]	PDF	20230629 Rapport Nr 15 EO INTER.pdf
[50]	PDF	20230706 Rapport Nr 16 EO INTER.pdf
[51]	PDF	20230713 Rapport Nr 17 EO INTER.pdf
[52]	PDF	20230717 Rapport Nr 18 EO INTER.pdf
[53]	PDF	20230720 Rapport Nr 19 EO INTER.pdf
[54]	PDF	20230727 Rapport Nr 20 EO INTER.pdf
[55]	PDF	20230803 Rapport Nr 21 EO INTER.pdf
[56]	PDF	20230810 Rapport Nr 22 EO INTER.pdf
[57]	PDF	20230817 Rapport Nr 23 EO INTER.pdf
[58]	PDF	20230824 Rapport Nr 24 EO INTER.pdf
[59]	PDF	20230831 Rapport Nr 25 EO INTER.pdf
[60]	PDF	20230907 Rapport Nr 26 EO INTER.pdf
[61]	PDF	20230914 Rapport Nr 27 EO INTER.pdf
[62]	PDF	310000327 ORMA Leistungspaket 2014 (Abruf 40311060850) Xplain.pdf
[63]	PDF	316000091 460 Einzelvertrag ORMA 2018+ Zusatzaufwände 2022 Xplain.pdf
[64]	PDF	316000091 470 Einzelvertrag CleanOrma Phase 2 2022 Xplain.pdf
[65]	PDF	316000091 480 Einzelvertrag ORMA Optimierungspaket SIENA Xplain.pdf
[66]	PDF	316000091 490 Einzelvertrag ORMA Schnittstelle PKS für 2022 Xplain.pdf
[67]	PDF	316000091 Abruf Option 2015 aus Vertrag vom 27112014.pdf
[68]	PDF	316000091 Abruf Option 2016 aus Vertrag.pdf
[69]	PDF	316000091 Einzelvertrag ORMA 2018+ Phase 2 Xplain.pdf
[70]	PDF	316000091 Nachtrag1 Xplain.PDF
[71]	PDF	316000091 Nachtrag2 Xplain.pdf
[72]	PDF	316000179 EP+ Release 2.0 Xplain.pdf



ID	Format	Dateiname
[73]	PDF	316001317 - WartungSupportvertrag BBL (Xplain).pdf
[74]	PDF	- WartungSupportvertrag Xplain.pdf
[75]	PDF	316001545 Werkvertrag für Life-Cycle Massnahmen fedpol Kleinapplikationen Xplain.pdf
[76]	PDF	316001855 Schnittstelle IPMail - ORMA Xplain.pdf
[77]	PDF	316002289 Dienstleistungen für mittelfristige Massnahmen Kleinapplikationen Xplain.pdf
[78]	PDF	316002311 EP-Plus Erweiterung für die Erfassung von Observationen GUSM Xplain.pdf
[79]	PDF	316002313 Betriebs- und Supportleistungen im Bereich ORMA Xplain.pdf
[80]	PDF	316002591 Dienstleistungen Erweiterungen Import HSDP-6 Xplain.pdf
[81]	PDF	316002783 Schnittstelle IPMail - Orma Xplain.pdf
[82]	PDF	316003157 Dienstleistungen Softwareanpassungen im Bereich ORMA Xplain.pdf
[83]	PDF	316003973 Dienstleistungen HSPD-6 - Windows 10 Xplain.pdf
[84]	PDF	316004097 Dienstleistungen ORMA Upgrade 2018+ Xplain.pdf
[85]	PDF	316004097 Nachtrag Nr. 1 Dienstleistungen ORMA Upgrade 2018+ Xplain.pdf
[86]	PDF	316006002 Los 4 eDocument Reader Xplain.pdf
[87]	PDF	316007876 Kleinapplikationen Xplain.pdf
[88]	PDF	316008195 ineXs mobile AFIS Lizenzen Xplain.pdf
[89]	PDF	316008704 OPGKBKP Lizenzen Xplain.pdf
[90]	PDF	4678 Bund übrige IKT Vertr"ge Xplain AG Interlaken 2015 0316000091 ORMA Betriebs Support Systemkomponenten.pdf
[91]	PDF	4678 ORMA - P041-Hi01 Schutzbedarfsanalyse V1.0 2016.08.29.pdf
[92]	PDF	4678 ORMA - P042-Hi02 ISDS-Konzept V2.0 2019.03.28.pdf
[93]	PDF	4678 ORMA - Si001-Hi01 IKT-Grundschutz V1.0 2016.08.28.pdf
[94]	PDF	Beilage 2_RIPOL-B - P042-Hi02 ISDS-Konzept V7.0 2020.07.14.pdf
[95]	PDF	Beilage 3_RIPOL-B - P041-Hi01 Schutzbedarfsanalyse V6.2 2020.07.14.pdf



ID	Format	Dateiname
[96]	PDF	Beilage 4_RIPOL-B - P042-Hi02 Risikoanalyse V1.0 2020.07.03.pdf
[97]	PDF	ISDS Konzept OPGKBKP vom 3.3.2017.pdf
[98]	PDF	K12-1280_2012-07-26 fedpol Xplain IKTDL40312071652 DL im Projekt Hoogan und Zutrittskontrolle Pilot 3100070 v.1.0.pdf
[99]	PDF	Nachtrag Nr. 1 zu Rahmenvertrag ORMA 0316000091.PDF
[100]	PDF	OPGKBKP - IKT-Grundschutz-sig-sig.pdf
[101]	PDF	OPGKBKP - Schutzbedarfsanalyse.pdf
[102]	PDF	Opt. 1 - Besondere Vereinbarungen.pdf
[103]	PDF	Opt. 1 - Spezifikationsblatt ASSA - Vertragsurkunde 403.000-1 - Kündigung.pdf
[104]	PDF	Opt. 1 - Spezifikationsblatt ASSA - Vertragsurkunde 403.000-1.pdf
[105]	PDF	Opt. 1 - Spezifikationsblatt JANUS EP+.pdf
[106]	PDF	Opt. 1 - Spezifikationsblatt OPGKBKP.pdf
[107]	PDF	Opt. 1 - Spezifikationsblatt ORMA.pdf
[108]	PDF	Opt. 1 - Vertragsurkunde 403.000-2.pdf
[109]	PDF	PKS - P041-Hi01 Schutzbedarfsanalyse V4.0 2016.11.03.pdf
[110]	PDF	PKS - P042-Hi02 ISDS-Konzept V0.92 2018.06.12.pdf
[111]	PDF	PKS - Si001-Hi01 IKT-Grundschutz V1.0 2016.07.20.pdf
[112]	PDF	RPO-120911-1 Hoogan vFix.pdf
[113]	PDF	RPO-120911-2 Hoogan vMob Panasonic.pdf
[114]	Excel	Übersicht Verträge Xplain.xlsx
[115]	Word	20240131 Protokoll_Sitzung EDÖB bez. Fehlerprotokollmeldungen.docx
[116]	PDF	20231116. NCSC – Bericht Cybervorfall bei der Firma Xplain
[117]	PDF	20240307. NCSC - Bericht zu den Datenanalysen nach dem Cyberangriff auf die Firma Xplain.pdf



8. Anhang 2: Glossar

Stichwort	Beschreibung
AV	Anwendungsverantwortlicher einer Applikation. Dieser stellt den Unterhalt und die Weiterentwicklung sowie den sicheren und wirtschaftlichen Betrieb gemäss den entsprechenden Anforderungen und Vereinbarungen sicher.
BAB-Client	Bundes-Standard-Büroautomations-Client.
Backup	Eine Sicherungskopie von Daten oder Systemen, die zur Wiederherstellung im Falle eines Datenverlusts oder einer Systemstörung erstellt wird.
BASE64	Ein Kodierungsverfahren zur Umwandlung von Binärdaten in einen ASCII-Text, häufig verwendet für die sichere Übertragung von Daten über unsichere Kanäle.
BJ	Bundesamt für Justiz.
Build-Pipeline	Ein automatisierter Prozess zur Kompilierung, Testung und Bereitstellung von Softwarecode, der die Entwicklungszyklen beschleunigt.
Build-Umge- bung	Die Infrastruktur und Werkzeuge, die für das Kompilieren und Erstellen von Softwareprojekten benötigt werden.
Cache	Ein schneller Speicherbereich, der häufig verwendete Daten temporär speichert, um den Zugriff zu beschleunigen.
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EZV	Eidgenössische Zollverwaltung
FAT-Clients	FAT-Clients sind Computer, die lokal über umfassende Ressourcen und Anwendungen verfügen, im Gegensatz zu Thin Clients, die von zentralen Servern abhängig sind.
fedpol	Bundesamt für Polizei.
File-Server	Ein Server, der Dateien und Ressourcen für Benutzer in einem Netzwerk bereitstellt und verwaltet.
Firewall	Ein Sicherheitssystem, das den Datenverkehr zwischen einem internen Netzwerk und externen Netzwerken überwacht und reguliert.
FTP-Server	Ein Server, der den File Transfer Protocol (FTP) Dienst bereitstellt, um Dateien zwischen Computern über ein Netzwerk zu übertragen.
GWK	Grenzwachtkorps. Aufgrund der Transformation der Eidgenössischen Zollverwaltung (EZV) zum neuen Bundesamt für Zoll und Grenzsicherheit (BAZG) wird der Begriff «Grenzwachtkorps» nicht mehr verwendet.
Hashwert	Wird bspw. eine Datei aus dem Internet heruntergeladen, stellt der Hashwert dieser Datei sicher, dass es sich um das Original und keine manipulierte Datei handelt, welche Schadsoftware enthalten könnte bzw. während des Downloads manipuliert wurde. Dazu wird einmalig der Hashwert der Original-Datei berechnet und hat damit einen Fingerabdruck der Datei. Ist die Datei heruntergeladen, kann



Stichwort	Beschreibung
	erneut ein Hashwert mit der gleichen Hashfunktion berechnet werden und nun können beide Hashwerte miteinander verglichen werden. Hashfunktionen ermöglichen damit das Aufdecken möglicher Manipulationen. Für den Hashwert wird auch der Begriff "Fingerprint" verwendet. Das symbolisiert die Einzigartigkeit eines jeden Hashwertes, vergleichbar mit der Einzigartigkeit des menschlichen Fingerabdrucks.
Hoster	Ein Unternehmen, das Hosting-Dienste bereitstellt, indem es Serverinfrastruktur und Ressourcen für Websites, Anwendungen oder Daten bereitstellt.
Hyper-V	Hyper-V ist eine Virtualisierungstechnik von Microsoft, die u. a. zur Virtualisierung ganzer Rechenzentren als auch von kleineren Umgebungen eingesetzt werden kann.
ISC-EJPD	Informatik Service Center des EJPD.
ISDS-Konzept	Informationssicherheits- und Datenschutzkonzept
Lateral Move- ment	Unter Lateral Movement versteht man in der Informationssicherheit den Prozess, bei dem ein Angreifer innerhalb eines Netzwerks oder Systems von einem Punkt zum anderen navigiert, um Zugriff auf verschiedene Ressourcen zu erlangen.
NAS	Network Attached Storage (NAS) ist eine dedizierte Datenspeicherlösung, die über ein Netzwerk zugänglich ist.
Patchlevel	Ein Patchlevel ist eine bestimmte Version eines Produkts, die durch eine Reihe von Patches aktualisiert wurde, um Fehler zu beheben und die Stabilität zu verbessern.
P2S	Mit einer Point-to-Site-VPN-Verbindung kann ausgehend von einem Clientcomputer (Point) eine sichere Verbindung mit einem Netzwerk (Site) hergestellt werden.
Port	Ein Port ist ein standardisierter virtueller Punkt, an dem Netzwerkverbindungen beginnen und enden, wobei jedem Port eine Nummer zugewiesen wird.
RAR	RAR ist ein proprietäres Archivdateiformat zur verlustfreien Datenkomprimierung und ist kostenpflichtig. Zum Komprimieren/Dekomprimieren ist die Anwendung «WinRAR» erforderlich.
SCHUBAN	Schutzbedarfsanalyse
SSZ	Eine «Shared Software Zone» ist ein Bereich, in dem mehrere Benutzer oder Systeme gemeinsam auf die gleichen Anwendungen, Dienste oder Ressourcen zugreifen können, was auch eine zentrale Verwaltung und Bereitstellung von Software ermöglicht. Eine SSZ wird üblicherweise in gemeinsam genutzten Infrastrukturen eines Unternehmensnetzwerkes implementiert, um die gemeinsame Nutzung von Software zu erleichtern.
VDI	Virtual Desktop Infrastructure (VDI) ermöglicht es, virtuelle Desktop-Umgebungen zentral zu hosten und Benutzern über das Netzwerk bereitzustellen.
VPN	Ein Virtual Private Network (VPN) schafft eine sichere Verbindung über ein unsicheres Netzwerk, wie das Internet.



Stichwort	Beschreibung
X-Account	Bezeichnet in der Bundesverwaltung Benutzerkonten externer Mitarbeiter.
ZIP	Ein Dateiformat, das die verlustfreie Komprimierung und Archivierung von Daten unterstützt. ZIP ist ein weit verbreitetes Format, darunter auch die integrierte ZIP-Unterstützung von Microsoft Windows und Mac OS X. ZIP-Dateien lassen sich mit jedem Programm öffnen, das ZIP-Dateien erstellen kann.