Untersuchungsorgan der Administrativuntersuchung *«Datenabfluss»*

Organe chargé de l'enquête administrative *«Fuite de données»*

Organo d'inchiesta amministrativa *«Fuga di dati»*

Administrativuntersuchung *«Datenabfluss»*

Bericht

28. März 2024

An die Koordinationsstelle (GS-EFD)

Übersetzung des französischen Originaltextes

Im Falle von Abweichungen zwischen der deutschen und der französischen Fassung ist die französische Fassung massgebend.

INHALTSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

Abkürzung	Definition
aBinfV	Verordnung vom 9. Dezember 2011 über die Informatik und Telekommunikation in der Bundesverwaltung (dieser Text ist nicht mehr in Kraft)
aBinfW	Weisungen vom 23. Februar 2000 des Bundesrats über die Informatik und Telekommunikation in der Bundesverwaltung (dieser Text ist nicht mehr in Kraft)
aCyRV	Verordnung vom 27. Mai 2020 über den Schutz vor Cyberrisiken in der Bundesverwaltung (dieser Text ist nicht mehr in Kraft)
aDSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz (dieser Text ist nicht mehr in Kraft)
aDSV	Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (dieser Text ist nicht mehr in Kraft)
AGB	Allgemeine Geschäftsbedingungen des Bundes
aISchV	Verordnung vom 4. Juli 2007 über den Schutz von Informationen des Bundes (dieser Text ist nicht mehr in Kraft)
aPSPV	Verordnung vom 4. März 2011 über die Personensicherheits-prüfungen (dieser Text ist nicht mehr in Kraft)
armasuisse	Bundesamt für Rüstung
AS	Amtliche Sammlung des Bundesrechts
BA	Bundesanwaltschaft
BACS	Bundesamt für Cybersicherheit
BAZG	Bundesamt für Zoll und Grenzsicherheit
BBL	Bundesamt für Bauten und Logistik
BBl	Bundesblatt
BGA	Bundesgesetz vom 26. Juni 1998 über die Archivierung
BGE	Bundesgerichtsentscheid
BGÖ	Bundesgesetz vom 17. Dezember 2004 über das Öffentlichkeits-prinzip der Verwaltung
BIT	Bundesamt für Informatik und Telekommunikation
BJ	Bundesamt für Justiz
BKB	Beschaffungskonferenz des Bundes
BKP	Bundeskriminalpolizei
BöB	Bundesgesetz vom 21. Juni 2019 über das öffentliche Beschaffungswesen
BPG	Bundespersonalgesetz vom 24. März 2000
BPI	Bundesgesetz vom 13. Juni 2008 über die polizeilichen Informationssysteme des Bundes
BSE	Betriebssicherheitserklärung
BSV	Betriebssicherheitsverfahren
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999

BVGE	Bundesverwaltungsgerichtsentscheid
BVGer	Bundesverwaltungsgericht
BWIS	Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit
CEO	Chief Executive Officer
DSG	Bundesgesetz vom 25. September 2020 über den Datenschutz
DSV	Verordnung vom 31. August 2022 über den Datenschutz
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EFD	Eidgenössisches Finanzdepartement
EFK	Eidgenössische Finanzkontrolle
Einheit	Verwaltungs- oder Organisationseinheit des Bundes
EJPD	Eidgenössisches Justiz- und Polizeidepartement
ELPAG-Verordnung	Verordnung vom 23. September 2016 über das elektronische Personen-, Akten- und Geschäftsverwaltungssystem des Bundesamtes für Justiz
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten, abgeschlossen in Rom am 4. November 1950
ESTV	Eidgenössische Steuerverwaltung
fedpol	Bundesamt für Polizei
FUB	Führungsunterstützungsbasis
GA	Geschäfts- und Aktenverwaltung
GS	Generalsekretariat
GS-EFD	Generalsekretariat des Eidgenössischen Finanzdepartements
GWK	Grenzwachtkorps
IKT	Informations- und Kommunikationstechnologien
IPAS	Informatisiertes Personennachweis-, Aktennachweis- und Verwaltungssystem des Bundesamtes für Polizei
IPAS-Verordnung	Verordnung vom 15. Oktober 2008 über das informatisierte Personennachweis-, Aktennachweis- und Verwaltungssystem im Bundesamt für Polizei
IRB	Informatikrat des Bundes
ISBO	Informatiksicherheitsbeauftragter der Organisationseinheit
ISC-EJPD	Informatik Service Center ISC-EJPD
ISDS-Konzept	Informationssicherheits- und Datenschutzkonzept
ISG	Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit beim Bund
ISV	Verordnung vom 8. November 2023 über die Informationssicherheit in der Bundesverwaltung und der Armee
Janus	Elektronisches Informationssystem der Bundeskriminalpolizei
JANUS-Verordnung	Verordnung vom 30. November 2001 über das Informationssystem der Bundeskriminalpolizei
JORASYS	Journal- und Rapportsystem der Militärpolizei

Kdo Cy	Kommando Cyber
Kdo Op	Kommando Operationen
MG	Bundesgesetz vom 3. Februar 1995 über die Armee und die Militärverwaltung
MIG	Bundesgesetz vom 3. Oktober 2008 über militärische und andere Informationssysteme im VBS
MIV	Verordnung vom 16. Dezember 2009 über militärische und andere Informationssysteme im VBS
MP	Militärpolizei
NCS	Nationale Cyberstrategie
NCSC	Nationales Zentrum für Cybersicherheit
NDB	Nachrichtendienst des Bundes
NDG	Bundesgesetz vom 25. September 2015 über den Nachrichtendienst
NES	Nationales Ermittlungssystem
NES-Verordnung	Verordnung vom 15. Oktober 2008 über das Nationale Ermittlungssystem
OA	OBERSON ABELS AG
OR	Bundesgesetz vom 30. März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches
Org-VöB	Verordnung vom 24. Oktober 2012 über die Organisation des öffentlichen Beschaffungswesens der Bundesverwaltung
PAGIRUS-Verordnung	Verordnung vom 16. Dezember 2009 über das Personen-, Akten- und Geschäftsverwaltungssystem PAGIRUS des Bundesamtes für Justiz
ParlG	Bundesgesetz vom 13. Dezember 2002 über die Bundesversammlung
PPS	Planung, Projektsteuerung und Standardisierung der Polizeilichen Informationsverarbeitung (Einheit, die bis Ende 2008 fedpol angehörte)
PSP	Personensicherheitsprüfung
RVOG	Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997
RVOV	Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998
SEM	Staatssekretariat für Migration
SEPOS	Staatssekretariat für Sicherheitspolitik
SHAB	Schweizerisches Handelsamtsblatt
SR	Systematische Sammlung des Bundesrechts
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937
TOMs	Technische und organisatorische Massnahmen des Datenschutzes
VASS	Verwaltung von Asservaten, Spuren und Spurenträgern

VBNIB	Verordnung vom 22. Februar 2012 über die Bearbeitung von Personendaten und Daten juristischer Personen bei der Nutzung der elektronischen Infrastruktur des Bundes
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
VBSV	Verordnung vom 8. November 2023 über das Betriebssicherheits-verfahren
VDTI	Verordnung vom 25. November 2020 über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung
VPSP	Verordnung vom 8. November 2023 über die Personensicherheits-prüfungen
VwVG	Bundesgesetz vom 20. Dezember 1968 über das Verwaltungs-verfahren
Xplain	Xplain AG
ZEMIS	Zentrales Migrationsinformationssystem
ZEMIS-Verordnung	Verordnung vom 12. April 2006 über das Zentrale Migrationsinformationssystem
ZGB	Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907

I. ZUSAMMENFASSUNG

FR (Anm. d. Übers.: siehe unten für die deutsche Fassung)

L'enquête administrative *« Fuite de données »* s'est déroulée entre le 1er septembre 2023 et le 28 mars 2024.

A la suite de la publication sur le darknet en juin 2023 de données dérobées à l'entreprise Xplain SA (ci-après « Xplain »), qui comprenaient des données de la Confédération, le Conseil fédéral a ordonné le 23 août 2023 l'ouverture d'une enquête administrative. L'enquête s'étendait à tous les départements et à la Chancellerie fédérale.

Notre étude OBERSON ABELS SA a été désignée comme organe chargé de l'enquête.

L'enquête visait d'abord à déterminer les circonstances, du côté de l'administration fédérale, qui ont permis à Xplain d'entrer en possession de données productives de ladite administration[1].

L'organe chargé de l'enquête devait ensuite déterminer (i) si des déficiences en matière technique, d'organisation ou de processus ont conduit à ce que des données productives de l'administration fédérale soient en possession de Xplain et (ii) si l'administration fédérale a satisfait à ses devoirs de manière adéquate lors du choix, de l'instruction et de la surveillance de Xplain ainsi que dans le cadre de la collaboration avec celle-ci.

Enfin, l'organe chargé de l'enquête devait évaluer de manière approfondie les problèmes identifiés indépendamment du cas Xplain et élaborer des solutions et des recommandations visant à réduire les

[1] Nous avons défini dans ce rapport les « données productives » de la Confédération comme suit : « données réelles issues des systèmes d'information de la Confédération, par opposition aux données tests ou anonymisées ».

risques pour la sécurité. Il n'était toutefois pas attendu que l'organe d'enquête procède à un examen technique de l'informatique.

Au terme de l'enquête, nous parvenons aux conclusions suivantes.

Un département et 11 unités administratives de trois autres départements[2] sont touchés par l'enquête :

Département fédéral des affaires étrangères (DFAE) ;

Commandement des Opérations (cdmt Op), auquel appartient la Police militaire (PM),

Office fédéral de l'armement (armasuisse) ;

Base d'aide au commandement (BAC) ;

Centre de services informatiques CSI-DFJP (CSI-DFJP) ;

Office fédéral de la police (fedpol) ;

Office fédéral des constructions et de la logistique (OFCL) ;

Office fédéral de la douane et de la sécurité des frontières (OFDF) ;

Office fédéral de l'informatique et de la télécommunication (OFIT) ;

Office fédéral de la justice (OFJ) ;

Secrétariat d'Etat aux migrations (SEM) ;

Service de renseignement de la Confédération (SRC).Parmi les Unités touchées par l'enquête, les unités suivantes (« Unités directement concernées ») utilisaient dans l'environnement informatique de la Confédération des produits développés par Xplain dans lesquels leurs données étaient traitées : fedpol, OFDF, OFJ, PM et SEM.

Les circonstances factuelles qui ont conduit à ce que des données productives de certaines unités de la Confédération soient présentes dans l'environnement informatique de Xplain peuvent être résumées comme suit :

Premièrement, des employés de Xplain ont envoyé, depuis le compte e-mail de la Confédération mis à leur disposition dans le cadre de la collaboration entre Xplain et une Unité directement concernée, vers leur compte e-mail auprès de Xplain ou vers le compte e-mail de leurs collègues auprès de Xplain, des données productives reçues d'employés de la Confédération. Dans un cas à tout le moins, un employé de Xplain a selon toute vraisemblance extrait lui-même des données d'un système de production de fedpol et ces données se sont ensuite trouvées dans l'environnement informatique de Xplain.

Deuxièmement, des employés de la Confédération en charge du support informatique interne ont traité des demandes d'utilisateurs contenant des données productives et les ont transmises à Xplain ou les ont mises à disposition de Xplain sur un serveur partagé, sans préalablement retirer, pseudonymiser ou caviarder les données productives.

Troisièmement, des employés de la Confédération participant à des travaux de développement, de test ou de migration informatique, ont transmis à Xplain des données productives dans le cadre de ces travaux.

[2] DFJP, DFF, DDPS.

Nous ne pouvons pas définitivement exclure l'existence d'autres canaux ayant conduit à la présence de données productives de la Confédération dans l'environnement informatique de Xplain. Par ailleurs, l'enquête a permis d'identifier des situations dans lesquelles des données productives de la Confédération sont parvenues dans l'environnement informatique de Xplain, sans que ces données ne se trouvent sur le darknet en juin 2023.

Les cas de transmission de données productives à Xplain apparaissent **isolés**, d'une part, à l'échelle de la correspondance entre Xplain et les Unités touchées par l'enquête et, d'autre part, à l'échelle de la correspondance entre Xplain et chaque employé de la Confédération ou chaque employé de Xplain ayant transmis à une occasion au moins des données productives à Xplain.

Toutefois, comme l'illustrent les cas examinés dans ce rapport, en matière de sécurité de l'information et de protection des données, **un seul transfert à un tiers suffit potentiellement** :

- Pour que la sécurité de l'information et la protection des données soient compromises.
- Pour que des volumes importants de données soient en mains d'un tiers.
- Pour que des données sensibles ou classifiées soient en mains d'un tiers.

Les principales **déficiences** mises en évidence par l'enquête administrative sont les suivantes.

Premièrement, une déficience en termes de **processus** : des employés de la Confédération et des employés d'un fournisseur externe, Xplain, ont pu extraire des données de systèmes de production de la Confédération et envoyer ces données par e-mail à Xplain sans qu'un processus n'encadre apparemment ces démarches et, en particulier, sans que le principe des quatre yeux ne soit respecté à chaque étape.

Deuxièmement, une déficience en termes de **technique** : aucune mesure technique n'est venue faire obstacle aux extractions de données productives précitées, ni à l'envoi par e-mail de données productives vers un fournisseur externe.

Troisièmement, les cas décrits dans ce rapport mettent en lumière un déficit en termes de **formation et de sensibilisation** des personnes appelées à traiter des données des systèmes en question au sein de la Confédération. En outre, après qu'une unité a identifié une fonctionnalité conduisant potentiellement à des flux de données productives dans le cadre de demandes de support, l'information n'apparaît pas avoir circulé entre les Unités directement concernées.

Sous l'angle de la **sécurité de l'information**, nous parvenons à la conclusion que, dans les relations des Unités directement concernées avec Xplain avant la fuite de données de juin 2023, la Confédération a partiellement rempli ses devoirs de choisir avec soin et d'instruire adéquatement. En revanche, le devoir de surveiller n'a pas été rempli dans ce contexte.

Sous l'angle de la **protection des données personnelles**, nous parvenons à la conclusion que, dans les cas de sous-traitance à Xplain qui ont été identifiés, la Confédération n'a pas rempli ses devoirs de choisir avec soin, d'instruire adéquatement et de surveiller.

Les cas de transmission de données productives à Xplain et les violations retenues par l'organe d'enquête, du côté de la Confédération, aux devoirs de choisir avec soin, instruire adéquatement et surveiller sont intervenus dans un **contexte** qui les a favorisés, mais non causés :

Sous l'angle de la gestion des cybermenaces des tiers, les Unités touchées par l'enquête paraissent avoir **sous-estimé**, pour certaines jusqu'à la fuite de données de juin 2023, les risques posés par des tiers, notamment les fournisseurs de logiciels.

L'enquête révèle des compréhensions parfois divergentes de la **répartition des responsabilités** en matière de sécurité de l'information entre, suivant les situations, (i) le service d'achat central, (ii) le service demandeur, (iii) le département auquel le service demandeur appartient, (iv) le CSI-DFJP, (v) l'OFIT, (vi) voire entre certains collaborateurs d'un même service.

Un consensus se dégage des interrogatoires selon lequel les ressources allouées à la sécurité de l'information au sein des Unités directement concernées étaient globalement **insuffisantes**.

L'enquête révèle une situation de **dépendance** des Unités directement concernées à l'égard de Xplain au cours des années sous enquête.

La relation entre Xplain et les Unités directement concernées semblent avoir reposé essentiellement sur la **confiance**.

Les enseignements tirés de la présente enquête administrative appellent à notre sens des recommandations tant sur le plan organisationnel, que sur le fond. Ces **recommandations** sont exposées au chapitre VI.B.

DE

Die Administrativuntersuchung «Datenabfluss» fand zwischen dem 1. September 2023 und dem 28. März 2024 statt.

Nachdem im Juni 2023 im Darknet Daten veröffentlicht worden waren, die der Firma Xplain AG («Xplain») entwendet worden waren und die auch Daten des Bundes enthielten, ordnete der Bundesrat am 23. August 2023 die Eröffnung einer Administrativuntersuchung an. Die Untersuchung erstreckte sich auf alle Departemente und die Bundeskanzlei.

Unsere Kanzlei OBERSON ABELS AG wurde als Untersuchungsorgan beauftragt.

Die Administrativuntersuchung sollte zunächst aufzeigen, welche Umstände es auf Seiten der Bundesverwaltung ermöglicht haben, dass Xplain in den Besitz von produktiven Daten der Bundesverwaltung kam.[3]

Das Untersuchungsorgan hatte ferner zu klären, (i) ob technische, organisatorische oder prozesshafte Mängel dazu geführt haben, dass Produktivdaten der Bundesverwaltung im Besitz von Xplain waren und (ii) ob die Bundesverwaltung bei der Auswahl, Instruktion und Überwachung der Xplain sowie bei der Zusammenarbeit mit dieser Firma die Pflichten angemessen erfüllt hat.

Schliesslich sollte das Untersuchungsorgan die unabhängig vom Fall Xplain erkannten Probleme vertieft beurteilen sowie Lösungsansätze und Empfehlungen zur Reduktion der Sicherheitsrisiken erarbeiten. Es wurde jedoch nicht erwartet, dass das Untersuchungsorgan eine technische Informatikprüfung durchführt.

Nach Abschluss der Untersuchung kommen wir zu den folgenden Schlussfolgerungen.

Ein Departement und 11 Verwaltungseinheiten aus drei weiteren Departementen[4] sind von der Untersuchung betroffen:

Eidgenössisches Departement für auswärtige Angelegenheiten (EDA)

Kommando Operationen (Kdo Op), dem die Militärpolizei (MP) angehört

Bundesamt für Rüstung (armasuisse)

Führungsunterstützungsbasis (FUB)

Informatik Service Center ISC-EJPD

Bundesamt für Polizei (fedpol)

Bundesamt für Bauten und Logistik (BBL)

Bundesamt für Zoll und Grenzsicherheit (BAZG)

Bundesamt für Informatik und Telekommunikation (BIT)

Bundesamt für Justiz (BJ)

Staatssekretariat für Migration (SEM)

Nachrichtendienst des Bundes (NDB)

[3] Wir haben in diesem Bericht die «produktiven Daten» der Bundesverwaltung wie folgt definiert: «tatsächliche Daten aus den Informationssystemen des Bundes, im Gegensatz zu Testdaten oder anonymisierten Daten».
[4] EJPD, EFD, VBS.

Von den von der Untersuchung betroffenen Einheiten nutzten die folgenden Einheiten («direkt betroffene Einheiten») in der IT-Umgebung des Bundes von Xplain AG entwickelte Produkte, in denen ihre Daten verarbeitet wurden: fedpol, BAZG, BJ, MP und SEM.

Die tatsächlichen Umstände, die dazu führten, dass Produktivdaten von bestimmten Verwaltungseinheiten in der IT-Umgebung von Xplain vorhanden waren, lassen sich wie folgt zusammenfassen:

> Erstens haben Mitarbeiter von Xplain vom E-Mail-Konto des Bundes, das ihnen im Rahmen der Zusammenarbeit zwischen Xplain und einer direkt betroffenen Einheit zur Verfügung gestellt wurde, an ihr E-Mail-Konto bei Xplain oder an das E-Mail-Konto ihrer Kollegen bei Xplain produktive Daten versendet, die sie von Mitarbeitern des Bundes erhalten haben. Zumindest in einem Fall hat ein Mitarbeiter von Xplain aller Wahrscheinlichkeit nach selbst Daten aus einem Produktionssystem von fedpol extrahiert, und diese Daten sind dann in die IT-Umgebung von Xplain gelangt.
>
> Zweitens bearbeiteten Mitarbeiter vom Bund, die für den internen IT-Support zuständig waren, Nutzeranfragen, die Produktivdaten enthielten, und leiteten sie an Xplain weiter oder stellten sie Xplain auf einem gemeinsam genutzten Server zur Verfügung, ohne die Produktivdaten zuvor zu entfernen, zu pseudonymisieren oder zu schwärzen.
>
> Drittens: Mitarbeiter des Bundes, die an IT-Entwicklungs-, Test- oder Migrationsarbeiten beteiligt waren, übermittelten Xplain im Rahmen dieser Arbeiten Produktivdaten.

Wir können nicht endgültig ausschliessen, dass es andere Kanäle gab, die dazu geführt haben, dass Produktivdaten des Bundes in der IT-Umgebung von Xplain vorhanden waren. Darüber hinaus wurden im Rahmen der Untersuchung Situationen identifiziert, in denen Produktivdaten des Bundes in die IT-Umgebung von Xplain gelangt sind, ohne dass sich diese Daten im Juni 2023 im Darknet befanden.

Die Fälle, in denen Produktivdaten an Xplain übermittelt wurden, erscheinen isoliert, einerseits auf der Ebene der Korrespondenz zwischen Xplain und den von der Untersuchung betroffenen Verwaltungseinheiten und andererseits auf der Ebene der Korrespondenz zwischen Xplain und jedem Mitarbeiter des Bundes oder jedem Mitarbeiter von Xplain, der mindestens einmal Produktivdaten an Xplain übermittelt hat.

Wie die in diesem Bericht untersuchten Fälle zeigen, reicht in Bezug auf Informationssicherheit und Datenschutz jedoch potenziell eine einzige Weitergabe an einen Dritten aus:

- um die Informationssicherheit und den Datenschutz zu gefährden.
- damit grosse Datenmengen in die Hände eines Dritten gelangen.
- damit besonders schützenswerte oder klassifizierte Daten in die Hände eines Dritten gelangen.

Im Folgenden werden die wichtigsten Mängel aufgeführt, die im Rahmen der Administrativuntersuchung festgestellt wurden.

> Erstens, ein Prozessmangel: Angestellte des Bundes und Angestellte eines externen Lieferanten, Xplain, konnten Daten aus Produktionssystemen des Bundes extrahieren und per E-Mail an Xplain senden, ohne dass es offensichtlich einen Prozess für diese Schritte gab und insbesondere ohne, dass das Vier-Augen-Prinzip bei jedem Schritt beachtet wurde.
>
> Zweitens, ein Mangel in technischer Hinsicht: Es gab keine technischen Massnahmen, die die oben genannten Extraktionen von Produktivdaten oder das Versenden von Produktivdaten per E-Mail an einen externen Anbieter verhinderten.

Drittens zeigen die in diesem Bericht beschriebenen Fälle ein Defizit in Bezug auf die **Ausbildung und Sensibilisierung** der Personen auf, die innerhalb des Bundes Daten aus den fraglichen Systemen bearbeiten. Nachdem eine Einheit eine Funktionalität identifiziert hat, die potenziell zu produktiven Datenflüssen im Rahmen von Support-Anfragen führt, scheint die Information ausserdem nicht zwischen den direkt betroffenen Einheiten zirkuliert zu haben.

Aus Sicht der **Informationssicherheit** kommen wir zum Schluss, dass der Bund in den Beziehungen der direkt betroffenen Einheiten zu Xplain vor dem Datenabfluss im Juni 2023 seine Pflichten, sorgfältig auszuwählen und angemessen zu instruieren, teilweise erfüllt hat. Die Überwachungspflicht wurde in diesem Zusammenhang hingegen nicht erfüllt.

Aus Sicht des **Datenschutzes** kommen wir zum Schluss, dass der Bund in den identifizierten Fällen der Bearbeitung von Personendaten durch Xplain als Auftragsbearbeiter seine Pflichten zur sorgfältigen Auswahl, zur angemessenen Instruktion und zur Überwachung nicht erfüllt hat.

Die Fälle der Weitergabe von Produktivdaten an Xplain und die vom Untersuchungsorgan festgestellten Verstösse gegen die Pflichten zur sorgfältigen Auswahl, angemessenen Anleitung und Überwachung auf Seiten des Bundes fanden in einem **Kontext** statt, der sie begünstigte, aber nicht verursachte:

Unter dem Aspekt des Umgangs mit Cyberbedrohungen durch Dritte scheinen die von der Untersuchung betroffenen Einheiten die von Dritten, insbesondere von Softwareanbietern, ausgehenden Risiken **unterschätzt** zu haben, einige von ihnen sogar bis zum Datenabfluss im Juni 2023.

Die Untersuchung zeigt ein teilweise unterschiedliches Verständnis der **Verteilung der Verantwortung** für die Informationssicherheit zwischen, je nach Situation, (i) der zentralen Beschaffungsstelle, (ii) der Bedarfsstelle, (iii) dem Departement, dem die Bedarfsstelle angehört, (iv) dem ISC-EJPD, (v) dem BIT oder (vi) sogar zwischen einzelnen Mitarbeitenden derselben Stelle.

Aus den Befragungen ergab sich ein Konsens, dass die Ressourcen, die in den direkt betroffenen Einheiten für die Informationssicherheit bereitgestellt wurden, insgesamt **unzureichend** waren.

Die Untersuchung zeigt, dass die direkt betroffenen Einheiten in den untersuchten Jahren von Xplain **abhängig** waren.

Die Beziehung zwischen Xplain und den direkt betroffenen Einheiten scheint im Wesentlichen auf **Vertrauen** beruht zu haben.

Die aus der vorliegenden Administrativuntersuchung gezogenen Lehren erfordern unserer Ansicht nach Empfehlungen sowohl in organisatorischer als auch in inhaltlicher Hinsicht. Diese **Empfehlungen** werden in Abschnitt VI.B. erläutert.

UNTERSUCHUNGSGEGENSTAND

1 Der Untersuchungsgegenstand wurde vom Bundesrat am 23. August 2023 wie folgt definiert:

> *«Die Administrativuntersuchung soll insbesondere aufzeigen, welche Umstände es auf Seiten der Bundesverwaltung ermöglicht haben, dass Xplain AG in den Besitz von produktiven Daten der Bundesverwaltung kam und ob bei der Auswahl, Instruktion und Überwachung der Xplain AG sowie bei der Zusammenarbeit mit dieser Firma die Pflichten angemessen erfüllt wurden. Ferner ist zu prüfen, welche Prozesse und Vorgaben in der Bundesverwaltung anzupassen sind, um künftig die Sicherheitsrisiken, die mit der Übermittlung von Informationen der Bundesverwaltung, darunter klassifizierten Informationen und Personendaten, an externe Dienstleister sowie mit deren Bearbeitung verbunden sind, besser erkennen, adressieren und mitigieren zu können.*
>
> *Die Administrativuntersuchung erstreckt sich auf alle Departemente und die Bundeskanzlei; sie richtet sich nicht gegen bestimmte Personen.*
>
> *Die Untersuchung ist in maximal zwei Etappen durchzuführen. In der ersten Etappe ist retrospektiv der Sachverhalt im Fall Xplain AG zu klären und es sind allfällige Sofort-massnahmen vorzuschlagen. Soweit nötig, sind in der zweiten Etappe unabhängig vom Fall Xplain AG erkannte Probleme vertieft zu beurteilen sowie Lösungsansätze und Empfehlungen zur Reduktion der Sicherheitsrisiken zu erarbeiten.»*
>
> [Anm. d. Übers.: Französische Übersetzung des deutschen Originaltextes nur in der französischen Version des Berichts.]

2 Der Zeitplan der Untersuchung wurde vom Bundesrat wie folgt festgelegt: *«Die Untersuchung soll am 1. September 2023 starten und ist spätestens am 31. März 2024 abzuschliessen.»*

3 Der Bundesrat hat ausserdem das Eidgenössische Finanzdepartement (EFD) als Koordinationsstelle für die Vorbereitung und Begleitung der Administrativuntersuchung ernannt (nachfolgend «**Koordinationsstelle**»). Die Koordinationsstelle hat eine «Kerngruppe» einberufen, die sie bei der Erfüllung ihrer Aufgaben unterstützt. Die Gruppe besteht aus Vertretern des (i) Generalsekretariats (GS) des EFD («**GS-EFD**»), (ii) des GS des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport («**VBS**»), (iii) des GS des Eidgenössischen Justiz- und Polizeidepartements («**EJPD**»), der Bundeskanzlei, (iv) des Bundesamtes für Rüstung («**armasuisse**»), (v) des Bundesamtes für Bauten und Logistik («**BBL**»), (vi) des Nationalen Zentrums für Cybersicherheit («**NCSC**») und (vii) des Bundesamtes für Informatik und Telekommunikation («**BIT**») (die «**Kerngruppe**»).

4 Am 24. August 2023 wurde ein entsprechender Mandatsvertrag zwischen der Schweizerischen Eidgenossenschaft, vertreten durch das GS-EFD, und der OBERSON ABELS AG geschlossen. Dieser Vertrag sieht unter Art. 1.2 insbesondere Folgendes vor:

> *«Die Administrativuntersuchung soll in maximal zwei Etappen durchgeführt werden. Die Etappierung erfolgt vor dem Hintergrund, dass rasch erste Lehren aus dem Vorfall Xplain AG gezogen werden können sollen (1. Etappe). Die erste Etappe soll retrospektiv untersuchen, unter welchen Umständen die Xplain AG von den Verwaltungseinheiten beauftragt worden war und ob auf Seiten der Bundesverwaltung bei der Auswahl, Instruktion und Überwachung der Xplain AG sowie bei der Zusammenarbeit mit Xplain AG Pflichten verletzt wurden (Offertanfrage Ziff. 2.2.1 Absatz 1).*
>
> *Ferner ist zu klären, ob technische, prozesshafte oder organisatorische Mängel dazu geführt haben, dass Produktivdaten der Bundesverwaltung im Besitz der Xplain AG waren und ob*

dabei die Sicherheitsrisiken falsch eingeschätzt oder übersehen wurden. Es ist aufzuzeigen, welche Sofortmassnahmen zu ergreifen sind, um Sicherheitsrisiken zu beheben. Zur ersten Etappe soll ein Bericht erstellt werden. Dieser soll die Erkenntnisse aus der ersten Etappe und Empfehlungen zum weiteren Vorgehen enthalten (Offertanfrage Ziff. 2.2.1 Absatz 2). Es wird jedoch nicht erwartet, dass die Anbieterin eine technische Informatikprüfung durchführt.

Je nach Erkenntnissen in diesem Bericht wird die Administrativuntersuchung fortgeführt oder nicht. Die zweite Etappe ist als Option ausgestaltet (Offertanfrage Ziff. 2.2.1 Absatz 3).

In einer allfälligen zweiten Etappe soll anhand der Befunde der ersten Etappe geprüft werden, welche Massnahmen unabhängig vom Fall Xplain AG zu treffen sind, um künftig die Sicherheitsrisiken, die mit der Leistungserbringung bzw. mit dem Informationszugriff durch externe Dienstleister verbunden sind, besser erkennen, adressieren und mitigieren zu können. Zum Abschluss der allfälligen zweiten Etappe bzw. zum Abschluss der Administrativuntersuchung soll ein Schlussbericht gemäss Art. 27j Abs. 1 und 2 RVOV mit Ergebnissen und Empfehlungen erstellt werden (vgl. Offertanfrage Ziff. 2.2.1 Absatz 4).»[Anm. d. Übers.: Französische Übersetzung des deutschen Originaltextes nur in der französischen Version des Berichts.]

5 Aufgrund unerwarteter Entwicklungen (Daten waren komplexer als angenommen und GS-EFD musste früher über erste Untersuchungsergebnisse verfügen) wurde am 7. Dezember 2023 eine Zusatzvereinbarung zum Vertrag unterzeichnet. Diese Zusatzvereinbarung sieht insbesondere die Zusammenlegung der beiden oben genannten Etappen vor:

«Neu wird die Etappierung der Untersuchungsteile und die optionale Ausgestaltung der zweiten Etappe aufgehoben. Die Anbieterin untersucht ab 22. November 2023 die oben beschriebenen retrospektiven und prospektiven Aspekte parallel und wird über beide gleichzeitig berichten. Der Gegenstand der Untersuchung bleibt aber insgesamt unverändert, wird also nicht auf weitere Lieferanten des Bundes oder Vorfälle ausgedehnt.»

[Anm. d. Übers.: Französische Übersetzung des deutschen Originaltextes nur in der französischen Version des Berichts.]

6 Entsprechend dem Mandat[5] wird in diesem Bericht der Sachverhalt nicht aus strafrechtlicher Sicht geprüft.

III. UNTERSUCHUNGSVERLAUF

A. Wichtigste Etappen

7 Die Administrativuntersuchung «*Datenabfluss*» begann am 1. September 2023. Die wichtigsten Etappen der Untersuchung werden in den folgenden Abschnitten beschrieben.

8 Die Administrativuntersuchung wurde von einem Team der OBERSON ABELS AG durchgeführt. Jedem Teammitglied wurde eine personenbezogene Sicherheitserklärung ausgestellt, nachdem die gesammelten Daten geprüft worden waren.[6] Der Begriff **«Untersuchungsorgan»** und die Abkürzung **«OA»**, die in diesem Bericht verwendet werden, bezeichnen dieses Team und nicht die Kanzlei als Ganzes.

[5] Vgl. Ziff. 2.2.2 der Offertanfrage, auf die der Mandatsvertrag verweist (AUD B01.01.04.87).
[6] Vgl. aPSPV vom 4. März 2011.

9 Am 4. September 2023 versandte OA acht Auskunftsgesuche: eines an die Bundeskanzlei und eines an jedes Generalsekretariat der sieben Departemente der Bundesverwaltung.[7] Die Gesuche bezogen sich im Wesentlichen auf folgende Elemente:[8]

- vollständige Liste der Verwaltungseinheiten des Departements bzw. der Bundeskanzlei, die Geschäftsbeziehungen mit der Xplain AG («**Xplain**») unterhalten oder in der Vergangenheit unterhalten haben;
- Kopien aller mit Xplain geschlossenen Verträge, insbesondere auch, wenn eine Drittstelle von einer Verwaltungseinheit beauftragt wurde, einen Vertrag in ihrem Namen zu schliessen;
- Identität der Personen, die in einem Departement oder in der Bundeskanzlei und dessen bzw. deren Verwaltungseinheiten an den oben genannten Geschäftsbeziehungen mit Xplain mitgewirkt haben;
- alle Richtlinien, Kreisschreiben und sonstigen internen Weisungen des Departements und der Bundeskanzlei und dessen bzw. deren Verwaltungseinheiten in Bezug auf a) die Bearbeitung (einschliesslich Schutz) von Daten (einschliesslich personenbezogener Daten) und b) die Cybersicherheit.

10 Am 26. September 2023 verschaffte die Eidgenössische Steuerverwaltung («**ESTV**») OA Zugang zur forensischen Plattform *Nuix Investigate*, auf der sich eine Kopie des «*Datendump*» befand, also des Datensatzes, der von der Hackergruppe «Play» im Juni 2023 online gestellt worden war und den das NCSC heruntergeladen und gefiltert hatte.[9]

11 Am 29. September 2023 richtete OA auf der Grundlage der Informationen, die OA als Antwort auf die Gesuche vom 4. September 2023 von der Bundeskanzlei und den Generalsekretariaten der Departemente erhalten hatte, 11 weitere Auskunftsgesuche an die folgenden Einheiten der Bundesverwaltung: Eidgenössisches Departement für auswärtige Angelegenheiten («**EDA**»)[10]; armasuisse[11]; Führungsunterstützungsbasis («**FUB**»)[12]; Informatik Service Center ISC-EJPD («**ISC-EJPD**»)[13]; Bundesamt für Polizei («**fedpol**»)[14]; BBL[15]; Bundesamt für Zoll und Grenzsicherheit («**BAZG**»)[16]; BIT[17]; Bundesamt für Justiz («**BJ**»)[18]; Staatssekretariat für Migration («**SEM**»)[19]; Nachrichtendienst des Bundes («**NDB**»)[20]. In diesen 11 Gesuchen wurden im Wesentlichen folgende Informationen von den betroffenen Einheiten verlangt (das an das EDA gesandte Gesuch ausgenommen, welches angesichts der in Bezug auf das Gesuch vom 4. September 2023 eingegangenen Antwort nur Ziff. ii umfasste): i) eine Liste der Personen, die eine Funktion in bestimmten Bereichen innerhalb der betroffenen Einheit ausüben oder in der Vergangenheit ausgeübt haben (Direktion; Rechtsabteilung; Beschaffungen;

[7] AUD 03.01.1-5; AUD 03.02.1-5; AUD 03.03.1-5; AUD 03.04.1-5; AUD 03.05.2-6; AUD 03.06.1-5; AUD 03.07.1-5; AUD 03.08.1-5.
[8] AUD 03.01.1-5; AUD 03.02.1-5; AUD 03.03.1-5; AUD 03.04.1-5; AUD 03.05.2-6; AUD 03.06.1-5; AUD 03.07.1-5; AUD 03.08.1-5.
[9] Zu diesem Thema: NCSC, Bericht zu den Datenanalysen nach dem Cyberangriff auf die Firma Xplain, 14.12.2023, S. 5 f. Insgesamt wurden uns 1 295 862 Objekte zur Verfügung gestellt, was gemäss dem oben genannten Bericht allen im Darknet veröffentlichten Daten entspricht.[10] AUD 03.02.25-28.
[10] AUD 03.02.25-28.
[11] AUD 03.05.01.1-4.
[12] AUD 03.05.02.1-4.
[13] AUD 03.04.02.1-4.
[14] AUD 03.04.01.1-4.
[15] AUD 03.06.03.1-4.
[16] AUD 03.06.01.1-4.
[17] AUD 03.06.02.1-4.
[18] AUD 03.04.04.1-4.
[19] AUD 03.04.03.1-4.
[20] AUD 03.05.03.1-4.

Informatik); ii) eine Liste der Organe, Mitarbeiter[21] oder Beauftragten von Xplain, die insbesondere über ein E-Mail-Konto der betroffenen Einheit verfügen oder in der Vergangenheit verfügt haben.

12 Diese (Verwaltungs- oder Organisations-)Einheiten werden nachfolgend gemeinsam als «**von der Untersuchung betroffene Einheiten**» bezeichnet.

13 In Anbetracht der zusätzlichen Informationen, die OA in einer Sitzung mit der Koordinationsstelle und der Kerngruppe am 10. Oktober 2023 in Bern erhalten hatte, schickte OA am 12. Oktober 2023 ein Auskunftsgesuch an die Militärpolizei. Inhaltlich entsprach dieses Gesuch den oben genannten Gesuchen vom 29. September 2023.

14 Am 20. Oktober 2023 versandte OA drei Anträge auf Herausgabe von Informationen an die betroffenen internen IKT-Leistungserbringer, nämlich an das BIT[22], die FUB[23] und die IT-Abteilung des EDA[24]. Diese Anträge stützten sich auf die Informationen, die auf die Gesuche von OA vom 4. und 29. September 2023 hin übermittelt worden waren, und betrafen insgesamt 421 Geschäfts-E-Mail-Konten (Exchange-Konten).[25]

15 Am 2. November 2023 versandte OA analog zu den oben genannten Anträgen vom 20. Oktober 2023 drei weitere Anträge auf Herausgabe von Informationen an die betroffenen internen IKT-Leistungserbringer (das BIT, die FUB und die IT-Abteilung des EDA). Gegenstand waren insgesamt 11 Exchange-Konten.[26]

16 Am 10. November 2023 ersuchte OA fedpol[27] und das BAZG[28], OA die Informationen zu übermitteln, die diese Ämter im Zusammenhang mit Xplain an den EDÖB weitergeleitet hatten und die für die Administrativuntersuchung von Interesse sein könnten.

17 Vom 14. November 2023 bis zum 14. Dezember 2023 führte OA Befragungen in Bern durch.

18 Ab dem 21. November 2023 hatte OA Zugriff auf alle Exchange-Daten auf der Plattform *Nuix Investigate*, nachdem diese von den internen IKT-Leistungserbringern des Bundes extrahiert und von der ESTV nach den von OA definierten Kriterien gefiltert worden waren.

19 Am 18. Dezember 2023 richtete OA ein Auskunftsersuchen an fedpol mit dem Ziel, sämtliche Verträge mit Xplain AG mit Bezug auf das ORMA-Projekt aus der Zeit vor 2011 vorgelegt zu bekommen, da OA bis dahin keine Verträge mit Bezug auf das ORMA-Projekt aus der Zeit vor 2011 übermittelt worden waren.[29]

20 Am 18. Dezember 2023 übermittelte OA dem Generalsekretariat des EFD eine Zusammenfassung der Erkenntnisse per 15. Dezember 2023.[30]

21 Im Januar/Februar 2024 führte OA weitere Befragungen durch – insgesamt 32 in Bern (30 Mitarbeitende des Bundes und zwei Drittpersonen) –, die am 9. Februar 2024 abgeschlossen wurden.

22 Am 1. März 2024 legte das Untersuchungsorgan der Koordinationsstelle einen Berichtsentwurf vor, um den von der Untersuchung betroffenen Einheiten die Ausübung ihres Anspruchs auf rechtliches Gehör zu ermöglichen (Art 27*g* Abs. 5 RVOV). Die Koordinationsstelle leitete den Entwurf am selben Tag an die von

[21] In diesem Dokument wird aus Gründen der besseren Lesbarkeit punktuell das generische Maskulinum verwendet.
[22] AUD 03.06.02.27-38 und B03.06.02.04.
[23] AUD 03.05.02.13-19 und B03.05.02.03.
[24] AUD 03.02.39-43 und B03.02.31.
[25] Vgl. diesbezüglich unten Rz. 43–49.
[26] AUD 03.02.68-72; AUD 03.05.02.23-27; AUD 03.06.02.40-44.
[27] AUD 03.04.01.17-19.
[28] AUD 03.06.01.9-11.
[29] AUD 03.04.01.22-24.
[30] AUD 01.02.514-515 und B01.02.91-92.

der Untersuchung betroffenen Einheiten weiter und bat sie, Anträge auf Akteneinsicht sowie Stellungnahmen zum Berichtsentwurf an das Untersuchungsorgan zu richten. Das Untersuchungsorgan hat alle erhaltenen Stellungnahmen geprüft. Wenn erforderlich, wurden Präzisierungen in diesem Bericht vorgenommen.

23 Zwischen dem 5. und 12. März 2024 kontaktierte das Untersuchungsorgan die Mitarbeitenden des Bundes, zu denen der Berichtsentwurf vom 1. März 2024 Feststellungen enthält.[31] Diese Personen erhielten die sie betreffenden Passagen des Berichtsentwurfs (Art. 27*g* Abs. 4 und 5 RVOV). Der Rest des Dokuments war geschwärzt. Sie wurden gebeten, allfällige Anträge auf Akteneinsicht oder Stellungnahmen an das Untersuchungsorgan zu richten. Das Untersuchungsorgan hat alle erhaltenen Stellungnahmen geprüft. Wenn erforderlich, wurden Präzisierungen in diesem Bericht vorgenommen.

B. Empfohlene Sofortmassnahmen

24 Gemäss dem Mandatsvertrag musste OA der Koordinationsstelle umgehend Situationen melden, die Sofortmassnahmen erfordern, einschliesslich Hinweisen auf individuelle Fehler.

1. Error-Reporting

25 In Anwendung der oben genannten Klausel berichtete OA der Koordinationsstelle in einer verschlüsselten E-Mail vom 1. Dezember 2023 über einen sogenannten «Error-Reporting»-Mechanismus, der zur Übertragung von produktiven Daten von der Bundesverwaltung an Xplain geführt haben könnte. OA erklärte, dass dieser Mechanismus für alle Kundinnen und Kunden von Xplain eingerichtet worden sei und daher nicht nur die Bundesverwaltung betreffe.

26 Die Koordinationsstelle meldete OA, dass es diese Informationen an die betroffenen Einheiten weitergeleitet habe. Nach den von der Koordinationsstelle übermittelten Informationen wurde die Error-Reporting-Funktion im Sommer 2023 deaktiviert. Die internen Richtlinien wurden angepasst und die betroffenen Produkte (Software) werden derzeit aktualisiert, um die Funktion endgültig zu entfernen.

2. Individuelle Fehler

27 In Anwendung der oben genannten Klausel berichtete OA der Koordinationsstelle in einer verschlüsselten E-Mail vom 1. Dezember 2023, einen Mitarbeiter von fedpol und einen Mitarbeiter des BJ identifiziert zu haben, die Xplain in einer oder mehreren anscheinend unverschlüsselten E-Mails produktive Daten ihrer Verwaltungseinheit übermittelt hatten.

28 Ferner teilte OA der Koordinationsstelle in einer verschlüsselten E-Mail vom 2. Februar 2024 mit, einen Mitarbeiter der FUB identifiziert zu haben, der produktive Daten einer Verwaltungseinheit per E-Mail an Xplain gesendet hatte.

29 Schliesslich übermittelte OA der Koordinationsstelle in einer verschlüsselten E-Mail vom 28. Februar 2024 zufällig entdeckte Elemente, die nahelegen, dass ein Mitarbeiter von fedpol zwischen 2009 und 2014 insgesamt vier Mal bei den Verwaltungsratsmitgliedern von Xplain bestimmte Privilegien angefragt haben könnte.[32]

[31] Es wurde auch ein ehemaliger Mitarbeiter des Bundes kontaktiert.
[32] Vgl. Rz. 560 unten.

C. Wichtigste Beweismittel

30 Folgende Beweismittel wurden im Laufe der Untersuchung zusammengetragen:

- Verträge, die von den von der Untersuchung betroffenen Einheiten infolge der Auskunftsgesuche vom 4. September 2023 eingereicht wurden;
- Weisungen und ähnliche Dokumente, die auf die Auskunftsgesuche vom 4. September 2023 hin übermittelt wurden;
- 32 Befragungen in Bern (30 Mitarbeiter des Bundes; zwei Drittpersonen) zwischen dem 14. November 2023 und dem 9. Februar 2024;
- Dokumente und Informationen, die dem EDÖB von fedpol und dem BAZG übermittelt und auf Anfrage an OA weitergeleitet wurden;
- NCSC-Bericht vom 14. Dezember 2023 über den Cyberangriff auf Xplain;[33]
- Entwurf vom SEPOS zur Auslegeordnung zur Supply Chain Security im Lichte des Informationssicherheitsgesetzes, datiert vom 22. Januar 2024 und vom GS-EFD am 23. Januar 2024 spontan übermittelt.[34]

31 Ausserdem wurden dem Untersuchungsorgan die folgenden elektronischen Daten zur Verfügung gestellt, um sie auszuwerten und potenziell relevante Elemente in die Untersuchungsakten aufzunehmen:

- Kopie des *Datendump* (1 295 862 Elemente), einschliesslich der NCSC-*Tags* (die speziell die Daten des Bundes markieren)[35], die OA auf der Plattform *Nuix Investigate* zur Verfügung gestellt wurde (der «***Datendump***»);
- Exchange-Daten (2 719 026 Elemente), die OA auf Anfrage auf der Plattform *Nuix Investigate* zur Verfügung gestellt wurden (die «**Exchange-Daten**»).

32 Nachdem sie per E-Mail an ihre Geschäftsadresse vorgeladen und über ihre Rechte und Pflichten[36] sowie über die vom Untersuchungsorgan angewandten Verfahrensregeln[37] informiert worden waren, wurden die folgenden Mitarbeiter des Bundes von OA in Bern befragt (in alphabetischer Reihenfolge des aktuellen Arbeitgebers):[38]

Arbeitgeber zum Zeitpunkt der Befragung	Hierarchieebene – Art der Verantwortung	Vorheriger Arbeitgeber, über den Fragen gestellt wurden
armasuisse	Direktion	-
BAZG	Direktion	-
BAZG	Delegierter für IT-Sicherheit	-

[33] «*Bericht zu den Datenanalysen nach dem Cyberangriff auf die Firma Xplain*» (AUD 01.02.520 und AUD B01.02.93).

[34] «*Auslegeordnung zur Supply Chain Security im Lichte des Informationssicherheitsgesetzes unter Berücksichtigung weiterer Modelle und der getroffenen Massnahmen*».

[35] Laut NCSC können von insgesamt 64 923 relevanten Objekten (d. h. nach Ausschluss insbesondere von Backup-Dateien, Systemdateien, Standardkomponenten und Duplikaten) 9 040 Objekte der Schweizerischen Eidgenossenschaft als «Dateneigentümerin» zugeordnet werden. Das NCSC hält fest, dass von diesen 9 040 Objekten 95,17 % vom EJPD, 3,38 % vom VBS, 0,76 % vom WBF, 0,61 % vom EFD, 0,07 % vom EDI und 0,01 % vom EDA sind.

[36] Insbesondere das Recht, sich nicht selbst zu belasten (Nemo-tenetur-Prinzip; Art. 27*h* Abs. 2 RVOV).

[37] AUD B01.02.65.

[38] Anm. d. Übers.: Diese Fussnote enthält eine sprachliche Präzisierung, die nur die französische Fassung des Berichts betrifft.

Arbeitgeber zum Zeitpunkt der Befragung	Hierarchieebene – Art der Verantwortung	Vorheriger Arbeitgeber, über den Fragen gestellt wurden
BAZG	Delegierter für IT-Sicherheit	-
BBL	Direktion	-
BIT	Projektleiter	ISC-EJPD
BJ	Applikationsverantwortlicher	ISC-EJPD
BJ	Leiter IT / Delegierter für IT-Sicherheit	-
BJ	Leiter RI / Projektleiter	-
BJ	Direktion	-
EDA	Direktion	-
fedpol	Delegierter für IT-Sicherheit	-
fedpol	Direktion	-
fedpol	Business Analyst	-
fedpol	Projektleiter	BAZG
fedpol	Projektleiter	-
FUB	Direktion	-
Kdo Operationen	Direktion	-
Kdo Operationen	Leiter Informatik und Cybersicherheit	-
MP	Leiter eines Führungsgrundgebiets	-
NCSC	Leiter Schwachstellen	-
NDB	Leiter Cyber	-
SEM	Direktion	-
SEM	Wissenschaftliche Assistenz	BAZG
SEM	Senior Business Analyst / Product Owner	-
SEM	Leiter IT-Sicherheit, Büroautomatisierung und Infrastruktur	BAZG
SEM	Delegierter für IT-Sicherheit	-
SEM	Leiter Planung und Ressourcen	-
SEPOS	Staatssekretär	-

33 Zudem begleitete der Leiter der Informationssicherheitsdienste des SEPOS den Staatssekretär für Sicherheitspolitik bei dessen Befragung.

34 Entsprechend dem Beschluss des Bundesrates vom 23. August 2023 wurden die derzeitigen und ehemaligen Mitarbeiter und Beauftragten des Bundes für die Dauer der Untersuchung in Bezug auf alle Informationen, die sich auf den Untersuchungsgegenstand beziehen, vom Berufs-, Geschäfts- und Amtsgeheimnis gegenüber OA als Untersuchungsorgan entbunden.

35 Vor dem Hintergrund des Inhalts der Beiträge dieser Personen in den Medien über die Beziehung zwischen dem Bund und Xplain wurden die folgenden Drittpersonen angehört (in alphabetischer Reihenfolge):

– Christian FOLINI, Ingenieur für Computersicherheit und Fachautor in diesem Bereich;

– Matthias STÜRMER, Professor an der Berner Fachhochschule, Direktor des Instituts *Public Sector Transformation*, spezialisiert auf die Digitalisierung, insbesondere im öffentlichen Sektor.

36 Die Herren FOLINI und STÜRMER wurden per E-Mail an ihre Geschäftsadresse vorgeladen und über ihre Rechte und Pflichten[39] sowie über die Verfahrensregeln des Untersuchungsorgans informiert.[40]

37 Alle Befragungen wurden aufgezeichnet (nur Tonaufnahmen), wobei in jedem Fall die Zustimmung der befragten Person eingeholt wurde. OA fertigte unverzüglich ein Protokoll an, das von den einzelnen Befragten unterzeichnet wurde. Das Protokoll enthält nur die formalen Informationen, die zu Beginn der Befragung mitgeteilt wurden (Gegenstand, Rechte und Pflichten). Ferner erstellte OA eine wörtliche Abschrift jeder Tonbandaufnahme, wobei die Aufnahme als verbindlich gilt. Die Aufnahmen, Protokolle und Abschriften wurden in die Untersuchungsakten aufgenommen.[41]

D. Zusammenarbeit

38 Das Untersuchungsorgan möchte betonen, dass die betroffenen Einheiten, die Generalsekretariate der jeweiligen Departemente sowie alle befragten Personen während der Untersuchung gut kooperiert haben. Alle Gesuche von OA wurden beantwortet und die von OA gesetzten Fristen, die aufgrund des vom Bundesrat beschlossenen Untersuchungszeitplans besonders kurz waren (vgl. Rz. 1 oben), wurden eingehalten.

39 Gemäss OA war die Zusammenarbeit mit den Einheiten, die an der Bereitstellung der Exchange-Daten des Bundes beteiligt waren (vgl. E.1 unten), besonders konstruktiv, wenn man die technischen Herausforderungen (Belastbarkeit der Hardware und Software unter Druck) bedenkt, die innerhalb eines besonders kurzen Zeitraums bewältigt werden mussten. Das Engagement des BIT und der ESTV erwies sich in diesem Zusammenhang als entscheidend.

40 OA lobt auch die ausgezeichnete Zusammenarbeit mit der Koordinationsstelle und der vom EFD eingesetzten Kerngruppe sowie die damit verbundene Unterstützung. OA stellt fest, dass die eigene Unabhängigkeit zu jeder Zeit gewahrt wurde.

41 Es kann lediglich angemerkt werden, dass OA von den von der Untersuchung betroffenen Einheiten relativ wenig spontane Informationen direkt oder über die Koordinationsstelle erhalten hat. Zu Beginn des Mandats am 1. September 2023 hatten die von der Untersuchung betroffenen Einheiten bereits seit mehreren Monaten Kenntnis vom Datenabfluss, und es gab bereits interne Bemühungen zur Klärung des Sachverhalts, zumindest in einigen der Einheiten, wie die anschliessenden Befragungen durch OA zeigten.

42 Von der Eidgenössischen Finanzkontrolle (EFK) hat das Untersuchungsorgan dagegen im September 2023 zwei Verdachtsmeldungen von Whistleblowern erhalten, die in der Untersuchung berücksichtigt wurden. Diese enthielten keine entscheidenden Elementen.

E. Limitationen

1. Vollständigkeit der Exchange-Daten

43 Von Beginn der Untersuchung an signalisierte OA der Koordinationsstelle ihre Bereitschaft, eine forensische Analyse der E-Mail-Daten des Bundes (insbesondere E-Mails und Kalendereinträge)

[39] Sie wurden insbesondere über ihr Recht auf Verweigerung der Aussage informiert (Art. 27*h* Abs. 3 RVOV).
[40] AUD 04.02.1-6; B01.02.65; B04.02.01 / AUD 04.03.1-6; B01.02.65; B04.03.01.
[41] Rubrik 4 im Dossier.

durchzuführen. Das BIT unterstützte OA proaktiv, insbesondere im Vorfeld der Datenextraktion, indem es technische Varianten zur Identifizierung relevanter Daten analysierte.

44 Zusammen mit rechtlichen Erwägungen (einschliesslich der Einhaltung des Grundsatzes der Verhältnismässigkeit) führten diese Analysen dazu, dass OA eine Extraktion sämtlicher E-Mail-Postfächer aller von der Untersuchung betroffenen Einheiten gemäss den von ihnen zur Verfügung gestellten Informationen ausschloss. Nach Schätzungen des BIT wäre die Extraktion einer solchen Datenmenge mit einem technischen Zeitaufwand von fast zwei Monaten verbunden.

45 OA nutzte daher die Listen der potenziell relevanten Personen, welche die betroffenen Einheiten auf Anfrage zur Verfügung stellten, um den Kreis der zu extrahierenden E-Mail-Postfächer festzulegen. Ferner bat OA die betroffenen Einheiten[42], die E-Mail-Postfächer von Personen aus bestimmten Bereichen (Direktion; Rechtsabteilung; Beschaffungen; falls zutreffend: Informatik) während eines bestimmten Zeitraums zu ermitteln. Darüber hinaus forderte OA die betroffenen Einheiten auf, alle Organe, Mitarbeiter oder Beauftragten von Xplain zu identifizieren, die über ein E-Mail-Konto der betroffenen Einheit, einen Zugang zu einem E-Mail-Konto eines Mitarbeiters der betroffenen Einheit, einen Zugang zu einem gemeinsamen bzw. geteilten E-Mail-Konto der betroffenen Einheit verfügen oder verfügt haben oder die automatisch Nachrichten von einem E-Mail-Konto der betroffenen Einheit erhalten bzw. erhalten haben.

46 OA stellte daraufhin Anträge an das BIT, die FUB und die IT-Abteilung des EDA, um (i) die ausgewählten E-Mail-Daten zu extrahieren, (ii) diese Daten nach von OA definierten Suchkriterien zu filtern und (iii) auf der von der ESTV betriebenen Plattform *Nuix Investigate* zur Verfügung zu stellen.

47 Nach Analyse dieser Daten nahm das Untersuchungsorgan nur die Elemente in die Untersuchungsakten auf (Art. 27*j* Abs. 1 RVOV), die (i) für die Untersuchung relevant erscheinen, wobei insbesondere alles, was in die Privatsphäre der betroffenen Personen fällt, ausgeschlossen wurde, und (ii) die nicht durch das Anwaltsgeheimnis geschützt sind (vgl. Art. 13 Abs. 1bis VwVG).

48 Die Methode ist somit eine Abwägung zwischen den anwendbaren rechtlichen Regeln (insbesondere der Verhältnismässigkeit), dem Interesse der Untersuchung (insbesondere der Wahrheitsfindung) und den zeitlichen Beschränkungen (insbesondere den dem Untersuchungsorgan eingeräumten Fristen).

49 Bei der Überprüfung der E-Mail-Daten kann daher kein Anspruch auf Vollständigkeit erhoben werden.

2. Keine Verpflichtung Dritter zur Zusammenarbeit

50 Dass Dritte nicht zur Zusammenarbeit verpflichtet sind, ist eine Beschränkung, die jede Administrativuntersuchung gemäss Art. 27*a* ff. RVOV gemein hat (vgl. Art. 27*h* Abs. 3 RVOV). Im vorliegenden Fall stellte sie in mehrfacher Hinsicht ein Hindernis für die Ermittlung des Sachverhalts dar.

51 Mit einem Schreiben vom 19. September 2023 weigerte sich Xplain zum Beispiel, die von OA am 6. September 2023 angeforderten Informationen und Dokumente bereitzustellen.[43]

52 Zudem reagierten weder die sieben kontaktierten Mitarbeiter noch der ehemalige CEO von Xplain auf die Aufforderungen von OA zu einer Befragung.

53 Ausserdem weigerte sich ein ehemaliger Kader von fedpol (2002–2018), der von OA aufgrund von Hinweisen von fedpol auf dem Postweg kontaktiert worden war, seiner Einladung zu einer Befragung

[42] Mit Ausnahme des EDA, das nur vom zweiten Teil dieser Aufforderung betroffen war (Kontakte mit Xplain).
[43] AUD 03.09.1-5.

Folge zu leisten.[44] Wie in der Rechtslehre dargelegt, sind ehemalige Mitarbeitende als Dritte zu betrachten, die nicht zur Zusammenarbeit verpflichtet sind (vgl. Art. 27*g* Abs. 2 *a contrario* und Art. 27*h* Abs. 3 RVOV).[45]

3. Weigerung des EDÖB zur Herausgabe von Dokumenten und Informationen

54 Am 15. September 2023 richtete OA ein Auskunftsgesuch an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten («**EDÖB**»).

55 Am 12. Oktober 2023 fragte OA den EDÖB, ob er bereit sei, als Drittpartei zu kooperieren, da dieser das erste Auskunftsgesuch von OA abgelehnt hatte.

56 In einem Schreiben vom 18. Oktober 2023 gab der EDÖB an, er wolle «*seinen vollen Handlungsspielraum und die vollständige Unabhängigkeit*» bewahren, und weigerte sich somit, die von OA erbetenen Dokumente und Informationen bereitzustellen.

4. Entscheid des Bundesstrafgerichts bezüglich der Rechtshilfe mit der Bundesanwaltschaft

57 Am 6. September 2023 richtete OA einen Antrag auf Akteneinsicht an die Bundesanwaltschaft («**BA**»).[46]

58 Mit Entscheid vom 7. Dezember 2023 gab die Beschwerdekammer des Bundesstrafgerichts einer Beschwerde von Xplain statt und hob die Verfügung der BA vom 10. Oktober 2023 auf, mit welcher OA der Zugang zu den Akten des Strafverfahrens gewährt worden war.[47] Gegen diesen Entscheid können keine ordentlichen Rechtsmittel eingelegt werden.

59 Folglich hatte OA keinen Zugang zu potenziell relevanten Informationen und Beweismitteln, die sich im Besitz der BA befanden.

5. Keine rechtlichen Mittel zur Lokalisierung ehemaliger Mitarbeitenden

60 Die Mittel, die dem Untersuchungsorgan nach Art. 27*a* ff. RVOV für die Lokalisierung von Personen, die nicht mehr bei der Bundesverwaltung angestellt sind, zur Verfügung stehen, sind begrenzt. Verfügt eine Einheit der Bundesverwaltung, bei der eine Person zuletzt angestellt war, über keine diesbezüglichen Informationen, bleibt OA als Untersuchungsorgan keine andere Möglichkeit, als auf öffentlich zugängliche Quellen zurückzugreifen, um die betreffenden ehemaligen Angestellten ausfindig zu machen.

61 So konnte ein ehemaliger Mitarbeiter von armasuisse, den OA befragen wollte, nicht ausfindig gemacht werden.

IV. Durch die Untersuchung ermittelte Tatsachen

A. Produktive Daten im Besitz der Xplain AG

62 Gemäss dem Vertrag vom 24. August 2023 und dem Mandat des Bundesrates vom 23. August 2023 zielte die Untersuchung insbesondere darauf ab, die tatsächlichen Umstände zu ermitteln, die dazu geführt hatten, dass produktive Daten des Bundes in die IT-Umgebung von Xplain gelangt waren.

---

[44] AUD 04.41.19.
[45] Bernhard Rüdy, in SVVOR Schweizerische Vereinigung für Verwaltungsorganisationsrecht (Hrsg.), Verwaltungsorganisationsrecht – Staatshaftungsrecht – öffentliches Dienstrecht, 2013, S. 128.
[46] AUD 07.01.1-2.
[47] Entscheid BB.2023.181 vom 7. Dezember 2023.

63 Der Begriff «produktive Daten» ist im Bundesrecht nicht definiert. Unter Bezugnahme der Botschaft des Bundesrates zum Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben vom 4. März 2022[48] verstehen wir unter «produktiven Daten» des Bundes Folgendes:

> *Tatsächliche Daten aus den Informationssystemen des Bundes, im Gegensatz zu Testdaten oder anonymisierten Daten.*

64 Insbesondere vor dem Hintergrund der Erläuterungen des NCSC während der Sitzung mit der Koordinationsstelle und der Kerngruppe am 4. September 2023 wurden von OA die folgenden Arbeitshypothesen formuliert:

1) Mitarbeitende von Xplain verfügten oder verfügen über Bundes-E-Mail-Postfächer und haben sich produktive Daten des Bundes an ihre Xplain-Adresse weitergeleitet («*Forward*»-Hypothese).
2) Mitarbeitende von Xplain verfügten oder verfügen über Zugriff auf Bundessysteme, der den Transfer produktiver Daten in die IT-Umgebung von Xplain ermöglicht hat («*Zugangs*»-Hypothese).
3) Bundesmitarbeitende haben aktiv produktive Daten des Bundes an Mitarbeitende von Xplain weitergegeben («*Aktiver Transfer*»-Hypothese).
4) Automatische Mechanismen führten dazu, dass produktive Daten in die IT-Umgebung von Xplain übertragen wurden («*Automatischer Transfer*»-Hypothese).

65 Wir haben versucht, diese Hypothesen zu überprüfen, indem wir sie den im Verlauf der Untersuchung gesammelten Beweismitteln, insbesondere dem *Datendump* und den uns bereitgestellten Exchange-Daten, gegenübergestellt haben.

66 Die «Forward»-Hypothese, die «Zugangs»-Hypothese und die «Aktiver Transfer»-Hypothese haben sich bestätigt. Die «Automatischer Transfer»-Hypothese wurde nicht bestätigt; es wurde jedoch ein Mechanismus identifiziert, der als «halbautomatisch» bezeichnet werden könnte (siehe unten Ziff. 9).

67 Wir haben keine anderen Kanäle identifiziert, durch die produktive Daten des Bundes in die IT-Umgebung von Xplain gelangt sein könnten.

68 Die unten aufgeführten Fälle zeigen die auf diese Weise identifizierten Kanäle, mit Ausnahme der Fälle Nr. 10 und 11, bei denen der Kanal bis heute unklar geblieben ist und die zu Informationszwecken erwähnt werden. Ein Teil dieser Fälle betrifft produktive Daten, über deren Auftauchen im Darknet im Jahr 2023 berichtet wurde (vgl. Ziff. 1, 2, 7 unten). Andere wurden im Rahmen der Untersuchung identifiziert (vgl. Ziff. 3, 4, 5, 6, 8, 9 unten).

69 Aufgrund der oben beschriebenen Limitationen ist die folgende Analyse nicht vollständig.

1. Forward-Fall Nr. 1: eine Excel-Tabelle (ORMA-Extraktion) mit Details zu strafrechtlichen Untersuchungen und Rechtshilfeverfahren (fedpol) (16. September 2020)

70 Die Forward-Hypothese hat sich bestätigt. Sie wird insbesondere durch den vorliegenden Fall veranschaulicht.

71 Der Hintergrund ist folgender: Ein Mitarbeiter von fedpol («A») hat in einer am 11. August 2020 an einen anderen Mitarbeiter von fedpol («B») gesendeten E-Mail gefragt, ob Xplain eine Anfrage bezüglich

[48] Botschaft zum Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben vom 4. März 2022, BBl 2022 804, S. 85.

fehlender Einträge in einer exportierten Datei beantworten konnte («*Hast du inzwischen seitens xPlain eine Rückmeldung betreffend der fehlenden Einträge beim VASS Export erhalten?*»).[49]

72 VASS ist die Abkürzung für «*Verwaltung von Asservaten, Spuren und Spurenträgern*».[50]

73 Am 7. September 2020 übermittelte B über eine verschlüsselte E-Mail eine komprimierte Datei mit dem Titel [redacted]zip» an A.[51]

74 Am 15. September 2020 leitete A diese Datei per E-Mail an einen Mitarbeiter von Xplain («Q») an dessen Adresse [Q]@fedpol.admin.ch mit folgender Nachricht weiter:

> *«Hallo [Vorname von Q]*
>
> *Anbei das ZIP-File, welches ich am 07.09.2020 von [B] erhalten habe.*
>
> *Wie erwähnt, sind insbesondere die Spalten AJ – AQ leer. Dabei ist insbesondere die Spalte AP (ASSERVAT_SPEZ_BEZEICHNUNG) für mich Elementar.*
>
> *Ich benötige insbesondere folgende Spalten:*
>
> *D (ASSERVATEN_NR)*
>
> *E (SERIEN_NR)*
>
> *I (KATEGORIE)*
>
> *L (VASS_BESCHREIBUNG)*
>
> *V (AD_DOCTYPE)*
>
> *AJ (ASSERVAT_MARKE)*
>
> *AK (ASSERVAT_TYP)*
>
> *AL (ASSERVAT_SERIE_NR)*
>
> *AM (ASSERVAT_MENGE)*
>
> *AN (ASSERVAT_OERTLICHKEIT)*
>
> *AO (ASSERVAT_BEM)*
>
> *AP (ASSERVAT_SPEZ_BEZEICHNUNG)*
>
> *Für Fragen stehe ich dir gerne zur Verfügung».*

75 Diese E-Mail vom 15. September 2020 war in den nachfolgenden unverschlüsselten E-Mails enthalten und der darin enthaltene Text war somit sichtbar. Es gibt keinen Hinweis darauf, dass der Text in den nachfolgenden E-Mails verändert wurde. Die ursprüngliche E-Mail ist jedoch nicht in den uns vorliegenden Daten enthalten, weshalb wir nicht feststellen konnten, ob sie verschlüsselt oder unverschlüsselt war.

76 Am nächsten Tag (16. September 2020) um 11.41 Uhr leitete Q über seine Adresse [Q]@fedpol.admin.ch die oben zitierte E-Mail von A an seine Adresse [Q]@xplain.ch weiter mit der oben genannten komprimierten Datei als Anhang.[52]

---

[49] AUD 03.10.03.2 und AUD 03.10.03.3.

[50] Vgl. [redacted]pdf (29.08.2016) (AUD 03.10.09.157).

[51] B hat im März 2024 im Rahmen seines Anspruchs auf rechtliches Gehör auf die Existenz dieser E-Mail hingewiesen. Diese E-Mail ist nicht in den Exchange-Daten enthalten, die dem Untersuchungsorgan vorliegen.

[52] AUD 03.10.03.1.

77 Diese unverschlüsselte E-Mail enthielt keinen Text, sondern nur die folgende automatische Signatur:

Mit freundlichen Grüssen
Meilleures salutations
Cordiali saluti
Best regards

Q [redacted]

Eidgenössisches Justiz- und Polizeidepartement - EJPD
Bundesamt für Polizei - fedpol
Direktionsbereich Polizeisysteme & Identifikation
Abteilung Polizei-Informationssysteme
Bereich Ermittlungssysteme

Guisanplatz 1a, 3003 Bern
Tel. +41 (0)58 [redacted]
Q [redacted]@fedpol.admin.ch
www.fedpol.ch

78 Der Anhang hatte die Bezeichnung [redacted].zip». Diese .zip-Datei war etwa 8 MB gross. Den Metadaten zufolge wurde sie am 7. September 2020 erstellt.

79 Diese komprimierte Datei enthielt die Excel-Datei mit der Bezeichnung [redacted].xlsx». Es handelte sich um eine Tabelle mit 39 938 Zeilen und etwa 50 Spalten. Diese Zeilen und Spalten enthielten Daten zu Strafverfahren oder internationalen Rechtshilfeverfahren in Strafsachen, in die fedpol involviert war. Je nach Fall enthielt die Tabelle einige oder alle der folgenden Elemente:

- betroffener Sachverhalt,
- Nummer des Verfahrens,
- vermutete Straftaten,
- Namen und Vornamen von natürlichen Personen, insbesondere von beschuldigten Personen, von Beschlagnahmen betroffenen Personen, Ermittlern von fedpol sowie Staatsanwälten der Bundesanwaltschaft,
- Firmenbezeichnung von beschuldigten oder dritten juristischen Personen,
- vorgenommene Rechtshilfe- oder Strafverfahrenshandlungen, einschliesslich der Adressen, an denen Hausdurchsuchungen durchgeführt wurden,
- sichergestellte oder beschlagnahmte Unterlagen und Gegenstände.

80 Ungefähr zwei Stunden später (16. September 2020, 13.33 Uhr) sendete Q von seiner Adresse [Q]@xplain.ch eine unverschlüsselte E-Mail an einen Mitarbeiter des ISC-EJPD («C»). A und B waren in Kopie gesetzt. Im Anhang der E-Mail fügte Q die Datei «[redacted].sql» an und schrieb in der E-Mail Folgendes:

«Hallo [Vorname von C],

darf ich Dich bitten, auf der ORMA Produktion das angehängte Statement auszuführen und das Resultat als Excel an [A]@fedpol.admin.ch zu senden.

Die Liste enthält die von [Vorname von A] gewünschten Spalten, ohne die Verbindung auf die Sicherstellung zu machen.

Danke.»

81 Diese .sql-Datei enthielt 46 Zeilen Code. Es handelte sich um technische Informationen. Keine der oben genannten Daten, die in der Excel-Datei enthalten waren, waren in dieser .sql-Datei enthalten.

82 Ungefähr 45 Minuten später (16. September 2020, 14.16 Uhr) sendete C eine verschlüsselte E-Mail an A, die den gleichen Betreff hatte wie die E-Mail vom selben Tag, die C von Q erhalten hatte. Das Untersuchungsorgan konnte diese Nachricht nicht entschlüsseln.

83 Am nächsten Tag (17. September 2020) sendete A eine unverschlüsselte E-Mail an Q an seine Adresse [Q]@xplain.ch, in der er angab, dass C ihm am Vortag die Excel-Tabelle geschickt habe. A bedankte sich bei Q für dessen Hilfe.

84 Die Datei [redacted].xlsx war Teil der Daten von Xplain, die im Juni 2023 im Darknet hochgeladen wurden. Laut den Metadaten der im Datendump gefundenen Datei befand sich diese Datei in der IT-Umgebung von Xplain in einem *User Share*, der mit dem Vornamen von Q versehen war.[53]

2. Forward-Fall Nr. 2: Verschiedene Dateien im Anhang einer E-Mail, die u. a. geheime Informationen über Bundesrätinnen und -räte und ausländische Beamte enthielt (5. Mai 2018)

85 Der Sachverhalt ist wie folgt: Am 1. Mai 2018 um 14.53 Uhr sendete ein Mitarbeiter von fedpol («D») von seiner Adresse [D]@fedpol.admin.ch eine E-Mail an einen Mitarbeiter von Xplain («R») an dessen Adresse [R]@fedpol.admin.ch mit dem Betreff [redacted]», die folgenden Text enthielt:

«Sehr geehrt[*] [Name von D]

Anbei sende ich Ihnen die versprochenen Unterlagen. Die vier jpg's zeigen Ausschnitte unserer jetzigen Ablage.

Vergessen wurde, dass wir monatlich Sicherheitsmassnahmen der diplomatischen Vertretungen an diverse Kantone versenden (siehe [redacted].pdf). In diesen Schreiben geht es darum, eine vorgefertigte Excel-Tabelle einzufügen.

Bei Fragen stehen wir Ihnen gerne zur Verfügung ».[54]

86 Vier Personen, anscheinend Mitarbeitende von fedpol, waren in Kopie dieser E-Mail gesetzt (über ihre Adresse @fedpol.admin.ch).

87 Diese E-Mail war verschlüsselt und das Untersuchungsorgan konnte sie nicht entschlüsseln. Der Text ist in einer nachfolgenden E-Mail vom 18. Mai 2018, die um 16.05 Uhr verschickt wurde, enthalten. Es gibt keine Hinweise darauf, dass der ursprüngliche Text in dieser nachfolgenden E-Mail verändert wurde.

88 Am 18. Mai 2018 um 16.05 Uhr leitete R die oben genannte E-Mail vom 1. Mai 2018 und ihre Anhänge ohne Text oder automatische Signatur von seiner Adresse [R]@fedpol.admin.ch an seine Adresse [R]@xplain.ch weiter. Der Betreff der E-Mail lautete «WG: [redacted]».

[53] Pfadname: […]/XPLAIN/User Shares/[Vorname von X].
[54] AUD 03.10.04.1.

89 Von den 11 Anhängen dieser E-Mail waren sechs mit dem Vermerk VERTRAULICH gekennzeichnet und stammten von Ende 2017 bzw. Anfang 2018. Es handelte sich um Dokumente (.pdf-Format) von fedpol, die für die kantonalen Polizeibehörden bestimmt waren und sich auf verschiedene Treffen (Empfang, Ankunft, Termine) mit hochrangigen nationalen und internationalen Beamten bezogen.

90 Die Anhänge enthielten insbesondere die Datei [redacted].pdf», deren Inhalt als VERTRAULICH eingestuft wurde und Informationen über Bundesrätinnen bzw. -räte enthielt.

91 Zudem enthielten die der oben genannten E-Mail vom 18. Mai 2018 beigefügten Dokumente die folgenden Arten von Informationen:

- Sicherheitsmassnahmen zugunsten von diplomatischem Personal und ausländischen Botschaften, einschliesslich Mobiltelefonnummern von fedpol-Mitarbeitenden,
- Programme für Veranstaltungen in Botschaften und
- Begleitschutz von Mitarbeitenden im Rahmen des diplomatischen Schutzes.

92 Ein Screenshot zeigte schliesslich einen Teil der Baumstruktur des Fedpol-Org-Laufwerks (O:).

3. Forward-Fall Nr. 3: Versand einer Excel-Tabelle mit mehr als 1 000 Zeilen in Bezug auf Interpol-Ausschreibungen (1. September 2021)

93 Am 1. September 2021 um 11.54 Uhr sendete ein Mitarbeiter von Xplain («Z») eine unverschlüsselte E-Mail mit dem Betreff [redacted]» an einen Mitarbeiter von Xplain («W»), und zwar sowohl an dessen Adresse [W]@fedpol.admin.ch als auch an dessen Adresse [W]@xplain.ch.

94 Z gab Folgendes an:

> *«Hallo [Vorname von W]*
>
> *Kannst Du das Select Skript für die Meldungen gemäss Excel ausführen. Und dann auf blockiert Zuteilungen untersuchen.*
>
> *Aber noch kein Update Script ausführen.*
>
> *Gruss [Vorname von Z]».*

95 Die E-Mail enthielt als Anhang die Datei [redacted].xlsx». Die 1 045 Zeilen dieser Tabelle enthielten Informationen zu Interpol-Ausschreibungen verschiedener Kategorien, d. h. rote, blaue oder gelbe Ausschreibungen, in 32 Spalten, darunter die folgenden:

- Dringlichkeit;
- Meldungsnummer;
- Meldungstyp;
- Datum Eingang;
- Absender;
- Referenz;
- Bemerkung.

96 In der Spalte «Bemerkung» waren in 785 Zeilen Informationen über natürliche Personen enthalten. Diese Personen sind wahrscheinlich Ziel der entsprechenden Interpol-Ausschreibung oder darin genannt. Je nach Fall enthielten diese Informationen die folgenden Elemente:

- Name und Vorname;
- Geschlecht;
- Geburtsdatum;
- Nationalität;
- Hyperlink zur Interpol-Ausschreibung;
- gegebenenfalls den Grund der Meldung (z. B.: «*extradited*»).

97 Die Untersuchung ergab nicht, ob Z die fragliche Excel-Datei zuvor von einem fedpol-Mitarbeitenden erhalten hatte oder ob Z selbst eine Datenextraktion aus dem ORMA-Produktionssystem vorgenommen hatte und wenn ja, unter welchen Umständen.

98 Zwei Tage später, am 3. September 2021 um 9.49 Uhr, sendete W eine E-Mail mit dem Betreff [redacted].*xlsx* [redacted]» von seiner Adresse [W]@fedpol.admin.ch an seine Adresse [W]@xplain.ch sowie an die Adresse eines anderen Mitarbeitenden von Xplain («X»; [X]@xplain.ch).[55]

99 Die E-Mail enthielt keinen Text.

100 Die E-Mail enthielt als Anhang eine Excel-Datei mit dem Titel [redacted].*xlsx*»[56]. Es handelte sich um eine Tabelle mit 228 Zeilen, die einen Teil der 1 045 Zeilen der Datei [redacted].xlsx» enthielten. Die Tabelle beinhaltete ausserdem die gleichen 32 Spalten wie die oben genannte Datei.

4. Zugriffs-Fall: eine Excel-Tabelle (ORMA-Extraktion), die den «Betreff» der Fälle enthielt (22. September 2011)

101 Die Zugriffs-Hypothese hat sich ebenfalls bestätigt, zumindest in Bezug auf fedpol. Das Untersuchungsorgan hat keine Zugriffs-Fälle bei den anderen von der Untersuchung direkt betroffenen Einheiten festgestellt.

102 Der Hintergrund ist folgender: fedpol betreibt mehrere polizeiliche Informationssysteme im Sinne von Artikel 9 ff. BPI. Diese Systeme enthalten Daten, die von Bundes- und Kantonsbehörden im Bereich der Strafverfolgung, der Polizei und der inneren Sicherheit verarbeitet werden.

103 Im Untersuchungszeitraum diente ORMA als IT-Lösung von fedpol für das computergestützte interne Geschäfts- und Aktenverwaltungssystem, d. h. für die Kategorie «Geschäftskontrolle und Aktenverwaltung» («GA») im Sinne von Artikel 18 BPI.[57] Die Anwendung bildet die Unterkategorie der Geschäftskontrolle insbesondere für die Informationssysteme JANUS (mittlerweile: «NES»; Art. 5 Bst. d der NES-Verordnung) und IPAS von fedpol (Art. 5 der IPAS-Verordnung).[58]

104 Daten, die sich auf die Unterkategorie GA von JANUS und IPAS beziehen, müssen grundsätzlich nach Ablauf einer Aufbewahrungsfrist von drei Jahren gelöscht werden, es sei denn, sie weisen eine Verbindung zu einem anderen Subsystem oder einer anderen Unterkategorie auf (Art. 22 Abs. 6 der NES-Verordnung; Art. 9 Abs. 8 der IPAS-Verordnung).

[55] AUD-03.10.06.1.
[56] AUD B03.10.06.01.
[57] AUD B03.04.10.1261.
[58] Ziff. 8 Abs. 2 Bst. d Bearbeitungsreglement IPAS (AUD-B03.03.10.886); Ziff. 27 Abs. 1 Bearbeitungsreglement JANUS (AUD B03.04.10.975).

105 Am 2. September 2010 um 11.01 Uhr sendete ein Mitarbeiter von fedpol («E») eine unverschlüsselte E-Mail mit dem Betreff [redacted] » an einen anderen Mitarbeiter von fedpol («F»).[59] E gab an, dass er, wie mündlich angekündigt, im Hinblick auf eine bevorstehende ORMA-Löschung eine Liste mit den folgenden Kriterien benötige:

> • *ORMA-Meldungen, vor dem 1.7.2007 erfasst und keinem Dossier zugeteilt (Feld Dossier = leer)*
>
> • *Meldungen und PR (keine EP)*

106 E bat F, ihm eine solche Liste im Excel-Format zu schicken, «*[a]nalog der Auswertung aus dem Jahr 2008*». E fügte noch Folgendes hinzu:

> *«Nach erhalt der Liste werde ich diverse Daten sichten und prüfen, evtl. werde ich mich erneut mit Dir in Verbindung setzen.*
>
> *Danach werden die Abteilungen informiert und gebeten, die Daten zu prüfen und wenn nötig mit dem fehlenden Dossier zu ergänzen, damit diese nicht gelöscht werden. Nicht bearbeitete Meldungen werden gemäss Janus VO Art. 22, Abs. 6 nach 3 Jahren ab deren Erfassung gelöscht.»*

107 Eine Stunde später, am 2. September 2010 um 12.04 Uhr, leitete F die oben genannte E-Mail an einen Mitarbeiter von Xplain («S») an dessen Adresse [S]@xplain.ch weiter und bat ihn um Folgendes:[60]

> *«Tschou [Spitzname von S]*
>
> *Dies wäre ein weiterer Task für nach Deinen Ferien.*
>
> *Bitte wie im Jahr 2008 dies mittels Skript auf der DB abschecken und die Ausgabe als Excel file zustellen. Bitte bis 20.09.2010 Feedback an [E] und mich ein "cc" senden.*
>
> *Gruess».*

108 Ungefähr zwei Wochen später, am 17. September 2010, sendete S eine unverschlüsselte E-Mail von seiner Adresse [S]@xplain.ch an E, mit F in Kopie.

109 S gab Folgendes an:[61]

> *«Hallo [Vorname von E],*
>
> *Im Anhang sende ich Dir die gewünschte Liste.*
>
> *Bei Fragen, bin ich nächsten Mittwoch wieder bei Fedpol erreichbar. Tel direkt: [*****]*
>
> *Grüsse,*
>
> *[Vorname von S]»*

110 Die unverschlüsselte E-Mail, die von S aus der IT-Umgebung von Xplain gesendet worden war, enthielt zwei Anhänge:

- eine Excel-Tabelle mit dem Titel [redacted] *.xls*»[62] und

[59] AUD 03.10.02.1.
[60] AUD 03.10.02.3.
[61] AUD 03.10.02.6.
[62] AUD B03.10.02.01.

- ein Dokument mit dem Titel [redacted]*.pdf*»[63] mit fedpol-Kopfzeile.

111 Im Wesentlichen enthielt die Excel-Tabelle [redacted]*.xls*» eine Spalte C mit dem Titel «Betreff» mit 8 446 Zeilen mit Informationen zu verschiedenen Verfahren, insbesondere Strafverfahren, in die fedpol involviert war, d. h. je nach Fall:

- Name oder Vorname der an den Verfahren beteiligten natürlichen Personen (insbesondere als Beschuldigte);
- vorgeworfene Straftat;
- Telefonnummern;
- E-Mail-Adressen;
- von fedpol durchgeführte Ermittlungsmassnahmen.

112 Die Datei enthielt ebenfalls eine Spalte «*Meldungs Nr und Kurzauskunft*», in der die Meldungsnummer und verschiedene damit zusammenhängende Informationen aufgeführt waren, darunter die beteiligten in- und ausländischen Behörden, die mögliche Beteiligung von Interpol und die betroffenen Daten.

113 Auf Nachfrage des Untersuchungsorgans gab F an, dass im Rahmen dieser ORMA-Datenlöschung nur die Meldungsnummer für die Arbeit von S erforderlich war: «*Und eben, die Löscharbeiten… [E] war jahrelang auch beim Kontrolldienst tätig, und sie haben uns gesagt, das, das, das muss gelöscht werden. Und da musste [S] auf die Datenbank ein Skript erstellen, das heisst für ihm relevant war natürlich die Nummer. Der Betreff war ihm eigentlich egal. Also es kam auch auf keinem Skript darauf*.»[64]

114 Das Untersuchungsorgan leitet aus den vorstehenden Ausführungen ab, dass S, ein Mitarbeiter von Xplain, zum Zeitpunkt der Ereignisse (September 2010) Zugang zum Produktionssystem ORMA von fedpol hatte, weshalb er in der Lage war, Daten aus diesem System zu extrahieren. Unter tatsächlichen Umständen, die im Rahmen der Untersuchung nicht abschliessend geklärt werden konnten, befand sich eine Excel-Datei mit Daten aus dem ORMA-Produktionssystem, die S im Auftrag von F (Mitarbeiter von fedpol) extrahiert hatte, in der IT-Umgebung von Xplain. Dann schickte S diese Datei in einer unverschlüsselten E-Mail von seiner Adresse [S]@xplain.ch an verschiedene Mitarbeiter von fedpol an deren Adresse @fedpol.admin.ch.

115 Aufgrund der Aussagen von F und der Tatsache, dass es sich um regelmässige Löscharbeiten handelt, ist es nicht ausgeschlossen, dass die oben beschriebenen Vorfälle auch bei der Löschung der ORMA-Daten vor oder nach 2010 aufgetreten sind. Wir haben jedoch auf Basis der Exchange-Daten keine weiteren E-Mails von S identifiziert, die einen Anhang enthalten, der mit dem im Randziffer 111 beschriebenen vergleichbar ist.

5. «Aktiver Transfer»-Fall Nr. 1: Screenshots, die im Rahmen der PAGIRUS-TROVA-Migration gesendet wurden (28. Januar 2016)

116 Die «Aktiver Transfer»-Hypothese wurde ebenfalls bestätigt. Sie wird insbesondere durch den vorliegenden Fall veranschaulicht.

117 Der Hintergrund ist folgender: Ein Mitarbeiter des BJ («G») sendete am 28. Januar 2016 um 10.50 Uhr von seiner Adresse [G]@bj.admin.ch eine unverschlüsselte E-Mail mit dem Titel [redacted]

[63] AUD B03.10.02.08.
[64] Tonaufnahme der Befragung Nr. 231129-000, ab 1’07’15.

[redacted] an einen Mitarbeiter von Xplain («T») an dessen Adresse [T]@xplain.ch und an eine bundesexterne Person («P»; [P]@[***].ch). Laut seiner Website bietet P Dienstleistungen als IT-Berater an. Zwei Mitarbeiter des BJ waren in Kopie gesetzt.[65]

118 Die fragliche E-Mail wurde im Zusammenhang mit der Datenmigration vom PAGIRUS-System zum TROVA-System versandt («[redacted] *Bei Fragen stehen wir gerne zur Verfügung*»).

119 Die fragliche E-Mail enthält 14 Anhänge im Word-Format mit folgenden Titeln:

- [redacted] *docx*[66]
- [redacted] *docx*[67]
- [redacted] *doc*[68]
- [redacted] *doc*[69]
- [redacted] *doc*[70]
- [redacted] *doc*[71]
- [redacted] *doc*[72]
- [redacted] *doc*[73]
- [redacted] *.doc*[75]
- [redacted] *.doc*[76]
- [redacted] *docx*[77]
- [redacted] *docx*[78]
- [redacted] *.doc*[79]

120 Einige dieser Anhänge enthielten Informationen über Personen, Gesellschaften oder Behörden, die insbesondere im Zusammenhang mit Rechtshilfeverfahren in Strafsachen stehen.

[65] AUD 03.10.01.1.
[66] B03.10.01.01.
[67] B03.10.01.02.
[68] B03.10.01.03.
[69] B03.10.01.04.
[70] B03.10.01.05.
[71] B03.10.01.06.
[72] B03.10.01.07.
[73] B03.10.01.08.
[74] B03.10.01.09.
[75] B03.10.01.10.
[76] B03.10.01.11.
[77] B03.10.01.12.
[78] B03.10.01.13.
[79] B03.10.01.14.

121 Der Anhang «[redacted].*doc*» enthielt einen Screenshot des Deckblatts einer Verfügung der Beschwerdekammer des Bundesstrafgerichts vom 22. Februar 2007, die im Rahmen eines internationalen Rechtshilfeverfahrens in Strafsachen erlassen wurde. Die Namen der Parteien wurden weder geschwärzt noch anonymisiert. Die Adresse der beschwerdeführenden Person ist ebenfalls angegeben.

122 Der Anhang [redacted].*docx*» ist ein Dokument mit Screenshots der PAGIRUS-Anwendung, in denen die Firmennamen von juristischen Personen, deren Vermögenswerte beschlagnahmt oder zurückgegeben wurden, sichtbar sind.

6. «Aktiver Transfer»-Fall Nr. 2: eine Excel-Tabelle mit 156 Patrouillen der Militärpolizei (30. Juli 2020)

123 Der Hintergrund ist folgender: Ein Mitarbeiter der Militärpolizei («H») sendete am 29. Juli 2020 um 13.40 Uhr eine E-Mail mit dem Titel [redacted]» von [H]@vtg.admin.ch an einen Mitarbeiter der FUB («I») an dessen Adresse [I]@vtg.admin.ch.[80]

124 Im Wesentlichen teilte H mit, dass er 156 neue Patrouillen in die JORASYS-Anwendung einfügen müsse, dass dies jedoch sehr zeitaufwendig sei und er deshalb Unterstützung benötige:

> *«Ich muss 156 neue Patrouillen im JORASYS-System anlegen.*
>
> *Aber diese Operation nimmt viel Zeit in Anspruch. Deshalb komme ich zu Ihnen, um zu sehen, ob es möglich ist, die derzeitige Liste "1970 Patrouillennummer" durch diese neue, von mir erstellte Liste zu ersetzen.»*

125 Diese E-Mail war in nachfolgenden E-Mails enthalten und der Text, den sie enthielt, war somit sichtbar. Es gibt keinen Hinweis darauf, dass der Text in den nachfolgenden E-Mails verändert wurde. Die ursprüngliche E-Mail ist jedoch nicht in den uns vorliegenden Daten enthalten.

126 Weniger als zehn Minuten später (29. Juli 2020, 13.49 Uhr) antwortete I in einer unverschlüsselten E Mail an H und bat ihn, einen «Incident» bei der Hotline der FUB zu eröffnen, damit I diesen «an den Dienstleister» weiterleiten könne:[81]

> *«Guten Tag [***] [Name von H]*
>
> *Damit ich das dem Lieferanten zustellen kann, benötige ich einen Incident. Können Sie bitte einen Incident bei ser FUB Hotline eröffnen lassen.»*

127 Etwa zwei Stunden später (29. Juli 2020, 15.44 Uhr) sendete H eine E-Mail von seiner Adresse [H]@vtg.admin.ch an den Service Desk der FUB, mit einer Kopie an I.[82]

128 Im Wesentlichen bat H den Desk Service der FUB, einen Vorfall zu eröffnen und diesen an folgende Adresse weiterzuleiten: «*bitte öffnen Sie einen Vorfall und leiten Sie ihn an [Name/Vorname von I] (*[I]*@vtg.admin.ch) weiter*.»

129 Diese E-Mail war in nachfolgenden E-Mails enthalten und der Text, den sie enthielt, war somit sichtbar. Es gibt keinen Hinweis darauf, dass der Text in den nachfolgenden E-Mails verändert wurde. Die ursprüngliche E-Mail ist jedoch nicht in den uns vorliegenden Daten enthalten.

[80] AUD 03.10.05.1-4.
[81] AUD 03.10.05.1-4.
[82] AUD 03.10.05.5-8.

130 Am nächsten Tag (30. Juli 2020, 7.50 Uhr) leitete I die E-Mail mit dem Betreff [redacted] als unverschlüsselte E-Mail an einen Mitarbeiter von Xplain («U») an dessen Adresse [U]@xplain.ch sowie an die Adresse support@xplain.ch weiter.[83] H erhielt eine Kopie.

131 Im Wesentlichen schrieb I Folgendes:

> *«Guten Tag Herr [Name von U]*
>
> *Können Sie das bitte anschauen.*
>
> [redacted]
>
> *Beste Grüsse*
>
> *[Vorname und Name von I] »*

132 Diese E-Mail enthielt einen Anhang mit dem Titel «[redacted]*.xls*».[84] Es handelte sich dabei um eine Excel-Tabelle (.xls) mit 264 Zeilen und einem Dutzend Spalten. Diese Zeilen und Spalten enthielten eindeutig Daten über die 156 Patrouillen der Militärpolizei, die H in seinen oben genannten E-Mails erwähnt hatte. Die Tabelle enthielt einige oder alle der folgenden Elemente:

- Vorname und Name der natürlichen Personen,
- Handynummern,
- Dienstort,
- Ort des Dienstantritts.

133 Etwa eine Stunde später (30. Juli 2020, 9.29 Uhr) sendete Q eine unverschlüsselte E-Mail von der Adresse support@xplain.ch an I. Q schrieb Folgendes:[85]

> *«Guten Tag,*
>
> *in der Beilage finden Sie das DB-Script, das die neuen Patrouillen einfügt und die alten inaktiv setzt.*
>
> *Darf ich Sie bitten, dieses Script zuerst auf der Test- und dann auf der Produktionsumgebung ausführen zu lassen.*
>
> *Freundliche Grüsse*
>
> *[Q].»*

134 Die unverschlüsselte E-Mail von Q enthielt als Anhang eine Datei mit dem Titel «[redacted]sql».[86] Diese Datei enthielt insbesondere die Informationen über die neuen Patrouillen der Militärpolizei aus der oben genannten Excel-Tabelle (einschliesslich Vorname, Name, Handynummer).

135 Am selben Tag (30. Juli 2020) um 15.52 Uhr informierte I schliesslich H per E-Mail über Folgendes, mit Kopie an U und an die Adresse support@xplain.ch: «*Wir haben das erfolgreich auf die Produktion gespielt*.»

---

[83] AUD 03.10.05.5-8.
[84] AUD B03.10.05.01.
[85] AUD 03.10.05.9-12.
[86] AUD B03.10.05.03.

7. «Aktiver Transfer»-Fall Nr. 3: Screenshot eines Ausschnitts einer Anhörung (12. Januar 2018)

136 Der Hintergrund ist folgender: Ein Mitarbeiter von fedpol sendete am 11. Januar 2018 um 11.37 Uhr von seiner Adresse @fedpol.admin.ch eine unverschlüsselte E-Mail an den Service Desk des JANUS-Systems (bkpjanushelp@fedpol.admin.ch) und bat um Unterstützung bezüglich eines Problems mit der Darstellung und Formatierung der in ORMA erzeugten Dokumente:[87]

> *«Beim Erstellen eines Berichtes, bzw. beim einfügen des Sachverhaltes wurde festgestellt, dass sich die Nummern der Untertitel in der Formatvorlage nicht auf den dazugehörenden Haupttitel beziehen. Der Nummerierungswert kann auch nicht neu festgelegt werden, da diese Funktion nicht aktiviert ist.*
>
> *Des Weiteren ist die ganze Formatvorlage in einer 1er-Zeilenschaltung definiert. Gemäss gängiger Rapportlehre sollte der ganze Sachverhalt in 1.5-Zeilenschaltung erstellt werden.»*

137 Diese E-Mail enthielt insbesondere einen Screenshot des Protokolls einer Anhörung, die offenbar von fedpol durchgeführt worden war. Der Vor- und Nachname der angehörten Person war ebenso zu sehen wie ihre Aussagen (jedoch nicht wörtlich).

138 Diese E-Mail war in nachfolgenden E-Mails enthalten und der Text sowie die Screenshots, die sie enthielt, waren somit sichtbar. Es gibt keinen Hinweis darauf, dass der Inhalt in den nachfolgenden E-Mails verändert wurde. Die ursprüngliche E-Mail ist jedoch nicht in den uns vorliegenden Daten enthalten.

139 Ungefähr sieben Stunden später (11. Januar 2018, 18.21 Uhr) leitete ein Mitarbeiter des Service Desk «Janus» diese E-Mail von der Adresse bkpjanushelp@fedpol.admin.ch per unverschlüsselter E-Mail an zwei Mitarbeitende von fedpol weiter.

140 Bei diesen Mitarbeitenden handelte es sich zum einen um F und zum anderen um S, der 2010 bei Xplain angestellt[88], 2018 aber bei fedpol beschäftigt war. Gemäss den von fedpol erhaltenen Informationen begann das Arbeitsverhältnis zwischen fedpol und S am 1. Dezember 2015.[89]

141 Der Mitarbeiter des Service Desk «Janus» schrieb Folgendes:

> *«Könntet ihr bitten den Vorschlag von Herrn [Name des fedpol-Nutzers], prüfen? Das Problem mit der Formatvorlagen kommt auch bei mir vor.*
>
> *Ich konnte leider nicht herausfinden, wie man die Anzeigeprobleme lösen kann. Wisst ihr wo das Problem liegt?»* [90]

142 Am nächsten Tag (12. Januar 2018, 11.56 Uhr) leitete F von seiner Adresse [F]@fedpol.admin.ch die beiden oben genannten E-Mails vom 11. Januar 2018 per unverschlüsselter E-Mail mit dem Titel «[redacted]» an T an seine Adresse [T]@xplain.ch weiter. S war in Kopie gesetzt.

143 In dieser E-Mail erwähnte F die Probleme bei der Darstellung der in ORMA erstellten Dokumente und bat ihn um Unterstützung:[91]

> *«Hallo [Vorname von T]*

[87] AUD 03.10.02.21.
[88] Vgl. Rz. 107 oben sowie AUD B03.04.10.237; AUD B03.04.10.208.
[89] AUD B03.04.10.715.
[90] AUD 03.10.02.21.
[91] AUD 03.10.02.26.

Da haben wir trotzt Fix noch ein Problem mit der Formatvorlage. Jede Überschrift muss nochmals eingestellt werden mittels der Wordfunktion.
Siehe Bild 1 welches ich erstellt habe und jenes von den User die es bemängelt haben. Desweiteren sind die Abstände nicht in Ordnung mit einer Überschrift 2 beispielsweise.

Schaue es Dir nochmals an und sag uns was hierfür gemacht werden kann.»

144 Am selben Tag (12. Januar 2018, 15.37 Uhr) antwortete T in einer unverschlüsselten E-Mail an F mit S in Kopie:[92]

«Hallo [Vorname von F]

Ich schaue dies mit diesem Focus an. (…)»

8. «Aktiver Transfer»-Fall Nr. 4: ein im Rahmen einer Supportanfrage übermitteltes Video, in dem Namen und Adressen von Beschuldigten, Zeugen, Anwälten sowie Ermittlern in einem Strafverfahren enthüllt werden (12. Dezember 2014)

145 Der Hintergrund ist folgender: Ende 2014 hatten Ermittlerinnen und Ermittler von fedpol anscheinend eine Verzögerungen und Probleme bei der Nutzung von ORMA festgestellt.[93] Die Anwendung war insbesondere im Offlinebetrieb («*offline Funktionalität*»)[94] beeinträchtigt.

146 Am 17. Dezember 2014 sendete F eine E-Mail an S ([S]@xplain.ch) und ein Verwaltungsratsmitglied von Xplain («V») ([V]@xplain.ch), in der er unter anderem Folgendes schrieb:

«Die grösste Problematik stellt die „offline Funktionalität". Die Ermittler haben mit ORMA zur Zeit kein stabiles offline Tool mehr, um ihre Hausdurchsuchungen und externe offline Einvernahmen zu bewerkstelligen!

(…)

Die derzeitige Situation ist wirklich sehr unglücklich und ernst zu nehmen!».[95]

147 Der hier beschriebene Fall steht im Zusammenhang mit den Arbeiten von fedpol und Xplain zur Behebung dieser Probleme.

148 Am 12. Dezember 2014 um 13.21 Uhr sendete F eine unverschlüsselte E-Mail mit dem Betreff «Fwd: [redacted]» an S an dessen Adresse [S]@xplain.ch:[96]

« Tschou [Spitzname von S]

Schau mal folgende Problematik mit den WinWord Instanzen. Meinst Du das wir solches auch in den Griff bekommen? Insgesamt sind 3 Dokumente geöffnet und es kann nicht richtig gesteuert werden.

LG

[Vorname von F]

[92] AUD 03.10.02.33.
[93] AUD 03.10.02.10-11.
[94] AUD 03.10.02.10-11.
[95] AUD 03.10.02.10-11.
[96] AUD 03.10.02.8.

Von meinem iPhone gesendet».

149 Die E-Mail enthielt einen Anhang mit dem Titel «[redacted]*.zip*». Diese komprimierte Datei (.zip) enthielt ihrerseits eine Datei mit dem Titel «[redacted]*MP4*».[97] Im Wesentlichen handelte es sich um eine 71 Sekunden lange Videoaufnahme im MP4-Format, die eine «*Windows-Remoteunterstützung*» wiedergibt, die einem fedpol-Ermittler gewährt wurde.

150 Ab Sekunde 00:29 der Aufzeichnung ist das Protokoll einer Zeugenbefragung, die von der Bundesanwaltschaft im Rahmen eines Strafverfahrens an fedpol delegiert wurde, auf dem Bildschirm zu sehen. Folgende Elemente sind sichtbar:

- Name und Vornamen des Zeugen;
- Geburtsdatum und -ort des Zeugen;
- Nationalität des Zeugen;
- Aufenthaltsgenehmigung und Gültigkeit der Genehmigung;
- Sprache des Zeugen;
- Name der Eltern des Zeugen;
- Zivilstand – Name und Vorname des Ehepartners;
- Beruf des Zeugen;
- Wohnanschrift des Zeugen;
- Datum, Ort und Uhrzeit der Befragung;
- Nr. des Strafverfahrens;
- Name und Vorname der beschuldigten Personen, mit den für jede von ihnen vermuteten Straftaten;
- Name und Vornamen des Ermittlers und des Protokollführers;
- Vermerk, dass der Dolmetscher der Bundeskriminalpolizei bekannt ist;
- Name und Vornamen von Anwälten.

151 Einige Wochen später, am 6. Januar 2015 um 11:34 Uhr, stellte der Ermittler, der die Remote-Unterstützung erhalten hatte, die in den oben genannten Videoaufnahmen aufgezeichnet worden war, neue Probleme mit ORMA fest und wandte sich per E-Mail an einen anderen Mitarbeiter von fedpol («J»).[98]

152 Diese E-Mail war in nachfolgenden E-Mails enthalten und der Text sowie die Screenshots, die sie enthielt, waren somit sichtbar. Es gibt keinen Hinweis darauf, dass der Inhalt in den nachfolgenden E-Mails verändert wurde. Die ursprüngliche E-Mail ist jedoch nicht in den uns vorliegenden Daten enthalten.

153 Etwa fünfzehn Minuten später (6. Januar 2015, 11.50 Uhr) leitete J die oben genannte E-Mail vom Ermittler unverschlüsselt mit dem Betreff «[redacted] !!!» an die Adresse support@xplain.ch mit einer Kopie an F weiter:

[97] AUD B03.10.02.09.
[98] AUD 03.10.02.13-17.

«Hallo zäme

Ich wünsche euch allen ein erfolgreiches und glückliches 2015!

Leider gibt's auch in diesem Jahr wieder Supportanfragen – hier hat [Vorname des Ermittlers] Probleme mit ORMA, die sogar sein Programm beenden.

Habt Ihr eine Idee, woran das liegen könnte?

Vielen Dank für eure Bemühungen».[99]

154 Die von J an Xplain weitergeleitete E-Mail enthielt vier Screenshots, auf denen ein Teil der ersten Seite eines Berichts von fedpol über die Zeugenbefragung, von der das Protokoll in den oben genannten Videoaufnahmen gezeigt wurde, sowie ein Teil der ersten Seite eines anderen Berichts von fedpol zu sehen waren. Im erstgenannten Bericht wird erwähnt, dass der fragliche Zeuge im Rahmen seiner Befragung zwei DVDs übergeben hat. Die folgenden Informationen waren ebenfalls zu sehen:

- Name des Zeugen;
- Geburtsdatum des Zeugen;
- Nationalität des Zeugen;
- Name der Eltern des Zeugen;
- Zivilstand – Name und Vorname des Ehepartners;
- Datum und Ort der Befragung.

155 Diese Informationen waren identisch mit denen, die auf der oben genannten Videoaufnahme ersichtlich waren.

9. «Halbautomatischer Transfer»-Fall: die «Error-Reporting»-Funktion

a) Allgemeine Beschreibung

156 Nach den Erkenntnissen des Untersuchungsorgans konnte mit der sogenannten «Error-Reporting»-Funktion (oder Fehlermeldungs-Funktion) ein in einer Anwendung aufgetretener Fehler zwecks Analyse und Behebung aufgezeichnet werden. Xplain hat diese Funktion in verschiedene von ihr entwickelte Anwendungen integriert. Das Ziel von Xplain bestand anscheinend darin, den Support für die Benutzerinnen und Benutzer zu erleichtern.[100]

157 Die Funktion wurde zumindest in den folgenden Anwendungen identifiziert: ORMA (fedpol), TROVA (BJ), eneXs (BAZG) und JORASYS (MP und FUB).[101]

158 Es gab Hinweise darauf, dass die Funktion in ORMA bereits im September 2017, aber auf jeden Fall ab 2019 integriert wurde.[102] Ein Handbuch vom Juli 2017 mit Xplain-Kopfzeile deutet darauf hin, dass die Error-Reporting-Funktion damals in TROVA vorhanden war.[103] Die Einführung scheint bereits 2015[104] innerhalb von eneXs erfolgt zu sein. In Bezug auf JORASYS scheint es, dass die Funktion auf jeden Fall ab

[99] AUD 03.10.02.13.
[100] AUD 03.10.08.48.
[101] AUD 03.10.10.1-200.
[102] AUD 03.10.10.135-201.
[103] AUD 03.10.10.202-231.
[104] AUD 03.10.10.130-134.

2020 vorhanden war.[105] Letztendlich konnte das genaue Datum der Einführung dieser Funktion in den von Xplain bereitgestellten Anwendungen nicht mit Sicherheit festgestellt werden. Die Funktion scheint in jedem Fall nicht zum selben Zeitpunkt in die oben genannten Anwendungen integriert worden zu sein.

159 Im Wesentlichen sah der Error-Reporting-Prozess wie folgt aus:[106]

- Ein Benutzer stellt während der Nutzung einer Anwendung einen Fehler fest.
- Er aktiviert die Funktion «Error-Reporting», indem er ein Kästchen oder eine Schaltfläche in der betreffenden Anwendung anklickt.
- Der Benutzer reproduziert den von ihm festgestellten Fehler, wodurch die Funktion im Hintergrund folgende Schritte durchführen kann:
    - Aufnahme von Screenshots von allen angeschlossenen Monitoren (ein Bild pro Sekunde);
    - Erstellung eines Protokolls und von Protokolldateien (einschliesslich Logdaten);
    - gegebenenfalls «Durchführung spezifischer Funktionsdiagnosen[107]».
- Der Benutzer beendet den Aufzeichnungsvorgang, indem er ein Kästchen oder eine Schaltfläche zu diesem Zweck anklickt.
- Eine .zip-Datei (in der Regel mit der Bezeichnung [redacted]*[xxx].zip*»), in der alle Screenshots und Protokolldateien (einschliesslich Logdaten) enthalten sind, wird automatisch erstellt.
- Der Benutzer erhält eine Bestätigung der Aufzeichnung und kann auf die gespeicherte .zip-Datei zugreifen.

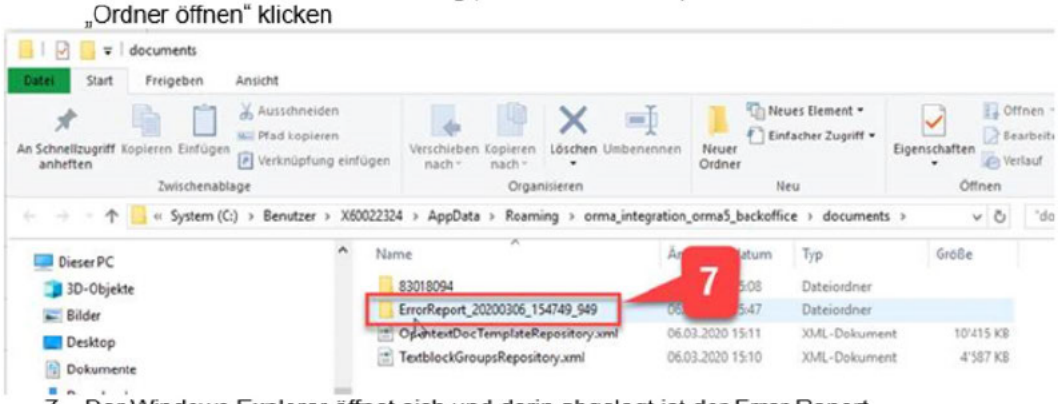
160 Damit der Fehler von den internen Supportmitarbeitenden bearbeitet werden kann, muss die Datei «[redacted]*[xxx].zip*» vom Benutzer an diese weitergeleitet werden. In mehreren Fällen stellten wir fest, dass die .zip-Datei anschliessend vom internen Support an Xplain weitergeleitet wurde. Die identifizierten Übermittlungskanäle sind die folgenden:

- Versand als E-Mail-Anhang;[108]
- Versand als Anhang über die JIRA-Anwendung («Ticketsystem»);
- Bereitstellung der Datei auf der WebFTP-Plattform des BIT;[109] oder
- Ablage der Datei auf dem Netzlaufwerk (T:) der betreffenden Einheit («*T-Laufwerk*»).[110]

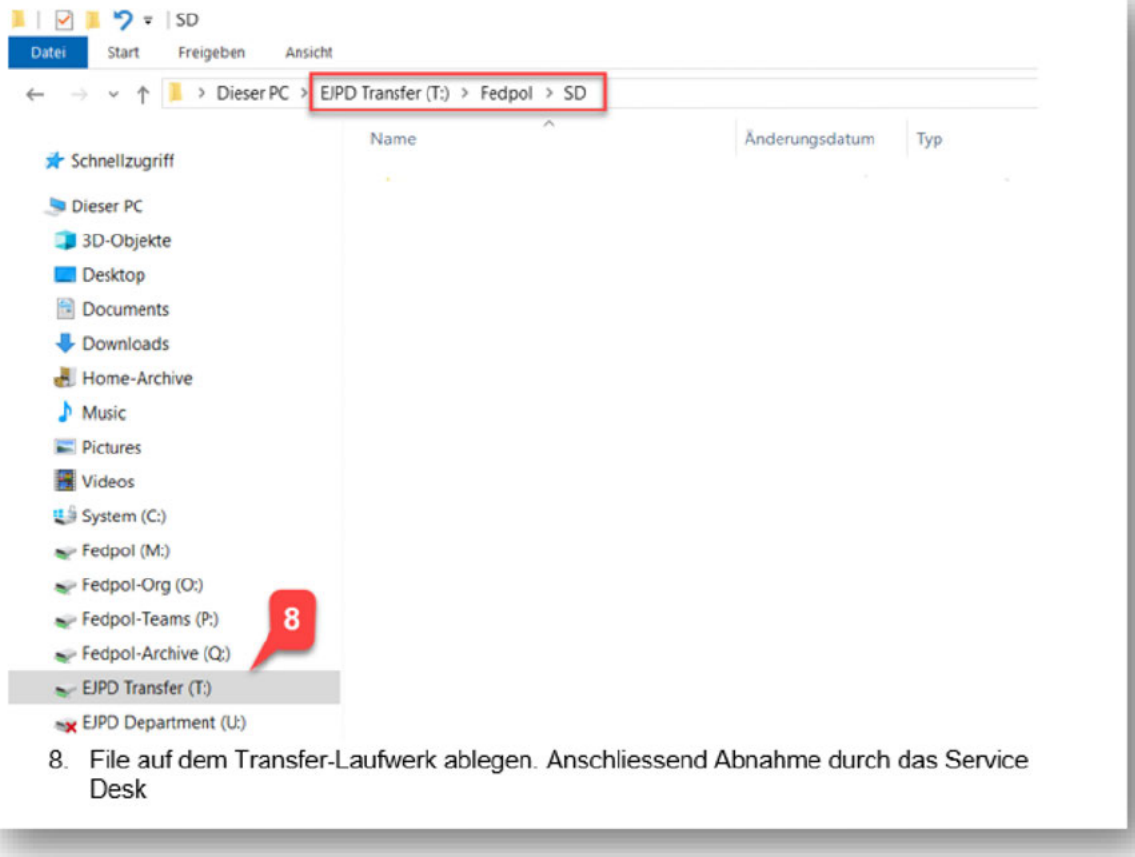
161 Zur Veranschaulichung: Das *Handbuch Service Desk* ORMA vom 23. Oktober 2020 (Version 1.2) mit fedpol-Kopfzeile («Service Desk & Digitale Ausbildung») und dem Vermerk «*Autoren verschiedene*» sah wie folgt aus (Auszug):

[105] AUD 03.10.10.46-129.
[106] AUD 03.04.02.11; AUD 03.06.01.17; B03.06.01.07; AUD 03.10.10.1-200.
[107] Der Begriff wird in einem Benutzerhandbuch verwendet, aber seine genaue Bedeutung ist nicht klar.
[108] Hierbei handelt es sich also, entsprechend den in dieser Untersuchung verwendeten Arbeitshypothesen, um einen «aktiven Transfer» oder einen «Forward».
[109] Siehe zum Beispiel: E-Mail an [R]@xplain.ch von webftp@bit.admin.ch am 15. Juni 2017 um 15.12 Uhr mit dem Betreff «*Word Dokumente im TROVA (www.webftp.admin.ch)*» (AUD 03.10.10.241-244).
[110] AUD 03.06.01.17.

6. Ein Fenster öffnet sich und bestätigt, dass der Error Report erstellt wurde. Nun auf „Ordner öffnen“ klicken



7. Der Windows Explorer öffnet sich und darin abgelegt ist der Error Report.



8. File auf dem Transfer-Laufwerk ablegen. Anschliessend Abnahme durch das Service Desk

162 Diese Funktion könnte als «halbautomatisch» bezeichnet werden.

163 Einerseits setzt sie notwendigerweise einen manuellen Eingriff durch den Benutzer voraus, um die Funktion zu aktivieren und die .zip-Datei an den internen Support zu übermitteln. Um in die IT-Umgebung von Xplain zu gelangen, müssen diese Daten dann übermittelt oder Xplain bereitgestellt werden.

164 Andererseits erfolgt die Aufzeichnung der Bildschirmaktivitäten (auf allen Monitoren) und die Erstellung anderer Daten (insbesondere Protokolldateien) sowie die Erstellung der .zip-Datei automatisch. Ausserdem wurde festgestellt, dass die Dateien [redacted]*[xxx].zip*» teilweise andere Dateien als Printscreens oder Protokolldateien enthalten. Nach den Erkenntnissen des BJ im Mai 2020 wurde am Ende der Aufzeichnung durch die Error-Reporting-Funktion in der Anwendung TROVA das gesamte temporäre Anwendungsverzeichnis automatisch in eine .zip-Datei komprimiert.[111]

165 OA ermittelte jedoch mehrere Benutzerhandbücher für die von Xplain bereitgestellten Anwendungen. Diese Benutzerhandbücher, in der Regel mit Xplain-Kopfzeile, beschreiben mehr oder weniger detailliert, wie der Error-Reporting-Prozess funktioniert.

166 Die meisten dieser Benutzerhandbücher beschränken sich auf den Hinweis, dass alles, was auf dem Bildschirm angezeigt wird, während des Prozesses aufgezeichnet wird («*es wird der gesamte Bildschirm dahinter aufgezeichnet*»). Dies ist zum Beispiel der Fall im Benutzerhandbuch für die oben erwähnte Anwendung TROVA vom August 2017.[112] In Bezug auf die ORMA-Anwendung listet das «ORMA Handbuch Service Desk» vom März 2021 die Schritte des Error-Reporting-Prozesses auf, allerdings ohne die oben genannte Präzisierung.[113]

167 Zwei Benutzerhandbücher enthalten jedoch eine Präzisierung, die in keinem der anderen von OA identifizierten Benutzerhandbücher vorhanden ist (Hervorhebung gemäss Original):

> *ATTENTION : Pendant l'enregistrement des rapports d'erreur, des captures d'écran sont faites de tous les moniteurs connectés. Pour des raisons de protection des données, veuillez fermer toutes les fenêtres contenant des informations sensibles.*[114]
>
> *[frei übersetzt: «ACHTUNG: Während der Aufzeichnung der Fehlerberichte werden Screenshots von allen angeschlossenen Monitoren gemacht. Aus Gründen des Datenschutzes schliessen Sie bitte alle Fenster, die besonders schützenswerte Informationen enthalten.»]*

168 Das erste Benutzerhandbuch betrifft anscheinend eneXs 2.6.2. Es trägt eine Xplain-Kopfzeile und ist in der deutschen Version mit 28. Februar 2020 datiert. Die oben zitierte Passage stammt aus einer französischen Übersetzung eines Teils des Handbuchs (4 Seiten), die anscheinend mit 29. Juli 2021 datiert sind.

169 Das erste Benutzerhandbuch befand sich am 29. Juli 2021 im E-Mail-Postfach eines Mitarbeiters des NDB, der es von Xplain erhalten hatte. Die Zustellung durch Xplain erfolgte auf die Anfrage dieses NDB-Mitarbeiters hin, eine französische Übersetzung für den folgenden Zweck zu erhalten: «*Haben Sie dies Anleitung auch auf französisch? Dann kann ich die Mitarbeiter PSI in Genf informieren.*»[115]

[111] AUD B12.02.01.38 und 40.
[112] AUD 03.10.10.41.
[113] AUD 03.10.10.201.
[114] AUD 03.10.10.132.
[115] AUD 03.10.232-237.

170 Das zweite Benutzerhandbuch betrifft anscheinend JORASYS 0.9.4. Es trägt eine Xplain-Kopfzeile, ist auf April 2022 datiert und umfasst 83 Seiten in deutscher Sprache. Auf Seite 79 enthält es eine ähnliche Erläuterung wie die oben zitierte.

171 Das zweite Benutzerhandbuch befand sich am 26. April 2022 im E-Mail-Postfach eines Mitarbeiters der Militärpolizei, zusammen mit zwei anderen .pdf-Dateien, die er bei derselben Gelegenheit von Xplain erhalten hatte. In seiner Begleit-E-Mail teilte der deutschsprachige Mitarbeiter von Xplain dem französischsprachigen Mitarbeiter der Militärpolizei Folgendes mit:[116]

> *Diese Dokumente benötigen wir am 31.05.2022. Wir können in der nächsten Woche besprechen, was wir am 31.05.2022 machen werden. Für diese Besprechung bitte ich dich, die beiden beigefügten PDF-Dateien zu lesen. Das Benutzerhandbuch musst du nicht lesen, da es einfacher ist, es mit der Anwendung zu benutzen.*

172 Das Untersuchungsorgan ermittelte keine weiteren Informationen, die Schlussfolgerungen über die mögliche Verbreitung dieser beiden Benutzerhandbücher durch die Personen, die sie erhalten haben, zulassen würden.

173 Die Untersuchung ergab zudem, dass ein Mitarbeiter des BJ («L») im Mai 2020 Risiken im Zusammenhang mit der Error-Reporting-Funktion erkannte. In einer E-Mail mit dem Betreff «Übermittlung von Inhalten in den TROVA ErrorReports», die am 7. Mai 2020 an einen Mitarbeiter von Xplain mit Kopie an einen anderen Mitarbeiter des BJ gerichtet war, schrieb er unter anderem Folgendes:

> *«Dabei ist mir aufgefallen, dass bei der Aufzeichnung geöffnete Inhalte (PDF, WORD etc.) pauschal im Report enthalten sind bzw. damit aus TROVA exportiert werden. Dies ist aus datenschutzrechtlichen Gründen und insbesondere aufgrund der sensiblen Daten in TROVA höchst fragwürdigst und schwer zu rechtfertigen.*
>
> *(…)*
>
> *Werde das in JIRA als Verbesserung für das Produkt eingeben, bis dahin können wir als Umgehungslösung ggf. die Inhalte aus dem Report löschen.»*[117]

174 Zwei Monate später, im Juli 2020, eröffnete L ein Ticket auf der JIRA-Plattform mit der Bezeichnung «*Fehlerbericht aufzeichnen: opt-in für Export von Inhalten*». Das Ticket bezieht sich auf einen Verbesserungsvorschlag für TROVA und ist wie folgt zusammengefasst:

> *«Als Benutzer/in von TROVA kann ich beim Erstellen einer Fehlermeldung selbst entscheiden, ob Inhalte, die beim Aufzeichnen des fehlerhaften Anwendungsfalls "betroffen" sind, zusammen mit den weiteren, notwendigen Inhalten/Daten (wie z. B. das Application Log aus dem %appdata%-Verzeichnis) exportiert werden, um die Anforderungen an den Datenschutz besser steuern zu können und die Inhalte nicht im Anschluss nach dem Export einzeln oder überhaupt aus dem ZIP entfernen zu müssen.»*[118]

175 Anschliessend teilte ein Mitarbeiter des BJ, dessen Name in dem uns vorliegenden Dokument nicht genannt wird, Xplain mit, dass die vom BJ gewünschte Verbesserung wahrscheinlich auch für andere Kundinnen und Kunden von Xplain von Interesse oder Relevanz sein könnte («*Vorstellen könnte ich mir hier, dass dies auch für andere Kunden interessant/relevant sein könnte?*»).[119]

---

[116] AUD 03.10.10.238-240.
[117] AUD 03.10.08.1-3.
[118] AUD 03.10.08.7.
[119] AUD 03.10.08.49.

176 Gemäss den uns vorliegenden Daten gab sich Xplain gegenüber der gewünschten Verbesserung zurückhaltend. Im September 2020 schrieb ein Mitarbeiter von Xplain in einer E-Mail Folgendes: «*Das Opt-Out für den Error-Report werden wir nicht umsetzen, da dies aus unserer Sicht keinen Sinn macht. Der Inhalt des Error Reports hilft uns Fehler zu klären. Es gäbe aber die Möglichkeit den Error Report zu deaktivieren, falls er zu Problemen beim Datenschutz führt*».[120]

177 Nachdem Xplain im März 2021 eine Schätzung von 80 Arbeitsstunden für die gewünschte Änderung vorgelegt hatte, schien das BJ die Forderung nach einer Verbesserung von TROVA vorläufig nicht weiter zu verfolgen. Im Juni 2021 vereinbarten Xplain und das BJ anscheinend, dass die besagte Verbesserung bei der Umstellung von Version 1.7 auf Version 2.0 integriert werden sollte, was letztlich offenbar nicht geschah. Trotz der Beibehaltung dieser Funktion in TROVA sollen laut der Befragung eines Mitarbeiters des BJ die Benutzerinnen und Benutzer von TROVA vom BJ Anweisungen zur Nutzung dieser Error-Reporting-Funktion erhalten haben.[121]

178 Nach Abschluss der Untersuchung scheint es nicht, dass das BJ andere Verwaltungseinheiten des Bundes über die Risiken informiert hat, welche die Error-Reporting-Funktion nach seiner eigenen Analyse aus Sicht des Datenschutzes birgt.

179 Wie oben erwähnt, informierte OA die Koordinationsstelle in einer verschlüsselten E-Mail vom 1. Dezember 2023 über die Existenz dieser Funktion. Nach den von der Koordinationsstelle erhaltenen Informationen wurde diese Funktion im Sommer 2023 deaktiviert. Die internen Richtlinien wurden angepasst und die betroffenen Produkte (Software) werden derzeit aktualisiert, um die Funktion endgültig zu entfernen.

b) <u>Beispiel: Versand von Screenshots von Ausweisdokumenten</u>

180 Ein Mitarbeiter des BAZG («M») sendete am 24. Oktober 2016 um 10.21 Uhr von seiner Adresse [M]@bazg.admin.ch eine unverschlüsselte E-Mail mit dem Betreff [redacted]» an einen Mitarbeiter von Xplain («Y») an dessen Adresse [Y]@xplain.ch. Ein weiterer Mitarbeiter des BAZG war in Kopie gesetzt.[122]

181 M teilte Y in dieser E-Mail mit, dass er ihn telefonisch nicht habe erreichen können und dass ZEMIS nicht richtig funktioniere. A bat X ebenfalls, ihn so bald wie möglich zurückzurufen:

> *«Hallo [Spitzname von Y].*
>
> *Konnte dich telefonisch nicht erreichen.*
>
> *Wir haben Probleme mit ZEMIS. Die Verteilung der 1.8.1.0 ist letzte Woche (am 18.10.16) erfolgt. Irgendwas stimmt aber nicht. Bin gerade etwas ratlos.*
>
> *Kannst du mich anrufen sobald du Zeit hast?*
>
> *Merci und Gruss*
>
> *[Spitzname von M]»*

182 ZEMIS ist die Abkürzung für Zentrales Migrationsinformationssystem[123].

[120] AUD 03.10.08.48.
[121] AUD 03.10.08.49.
[122] AUD 03.10.07.1.
[123] SR 142.513.

183 Diese E-Mail enthält einen Anhang mit dem Titel «[redacted].*zip*». Diese komprimierte Datei ist etwa 21 MB gross. Sie enthält Screenshots von Ausweisdokumenten von Personen. Im Wesentlichen sind Name, Vorname, Nationalität und in einem Fall das Passfoto der betreffenden Personen sichtbar.

184 Weniger als fünf Minuten später (24. Oktober 2016, 10.25 Uhr) sendete M eine weitere E-Mail an Y an seine Adresse [Y]@xplain.ch, jedoch ohne Anhang. Der Text ist identisch mit der ersten E-Mail, ausser dass der folgende Satz hinzugefügt wurde:[124]

> *«Habe dir das Error Zip und eine eneXs2 Version welche das Problem hat auf das Transfer LW gelegt. T:\EFD\EZV\GWK ZEMIS.»*

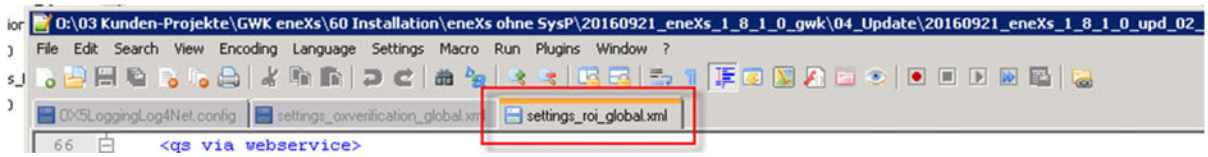
185 «LW» kann in diesem Zusammenhang nur «Laufwerk» bedeuten. Mit anderen Worten, M speicherte die oben genannte komprimierte Datei mit der Bezeichnung «[redacted].*zip*» auf einem Netzlaufwerk des Bundes zuhanden von Y ab.

186 Die Tatsache, dass M zunächst um 10.21 Uhr eine E-Mail an Y an seine Adresse [Y]@xplain.ch mit einer .zip-Datei von etwa 21 MB sendete und dann um 10.25 Uhr dieselbe .zip-Datei auf dem Server T: des Bundes für Y bereitstellte, wirft die Frage auf, ob Y die E-Mail von 10.21 Uhr erhalten hat oder ob sie ihm nicht zugestellt wurde (z. B. wegen der Grösse des Anhangs). In den uns vorliegenden Daten fanden wir keine Fehlermeldung, dass die E-Mail nicht zugestellt wurde, aber wir fanden auch keine Antwort auf die E-Mail von 10.21 Uhr.

187 Dagegen wurde eine Antwort von Y auf die zweite E-Mail von M, die um 10.25 Uhr gesendet wurde, ermittelt.

188 Y übermittelte M in einer unverschlüsselten E-Mail, die am selben Tag (24. Oktober 2016, 14.39 Uhr) von [Y]@xplain.ch gesendet wurde, eine Datei mit der Bezeichnung «[redacted].xml» mit Code und der Bitte, Folgendes zu überprüfen:[125]

Kannst du bitte prüfen ob dort bei dir nach der Verteilung folgendes drin steht:



189 Die folgende automatische Signatur erschien in der Fusszeile der E-Mail, die Y von seiner Adresse [Y]@xplain.ch aus gesendet hat:

Freundliche Grüsse
Y [redacted]

deXplain GmbH
Y [redacted]
Ring 38
D-04416 Markkleeberg
+49 [redacted]
Y [redacted]@xplain.ch
www.xplain.ch

[124] AUD 03.10.07.4.
[125] AUD 03.10.07.7.

190 M antwortete Y weniger als dreissig Minuten später (24. Oktober 2016, 15.04 Uhr) per unverschlüsselter E-Mail und teilte ihm mit, dass das Problem gelöst worden sei: «*Habe den Fehler gefunden*»[126].

10. Datei «[redacted].xml» (September 2015), die einige Daten aus dem Informationssystem HOOGAN enthielt und über die in den Medien berichtet wurde (unbekannter Kanal)

191 Der *Datendump* enthielt eine Datei mit der Bezeichnung [redacted]*.xml*» vom 4. September 2015. Diese Datei beinhaltete Auszüge aus dem von fedpol betriebenen Informationssystem HOOGAN.

192 Im Rahmen der Untersuchung konnten die tatsächlichen Umstände, unter denen diese Datei in die IT-Umgebung von Xplain gelangte, nicht geklärt werden.

11. Excel-Tabelle mit Daten von JORASYS-Benutzerinnen und -Benutzern innerhalb der Militärpolizei, über die in den Medien berichtet wurde (Kanal unbekannt)

193 Der *Datendump* enthielt eine Datei mit der Bezeichnung «[redacted].*xlsx*», die auf den 18. September 2020 datiert ist. Diese Datei enthält 718 Zeilen mit Daten von JORASYS-Benutzerinnen und -Benutzern innerhalb der Militärpolizei.

194 Im Rahmen der Untersuchung konnten die tatsächlichen Umstände, unter denen diese Datei in die IT-Umgebung von Xplain gelangte, nicht geklärt werden.

B. Beziehungen zu Xplain

1. Aufnahme der Geschäftsbeziehung

195 Die lange zurückliegenden Fakten machen es schwierig, den Ursprung der Beziehungen zwischen dem Bund und Xplain zu klären. Die meisten Befragten gaben somit an, nicht zu wissen, wann und wie ihre Verwaltungseinheit mit dem Unternehmen Xplain eine Geschäftsbeziehung aufgenommen habe. Ebenso enthalten die von den betroffenen Einheiten eingereichten Unterlagen und die dem Untersuchungsorgan vorliegenden elektronischen Daten nur wenige Informationen über die Jahre vor 2005.

196 Aus einigen Befragungen sowie aus Verträgen und bestimmten Exchange-Daten geht allerdings hervor, dass die Aufnahme der Geschäftsbeziehungen zwischen Bund und Xplain in den Jahren 2001/2002 stattgefunden hat.

197 Damals erhielten die beiden Xplain-Gründer, die uns als ehemalige Mitarbeiter der in Deutschland ansässigen Firma rola Security Solutions GmbH beschrieben wurden, einen Auftrag des Grenzwachtkorps (GWK). Der Auftrag war Teil des «*Rumaca*»-Projekts des GWK[127]. Xplain hatte nicht die Aufgabe, eine Software zu entwickeln – dies war Sache der Firma UNISYS –, sondern das GWK im Rahmen dieses Projekts zu beraten.

198 Zwischen 2000 und 2003 lieferte Xplain anscheinend zwei Produkte an fedpol (doXstore und noteboX). Eine interne E-Mail von fedpol aus dem Jahr 2010 zeigte, dass die Mitarbeitenden von fedpol Schwierigkeiten hatten, die Dokumentation über die Erteilung dieser Aufträge an Xplain zu ermitteln.[128]

[126] AUD 03.10.07.7.
[127] SHAB, 04.07.2008 (128), Nr. 00311117.
[128] AUD 03.10.09.150-152.

199 Im Anhang zu der betreffenden E-Mail befand sich ein vierseitiges Dokument vom 29. April 2003 mit der Bezeichnung «*Argumentarium für Ausnahmegenehmigung EJPD-GEVER-STRATEGIE*» mit fedpol-Kopfzeile (damals «fedpol.ch»). In diesem Dokument, dessen Verfasser nicht identifiziert wurde, hiess es, dass die Bundeskriminalpolizei (BKP) die Einführung der Anwendung «ORMA» im Jahr 2004 als Tool für die Geschäfts- und Dossierverwaltung plante.

200 Gemäss dem Dokument wurde im Rahmen eines «detaillierten Vergleichs» zwischen den Produkten «FABASOFT» (der gleichnamigen Firma) und «worX» (der Firma Xplain) festgestellt, dass nur das Produkt von Xplain die gestellten Anforderungen erfüllte. Im Zuge der Untersuchung ist es nicht gelungen, diesen «detaillierten Vergleich» ausfindig zu machen.

201 In dem Dokument hiess es dann unter Punkt 5:

5 Zusammenfassung / Vorgaben / Bedingungen

- Termin, Geschäfts- und Dossierverwaltung muss bei Beginn der Dezentralisierung im Februar 2004 voll einsatzfähig sein.
- Die Geschäfts- und Dossierverwaltung muss durchgängig zu bestehenden Systemen wie Rapportsystem, Journal, und Janus+ PV sein. Zudem muss eine Schnittstelle zu IPAS realisiert werden.
- Die Vorschläge von PPS sind zu berücksichtigen.
- Die Lösung soll kostengünstig und flexibel sein, sowie keine präjudizierende Wirkung haben.

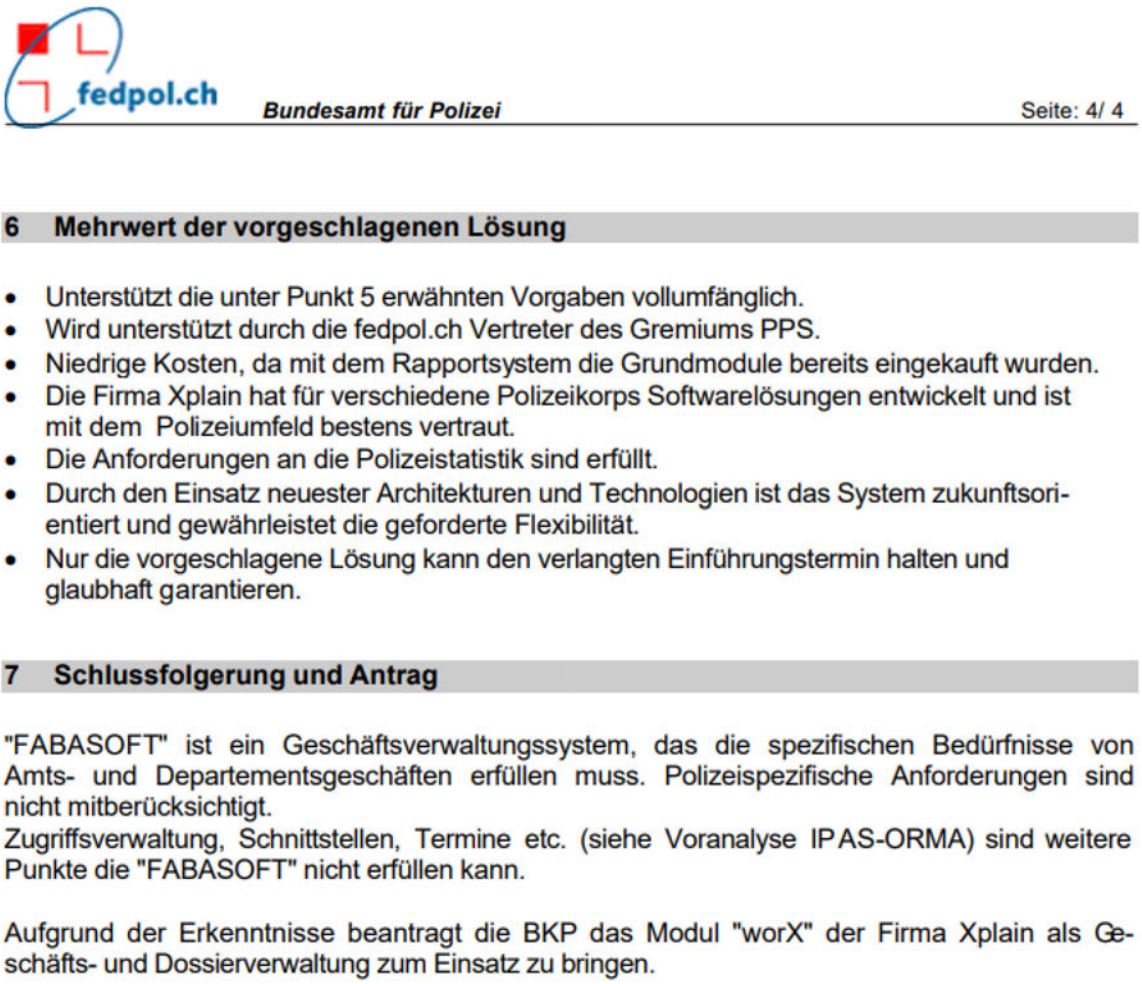
202 Die Abkürzung IPAS bezieht sich auf ein Informationssystem von fedpol: Informatisiertes Personennachweis-, Aktennachweis- und Verwaltungssystem des Bundesamtes für Polizei[129].

203 Die Abkürzung JANUS bezieht sich auf ein Informationssystem der BKP: Elektronisches Informationssystem der Bundeskriminalpolizei[130].

204 Die Abkürzung PPS bezieht sich auf die Einheit «Planung, Projektsteuerung und Standardisierung der polizeilichen Informationsverarbeitung», die bis Ende 2008 zur Abteilung Ressourcen von fedpol gehörte.[131]

205 Das Dokument enthielt schliesslich die folgenden Punkte:[132]

[129] Fedpol, Rechenschaftsbericht 2008, S. 47.
[130] Fedpol, Rechenschaftsbericht 2008, S. 47.
[131] Fedpol, Rechenschaftsbericht 2008, S. 7.
[132] 2003.04.29 Argumentarium Ausnahmegenehmigung.pdf (AUD 03.10.09.62).



fedpol.ch Bundesamt für Polizei Seite: 4/ 4

6 Mehrwert der vorgeschlagenen Lösung

- Unterstützt die unter Punkt 5 erwähnten Vorgaben vollumfänglich.
- Wird unterstützt durch die fedpol.ch Vertreter des Gremiums PPS.
- Niedrige Kosten, da mit dem Rapportsystem die Grundmodule bereits eingekauft wurden.
- Die Firma Xplain hat für verschiedene Polizeikorps Softwarelösungen entwickelt und ist mit dem Polizeiumfeld bestens vertraut.
- Die Anforderungen an die Polizeistatistik sind erfüllt.
- Durch den Einsatz neuester Architekturen und Technologien ist das System zukunftsorientiert und gewährleistet die geforderte Flexibilität.
- Nur die vorgeschlagene Lösung kann den verlangten Einführungstermin halten und glaubhaft garantieren.

7 Schlussfolgerung und Antrag

"FABASOFT" ist ein Geschäftsverwaltungssystem, das die spezifischen Bedürfnisse von Amts- und Departementsgeschäften erfüllen muss. Polizeispezifische Anforderungen sind nicht mitberücksichtigt.
Zugriffsverwaltung, Schnittstellen, Termine etc. (siehe Voranalyse IPAS-ORMA) sind weitere Punkte die "FABASOFT" nicht erfüllen kann.

Aufgrund der Erkenntnisse beantragt die BKP das Modul "worX" der Firma Xplain als Geschäfts- und Dossierverwaltung zum Einsatz zu bringen.

206 Xplain wurde daraufhin von fedpol mit der Entwicklung der ORMA-Anwendung beauftragt, die ab Februar 2004[133] bei fedpol eingesetzt und seitdem von Xplain mehrfach modifiziert und weiterentwickelt wurde.

207 Ab 2008 weiteten sich die Geschäftsbeziehungen zwischen Bund und Xplain auf mehrere Einheiten aus und die Zahl der Verträge vervielfachte sich. Zu den wichtigsten Projekten gehören:

- eneXs (BAZG, früher EZV),
- ESYSP Los4 (ISC-EJPD/SEM/fedpol/EDA),
- JORASYS (MP/FUB),
- ZEUSS (fedpol) und
- ZUPA/TROVA (BJ).

2. Zusammenarbeit

208 In Bezug auf die Zusammenarbeit zwischen den betroffenen Einheiten und Xplain lässt sich Folgendes festhalten.

[133] ORMA 2.3- Optimierungen – Pflichtenheft V1-0, p. 6 (AUD 03.10.09.158).

209 Grundsätzlich liegt dem Untersuchungsorgan bis heute keine vollständige Liste der Verträge vor, die zwischen den von der Untersuchung betroffenen Einheiten und Xplain abgeschlossen wurden. In Anbetracht der Antworten der von der Untersuchung betroffenen Einheiten auf unsere Auskunftsgesuche und der in einigen Antworten genannten Vorbehalte kann nicht mit Sicherheit gesagt werden, dass alle zwischen den von der Untersuchung betroffenen Einheiten und Xplain geschlossenen Verträge identifiziert wurden. Uns ist bewusst, dass, obwohl der Bund über ein Vertragsmanagementsystem verfügt, dieses nicht zwangsläufig alle Verträge enthält, die mit einem bestimmten externen Lieferanten abgeschlossen wurden. Aufgrund dieser Feststellung wird eine Empfehlung ausgesprochen, die im Folgenden erläutert wird.[134]

210 Der Umfang der vertraglichen Beziehungen zwischen dem Bund und Xplain kann auf der Grundlage der Verträge, die OA vorgelegt wurden, wie folgt zusammengefasst werden:

- fedpol fungierte bei rund 100 Verträgen und Zusatzvereinbarungen als Bedarfsstelle im Sinne von Artikel 3 Buchstabe b Org-VöB.
- Das BJ fungierte bei rund 30 Verträgen und Zusatzvereinbarungen als Bedarfsstelle im Sinne von Artikel 3 Buchstabe b Org-VöB.
- Das BAZG fungierte bei rund 20 Verträgen und Zusatzvereinbarungen als Bedarfsstelle im Sinne von Artikel 3 Buchstabe b Org-VöB.
- Das ISC-EJPD fungierte bei fünf Verträgen als Bedarfsstelle im Sinne von Artikel 3 Buchstabe b Org-VöB.
- Das SEM fungierte bei zwei Verträgen als Bedarfsstelle im Sinne von Artikel 3 Buchstabe b Org-VöB. Das SEM schloss zudem im Jahr 2017 einen Vertrag mit dem GWK ab, durch den das GWK dem SEM Zugang zu bestimmten Daten auf dem eneXs-Server des GWK gewährte.
- Die FUB fungierte bei drei Verträgen als Bedarfsstelle im Sinne von Artikel 3 Buchstabe b Org-VöB.
- armasuisse war bei einem der drei oben genannten Verträge, bei denen die FUB als Bedarfsstelle fungierte, die zentrale Beschaffungsstelle im Sinne von Artikel 3 Buchstabe a Org-VöB. armasuisse bestellte zudem Lizenzen bei Xplain in Verbindung mit Quattro P (vgl. weiter unten).
- Das BBL war bei einigen, aber nicht allen Verträgen, in denen fedpol, das BJ, das BAZG, das ISC-EJPD oder die FUB als Bedarfsstellen fungierten, die zentrale Beschaffungsstelle im Sinne von Artikel 3 Buchstabe a Org-VöB.
- Das EDA unterhält keine vertragliche Beziehung zu Xplain. Das EDA erteilte Xplain zwischen 2020 und 2022 vier Aufträge, die auf dem oben genannten Rahmenvertrag zwischen Xplain und dem ISC-EJPD («Los 4 WTO 18021») basierten.
- Das BIT unterhält keine vertragliche Beziehung zu Xplain. Das BIT finanzierte in einem Fall in Absprache mit dem NDB 16 Arbeitsstunden mit dem Vermerk «*Installation/Deployment*», die von Xplain in Verbindung mit Quattro P ausgeführt wurden (vgl. weiter unten).[135]

[134] vgl. Abschnitt VI.B unten.
[135] AUD 03.06.28; AUD B03.06.36; AUD B03.06.37; AUD B03.06.38.

- Die MP, eine Organisationseinheit des Kommandos Operationen (Kdo Op)[136], unterhält keine vertragliche Beziehung zu Xplain. Sie ist Benutzerin einer von Xplain entwickelten Anwendung (JORASYS), die in den oben genannten Verträgen zwischen Xplain und der FUB (Bedarfsstelle) geregelt ist.
- Der NDB unterhält keine vertragliche Beziehung zu Xplain. Im Rahmen von Quattro P (Art. 55 NDG) hat der NDB Zugang zu bestimmten Daten aus dem Bereich Zoll- und Grenzkontrollen.

211 Im Rahmen der Überprüfung der Verträge und mittels der von den befragten Personen bereitgestellten Informationen konnten wir ausserdem unter den von der Untersuchung betroffenen Einheiten diejenigen identifizieren, die innerhalb der IT-Umgebung des Bundes von Xplain entwickelte Produkte genutzt haben, in denen ihre Daten verarbeitet wurden:[137]

- fedpol
- BAZG
- BJ
- MP
- SEM

212 Diese Einheiten werden nachfolgend gemeinsam als «direkt betroffene Einheiten» bezeichnet.

213 Alle OA vorliegenden Verträge wurden zwischen dem Bund und Xplain, der Aktiengesellschaft mit Sitz in Interlaken, geschlossen.[138] Gemäss öffentlich zugänglichen Quellen und mehreren Befragungen verfügt Xplain über Büros in Interlaken.

214 Laut der Website unterhält Xplain auch Büros im Ausland, und zwar in Spanien und Deutschland. In diesem Zusammenhang ergibt sich ebenfalls aus öffentlich zugänglichen Quellen, dass zwei der Verwaltungsratsmitglieder von Xplain zusammen mit anderen Personen ebenfalls Verwaltungsratsmitglieder einer Gesellschaft namens Xplain AG Ibérica S.L. in Madrid sind.[139]

215 In einem Angebot, das Xplain im Jahr 2020 im Rahmen einer Ausschreibung des BAZG mit dem Titel «Personenverwaltung ID-Center» einreichte, heisst es, dass die beiden folgenden Unternehmen «im Besitz der Xplain AG und von Mitarbeitern» sind:[140]

- Xplain AG Ibérica s.L, in Madrid (ES), gegründet 2011, Geschäftsführer: Daniel Löwinger. In dem Dokument heisst es weiter: «*In der Niederlassung Madrid werden Server- und Clientkomponenten sowie mobile Systeme entwickelt. Ein zweites Büro der Xplain AG Ibérica s.L. befindet sich in Ciudad Real. Dort werden wie in Madrid, Server- und Clientkomponenten entwickelt.*»
- deXplain GmbH, in Markkleeburg (DE), gegründet 2013, Geschäftsführer: Sebastian Becker. In dem Dokument heisst es weiter: «*In der Niederlassung Markkleeberg/Leipzig werden u.a. spezialisierte Biometrie-Lösungen entwickelt*».

216 Im oben genannten Angebot von Xplain wird der Begriff «Niederlassungen» verwendet, um diese Unternehmen in Spanien und Deutschland zu beschreiben. Es handelt sich jedoch offensichtlich um

[136] Das Kdo Op ist eine Verwaltungseinheit im Sinne der RVOV.
[137] Der NDB erhielt Daten von einem von Xplain entwickelten Produkt, gab jedoch keine eigenen Daten ein (Tonaufnahme der Befragung Nr. 231116-001, ab 6'20 und ebenso ab 37'30).
[138] UID: CHE-105.545.833.
[139] AUD 13.02.22-23.
[140] AUD 03.10.09.264-265.

Tochtergesellschaften, da eine «S.L. »[141] nach spanischem Recht und eine «GmbH» nach deutschem Recht juristische Personen mit Rechtspersönlichkeit sind.[142]

217 Laut demselben Dokument arbeiteten 21 Personen in Interlaken, 33 Personen in Madrid und eine Person in Leipzig.

218 Zusammengefasst gaben die Befragten an, nicht gewusst zu haben, dass Xplain Standorte im Ausland hat. Andere sagten, ihnen sei dies bekannt gewesen, aber im Grunde sei dies eine interne organisatorische Entscheidung von Xplain und nicht relevant für die Beziehungen zwischen Xplain und dem Bund.

219 Die analysierten Fälle,[143] in denen produktive Daten an Xplain übermittelt wurden, erfolgten im Rahmen von Projekten.

220 Diese Projekte waren durch eine Vertragsdokumentation geregelt, die je nach Datum, an dem die Verträge abgeschlossen wurden, eine starke Heterogenität zwischen den Einheiten sowie innerhalb einer Einheit aufweist, denn uns wurden mehr als 150 Verträge und Zusatzvereinbarungen vorgelegt, wobei die ältesten auf die frühen 2000er Jahren zurückreichen.

221 Die Verträge weisen jedoch einige gemeinsame Merkmale auf:

- Alle Verträge beziehen sich auf die Allgemeinen Geschäftsbedingungen des Bundes und schliessen die Allgemeinen Geschäftsbedingungen von Xplain aus.
- Keiner der Verträge enthält eine Klausel, wonach Xplain mit der Durchführung einer Datenbearbeitung beauftragt wurde.[144] Die von Xplain erwarteten Leistungen sind Beratung, Lieferung, Wartung, Unterstützung und/oder Entwicklung im Bereich Software.

222 Wir werden auf den Inhalt der Verträge in der nachfolgenden rechtlichen Analyse zurückkommen.[145]

223 In Bezug auf die Korrespondenz zwischen den direkt betroffenen Einheiten und Xplain haben wir in den oben analysierten Fällen[146], in denen produktive Daten zur Verfügung gestellt wurden, keine Anweisungen an Xplain in Verbindung mit der Bereitstellung oder Löschung der fraglichen Daten gefunden.

224 Ferner haben wir keine Audits oder Berichte über die Informationssicherheit oder den Datenschutz bei Xplain ausgemacht.

225 Nach dem Wissen der zu diesem Thema befragten Personen hat der Bund bei Xplain nie ein Audit in Bezug auf die Informationssicherheit oder den Datenschutz durchgeführt.

---

[141] «*Sociedad de responsabilidad limitada*».

[142] Artikel 1 und 33 Ley de Sociedades de Capital (Real Decreto Legislativo 1/2010, de 2 de julio; letzte Änderung 29.06.2023; Referenz BOE-A-2010-10544); § 13 GmbH-Gesetz (Gesetz betreffend die Gesellschaften mit beschränkter Haftung; letzte Änderung 22.02.2023; BGBl. I S. 3436).

[143] vgl. Abschnitt IV.A oben.

[144] Xplain unterbreitete der Militärpolizei im November 2022 ein Angebot bezüglich der Archivierung von JORASYS-Ereignissen vom 01.01.1900 bis 31.01.2013, das von der Militärpolizei offenbar nicht akzeptiert wurde (E-Mail vom 1. Dezember 2022, AUD 03.10.09.167-172).

[145] vgl. Abschnitt V.A unten.

[146] vgl. Abschnitt IV.A oben.

V. RECHTLICHE WÜRDIGUNG DES SACHVERHALTS

226 Die vorliegende Administrativuntersuchung betrifft Sachverhalte, die sich über einen Zeitraum von fast 25 Jahren ereignet haben. Während dieses Zeitraums wurden die relevanten Rechtsnormen mehrfach geändert.

227 Der untersuchte Sachverhalt wird unter Berücksichtigung der Rechtsnormen analysiert, die zum Zeitpunkt der Ereignisse galten. Um daraus Erkenntnisse zu gewinnen und Vorschläge zu formulieren (vgl. Abschnitt VI unten), erscheint es uns jedoch notwendig, auch die zum Zeitpunkt dieses Berichts, d. h. am 28. März 2024, geltenden Rechtsnormen darzustellen.

228 Dieser Bericht hat nicht das Ziel oder den Anspruch, die früheren und gegenwärtigen Rechtsnormen in Bezug auf Informationssicherheit oder Datenschutz umfassend zu behandeln. Die Prüfung konzentriert sich auf die im Untersuchungsmandat gestellten Fragen, die wie folgt zusammengefasst werden können (Abschnitte A und B unten).

A. Haben technische, organisatorische oder prozesshafte Mängel innerhalb des Bundes dazu geführt, dass die Xplain AG in den Besitz von produktiven Daten des Bundes gelangt ist?

229 Nach einer Darstellung der relevanten Rechtsnormen (vgl. Ziff. 1 unten) werden wir eine rechtliche Analyse der ermittelten Tatsachen vornehmen (vgl. Ziff. 2 unten).

230 Konkret werden wir einige Beispiele für die Weitergabe produktiver Daten an Xplain über die Kanäle, die in Abschnitt IV.A ermittelt wurden, untersuchen. In Fällen, in denen festgestellt wurde, dass produktive Daten in der IT-Umgebung von Xplain vorhanden waren, aber der Kanal, der dies erklärt, nicht ermittelt werden konnte, beruht die rechtliche Analyse auf Annahmen.

231 Bei der Analyse der einzelnen Fälle werden wir zunächst die Vereinbarkeit der Weitergabe der betreffenden Daten mit dem damals geltenden Recht (mit Ausnahme des Strafrechts) und dann das allfällige Vorliegen von technischen, organisatorischen oder prozesshaften Mängeln untersuchen.

1. Relevante Rechtsnormen

a) Einleitende Bemerkungen

232 Die gestellte Frage bedarf einiger allgemeiner Erläuterungen zum gesetzlichen Rahmen, in dem sie gestellt wird (vgl. b unten). Anschliessend werden die wichtigsten Gesetze und Rechtsverordnungen aufgelistet, die in den für uns relevanten Bereichen aufgehoben wurden (vgl. c unten). Schliesslich werden wir die wichtigsten Themen, die in den relevanten Rechtsnormen behandelt werden, besprechen (vgl. d unten).

233 Vorab muss auch der Ansatz erläutert werden, auf Verwaltungsverordnungen (insbesondere: Weisungen, Kreisschreiben oder Anweisungen) nicht in diesem Überblick über die Rechtsnormen einzugehen, sondern in dem Teil, welcher der Analyse des vorliegenden Falles gewidmet ist (vgl. Ziff. 2 unten).

234 Verwaltungsverordnungen[147], die sich insbesondere von Rechtsverordnungen[148] unterscheiden, richten sich an die Verwaltungsmitarbeitenden und schreiben ihnen vor, wie diese ihre Aufgaben zu erfüllen haben. Verwaltungsverordnungen verfolgen die unterschiedlichsten Ziele administrativer und organisatorischer Art.[149] Sie haben keine Gesetzeskraft und sind weder für die Bürgerinnen und Bürger noch die Gerichte oder die Verwaltung[150] im eigentlichen Sinne bindend, obwohl ihre Verbindlichkeit unterschiedlich stark ausgeprägt ist[151] (insbesondere: die untergeordnete Verwaltungsbehörde ist grundsätzlich an den von der übergeordneten Behörde erlassenen Text gebunden, wobei dieser Text zudem – manchmal sogar direkt – die Rechtslage der Bürgerinnen und Bürger betreffen kann); sie sind für die Behörden, die das Gesetz anwenden, nur insofern bindend, als sie den genauen Sinn des Gesetzes wiedergeben.[152] Sie befreien die Verwaltung nicht davon, unter Berücksichtigung der Umstände des Einzelfalls Entscheidungen zu fällen, und dürfen nicht über den Rahmen hinausgehen, der von der übergeordneten Norm, die sie konkretisieren sollen, vorgegeben wird. Sofern keine Lücke vorhanden ist, können Verwaltungsverordnungen nichts anderes vorsehen als das, was sich aus der Gesetzgebung oder der Rechtsprechung ergibt.[153]

235 Verwaltungsverordnungen haben daher keine Gesetzeskraft. Aus systematischen Gründen ist es daher nicht notwendig, sie bei den Rechtsnormen aufzuführen. Verwaltungsverordnungen werden daher bei der Analyse konkreter Fälle besprochen, wenn es darum geht, mögliche technische, organisatorische oder prozesshafte Mängel zu untersuchen.

b) *Rechtlicher Rahmen*

236 Die Untersuchung, ob technische, organisatorische oder prozesshafte Mängel innerhalb des Bundes dazu geführt haben, dass die Xplain AG in den Besitz von produktiven Daten des Bundes gelangt ist, wirft allgemein die Frage nach der Informationssicherheit auf (*i*). Je nach Art der betroffenen Daten wirft dies insbesondere die Frage nach der Klassifizierung der Informationen auf (*ii*). Ferner kann je nach Art der betroffenen Daten auch hier die Datenschutzgesetzgebung Anwendung finden (*iii*).

237 Die Analyse des Sachverhalts aus strafrechtlicher Sicht ist entsprechend dem Wesen der Administrativuntersuchung (Art. 27*a* RVOV) und der Offertanfrage vom 21. Juli 2023, auf die der Vertrag zwischen dem Bund und OA verweist, nicht Teil des Mandats.

---

[147] Die primäre Funktion von Verwaltungsverordnungen besteht darin, die Vereinheitlichung und Rationalisierung der Praxis zu gewährleisten. Dadurch stellen sie auch die Gleichbehandlung sowie die administrative Vorhersehbarkeit sicher und erleichtern ausserdem die gerichtliche Kontrolle (BGE 131 V 42, E. 2.3; BVGE 2009/15, E. 5.1).

[148] Rechtsverordnungen sind Verordnungen, die sich wie Gesetze an alle Behörden sowie Privatpersonen richten und Rechtsnormen enthalten. Damit sie gegenüber Privatpersonen durchsetzbar sind, müssen sie veröffentlicht werden (siehe u. a. Urteil des BVGer A-5446/2016 vom 23. Mai 2018 E. 3.1.4).

[149] Im Deutschen findet man z. B. die folgenden Begriffe: «Direktiven, Weisungen, Dienstanweisungen, Dienstreglemente, allgemeine Dienstbefehle, Rundschreiben, Kreisschreiben, Zirkulare, Wegweisungen, Anleitungen, Instruktionen, Merkblätter, Leitbilde» ; vgl. BGE 128 I 167 E. 4.3. Meistens werden Verwaltungsverordnungen von den Departementen oder sogar von den Bundesämtern erlassen und in der Regel nicht veröffentlicht.

[150] BGE 141 V 175 E. 2.1; BGE 133 II 305 E. 8.1 ; Thierry Tanquerel, Manuel de droit administratif, 2. Ausgabe, 2018, Rz. 331 S. 115.

[151] Pierre Moor/Alexandre Flückiger/Vincent Martenet, Droit administratif, Vol. I: Les fondements, 3. Ausgabe, 2012, S. 398.

[152] BGE 142 II 182 2.3.2.

[153] BGE 141 V 175 E. 4.1, 138 II 536 E. 5.4.3; Entscheide des BVGer A-1412/2015, A-1422/2015 vom 14. Dezember 2016 E. 4, A-4357/2015 vom 10. Juli 2017 E. 2.5.

(i) *Informationssicherheit*

238 Die Informationssicherheit umfasst die Gesamtheit aller Anforderungen und Massnahmen, mit denen die Vertraulichkeit, die Integrität, die Verfügbarkeit und die Nachvollziehbarkeit von Informationen und Daten aller Art sowie die Verfügbarkeit und die Integrität von Informatikmitteln geschützt werden.[154]

239 Das Informationssicherheitsgesetz (ISG), das am 1. Januar 2024 in Kraft getreten ist und insbesondere für die Bundesverwaltung und die Armee gilt (Art. 2 Abs. 2 Bst. b und d ISG), verfolgt zwei Ziele:

1. Es fasst in einem einzigen Rechtsakt die zentralen Rechtsgrundlagen zusammen, welche die Sicherheit von Informationen und Informatikmitteln des Bundes regeln, die bis dahin – meist ohne Präzisierung – in einer Vielzahl von Rechtsakten verstreut waren (z. B. RVOG, ParlG, MG, StGB, BWIS, BPG, BöB, BGA, DSG, BGÖ), die nur für bestimmte Behörden galten.[155]

2. Es gilt für alle Behörden und Organisationen des Bundes, sodass ein möglichst einheitliches Sicherheitsniveau erreicht werden kann.[156]

240 Grundsätzlich sieht das ISG (Art. 6 Abs. 1) vor, dass die dem ISG unterstellten Behörden und Organisationen dafür sorgen, dass der Schutzbedarf der Informationen, für die sie zuständig sind, hinsichtlich einer allfälligen Beeinträchtigung der Interessen beurteilt wird. Der spezifische, sachbedingte Schutzbedarf wird implizit sehr häufig von anderen Gesetzen vorgegeben.[157] In sachlicher Hinsicht legt Artikel 6 Absatz 2 ISG, der auf Lehre und Praxis ausgerichtet ist, vier Schutzkriterien der Informationssicherheit fest (Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit). Der Schutz der Vertraulichkeit ist beispielsweise nur erforderlich, wenn sie aus einem rechtlichen Grund gewährleistet werden muss. Bestimmte Informationen können höhere Anforderungen an den Schutz ihrer Integrität oder Verfügbarkeit haben, ohne dass diese besonderen Anforderungen gesetzlich festgelegt sind, etwa dann, wenn die entsprechenden Informationen für die Aufgabenerfüllung einer Behörde unbedingt richtig oder verfügbar sein müssen. Dies trifft insbesondere für Informationen und Informatikmittel zu, die geschäftskritische Prozesse unterstützen.[158]

241 Die betroffenen Behörden und Organisationen sorgen dafür, dass die Informatikmittel, die sie zur Erfüllung ihrer gesetzlichen Aufgaben einsetzen, vor Missbrauch und Störungen geschützt sind (Art. 6 Abs. 3 ISG).

242 Artikel 17 ISG sieht Sicherheitsstufen vor («Grundschutz»; «hoher Schutz»; «sehr hoher Schutz»), die darauf abzielen, die Kritikalität eines bestimmten Informatikmittels in Bezug auf die öffentlichen Interessen nach Artikel 1 Absatz 2 ISG zu ermitteln. Diese Kritikalität wird von der Schwere des Schadens abgeleitet, der durch die Informationen, die mit dem betroffenen Informatikmittel bearbeitet werden, oder durch die Informatikmittel selbst verursacht werden kann, wenn diese missbraucht oder gestört werden. Massgebend für die Einstufung sind entsprechend sowohl der Schutzbedarf von Informationen in Bezug auf die Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit als auch die Kritikalität einer zeitnahen und sachgemässen Erfüllung der Geschäftsprozesse, die mit dem Informatikmittel unterstützt werden.[159]

---

[154] Generalsekretariat des VBS, Ausführungsgesetzgebung zum Informationssicherheitsgesetz – Erläuterungen, 8. November 2023, S. 2.
[155] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 2954.
[156] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 2954 f.
[157] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 3016.
[158] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 3017.
[159] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 3027.

243 Gemäss der Botschaft legt das ISG jedoch keine detaillierten Massnahmen zur Gewährleistung der Informationssicherheit fest, sondern schafft lediglich einen formell-gesetzlichen Rahmen, auf dessen Grundlage die jeweiligen Bundesbehörden auf Verordnungs- und Weisungsebene die Informationssicherheit konkretisieren werden.[160] Gemäss Artikel 85 ISG wird der Bundesrat beauftragt, standardisierte Anforderungen und Massnahmen nach dem Stand von Wissenschaft und Technik festzulegen. Es handelt sich dabei nicht um grundsätzliche organisatorische Anforderungen und Massnahmen, die auf Verordnungsebene festgelegt werden, sondern vorab um Anforderungen untergeordneter oder technischer Natur.[161] Viele andere Länder und internationale Organisationen haben bereits Standards für ihren Bereich bestimmt. «*Die Bundesbehörden werden also nicht das Rad neu erfinden müssen*».[162] Gemäss der Botschaft kann der Bundesrat, wenn nötig, um nicht mit dem Erlass von operativ-technischen Sicherheitsmassnahmen belastet zu sein, die Erarbeitung und Verabschiedung der Standards an untergeordnete Stellen, an die Generalsekretärenkonferenz (Art. 53 RVOG), an die Fachstelle des Bundes für Informationssicherheit oder an fedpol im Bereich des Objektschutzes delegieren.[163]

244 Gemäss Artikel 4 Absatz 2 ISG gilt: «*Für Informationen, deren Schutz auch in anderen Bundesgesetzen geregelt ist, finden die Bestimmungen dieses Gesetzes ergänzend Anwendung.*»

245 Zu diesen «anderen Bundesgesetzen» gehört das DSG, das am 1. September 2023 in Kraft trat. Während das ISG auf alle Arten von Informationen und Daten abzielt, ist der sachliche Anwendungsbereich des DSG auf personenbezogene Daten beschränkt, d. h. «*alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen*» (Art. 5 Bst. a DSG).

246 Das DSG sieht vor, dass der Verantwortliche und der Auftragsbearbeiter durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit gewährleisten (Art. 8 Abs. 1 DSG). Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden (Abs. 2). Darin kommt der risikobasierte Ansatz zum Ausdruck. Je grösser das Risiko einer Verletzung der Datensicherheit, umso höher sind die Anforderungen an die zu treffenden Massnahmen.[164]

247 Ergänzend dazu verpflichtet Artikel 2 DSV den Verantwortlichen und den Auftragsbearbeiter, Massnahmen zum Schutz der Vertraulichkeit, der Verfügbarkeit, der Integrität der Daten und der Nachvollziehbarkeit durch Datensicherheit zu ergreifen (Art. 2 DSV).[165] Artikel 3 DSV definiert diese technischen und organisatorischen Massnahmen.

(ii) *Klassifizierung der Informationen*

248 Die Klassifizierung von Informationen ist eine der Massnahmen des ISG zum Schutz von Informationen.[166]

---

[160] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953 2954 f.

[161] Die Botschaft enthält Beispiele (Standard für die Erhebung des Schutzbedarfs von Informationen in Bezug auf die vier Kriterien von Art. 6 Abs. 2; Standardmethode für die Risikobewertung; Standards für organisatorische, personelle, technische und bauliche Massnahmen (Art. 8); Standards für bestimmte Prozesse und Mittel zum Schutz klassifizierter Informationen (Art. 11–15); Standards für den Grundschutz, für die Erstellung von Informationssicherheitskonzepten sowie für die Sicherheit von Informatikmitteln der Sicherheitsstufen «hoher Schutz» und «sehr hoher Schutz» (Art. 16–19) (Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 3069).

[162] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953 , 3069.

[163] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953 , 3069.

[164] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941.

[165] NICOLAS BEGUIN, in Benhamou/Cottier (Hrsg.), Petit Commentaire LPD, 2023, Rz. 1 ad Art. 8 DSG

[166] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953 , 2978.

249 Es werden nicht alle Informationen klassifiziert. Eine Klassifizierung ist obligatorisch, wenn die entsprechenden Kriterien erfüllt sind (vgl. Art. 11 ISG). Artikel 13 ISG regelt die materiellen Voraussetzungen für die Klassifizierung von Informationen für alle dem ISG unterstellten Behörden und Organisationen und legt die Klassifizierungsstufen fest.

250 Die Klassifizierungsstufen sind wie folgt:

- intern
- vertraulich
- geheim

251 Für die Klassifizierungsstufe selbst ist der Grad der Beeinträchtigung massgebend, den eine Kenntnisnahme durch Unberechtigte den Interessen nach Artikel 1 Absatz 2 Buchstaben a–d ISG zufügen kann (Kenntnisnahme, die *diese Interessen beeinträchtigen kann* [«intern»]; Kenntnisnahme, die *diese Interessen erheblich beeinträchtigen kann* [«vertraulich»]; Kenntnisnahme, die *diese Interessen schwerwiegend beeinträchtigen kann* [«geheim»]).

252 Mit dem ISG werden Informationen, die nach der alten ISchV als «vertraulich» eingestuft wurden, nunmehr tendenziell in die Kategorie «intern» fallen. Gemäss dem Bundesrat soll dies die Anzahl der klassifizierten Informationen massiv reduzieren und unter anderem die Anzahl der Personensicherheitsprüfungen (PSP) verringern.[167]

(iii) *Datenschutz*

253 Während das ISG öffentliche Interessen und bestimmte Eigeninteressen des Bundes als Institution schützt (Art. 1 Abs. 2 ISG)[168], bezweckt das DSG den Schutz der Persönlichkeit (Art. 28 ZGB) und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden (Recht auf persönliche Freiheit [Art. 10 Abs. 2 BV]; Schutz der Privatsphäre [Art. 13 Abs. 1 BV]; Recht auf informationelle Selbstbestimmung [Art. 13 Abs. 2 BV und Art. 8 EMRK]).[169]

254 Der Schutz von Personendaten durch Bundesorgane wird im Wesentlichen durch das DSG und die DSV bzw. durch Artikel 57*h* ff. RVOG geregelt. Seit dem Inkrafttreten des DSG am 1. September 2023 fällt die Verarbeitung von Daten juristischer Personen durch Bundesorgane unter Artikel 57*r* ff. RVOG.[170]

255 Das DSG sieht insbesondere vor, dass Personendaten nur auf rechtmässige Weise und unter Beachtung des Grundsatzes der Verhältnismässigkeit für bestimmte und erkennbare Zwecke erhoben und in einer mit diesen Zwecken zu vereinbarenden Weise weiterverarbeitet werden dürfen (Art. 6 Abs. 1–3 DSG).

---

[167] Bundeskanzlei, Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung, Bericht in Umsetzung vom Meilenstein 5 der Cloud-Strategie des Bundesrates, 31. August 2022, S. 32.

[168] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 3010.

[169] JULIEN FRANCEY, in Benhamou/Cottier (Hrsg.), Petit Commentaire LPD, 2023, Rz. 11 ad Art. 1 DSG.

[170] Das DSG führt im RVOG eine Reihe von Gesetzesbestimmungen ein, welche für Bundesorgane den Umgang mit Daten juristischer Personen regeln. Denn aufgrund der Aufhebung des Schutzes der Daten juristischer Personen im DSG sind die bundesrechtlichen Gesetzesgrundlagen für die Bearbeitung von Personendaten durch Bundesorgane seit dem 1. Januar 2024 nicht mehr anwendbar, wenn diese Daten juristischer Personen bearbeiten. So werden die Artikel 5, 13 Absatz 2 und 36 BV gewahrt (Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941, 6981, 7118).

c) Überblick über die wichtigsten aufgehobenen Rechtsakte

256 In der folgenden Tabelle sind die wichtigsten aufgehobenen Gesetze und Rechtsverordnungen aufgeführt. Diese Tabelle veranschaulicht die Fragmentierung der gesetzlichen Vorschriften, die durch das ISG jedoch ab dem 1. Januar 2024 eine gewisse Systematik erhalten haben.

<table>
<tr><th>Informationssicherheit (einschliesslich Klassifizierung)</th><th>Informatik/Telekommunikation</th><th>Cyberrisiken</th><th>Datenschutz</th></tr>
<tr>
<td>Verordnung vom 1. Mai 1990 über den Schutz militärischer Informationen (Verordnung über den Schutz von Informationen des Bundes) (vorher in SR 510.411)
<table><tr><td>In Kraft getreten am</td><td>1. Januar 1991[171]</td></tr><tr><td>Aufgehoben am</td><td>1. August 2007[172]</td></tr><tr><td>Ersetzt durch</td><td>Verordnung über den Schutz von Informationen des Bundes, aISchV</td></tr></table></td>
<td>Verordnung vom 23. Februar 2000 über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung, aBinfV)
<table><tr><td>In Kraft getreten am</td><td>1. April 2000[173]</td></tr><tr><td>Aufgehoben am</td><td>1. Oktober 2003[174]</td></tr><tr><td>Ersetzt durch</td><td>Verordnung vom 26. September 2003 über die Informatik und Telekommunikation in der Bundesverwaltung</td></tr></table></td>
<td>Verordnung vom 27. Mai 2020 über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, aCyRV)
<table><tr><td>In Kraft getreten am</td><td>1. Juli 2020[175]</td></tr><tr><td>Aufgehoben am</td><td>1. Januar 2024[176]</td></tr><tr><td>Ersetzt durch</td><td>Verordnung vom 8. November 2023 über die Informationssicherheit (ISV)</td></tr></table></td>
<td>Bundesgesetz vom 19. Juni 1992 über den Datenschutz (aDSG)
<table><tr><td>In Kraft getreten am</td><td>1. Juli 1993[177]</td></tr><tr><td>Aufgehoben am</td><td>1. September 2023[178]</td></tr><tr><td>Ersetzt durch</td><td>Bundesgesetz vom 25. September 2020 über den Datenschutz (DSG)</td></tr></table></td>
</tr>
<tr>
<td>Verordnung vom 10. Dezember 1990 über die Klassifizierung und Behandlung von Informationen im zivilen Verwaltungsbereich (vorher in SR 172.015)
<table><tr><td>In Kraft getreten am</td><td>1. Januar 1991[179]</td></tr><tr><td>Aufgehoben am</td><td>1. August 2007[180]</td></tr><tr><td>Ersetzt durch</td><td>Verordnung vom 4. Juli 2007 über den Schutz von Informationen des Bundes (aISchV)</td></tr></table></td>
<td>Weisungen vom 23. Februar 2000 des Bundesrats über die Informatik und Telekommunikation in der Bundesverwaltung (Informatikweisungen Bundesrat, aBinfW)
<table><tr><td>In Kraft getreten am</td><td>1. April 2000[181]</td></tr><tr><td>Aufgehoben am</td><td>1. Oktober 2003[182]</td></tr><tr><td>Ersetzt durch</td><td>Verordnung vom 26. September 2003 über die Informatik und Telekommunikation in der Bundesverwaltung</td></tr></table></td>
<td></td>
<td></td>
</tr>
</table>

[171] AS 1990 887.
[172] AS 2007 3401.
[173] AS 2000 1227.
[174] AS 2003 3687.
[175] AS 2020 2107.
[176] AS 2023 735.
[177] AS 1993 1945.
[178] AS 2022 491.
[179] AS 1991 44.
[180] AS 2007 3401.
[181] AS 2000 2708.
[182] AS 2003 3687.

<table>
<tr>
<td>Verordnung vom 4. Juli 2007 über den Schutz von Informationen des Bundes (Verordnung über den Schutz von Informationen, aISchV) (vorher in SR 510.411)
<table><tr><td>In Kraft getreten am</td><td>1. August 2007[183]</td></tr><tr><td>Aufgehoben am</td><td>1. Januar 2024</td></tr><tr><td>Ersetzt durch</td><td>ISV[184]</td></tr></table></td>
<td>Verordnung vom 26. September 2003 über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung, BinfV)
<table><tr><td>In Kraft getreten am</td><td>1. Oktober 2003[185]</td></tr><tr><td>Aufgehoben am</td><td>1. Januar 2012[186]</td></tr><tr><td>Ersetzt durch</td><td>Verordnung vom 9. Dezember 2011 über die Informatik und Telekommunikation in der Bundesverwaltung (aBinfV).</td></tr></table></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verordnung vom 9. Dezember 2011 über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung, aBinfV) (vorher in SR 172.010.58)
<table><tr><td>In Kraft getreten am</td><td>1. Januar 2012[187]</td></tr><tr><td>Aufgehoben am</td><td>1. Januar 2021[188]</td></tr><tr><td>Ersetzt durch</td><td>Verordnung vom 25. November 2020 über die digitale Transformation und die Informatik (VDTI)[189]</td></tr></table></td>
<td></td>
<td></td>
</tr>
</table>

[183] AS 2007 3401.
[184] Verordnung vom 8. November 2023 über die Informationssicherheit in der Bundesverwaltung und der Armee (Informationssicherheitsverordnung, ISV) (SR 128.1) (am 1. Januar 2024 in Kraft getreten [AS 2023 735]). Gemäss einem erläuternden Bericht ersetzt die ISV die Cyberrisikenverordnung vom 27. Mai 2020 (CyRV) und die Verordnung vom 4. Juli 2007 über den Schutz von Informationen des Bundes (ISchV) (siehe GS-VBS, Ausführungsgesetzgebung zum Informationssicherheitsgesetz, erläuternder Bericht, 24. August 2022, S. 6).
[185] AS 2003 3687.
[186] AS 2011 6093.
[187] AS 2011 6093.
[188] AS 2020 5871.
[189] Verordnung vom 25. November 2020 über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung (Verordnung über die digitale Transformation und die Informatik, VDTI) (SR 172.010.58) (am 1. Januar 2021 in Kraft getreten [AS 2020 5871]).

d) Wichtigste Bestimmungen

257 Die derzeit geltenden Gesetze und Rechtsverordnungen enthalten die folgenden wichtigsten Bestimmungen, die für die gestellte Frage potenziell relevant sind.

(i) *Legalitätsprinzip*

258 Im vorliegenden Fall ist das Legalitätsprinzip in Artikel 34 Absatz 1 DSG[190] (Art. 17 Abs. 1 aDSG) verankert, wonach Bundesorgane Personendaten nur bearbeiten dürfen, wenn dafür eine gesetzliche Grundlage besteht.

259 Die Anforderung einer gesetzlichen Grundlage für die Verarbeitung von Personendaten durch Bundesorgane (Art. 5 Bst. i DSG) zielt sowohl darauf ab, staatlichem Handeln demokratische Legitimität zu verleihen, staatlichen Massnahmen Grenzen zu setzen (gesetzlicher Rahmen), als auch die Vorhersehbarkeit des Rechts und Gleichbehandlung zu gewährleisten; in diesem Sinne garantiert die Anforderung eine gewisse Transparenz.[191]

260 Der Präzisionsgrad (Regelungsdichte) der gesetzlichen Grundlage muss in einem angemessenen Verhältnis zur Schwere des Eingriffs in das Grundrecht stehen. Anhand der gesetzlichen Grundlage muss die betroffene Person wissen

- welches Bundesorgan
- welche Kategorie von Daten
- zu welchem Zweck verarbeitet,
- wer Zugang zu den Daten hat,
- wem die Daten mitgeteilt werden können
- und zu welchem Zweck
- und wie gross der Umfang der Verarbeitung im Grossen und Ganzen ist.[192]

261 Die Rechtsgrundlage muss in einem formellen Gesetz vorgesehen sein, insbesondere wenn es sich um die Verarbeitung besonders schützenswerte Personendaten handelt (Art. 5 Bst. c DSG) oder wenn der Bearbeitungszweck oder die Art und Weise der Datenbearbeitung zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Person führen können (Art. 34 Abs. 2 Bst. a und c DSG).

262 Artikel 57*h*^{bis} Absatz 1 RVOG erlaubt die Verarbeitung von Personendaten im Hinblick auf den ordnungsgemässen Ablauf der Geschäftsprozesse (Geschäftsverwaltungssystem). Die Rechtsgrundlage für die Verarbeitung (insbesondere die Erhebung und Weitergabe) von Personendaten muss sich jedoch immer aus dem auf die betreffenden Daten anwendbaren Sonderrecht ergeben.[193]

263 Handelt ein Bundesorgan jedoch privatrechtlich, so gelten die Bestimmungen für die Datenbearbeitung durch private Personen (Art. 40 DSG), insbesondere Artikel 5 bis 32 DSG.[194] Privatpersonen handeln frei,

---

[190] Die Bestimmung konkretisiert das Legalitätsprinzip im Sinne von Artikel 5 und 164 BV und berücksichtigt Artikel 36 Absatz 1 BV, wonach jede Grundrechtseinschränkung einer gesetzlichen Grundlage bedarf (vgl. Monique Cossali Sauvain, in Benhamou/Cottier (Hrsg.), Petit Commentaire LPD, 2023, Rz. 2 ad Art. 34 DSG).

[191] MONIQUE COSSALI SAUVAIN, in Benhamou/Cottier (Hrsg.), Petit Commentaire LPD, 2023, Rz. 10 ad Art. 34 DSG.

[192] DSG, Gesetzgebungsleitfaden, Leitfaden für die Ausarbeitung von Erlassen des Bundes, 4. Ausgabe, 2019, S. 221, Rz. 824; MONIQUE COSSALI SAUVAIN, in Benhamou/Cottier (Hrsg.), Petit Commentaire LPD, 2023, Rz. 12 ad Art. 34 DSG.

[193] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941, 6981, 7116.

[194] Vgl. Rz. 285 unten.

solange das Gesetz keine Einschränkungen vorsieht, weshalb das System in dieser Hinsicht für Privatpersonen weniger streng ist als für Bundesorgane.[195]

264 Die Unterscheidung zwischen privatrechtlicher Tätigkeit und hoheitlicher Tätigkeit (d. h. eines Bundesorgans) im Sinne des DSG ist nicht immer eindeutig. Zu den privatrechtlichen Tätigkeiten gehören insbesondere kommerzielle Tätigkeiten von autonomen öffentlich-rechtlichen Einrichtungen, Tätigkeiten zur Unterstützung der Verwaltung wie die Beschaffung von Gütern (z. B. Büromaterial) oder Dienstleistungen (z. B. Unterhaltung von Büroräumen) oder die Ausübung einer gewerblichen Tätigkeit.[196]

(ii) *Verhältnismässigkeitsprinzip*

265 Jede Verarbeitung von Daten (ob Personendaten oder nicht) muss dem Verhältnismässigkeitsprinzip entsprechen (Art. 5 Abs. 2 BV und Art. 36 Abs. 3 BV; vgl. auch Art. 6 Abs. 2 DSG und Art. 6 Abs. 4 ISG).[197]

266 Im Bereich des Schutzes von Personendaten sind die Grundsätze der Datenvermeidung und der Datensparsamkeit zwei Ausprägungen des Verhältnismässigkeitsprinzips. Die erste besagt, dass, wenn der Zweck der Verarbeitung ohne die Erhebung neuer Daten erreicht werden kann, diese Option bevorzugt werden muss. Die zweite besagt, dass nur die Daten verarbeitet werden dürfen, die für den verfolgten Zweck absolut notwendig sind[198] (siehe auch Grundsatz der Zweckbestimmung [Art. 6 Abs. 3 DSG]).

(iii) *Zum Schutz von Informationen verpflichtete Personen und Verantwortung der Behörden*

267 Im Bereich des Schutzes von Personendaten ist der Verantwortliche (Bundesorgane), gegebenenfalls der Auftragsbearbeiter[199], verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, insbesondere die Grundsätze nach Artikel 6. Er berücksichtigt dies ab der Planung (Art. 7 Abs. 1 DSG; «*privacy by design*»).

268 Im Rahmen des Geltungsbereichs des ISG sorgen die Behörden in ihrem Zuständigkeitsbereich dafür, dass die Informationssicherheit nach dem Stand von Wissenschaft und Technik organisiert, umgesetzt und überprüft wird (Art. 7 Abs. 1 ISG).

269 Die Bundeskanzlerin oder der Bundeskanzler, die Generalsekretärinnen und Generalsekretäre sowie die Direktorinnen und Direktoren der Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c ISV tragen in ihrem Zuständigkeitsbereich die Verantwortung für die Informationssicherheit (Art. 36 Abs. 1 ISV). Sie können die Informationssicherheitsverantwortung jedoch einem Mitglied der Geschäftsleitung delegieren, sofern diesem die erforderlichen Befugnisse zustehen, Massnahmen zu veranlassen, zu kontrollieren und zu korrigieren (Art. 36 Abs. 2 ISV).

270 Somit liegt die Verantwortung für die Sicherheit bei der Leitung. Die dem ISG unterstellten Behörden müssen die Informationssicherheit in ihrem Zuständigkeitsbereich organisieren, umsetzen und überprüfen, wobei sie die neuesten wissenschaftlichen und technischen Erkenntnisse berücksichtigen. In einer Reihe von Normen wird formuliert, was gemeinhin als bewährte Praktiken bei der Verwaltung der Informationssicherheit bezeichnet wird, und darin werden auch die Anforderungen für die Anwendung

[195] MONIQUE COSSALI SAUVAIN, in Benhamou/Cottier (Hrsg.), Petit Commentaire LPD, 2023, Rz. 9 ad Art. 34 DSG.
[196] TEO GÉNÉCAND, in Benhamou/Cottier (Hrsg.), Petit Commentaire LPD, 2023, Rz. 4 f. ad Art. 40 DSG.
[197] BGE 138 II 346 E. 9.2.
[198] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6565, 6644.
[199] NICOLAS BEGUIN, in Benhamou/Cottier (Hrsg.), Petit Commentaire LPD, 2023, Rz. 11 ad Art. 7 DSG.

von Sicherheitsmassnahmen festgelegt, die an die Bedürfnisse der verschiedenen Behörden oder Organisationen angepasst werden können.[200]

271 Das Gesetz verlangt nicht, dass die Behörden beispielsweise ein ISMS nach DIN ISO/IEC Norm 27 001 umsetzen. Ihre Organisation sollte sich aber zumindest darauf ausrichten.[201]

(iv) *Sicherheit von Personendaten: organisatorische und technische Massnahmen*

272 Beim Datenschutz geht es um den Persönlichkeitsschutz des Einzelnen. Die Datensicherheit zielt hingegen generell auf die bei einem Verantwortlichen oder Auftragsbearbeiter vorhandenen Daten ab und umfasst den allgemeinen technischen und organisatorischen Rahmen der Datenbearbeitung.[202]

273 Die Verantwortlichen und Auftragsbearbeiter müssen durch geeignete technische und organisatorische Massnahmen («TOMs» [«*technical and organisational measures*»]) eine dem Risiko angemessene Datensicherheit gewährleisten (Art. 8 Abs. 1 DSG; Art. 7 Abs. 1 aDSG). Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden (Art. 8 Abs. 2 DSG) (vgl. Art. 3 DSV).

274 Art. 8 DSG verpflichtet sowohl den Verantwortlichen als auch den Auftragsbearbeiter, eine angemessene Sicherheitsarchitektur für ihre Systeme vorzusehen und sie beispielsweise gegen Malware oder Datenverlust zu schützen.[203]

275 Zu den technischen Massnahmen gehören unter anderem Verschlüsselung, Chiffrierung, Pseudonymisierung von Daten, Passwortschutz, ein regelmässiges Backup-System, die Registrierung der Identität von Personen, die bestimmte Arten von Daten abrufen, oder die Verwendung eines verschlüsselten HTTPS-Protokolls.[204]

276 Die organisatorischen Massnahmen betreffen die Struktur und die Verfahren, die innerhalb eines Bundesorgans eingerichtet wurden, um das Prinzip der Datensicherheit zu erfüllen (z. B. Schulung des Personals und möglicher Auftragsbearbeiter, Erarbeitung von Verhaltensregeln für Mitarbeitende oder Bewertung der Wirksamkeit getroffener Massnahmen, Abgrenzung von Aufgaben, Funktionen und Verantwortlichkeiten im Bereich der Datensicherheit oder Erarbeitung eines Massnahmenplans für den Fall einer Sicherheitslücke).[205]

277 Der EDÖB hat diesbezüglich am 15. Januar 2024 einen Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes (TOM) veröffentlicht. Dieser Leitfaden führt in erster Linie die Pflichten privater Verantwortlicher aus; jedoch finden auch Verantwortliche von Bundesorganen im Abschnitt «Bundesorgane» spezifische sie betreffende Informationen.

(v) *Risikomanagement*

278 Im Hinblick auf die Sicherheit von Personendaten konkretisiert Artikel 8 DSG (Art. 7 aDSG) den risikobasierten Ansatz. Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit. Je grösser

[200] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 3017 f.
[201] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 3017 f.
[202] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941, 7031.
[203] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941, 7031.
[204] NICOLAS BEGUIN, in Benhamou/Cottier (Hrsg.), Petit Commentaire LPD, 2023, Rz. 10 ad Art. 8 DSG.
[205] NICOLAS BEGUIN, in Benhamou/Cottier (Hrsg.), Petit Commentaire LPD, 2023, Rz. 11 ad Art. 8 DSG.

das Risiko einer Verletzung der Datensicherheit, umso höher sind die Anforderungen an die zu treffenden Massnahmen (eine dem Risiko angemessene Datensicherheit).[206]

279 Gemäss ISG sorgen die verpflichteten Behörden und Organisationen in ihrem Zuständigkeitsbereich dafür, dass die Risiken für die Informationssicherheit laufend beurteilt werden (Art. 8 Abs. 1 ISG). Sie treffen die erforderlichen Massnahmen, um die Risiken zu vermeiden oder auf ein tragbares Mass zu reduzieren (Art. 8 Abs. 2 ISG). Risiken, die getragen werden sollen, müssen nachweislich akzeptiert werden (Art. 8 Abs. 3 ISG).

280 Die Beurteilung der Risiken setzt profunde Kenntnisse der gesetzlichen Aufgaben und der entsprechenden Geschäftsprozesse, die regelmässige Beurteilung der Bedrohungen, die Analyse der Schwachstellen sowie die Einschätzung der Eintrittswahrscheinlichkeit und des potenziellen Schadensausmasses bestimmter Gefahren voraus.[207] Ein wichtiges Ziel des Risikomanagements besteht darin, die geeignetsten Massnahmen zur Risikovermeidung oder -reduktion treffen zu können. Risiken können vermieden werden, indem auf eine bestimmte, zu riskante Tätigkeit ganz verzichtet wird (z. B. wird auf ein Informatikvorhaben verzichtet, für welches die Umsetzung von risikogerechten Massnahmen wirtschaftlich nicht vertretbar ist).[208]

281 Selbstverständlich können Risiken auch in Kauf genommen oder getragen werden. Sie sollten aber nicht ignoriert werden. Risiken, die nach der Umsetzung der vorgesehenen Sicherheitsmassnahmen bestehen bleiben (sogenannte Restrisiken), oder Risiken, die nicht vermindert werden sollen, sind klar auszuweisen. Die Entscheidungsträger sind für ihre diesbezügliche Güterabwägung in dokumentierter Form auf diese Risiken und die potenziellen Auswirkungen hinzuweisen. Die verbleibenden Risiken müssen nachweisbar akzeptiert und entsprechend getragen werden.[209]

282 Gemäss der Botschaft werden im Bereich der Informationssicherheit regelmässig organisatorische Massnahmen entwickelt, die wirksamer oder wirtschaftlicher sind. Neue technische Entwicklungen erfolgen noch rascher, insbesondere bei den Informatikmitteln. Es ist sehr wichtig, dass Sicherheitsmassnahmen nicht auf veralteten Technologien basieren, sondern gegen aktuelle Bedrohungen wirken. Hierzu sollen Standardanforderungen nach dem Stand von Wissenschaft und Technik festgelegt werden (vgl. Art. 85 ISG). Dies im Wissen darum, dass die Kriterien für die Risikoakzeptanz, die für die Bewertung der Risiken massgebend sind, von den jeweiligen verpflichteten Behörden gestützt auf ihre eigenen Informationssicherheitsbedürfnisse festgelegt werden.[210]

(vi) *Bekanntgabe (Zugriff)*

283 *In Bezug auf Personendaten.* In Bezug auf die Bekanntgabe sieht das DSG vor, dass Bundesorgane nur dann berechtigt sind, persönliche Daten bekanntzugeben, wenn eine gesetzliche Grundlage im Sinne von Artikel 34 Absätze 1 bis 3 DSG dies vorsieht (Art. 36 Abs. 1 DSG; vgl. auch Art. 57*h*[bis] Abs. 2 RVOG, der die Notwendigkeit einer gesetzlichen Grundlage für die Bekanntgabe von Personendaten sowie von Daten über juristische Personen vorsieht).[211]

---

[206] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 2977.
[207] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 3019.
[208] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 3019.
[209] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 3019.
[210] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 3019.
[211] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941, 7116.

284 Sie dürfen Personendaten in Abweichung von dieser Regel im Einzelfall bekanntgeben, wenn eine der in Artikel 36 Absatz 2 DSG genannten Voraussetzungen erfüllt ist, zu denen die folgenden Fälle gehören: a) Die Bekanntgabe der Daten ist für den Verantwortlichen oder für die Empfängerin oder den Empfänger zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich; c) Die Bekanntgabe der Daten ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen. Jedoch lehnen die Bundesorgane die Bekanntgabe ab, schränken sie ein oder verbinden sie mit Auflagen, wenn a) wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen der betroffenen Person es verlangen oder b) gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen.

285 Handelt ein Bundesorgan jedoch privatrechtlich, so gelten die Bestimmungen für die Datenbearbeitung durch private Personen (Art. 40 DSG). In diesem Fall ist keine gesetzliche Grundlage für die Weitergabe von Personendaten erforderlich, und die Bundesorgane können sich gegebenenfalls auf die Rechtfertigungsgründe in Artikel 31 DSG berufen.[212]

286 Was die Nutzung der elektronischen Infrastruktur des Bundes betrifft, so dürfen gemäss VBNIB auf bewirtschaftete Daten dürfen nur zugreifen: a) die Betreiberin; b) die nach dem Datenschutzkonzept eines Bundesorgans vorgesehenen Stellen (Art. 2 Abs. 1). Auf nicht bewirtschaftete Daten darf nur das Bundesorgan zugreifen, das die Geräte, auf denen diese Daten aufgezeichnet werden, selbst nutzt (Art. 2 Abs. 2).

287 *In Bezug auf klassifizierte Informationen.* Das ISG sieht vor, dass nur Personen Zugang zu klassifizierten Informationen erhalten, die Gewähr dafür bieten, dass sie damit sachgerecht umgehen, und: a) die Informationen zur Erfüllung einer gesetzlichen Aufgabe benötigen; oder b) über eine vertraglich vereinbarte Zugangsberechtigung verfügen und die Informationen zur Erfüllung der ihnen übertragenen Aufgaben benötigen (Art. 14 ISG).

288 Der Grundsatz «Kenntnis nur wenn nötig» («*need to know*») gilt für jede einzelne klassifizierte Information. Es besteht also kein allgemeines Recht, Zugang zu allen klassifizierten Informationen zu haben.[213]

289 Dies trifft auch für Prüf-, Kontroll- oder Aufsichtsorgane zu, die gegebenenfalls zwar ein allgemeines Informationsrecht haben, die aber für jede einzelne klassifizierte Information den Nachweis dafür erbringen müssen, dass sie zur Erfüllung ihres Auftrags tatsächlich von den betreffenden Informationen Kenntnis haben müssen. Bei einem vertraglich vereinbarten Zugangsrecht müssen die entsprechenden Verträge den Zugang zu klassifizierten Informationen vorsehen und deren Bearbeitung regeln.[214]

(vii) *Rahmen für die Zusammenarbeit mit Dritten*

290 Die Informationssicherheit regelt die Massnahmen, die ergriffen werden müssen, um zu verhindern, dass nicht autorisierte Personen Zugang zu den betreffenden Daten erhalten. Der Grundsatz der Sicherheit gilt sowohl für den privaten Sektor als auch für Bundesorgane. Die Sicherheitsanforderungen müssen auch von dem Auftragnehmenden beachtet werden, dem die gesamte oder ein Teil der Verarbeitung übertragen wurde.[215]

---

[212] Anja Martina JOSURAN-BINDER, in: Bieri/Powell (Hrsg.), DSG Kommentar, Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023, Art. 40 Rz. 7.
[213] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 3025.
[214] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 3025.
[215] SYLVAIN MÉTILLE, L'utilisation de l'informatique en nuage par l'administration publique, PJA 2019 S. 609, 610.

291 Die Frage der Zusammenarbeit mit Dritten ist Gegenstand verschiedenster Bestimmungen. Insbesondere folgende Bestimmungen sind hervorzuheben.

292 *Datenschutzgesetz (DSG)*: Das DSG definiert die Begriffe «Verantwortlicher» (private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet [Art. 5 Bst. j DSG]) und «Auftragsbearbeiter» (private Person oder Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet [Art. 5 Bst. k DSG]). Der Gesetzgeber beabsichtigte, den neuen europäischen Standards zu entsprechen.[216] Die Zuweisung der Eigenschaft als Verantwortlicher bzw. als Auftragsbearbeiter hängt von den tatsächlichen Umständen ab und liegt nicht in der freien Entscheidung der Parteien.[217]

293 Mit anderen Worten, wenn eine Übermittlung von Personendaten stattfindet, kann es sich um i) zwei unabhängige Verantwortliche («*Controller to Controller*»)[218], ii) zwei gemeinsame Verantwortliche («*Joint Controllers*»)[219] oder iii) einen Verantwortlichen und einen Auftragsbearbeiter («*Controller to Processor*») handeln. Die Frage ist von entscheidender Bedeutung[220], aber im Einzelfall nicht immer eindeutig zu beantworten.[221]

294 Insbesondere handeln Dienstleiterinnen oder Dienstleister, die zwar Zugang zu Personendaten haben, diese aber nicht im Rahmen der Dienstleistungserbringung verarbeiten, nicht als Auftragsbearbeiter im Sinne des DSG. Die blosse Kenntnisnahme oder die blosse Möglichkeit der Kenntnisnahme von Personendaten stellt noch keine Verarbeitung dar.[222] Ein Fall von Auftragsbearbeitung kann jedoch im Rahmen eines Wartungs- und Supportdienstes auftreten; dies ist der Fall, wenn die Dienstleistung auch die Verarbeitung von Kundendaten für die Kundinnen und Kunden umfasst.[223]

295 Der Verantwortliche und der Auftragsbearbeiter unterliegen zwar beide manchmal identischen Verpflichtungen (vgl. z. B. Art. 8 DSG, der direkte Pflichten sowohl gegenüber dem Verantwortlichen als auch gegenüber dem Auftragsbearbeiter vorsieht[224]).

296 Die Zusammenarbeit mit einem Dritten wird jedoch, wenn sie als Auftragsbearbeitung zu qualifizieren ist, speziell durch Artikel 9 DSG geregelt, der im Wesentlichen dem alten Recht entspricht (Art. 10*a* aDSG mit dem Titel «Datenbearbeitung durch Dritte»[225], der Art. 14 aDSG aufgriff, der früher nur für die Datenbearbeitung durch Privatpersonen galt[226]). Die Bearbeitung von Personendaten kann vertraglich

---

[216] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941, 7023.

[217] EMILIE JACOT-GUILLARMOD, in Benhamou/Cottier (Hrsg.), Kurzkommentar DSG, 2023, Rz. 59 ad Art. 5 DSG.

[218] DAVID ROSENTHAL, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in Jusletter 17. Juni 2019 Rz. 58.

[219] DAVID ROSENTHAL, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in Jusletter 17. Juni 2019 Rz. 58.

[220] DAVID ROSENTHAL, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in Jusletter 17. Juni 2019.

[221] Siehe European Data Protection Board (EDPB), Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, 2. September 2020, Annex I – Flowchart for applying the concepts of controller, processor and joint controllers in practice.

[222] DAVID ROSENTHAL, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in Jusletter 17. Juni 2019 Rz. 96 und 100.

[223] DAVID ROSENTHAL, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in Jusletter 17. Juni 2019 Rz. 103.

[224] EMILIE JACOT-GUILLARMOD, in Benhamou/Cottier (Hrsg.), Kurzkommentar DSG, 2023, Rz. 3 ad Art. 9 DSG.

[225] BJ, Totalrevision des Datenschutzgesetzes (DSG) Übersicht zu den wichtigsten Änderungen für die Erarbeitung der Rechtsgrundlagen betreffend Datenbearbeitungen durch Bundesorgane. Oktober 2022, S. 31.

[226] Artikel 14 aDSG galt ursprünglich nur für die Verarbeitung von Daten durch *Privatpersonen*. Das aDSG enthielt keine ähnliche Bestimmung für die Verarbeitung von Daten durch *Bundesorgane*. Mit der Übertragung in den allgemeinen Teil (Art. 10a aDSG) wurde die Regel nicht nur auf Privatpersonen, sondern auch auf Bundesorgane anwendbar (Botschaft vom 19. Februar 2003 zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung, BBl 2003 2101 2135).

oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn: a) die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und b) keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

297 Ähnlich wie die Artikel 14 und 10*a* aDSG verpflichtet Artikel 9 DSG den Verantwortlichen, der die Dienste eines Auftragsbearbeiters in Anspruch nehmen möchte, die drei von Artikel 55 OR inspirierten *curae* einzuhalten: (i) den Auftragsbearbeiter, den er mit der Verarbeitung von Personendaten betraut, sorgfältig auszuwählen (*cura in eligendo*), (ii) ihm alle angemessenen Instruktionen zur Erfüllung seines Auftrags zu geben (*cura in instruendo*) und (iii) im Rahmen des Möglichen die erforderliche Aufsicht auszuüben (*cura in custodiendo*).[227]

298 Die Auftragsbearbeitung entbindet den Verantwortlichen nicht von seinen Pflichten im Bereich des Datenschutzes.[228] Dieser muss aktiv – durch die sorgfältige Auswahl des Auftragsbearbeiters, die erteilten Instruktionen und die durchgeführte Überwachung (Sicherheitsaudits beim Lieferanten[229]) – sicherstellen, dass die Arbeiten in Übereinstimmung mit den gesetzlichen Anforderungen (insbesondere in Bezug auf die Datensicherheit) durchgeführt werden, als ob er sie selbst durchführen würde. Die externe Vergabe der Datenverarbeitung darf die Rechtsposition der betroffenen Person nicht beeinträchtigen.[230]

299 Gemäss der Botschaft begründet Artikel 9 Absatz 1 DSG «*eine Sorgfaltspflicht für den Verantwortlichen, bei der Auftragsbearbeitung die Rechte der betroffenen Person zu wahren. Der Verantwortliche muss aktiv sicherstellen, dass der Auftragsbearbeiter das Gesetz im selben Umfang einhält, wie er selbst es tut. Das betrifft insbesondere die Einhaltung der allgemeinen Grundsätze, der Regeln betreffend die Datensicherheit, die in Absatz 2 ausdrücklich erwähnt werden, sowie der Regeln betreffend die Bekanntgabe ins Ausland. Der Verantwortliche muss analog wie bei Artikel 55 OR Verstösse gegen das DSG verhindern. Er ist daher verpflichtet, seinen Auftragsbearbeiter sorgfältig auszuwählen, ihn angemessen zu instruieren und soweit als nötig zu überwachen*»[231].

300 Ausserdem muss der Verantwortliche bei der Beauftragung eines Auftragsbearbeiters, der Daten ausserhalb der Schweiz verarbeitet, nicht nur die Anforderungen für die Auftragsbearbeitung (Art. 9 DSG), sondern auch die Anforderungen für die Übermittlung von Daten ins Ausland (Art. 16 ff. DSG)[232] erfüllen, was gegebenenfalls die Verwendung von Standardvertragsklauseln voraussetzt.[233]

301 *Informationssicherheitsgesetz (ISG).* Arbeiten die verpflichteten Behörden und Organisationen mit Dritten zusammen, so sorgen sie dafür, dass die Anforderungen und Massnahmen nach dem ISG in den entsprechenden Vereinbarungen und Verträgen festgehalten werden (Art. 9 Abs. 1 ISG). Sie sorgen für eine angemessene Überprüfung der Umsetzung der Massnahmen (Art. 9 Abs. 2 ISG).

---

[227] Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, BNl 1988 II 413 463; Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941, 7032; siehe auch u. a.: PHILIPPE MEIER, Protection des données, 2011, Rz. 1217 f.

[228] BJ, Totalrevision des Datenschutzgesetzes (DSG) Übersicht zu den wichtigsten Änderungen für die Erarbeitung der Rechtsgrundlagen betreffend Datenbearbeitungen durch Bundesorgane, Oktober 2022, S. 30.

[229] SYLVAIN MÉTILLE, L'utilisation de l'informatique en nuage par l'administration publique, PJA 2019 S. 609, 617.

[230] BJ, Totalrevision des Datenschutzgesetzes (DSG) Übersicht zu den wichtigsten Änderungen für die Erarbeitung der Rechtsgrundlagen betreffend Datenbearbeitungen durch Bundesorgane, Oktober 2022, S. 30.

[231] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941, 7032.

[232] BJ, Totalrevision des Datenschutzgesetzes (DSG) Übersicht zu den wichtigsten Änderungen für die Erarbeitung der Rechtsgrundlagen betreffend Datenbearbeitungen durch Bundesorgane, Oktober 2022, S. 30.

[233] TEO GENECAND, in in Benhamou/Cottier (Hrsg.), Petit Commentaire LPD, 2023, Rz. 57 f. ad Art. 16 DSG.

302 Die Botschaft erinnert daran, dass die Bundesbehörden für ihre Aufgabenerfüllung häufig auf eine Mitwirkung der Privatwirtschaft oder anderer Stellen angewiesen sind. Die auftragserteilenden Behörden und Organisationen haben in diesem Fall dafür zu sorgen, dass bei der Auftragserteilung und -ausführung die gesetzlich vorgesehenen Massnahmen eingehalten werden. Externe Leistungserbringerinnen dagegen gelten als Dritte im Sinne von Artikel 9 ISG und müssen vertraglich verpflichtet werden, die im ISG vorgesehenen Massnahmen einzuhalten.[234] Grundsätzlich sollten Dritte erst dann Zugang zu Informationen oder zu Informatikmitteln des Bundes erhalten, wenn sie die erforderlichen Massnahmen umgesetzt haben. Das ISG verlangt von den verpflichteten Behörden und Organisationen zudem, dass sie die Umsetzung der Massnahmen angemessen (d. h. risikogerecht) überprüfen. Dies kann zum Beispiel im Rahmen eines Besuchs vor Ort oder mittels schriftlicher Bestätigung durch die Drittpartei erfolgen.[235]

303 Ferner müssen diese Behörden und Organisationen, wenn das Mandat eine sensible Tätigkeit umfasst, die Einleitung eines Verfahrens zur Personensicherheitsprüfung (PSP; vgl. Art. 27 ff. ISG) oder gegebenenfalls eines Betriebssicherheitsverfahrens (BSV; vgl. Art. 49 ff. ISG) beantragen.[236]

304 Artikel 10 ISV, der Artikel 9 ISG präzisiert, sieht vor, dass die Verwaltungseinheiten die Risiken für ihre Schutzobjekte bei der Zusammenarbeit mit Dritten und ihre Abhängigkeit von Dritten beurteilen (Abs. 1). Zudem wirken die Beschaffungsstellen nach den Artikeln 9 und 10 der Verordnung vom 24. Oktober 2012 über die Organisation des öffentlichen Beschaffungswesens der Bundesverwaltung (Org-VöB) bei der Beurteilung mit und stellen die nötigen Informationen zur Verfügung (Abs. 2).

305 Wenn die Zusammenarbeit mit einem Dritten den Zugang dieses Dritten zu Informationen, Informatikmitteln, Räumlichkeiten oder anderen Infrastrukturen des Bundes beinhaltet, sieht Artikel 20 ISG vor, dass die dem ISG unterstellten Behörden und Organisationen dafür sorgen, dass diese Dritten (i) sorgfältig ausgewählt werden, (ii) risikogerecht identifiziert werden, (iii) stufengerecht aus- und weitergebildet werden und (iv) gegebenenfalls zur Geheimhaltung verpflichtet werden.

306 *Verordnung über die Bearbeitung von Personendaten und Daten juristischer Personen bei der Nutzung der elektronischen Infrastruktur des Bundes (VBNIB)*.[237] Insbesondere dürfen Personen, die mit technischen Arbeiten wie der Wartung oder Unterhalt der elektronischen Infrastruktur betraut sind, die Daten nur dann bearbeiten, soweit dies zur Erfüllung dieser Aufgaben erforderlich ist. Die sichere Aufbewahrung, der Zugriffsschutz und die Vertraulichkeit müssen gewährleistet bleiben (Art. 7 Abs. 1 und 2 VBNIB)

307 *Verordnung über die digitale Transformation und die Informatik (VDTI)*. Diese Verordnung gilt insbesondere für die Einheiten der zentralen Bundesverwaltung (Art. 2 Abs. 1 VDTI). In Bezug auf die Bereitstellung von Leistungen und die Entscheidung über deren Beschaffung entscheiden die Departemente und die Bundeskanzlei, gestützt auf Marktanalysen und unter Berücksichtigung der Grundsätze der Zweckmässigkeit, Interoperabilität, Wirtschaftlichkeit und Sicherheit, ob eine Leistung intern erbracht oder extern beschafft werden soll (Art. 8 VDTI).

308 Die Frage des Zugangs zu Daten für externe Leistungserbringer wird speziell geregelt: Daten, die nicht allgemein zugänglich sind, dürfen externen Leistungserbringern zugänglich gemacht werden, wenn die folgenden Voraussetzungen erfüllt sind: a) Es ist zur Erbringung der Leistung erforderlich; b) die für die Daten verantwortliche Behörde hat schriftlich zugestimmt; c) es wurden angemessene vertraglichen, organisatorischen und technischen Vorkehrungen getroffen, um eine weitere Verbreitung der Daten zu verhindern (Art. 11 Abs. 1 VDTI). Macht die für die Daten verantwortliche Behörde die Daten selber

[234] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 3029 f.
[235] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 3020.
[236] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 3020.
[237] Basierend auf Art. 57*q* Abs. 1 RVOG und in Kraft getreten am 1. April 2012 (AS 2012 947).

zugänglich, so ist für die Zustimmung nach Absatz 1 Buchstabe b ihre vorgesetzte Stelle zuständig (Art. 11 Abs. 2 VDTI).

(viii) *Angemessene Ressourcen im Bereich der Informationssicherheit*

309 Die Bundeskanzlerin oder der Bundeskanzler, die Generalsekretärinnen und Generalsekretäre sowie die Direktorinnen und Direktoren der Verwaltungseinheiten betrauen ihre Informationssicherheitsbeauftragten mit Aufgaben und stellen insbesondere sicher, dass diese über angemessene Kompetenzen und Ressourcen verfügen (Art. 36 Abs. 4 Bst. a ISV).

2. Beurteilung von Einzelfällen

310 Die rechtliche Analyse der Fälle, in denen Daten an Xplain übermittelt wurden, beinhaltet beiläufig die Erwähnung von Verhaltensweisen, die von Mitarbeitenden des Bundes, von ehemaligen Mitarbeitenden des Bundes oder von Mitarbeitenden von Xplain begangen wurden. Bei der vorliegenden Administrativuntersuchung handelt es sich jedoch nicht um eine Disziplinaruntersuchung. Die Prüfung von strafrechtlichen Normen ist ebenfalls nicht Teil des Mandats des Untersuchungsorgans.[238] Unter diesen Umständen können die nachfolgenden Abschnitte nicht als eine Beurteilung des Sachverhalts aus disziplinarischer oder strafrechtlicher Sicht interpretiert werden und sind per Definition nicht bindend für die Behörden, die mit der Anwendung dieser Gesetze betraut sind.

311 Es versteht sich auch von selbst, dass die Beurteilungen des Untersuchungsorgans zum Datenschutz für den EDÖB nicht bindend sind.[239]

312 Keine der in diesem Fall relevanten Normen enthält subjektive Bedingungen für ihre Anwendung. Die Feststellung, was die Personen, deren Verhalten in den folgenden Abschnitten beschrieben wird, wussten und wollten, ist daher im Rahmen der vorliegenden Administrativuntersuchung weder notwendig noch relevant.

a) Forward-Fall Nr. 1: eine Excel-Tabelle (ORMA-Extraktion) mit Details zu strafrechtlichen Untersuchungen und Rechtshilfeverfahren (fedpol) (16. September 2020).

313 Dieser Fall muss unter Berücksichtigung des aBPI, der aBinfV, aISchV und des aDSG in ihrer im September 2020 geltenden Fassung analysiert werden.

(i) *Besondere auf ORMA anwendbare Vorschriften*

314 ORMA basierte und basiert auf Artikel 18 des Bundesgesetzes über die polizeilichen Informationssysteme des Bundes (BPI; SR 361).[240] Gemäss Artikel 18 Absätze 1 und 2 aBPI (Stand September 2020) betreibt Fedpol das interne elektronische Geschäfts- und Aktenverwaltungssystem, das besonders schützenswerte Personendaten und Persönlichkeitsprofile enthalten darf. Das System kann alle ein- und ausgehenden Meldungen von fedpol (Telefonmitschnitte oder -mitschriften, E-Mails, Briefe, Fax) erfassen. Zweck des Informationssystems ist es, Daten über die Geschäfte von fedpol zu bearbeiten, die Arbeitsabläufe effizient und rationell zu gestalten, eine Geschäftskontrolle zu führen und Statistiken zu erstellen.

[238] Vgl. Ziff. 2.2.2 der Offertanfrage, auf die der Mandatsvertrag verweist (AUD B01.01.04.87).
[239] Art. 43 Abs. 4 DSG.
[240] AUD B03.04.01.10.13.

315 Gemäss Artikel 3 Absatz 2 zweiter Satz BPI dürfen «*Personendaten [...] bearbeitet werden, soweit und solange es zur Erfüllung der gesetzlichen Aufgaben notwendig ist*».

316 Die Excel-Datei «[redacted].xlsx» enthält offensichtlich Personendaten. Der Versand dieser Datei per E-Mail an den Mitarbeiter von Xplain an seine Adresse [x]@fedpol.admin.ch stellt *prima facie* eine Datenbearbeitung dar, die nicht für die Erfüllung der gesetzlichen Aufgaben von fedpol erforderlich zu sein scheint. Unserer Auffassung nach scheint dieser Versand daher nicht mit dem BPI vereinbar zu sein.

317 Ferner scheint Xplain in keine der Kategorien von Empfängern zu fallen, an die fedpol ORMA-Daten unter den Bedingungen der Verordnung über das informatisierte Personennachweis-, Aktennachweis- und Verwaltungssystem im Bundesamt für Polizei (IPAS-Verordnung; SR 361.2; Stand September 2020), die auf ORMA anwendbar ist[241], und der Verordnung über das Informationssystem der Bundeskriminalpolizei (JANUS-Verordnung[242]; SR 360.2; Stand September 2020), die ebenfalls auf ORMA anwendbar ist[243], weitergeben konnte.

(ii) *Informationssicherheit*

318 Artikel 26*a* aBinfV, der am 1. November 2016[244] in Kraft trat und dessen Inhalt von Artikel 11 VDTI übernommen wurde, legte die Bedingungen fest, unter denen externe Anbieter Zugang zu Daten erhalten können, die nicht öffentlich zugänglich sind: (i) Es ist zur Erbringung der Leistung erforderlich; (ii) die für die Daten verantwortliche Behörde hat schriftlich zugestimmt und (iii) es wurden angemessene vertragliche, organisatorische und technische Vorkehrungen getroffen, um eine weitere Verbreitung der Daten zu verhindern.

319 Artikel 12 der IPAS-Verordnung (Stand September 2020) verwies auf die aBinfV bezüglich der Sicherheit «der Daten». Dasselbe gilt für Artikel 29w der JANUS-Verordnung (Fassung September 2020).

320 Die in der betroffenen Excel-Datei enthaltenen Daten beziehen sich auf strafrechtliche Ermittlungsverfahren und Rechtshilfeverfahren in Strafsachen, die der Öffentlichkeit nicht zugänglich sind. Der Zugang zu diesen Daten durch Xplain als externer Anbieter setzte daher voraus, dass die Bedingungen von Artikel 26*a* aBinfV erfüllt sind.

321 In Anbetracht des Kontexts sowie des Umfangs und der Art der betroffenen Daten ist es unserer Auffassung nach von vornherein ausgeschlossen, dass der Versand der Daten per E-Mail durch den Mitarbeiter von fedpol an den Mitarbeiter von Xplain – einschliesslich an dessen E-Mail-Adresse beim Bund – im Sinne von Artikel 26*a* aBinfV *erforderlich* war.

322 Das Problem, auf das die Mitarbeiter von fedpol im vorliegenden Fall stiessen, war nämlich das folgende: Bei der Extraktion von ORMA-Daten in eine Excel-Tabelle blieben einige Spalten der Tabelle leer. In seiner E-Mail an den Mitarbeiter von Xplain listete der Mitarbeiter von fedpol die betroffenen Spalten auf und beschrieb sie (insbesondere: ASSERVATEN_NR, SERIEN_NR., VASS_BESCHREIBUNG, ASSERVAT_OERTLICHKEIT etc.).

323 Das Untersuchungsorgan kann sich nicht erklären, warum es in diesem Kontext erforderlich war, die Excel-Tabelle selbst per E-Mail zu versenden. Wenn es aus irgendeinem Grund technisch notwendig war,

[241] Art. 1 Abs. 2 Bst. c IPAS-Verordnung in der Fassung vom September 2020.
[242] Heute: Verordnung über das Nationale Ermittlungssystem (NES-Verordnung).
[243] Art. 1 Abs. 2 Buchstabe d JANUS-Verordnung in der Fassung vom September 2020. Vgl. E-Mail der Rechtsabteilung von fedpol vom 21. Februar 2019 (AUD 03.10.09.211-215).
[244] AS 2016 3445.

Xplain die Excel-Tabelle zur Lösung des Problems mit ORMA zuzusenden, dann ist es dennoch unerklärlich, dass dies geschah, ohne vorher die produktiven Daten der Zeilen 2 bis Zeile 39 938 zu löschen. Das Markieren und Löschen dieser Zeilen dauern nicht länger als ein paar Sekunden. Hätte man – entgegen jeglicher offensichtlicher Notwendigkeit – einen Inhalt als Beispiel in der Tabelle belassen wollen, wäre es leicht gewesen, nur eine oder zwei Zeilen zu belassen, nachdem die darin enthaltenen Daten pseudonymisiert worden wären.

324 Es muss deshalb nicht untersucht werden, ob die verantwortliche Behörde ihre schriftliche Zustimmung zum Zugang durch Xplain gegeben hatte oder ob Massnahmen ergriffen wurden, um den Zugang Dritter zu den an Xplain übermittelten Daten zu verhindern.

325 Zusammenfassend lässt sich sagen, dass unserer Auffassung nach der Versand der Datei «[redacted].zip» per E-Mail an einen Mitarbeiter von Xplain an seine Adresse [Q]@fedpol.admin.ch nicht mit der zum Zeitpunkt des Vorfalls geltenden aBinfV vereinbar zu sein scheint.

(iii) *Klassifizierung der Informationen*

326 Gemäss der von fedpol übernommenen Klassifizierung fielen die in ORMA enthaltenen Informationen unter die Stufe «VERTRAULICH» im Sinne von Artikel 6 aISchV in der Fassung vom September 2020.[245]

327 In Artikel 13 Absätze 1 und 2 aISchV in der Fassung vom September 2020 heisst es: «*Die Erstellung, die Bekanntgabe und das Zugänglichmachen klassifizierter Informationen sind auf ein Minimum zu beschränken; dabei sind Lage, Auftrag, Zweck und Zeit zu berücksichtigen. Klassifizierte Informationen dürfen nur jenen Personen bekannt gegeben oder zugänglich gemacht werden, die davon Kenntnis haben müssen.*»

328 Wie oben dargelegt (Vgl. Rz. 321–323 oben), bestand unserer Auffassung nach in diesem Zusammenhang keine Notwendigkeit, die in der fraglichen Excel-Datei enthaltenen Informationen an Xplain, einen externen Anbieter, weiterzugeben.

329 Folglich lässt sich sagen, dass unserer Auffassung nach der Versand der Datei «[redacted].zip» per E-Mail an einen Mitarbeiter von Xplain an seine Adresse [Q]@fedpol.admin.ch nicht mit der zum Zeitpunkt des Vorfalls geltenden aISchV vereinbar zu sein scheint.

330 Die Tatsache, dass die Excel-Datei nicht mit dem Vermerk «VERTRAULICH» versehen war, scheint zudem nicht mit den Anforderungen der aISchV vereinbar zu sein.

(iv) *Datenschutz*

331 Unserer Analyse zufolge fallen die Daten von ORMA, einem System, das auf Artikel 18 aBPI basiert, nicht unter die Ausnahme von Artikel 2 Absatz 2 Buchstabe c aDSG (Stand September 2020). Anders formuliert, fand das aDSG und findet nun das DSG Anwendung auf das ORMA-System von fedpol.

332 Die Excel-Datei [redacted].xlsx» enthält offensichtlich (besonders schützenswerte) Personendaten.[246] fedpol muss als «Inhaber der Datensammlung» im Sinne des aDSG (d. h. als «Verantwortlicher» in der Terminologie des DSG) bezeichnet werden.

[245] Vgl. [redacted].pdf (29.08.2016) (AUD 03.10.09.179).

[246] Personendaten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen (Art. 3 Bst. c Ziff. 4 aDSG; Art. 5 Bst. c Ziff. 5 DSG).

333 Wie oben dargelegt (Vgl. Rz. 321–323 oben), bestand unserer Auffassung nach in diesem Zusammenhang keine Notwendigkeit, die in der fraglichen Excel-Datei enthaltenen Informationen an Xplain, einen externen Anbieter, weiterzugeben.

334 Xplain verarbeitet keine Personendaten. Xplain hat zwar die Möglichkeit, die (besonders schützenswerten) Personendaten in der Excel-Datei einzusehen. Die Leistung von Xplain besteht jedoch darin, ein Skript zu schreiben, das dann in ORMA (Produktion) verwendet werden kann, damit bei einer nächsten Extraktion in eine Excel-Tabelle die von dem Mitarbeiter von fedpol gemeldeten Spalten nun die Daten enthalten, die dort stehen sollten. Dieses Skript enthält ausschliesslich technische Informationen; es enthält keine Personendaten.[247] Xplain kann daher im vorliegenden Fall nicht als Auftragsbearbeiter von fedpol bezeichnet werden.

335 Unserer Auffassung nach könnte der Versand dieser Excel-Datei per E-Mail an den Mitarbeiter von Xplain an seine Adresse [Q]@fedpol.admin.ch somit eine unzulässige Verarbeitung im Sinne von Artikel 7 aDSG darstellen, die *prima facie* gegen Artikel 12 Absatz 2 Buchstabe a aDSG in seiner Fassung vom September 2020 verstösst. Keiner der Rechtfertigungsgründe von Artikel 13 aDSG scheint uns in diesem Fall gegeben zu sein.[248]

336 Was Artikel 7 VBNIB betrifft, dessen Inhalt sich seit seinem Inkrafttreten im Jahr 2012 nicht geändert hat, und sofern er anwendbar ist (er trägt den Titel: «[redacted]»), gestattet er eine Bearbeitung im Zusammenhang mit technischen Arbeiten nur, wenn dies für die Ausführung dieser Arbeiten *erforderlich* ist (Art. 7 Abs. 1 VBNIB). Wie bereits erwähnt, ist die Weitergabe der in der Excel-Datei enthaltenen (besonders schützenswerten) Personendaten an Xplain in diesem Fall nicht erforderlich. Daher könnte auch diese Bestimmung verletzt worden sein.

(v) *Technische, organisatorische oder prozesshafte Mängel*

337 Es muss nun untersucht werden, welche Verwaltungsverordnungen in diesem Fall relevant sind und ob es mögliche technische, organisatorische oder prozesshafte Mängel gibt.

Identifizierte Verwaltungsverordnungen

338 OA identifizierte unter den ihr vorgelegten Dokumenten die folgende Verwaltungsverordnung des EJPD (in Kraft getreten am 01.03.2018): «Richtlinie für die IKT-Sicherheit im EJPD (EJPD IKT-Richtlinie Sicherheit)»

339 In dem Dokument heisst es in Abschnitt 3.7 «Externe Datenverarbeitung»: «*Die Bearbeitung von geschäftlichen Informationen auf nicht bundeseigenen IKT-Systemen ist nur aufgrund einer vertraglichen Regelung zulässig, welche die sicherheitsrelevanten Belange regelt (IKT-Grundschutz 4.1.3). Für Externe ist dies vertraglich zu regeln*».[249] Des Weiteren heisst es darin: «*Es dürfen keine Informationen an Unberechtigte weitergegeben werden*»[250].

340 Mit anderen Worten, dieses Dokument sieht vor, dass die geschäftlichen Informationen des EJPD nur dann in einem IT-System ausserhalb des Bundes verarbeitet werden dürfen, wenn (i) dies in einem Vertrag vorgesehen ist und (ii) dieser Vertrag Anforderungen an die IT-Sicherheit stellt. Im Wesentlichen

[247] Vgl. Rz. 81 oben.
[248] Als fedpol die Unterstützung dieses externen Anbieters in Anspruch nahm, «handelte es privatrechtlich» im Sinne von Art. 23 aDSG (Art. 40 DSG). fedpol unterlag daher den für Privatpersonen geltenden Bestimmungen des aDSG und nicht den für Bundesorgane geltenden Bestimmungen. Folglich ist die Anforderung einer gesetzlichen Grundlage hier nicht anwendbar (Art. 17 Abs. 1 aDSG für Bundesorgane).
[249] AUD B03.04.11.10.
[250] AUD B03.04.11.12.

übernimmt dieser Text daher nur einen Teil des Inhalts der oben erwähnten Bestimmungen zur Informationssicherheit (Art. 26*a* aBinfV) und zum Datenschutz (Art. 7 Abs. 1 aDSG), insbesondere die Anforderung, technische und vertragliche Vorkehrungen zu treffen, um eine weitere Verbreitung der Daten zu verhindern.

341 Insbesondere in Bezug auf fedpol wird in einem anderen Dokument mit der Bezeichnung «IT Security - Handbuch Informatiksicherheit fedpol.ch», datiert vom 01.02.2003, Folgendes festgehalten: «*Die Wartung aller Informatik-Systeme des Amtes erfolgt durch den Leistungserbringer ISC-EJPD. Soweit Komponenten vor Ort gewartet werden, sind die Aktionen des externen Dienstleisters zu beaufsichtigen. Vor Weitergabe von Geräten an Externe, sind Informationen des Amts auf diesen zu löschen. Sofern die Informationen nicht vollständig gelöscht werden können, ist der externe Dienstleister vertraglich zur Geheimhaltung zu verpflichten mit dem Hinweis auf zivil-, verwaltungs- und strafrechtliche Konsequenzen bei Verletzung dieser Pflicht.*»[251]

342 Diesem Text ist zu entnehmen, dass offizielle Daten («*Informationen des Amtes*») nicht an Dritte weitergegeben werden dürfen. Wenn dies dennoch der Fall ist, sollten die externen Dienstleister einer Geheimhaltungspflicht unterstellt werden. Dieser Text übernimmt somit teilweise den Inhalt der oben erwähnten Bestimmungen zur Informationssicherheit (Art. 26*a* aBinfV) und zum Datenschutz (Art. 7 Abs. 1 aDSG), insbesondere die Anforderung, technische und vertragliche Vorkehrungen zu treffen, um eine weitere Verbreitung der Daten zu verhindern.

343 Diese Verordnung legt auch Folgendes fest: «*Der Zugang zu Informatik-Systemen und der Zugriff auf Informatik-Anwendungen und Informationen wird stets nur in dem Umfang gewährt, der für die Aufgabenerfüllung erforderlich ist. Gleichermassen ist jeder Mitarbeiter gefordert, den Zugang zu Informatik-Systemen und Zugriff auf Prozesse oder Informationen unberechtigten Dritten zu verwehren. Die Verarbeitung personenbezogener Daten ist nur im festgelegten, gesetzlichen Rahmen zulässig. Eine Nutzung ausserhalb des rechtlichen Rahmens oder die Weitergabe in logischer oder physischer Form ist untersagt.*»[252]

344 In einer weiteren Verwaltungsverordnungen mit der Bezeichnung «*Weisung des Direktors betreffend Informationssicherheit fedpol*» vom 01.01.2012 ist Folgendes festgelegt:

> *«Um Risiken beim Einsatz von E-Mail zu minimieren, gelten folgende Regelungen:*
>
> *- Das Umleiten der persönlichen Mailbox an eine bundesfremde (nicht admin.ch) E Mail-Adresse (z.B. während den Ferien, Geschäftsreisen usw.) ist untersagt.*
>
> *- Das Verwenden von unverschlüsselten E-Mail-Diensten des Internets für den Transfer von dienstlichen Dokumenten oder von Personendaten zur und von der persönlichen Mailbox im EJPD ist verboten (z.B. das Übermitteln von Dokumenten, an denen man zu Hause weiterarbeiten möchte).*
>
> *- Klassifizierte Informationen und datenschutzrechtlich geschützte Personendaten dürfen auf elektronischem Weg nur verschlüsselt übermittelt werden ».*[253]

345 Aus dieser Verordnung geht hervor, dass die Weiterleitung von E-Mails von einer persönlichen Adresse des Bundes an eine «*bundesfremde*» Adresse ausdrücklich untersagt ist. Darüber hinaus ist es verboten, «*dienstliche Dokumente*» und Personendaten per unverschlüsselter E-Mail von oder an die persönliche

[251] AUD-B03.04.10ter.10.
[252] AUD-B03.04.10ter.13.
[253] AUD-B03.04.10.1248.

E-Mail-Adresse des Bundes zu übermitteln. Ausserdem muss jede elektronische Kommunikation von klassifizierten oder Personendaten verschlüsselt werden.

346 Diese Verordnung wurde jedoch durch die «*Weisung des Direktors betreffend Informationssicherheit fedpol*» vom 01.08.2013 aufgehoben, die den oben erwähnten Abschnitt nicht mehr enthielt.[254]

Beurteilung im vorliegenden Fall

347 Bei der Analyse der oben genannten Verwaltungsverordnungen entsteht ein nicht sehr klarer und prägnanter Gesamteindruck. Die Texte greifen weitgehend die geltenden Gesetze und Verordnungen auf, halten sich aber nicht immer an deren Terminologie, was zu Unklarheiten oder Verwirrung führen kann. Beispielsweise könnte man sich fragen, wer die *Unberechtigten* sind, die in der Richtlinie für die IKT-Sicherheit im EJPD genannt werden. Daher scheint eine Bereinigung im Sinne einer Reduzierung von Redundanzen und einer Harmonisierung der Terminologie erforderlich zu sein.[255]

348 Die uns vorgelegten Verwaltungsverordnungen weisen unserer Auffassung nach den Mangel auf, dass sie weder ein klares Verbot bezüglich der Weitergabe produktiver Daten an externe Anbieter noch klare und restriktive Regeln für den On-Premise- oder Remote-Zugang externer Anbieter zu produktiven Daten enthalten.[256]

349 Die Tatsache, dass der Mitarbeiter von fedpol diese Excel-Datei im September 2020 per E-Mail an den Mitarbeiter von Xplain sandte, und die Tatsache, dass die besagte Datei nach dem Datenabfluss im Juni 2023 ins Darknet gelangte, zeigen ebenfalls, dass fedpol nicht genügend Massnahmen ergriffen hat, um sich gegen den Zugriff auf seine Daten durch Dritte zu schützen.[257]

350 In Bezug auf den ersten Aspekt (Versand durch den Mitarbeiter von fedpol an die Adresse [Q]@fedpol.admin.ch) war der Mitarbeiter von fedpol («A») in der Lage, (i) die Daten aus dem ORMA-Produktionssystem zu extrahieren und (ii) eine 8 MB grosse komprimierte Datei, die eine Excel-Datei mit dem Namen des ORMA-Systems und 39 938 Zeilen mit aus diesem Produktionssystem extrahierten Daten enthielt, per E-Mail an einen Mitarbeiter von Xplain an die Adresse [Q]@fedpol.admin.ch zu senden. Im Rahmen der Untersuchung wurde weder ein Prozess (z. B. Freigabe der E-Mail durch einen anderen Mitarbeiter von fedpol) noch eine technische Massnahme (z. B. automatische Blockierung des Versands von E-Mails, die bestimmte vordefinierte Kriterien erfüllen) identifiziert, die vor dem Versand durchgeführt wurden.

351 Die Tatsache, dass dieser Mitarbeiter von fedpol die Extraktion und den Versand per E-Mail an einen Mitarbeiter von Xplain durchführte, ist ebenfalls ein starker Hinweis darauf, dass die von fedpol ergriffenen organisatorischen Massnahmen im Hinblick auf die Schulung und Sensibilisierung von Personen, die produktive Daten von ORMA bearbeiten, unzureichend waren.

352 Ferner waren unserer Auffassung nach keine organisatorischen oder technischen Massnahmen ergriffen worden, um sicherzustellen, dass die Tatsache, dass Q ein Mitarbeiter eines externen Anbieters war, für jeden Mitarbeiter des Bundes, der mit Q in Kontakt kam, sofort erkennbar war: Beispielsweise hätte die E-Mail-Adresse [Q]@fedpol.admin.ch einen Vermerk (z. B. «extern» oder Ähnliches) enthalten können. Es ist ausserdem problematisch, dass die automatische Signatur in der Fusszeile der E-Mail des Mitarbeiters von Xplain den Eindruck erweckte, dass er ein Mitarbeiter von fedpol ist.

[254] AUD-B03.04.10.1242-1245.
[255] Vgl. die Empfehlungen am Ende des Berichts (Abschnit VI.B unten).
[256] Vgl. die Empfehlungen am Ende des Berichts (Abschnit VI.B unten).
[257] Vgl. die Empfehlungen am Ende des Berichts (Abschnit VI.B unten).

353 Aus technischer Sicht stellen wir ausserdem fest, dass das System bei der Extraktion in eine Excel-Datei nicht automatisch den Vermerk «VERTRAULICH» anbrachte, obwohl die aus dem ORMA-Produktionssystem extrahierten Daten als vertraulich eingestuft waren.

354 Was den zweiten Aspekt (die Datei befand sich in der IT-Umgebung von Xplain und letztendlich im Darknet) betrifft, so war der Mitarbeiter von Xplain in der Lage, die gleiche Datei von seiner Adresse [Q]@fedpol.admin.ch an seine Adresse [Q]@xplain.ch zu senden. Auch hier ergab die Untersuchung, dass vor diesem Versand weder ein Prozess durchgeführt noch eine technische Massnahme angewandt wurde.

355 Xplain hätte gemäss den Allgemeinen Geschäftsbedingungen des Bundes, welche in die Verträge mit fedpol aufgenommen wurden, alle wirtschaftlich zumutbaren sowie alle möglichen technischen und organisatorischen Massnahmen ergreifen müssen, um sicherzustellen, dass die im Rahmen der Vertragserfüllung generierten und ausgetauschten Daten nicht in den Besitz unbefugter Dritter gelangen. Diese vertragliche Massnahme ist notwendig, aber unzureichend. Im vorliegenden Fall:

i. Von Xplain wurden vertraglich keine konkreten Massnahmen verlangt.

ii. Wir konnten hinsichtlich der Einhaltung dieser Pflicht keine Kontrolle durch fedpol feststellen.

356 Mehrere Befragte gaben an, dass Mitarbeitende von Xplain eine Personensicherheitsprüfung (PSP) bestanden hatten. Dies war insbesondere der Fall bei Q.

357 Die PSP bietet jedoch nur einen retrospektiven Blick zu einem bestimmten Zeitpunkt und deckt nicht die Zukunft ab, bis sie innerhalb der in der Verordnung festgelegten Fristen erneuert wird. Historisch gesehen diente die PSP gemäss dem BWIS in erster Linie dem Schutz von Informationen im Zusammenhang mit der inneren oder äusseren Sicherheit der Schweiz, wobei verschiedene Verordnungen den Anwendungsbereich der PSP später erweitert haben.[258] Grundsätzlich zog die mit der Durchführung der Kontrolle beauftragte Fachstelle vor allem gerichtliche und polizeiliche Datenregister heran und ersuchte gegebenenfalls ausländische Staaten um Unterstützung, wenn ein Abkommen dies zuliess. Bei bestimmten Personenkategorien führte die Fachstelle zusätzlich eine Befragung der zu überprüfenden Person durch («erweiterte Personensicherheitsprüfung mit Befragung»). Im vorliegenden Fall und nach unserem Wissen wurde keiner der Mitarbeitenden von Xplain einer solchen erweiterten Personensicherheitsprüfung mit Befragung unterzogen.

358 Wir sind der Auffassung, dass solche Kontrollen notwendig, aber nicht ausreichend sind, um sicherzustellen, dass eine Person über die erforderliche Sensibilität im Bereich der Informationssicherheit verfügt.

359 Ferner bezog sich die PSP nur auf natürliche Personen und lieferte keine Angaben zur Informationssicherheit des Unternehmens, mit dem der Bund eine vertragliche Beziehung einging oder unterhielt.[259] In diesem Zusammenhang sah die zum Zeitpunkt des Vorfalls geltende Verordnung über die Personensicherheitsprüfungen (PSPV) die Möglichkeit vor, ein bundesexternes Unternehmen, das Zugang zu Informationen des Bundes hat, die als VERTRAULICH oder GEHEIM eingestuft sind, einem Verfahren zur Betriebssicherheitserklärung (BSE) zu unterziehen. Im Rahmen der Untersuchung wurde

[258] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953, 2984. Siehe auch Botschaft zum Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit und zur Volksinitiative «S.O.S. Schweiz ohne Schnüffelpolizei» vom 7. März 1994, BBl 1994 II 1127, 1147: «Eine der heikelsten und intensivsten Bedrohungen der inneren Sicherheit entsteht dann, wenn an wichtigen Schlüsselstellen eingesetzte Personen Verrat üben, gegen den Staat selber arbeiten oder seine Institutionen auf rechtswidrige Art verändern wollen.»

[259] Vgl. mit der Kontrolle, die in der am 1. Januar 2024 in Kraft getretenen Verordnung über das Betriebssicherheitsverfahren (VBSV) vorgesehen ist.

im Zusammenhang mit Xplain keine BSE identifiziert. Ein interner E-Mail-Austausch vom Dezember 2020 deutet darauf hin, dass Xplain nie über eine BSE verfügte.[260]

360 Bezieht sich die vom Mitarbeiter von Xplain unterzeichnete Verpflichtungserklärung auf die Übertragung von nicht öffentlich zugänglichen Daten durch diesen Mitarbeiter von einer E-Mail des Bundes an seine E-Mail-Adresse bei Xplain? Insbesondere, bezieht sich die Übertragung «ausserhalb der Räumlichkeiten des Auftraggebers» nur auf die physische Übertragung, wie eine wörtliche Auslegung nahelegt, oder auch auf die Übertragung per E-Mail, wie es eine teleologische Auslegung wohl implizieren würde? Wir stellen daher fest, dass die vom Mitarbeiter von Xplain unterzeichnete Verpflichtungserklärung zu viel Raum für Interpretationen liess.

361 Die oben beschriebenen technischen, vertraglichen und organisatorischen Massnahmen werden alle im Vorfeld der vertraglichen Beziehung ergriffen. Massnahmen, die während des Vertragsverhältnisses ergriffen werden – wie Kontrollen oder Audits – bleiben jedoch unerlässlich, wenn auch nur, um die Einhaltung der vertraglichen Pflichten zu überprüfen. Im vorliegenden Fall wurden jedoch keine solchen Massnahmen identifiziert.

362 In den Empfehlungen weiter unten werden die vorgeschlagenen Verbesserungen dargelegt, sodass weitere Schutzmassnahmen vorgesehen und die erwähnten Mängel behoben werden können.

b) Forward-Fall Nr. 2: verschiedene Dateien im Anhang einer E-Mail, die u. a. geheime Informationen über Bundesrätinnen und -räte und ausländische Beamte enthielt (5. Mai 2018)

363 Die oben aufgeführte Analyse (Buchstabe a) trifft grösstenteils auf den vorliegenden Fall zu. Dieser betrifft im Wesentlichen den Versand von als «VERTRAULICH» eingestuften fepdol-Dokumenten von Ende 2017 bzw. Anfang 2018 an einen Mitarbeiter von Xplain an dessen Adresse [R]@fedpol.admin.ch. Diese Dokumente beziehen sich auf Treffen mit ranghohen nationalen und internationalen Beamten sowie auf Informationen über Bundesrätinnen und Bundesräte.

364 Zusammenfassend lässt sich sagen, dass die für ORMA geltenden besonderen Normen (insbesondere das BPI) sowie die Bestimmungen zur Informationssicherheit (aBinfV) und zur Klassifizierung von Informationen (aISchV) *prima facie* nicht eingehalten worden zu sein scheinen. Dasselbe gilt für die Datenschutzbestimmungen (aDSG).

365 Die Untersuchung der technischen, organisatorischen oder prozesshaften Mängel, die dazu beigetragen haben, dass dem Mitarbeiter von Xplain die fraglichen Dokumente unter Verletzung der in den vorherigen Abschnitten erörterten Normen zugesandt wurden, wurde bereits weiter oben erläutert, weshalb an dieser Stelle darauf verwiesen wird.

c) Forward-Fall Nr. 3: Versand einer Excel-Tabelle mit mehr als 1 000 Zeilen in Bezug auf Interpol-Ausschreibungen (1. September 2021)

366 Im Grunde geht es um eine Excel-Datei mit der Bezeichnung «[redacted]xlsx».

367 Diese Datei umfasst 1 045 Zeilen und 32 Spalten mit Informationen zu Interpol-Ausschreibungen verschiedener Kategorien. Sie enthält (besonders schützenswerte) Personendaten. Diese Excel-Tabelle wurde offensichtlich aus ORMA extrahiert – einem System, dessen Inhalt als «VERTRAULICH» eingestuft wird.

[260] E-Mail-Austausch zwischen dem Informatiksicherheitsbeauftragten der Organisationseinheit (ISBO) von armasuisse und einem Projektmanager von armasuisse zwischen dem 10. und 17. Dezember 2020 (AUD 03.10.09.257-260).

368 Die Untersuchung ergab nicht, ob der Mitarbeiter von Xplain (Z) die fragliche Excel-Datei zuvor von einem fedpol-Mitarbeiter erhalten hatte oder ob Z selbst eine Datenextraktion aus dem ORMA-Produktionssystem vorgenommen hatte und wenn ja, unter welchen Umständen.

369 Im Falle der ersten Annahme (Versand durch einen Mitarbeiter von fedpol an diesen Mitarbeiter von Xplain) ist die oben beschriebene Analyse (siehe Buchstabe a) ebenfalls anwendbar. Die zweite Annahme (Zugang zum Produktionssystem durch den Mitarbeiter von Xplain) wird weiter unten behandelt, weshalb auf sie verwiesen wird.[261]

370 In beiden Fällen und zusammengefasst lässt sich sagen, dass die für ORMA geltenden besonderen Vorschriften (insbesondere das BPI) sowie die Bestimmungen zur Informationssicherheit (aBinfV) und zur Klassifizierung von Informationen (aISchV) *prima facie* nicht eingehalten worden zu sein scheinen. Dasselbe gilt für die Datenschutzbestimmungen (aDSG).

371 Zwecks Vermeidung von Wiederholungen kann mutatis mutandis auf die Analyse der technischen, organisatorischen oder prozesshaften Mängel verwiesen werden, die im ersten Fall oben vorgenommen wurde.

d) Zugriffs-Fall: eine Excel-Tabelle (ORMA-Extraktion), die den «Betreff» der Fälle enthielt (22. September 2011).

372 Dieser Fall muss unter Berücksichtigung des aBPI, der aBinfV 2003, der aISchV und des aDSG in ihrer im September 2010 geltenden Fassung analysiert werden.

(i) *Besondere auf ORMA anwendbare Vorschriften*

373 Die speziellen Vorschriften, die auf ORMA anwendbar sind, wurden oben (Rz. 314–315) erläutert, weshalb an dieser Stelle darauf verwiesen wird.

374 Wie im faktischen Teil dieses Berichts dargelegt[262], scheint es, dass S, der damals bei Xplain angestellt war, zum Zeitpunkt des Vorfalls (September 2010) Zugriff auf das ORMA-Produktionssystem von fedpol hatte. Die genauen Umstände, unter denen dieser Zugriff erfolgte, konnten nicht ermittelt werden.

375 Es scheint jedoch so, dass S aller Wahrscheinlichkeit nach in der Lage war, Daten aus dem ORMA-Produktionssystem in eine Excel-Datei zu extrahieren. Unter tatsächlichen Umständen, die im Rahmen der Untersuchung nicht abschliessend geklärt werden konnten, gelangte diese Excel-Datei in die IT-Umgebung von Xplain.

376 S schickte diese Datei schliesslich in einer unverschlüsselten E-Mail von seiner Adresse [S]@xplain.ch an verschiedene Mitarbeitende von fedpol an deren Adresse @fedpol.admin.ch.

377 Die Excel-Datei «[redacted]*.xls*», insbesondere die Spalte C mit der Bezeichnung «*Betreff*», enthält offensichtlich Personendaten, einschliesslich besonders schützenswerter Personendaten (mehr als 8 000 Zeilen mit detaillierten Informationen zu verschiedenen Verfahren, insbesondere Strafverfahren).

378 Der Zugriff auf diese Daten, deren Extraktion, die Speicherung in der IT-Umgebung eines externen Anbieters und der Versand aus dieser Umgebung per unverschlüsselter E-Mail an die IT-Umgebung von fedpol stellen *prima facie* eine Datenbearbeitung dar, die für die Erfüllung der gesetzlichen Aufgaben von

[261] Vgl. V.A.2.d) unten.
[262] Vgl. Rz. 101–115 oben.

fedpol nicht erforderlich zu sein scheint. Unserer Auffassung nach scheinen diese Datenbearbeitungen nicht mit dem BPI vereinbar zu sein.

379 Während seiner Befragung sagte F im Wesentlichen aus, dass S die Informationen in Spalte C mit der Bezeichnung «*Betreff*» nicht benötigt habe, um die von ihm erwartete Aufgabe zu erfüllen.[263]

380 Ferner scheint der vorliegende Fall nicht unter eine Konstellation zu fallen, in der Xplain auf der Grundlage der Verordnung über das informatisierte Personennachweis-, Aktennachweis- und Verwaltungssystem im Bundesamt für Polizei (IPAS-Verordnung; SR 361.2; Stand September 2020), die auf ORMA anwendbar ist[264], und der Verordnung über das Informationssystem der Bundeskriminalpolizei (JANUS-Verordnung;[265] SR 360.2; Stand September 2020), die ebenfalls auf ORMA anwendbar ist,[266] ein Zugriffsrecht hätte gewährt werden können; Xplain scheint ebenfalls nicht in die Kategorien von Empfängern zu passen, an die fedpol ORMA-Daten gemäss den beiden oben genannten Verordnungen weitergeben konnte.

(ii) *Informationssicherheit*

381 Artikel 12 der IPAS-Verordnung (Stand September 2010) verwies bezüglich der «Datensicherheit» auf die aBinfV 2003 und die Richtlinien des Informatikrats des Bundes (IRB) vom 27. September 2004 über die Informatiksicherheit in der Bundesverwaltung. Dasselbe gilt für Artikel 26 der JANUS-Verordnung (Stand September 2010).

382 Keiner dieser Texte regelte jedoch den Zugriff auf Daten durch externe IKT-Leistungserbringer.

383 Der in den vorherigen Fällen erwähnte Artikel 26*a* aBinfV enthielt eine Regelung zum Datenzugriff für externe IKT-Leistungserbringer, trat aber erst nach den Ereignissen am 1. November 2016 in Kraft.[267]

(iii) *Klassifizierung der Informationen*

384 Gemäss der von fedpol übernommenen Klassifizierung fielen die in ORMA enthaltenen Informationen unter die Stufe «VERTRAULICH» im Sinne von Art. 6 aISchV in der Fassung vom September 2010.[268]

385 In Artikel 13 Absätze 1 und 2 aISchV in der Fassung vom September 2010 heisst es: «*Die Erstellung, die Bekanntgabe und das Zugänglichmachen klassifizierter Informationen sind auf ein Minimum zu beschränken; dabei sind Lage, Auftrag, Zweck und Zeit zu berücksichtigen. Klassifizierte Informationen dürfen nur jenen Personen bekannt gegeben oder zugänglich gemacht werden, die davon Kenntnis haben müssen*.»

386 Wir sind der Auffassung, dass der Zugriff auf diese Daten durch S, deren Extraktion, die Speicherung in der IT-Umgebung eines externen Anbieters und der Versand aus dieser Umgebung per unverschlüsselter

---

[263] Siehe oben Rz. 113.
[264] Art. 1 Abs. 2 Bst. c IPAS-Verordnung in der Fassung vom September 2010.
[265] Heute: Verordnung über das Nationale Ermittlungssystem (NES-Verordnung).
[266] Art. 1 Abs. 2 Bst. d JANUS-Verordnung in der Fassung vom September 2020. Vgl. E-Mail der Rechtsabteilung von fedpol vom 21. Februar 2019 (AUD 03.10.09.211-215).
[267] AS 2016 3445. Der Inhalt von Art. 26a aBinfV, der von Art. 11 VDTI übernommen wurde, legte die Bedingungen fest, unter denen externe IKT-Leistungserbringer Zugang zu Daten erhalten können, die nicht öffentlich zugänglich sind, nämlich: (i) Es ist zur Erbringung der Leistung erforderlich; (ii) die für die Daten verantwortliche Behörde hat schriftlich zugestimmt und (iii) es wurden angemessene vertragliche, organisatorische und technische Vorkehrungen getroffen, um eine weitere Verbreitung der Daten zu verhindern. Vgl. auch: Pressemitteilung des Bundesrates vom 30. September 2016 «Bundesrat minimiert die Datenweitergabe an externe IKT-Dienstleister beim Bau und Betrieb von Informationssystemen».
[268] Vgl. [redacted].pdf (29.08.2016) (AUD 03.10.09.179).

E-Mail an die IT-Umgebung von fedpol im Kontext des fraglichen Sachverhalts nicht notwendig erscheint. Die aISchV scheint daher in diesem Fall verletzt worden zu sein.

387 Die Tatsache, dass die betreffende Excel-Datei nicht mit dem Vermerk «VERTRAULICH» versehen wurde, scheint zudem nicht mit den Anforderungen der aISchV vereinbar zu sein.

(iv) *Datenschutz*

388 Unserer Analyse zufolge fallen die Daten von ORMA, einem System, das auf Artikel 18 aBPI basiert, nicht unter die Ausnahme von Artikel 2 Absatz 2 Buchstabe c aDSG (Stand September 2010). Anders formuliert, fand das aDSG und findet nun das DSG auf das ORMA-System von fedpol Anwendung.

389 Die Excel-Datei «[redacted]*.xls*» enthält offensichtlich (besonders schützenswerte) Personendaten.[269] fedpol muss als «Inhaber der Datensammlung» im Sinne des aDSG (d. h. als «Verantwortlicher» in der Terminologie des DSG) bezeichnet werden.

390 Wie oben ausgeführt, bestand im vorliegenden Kontext unserer Auffassung nach keine Notwendigkeit, einem Mitarbeiter von Xplain, d. h. einem externen Anbieter, Zugang zum ORMA-Produktionssystem zu gewähren, wodurch dieser Mitarbeiter in die Lage versetzt wurde, eine Extraktion von (besonders schützenswerten) Personendaten aus ORMA vorzunehmen und diese anschliessend aus der IT-Umgebung von Xplain an eine E-Mail-Adresse @fedpol.ch zu senden.

391 Zudem führte Xplain *de facto* eine Verarbeitung von Personendaten auf Anweisung von fedpol durch. Xplain extrahierte nämlich (besonders schützenswerte) Personendaten von ORMA und sandte sie anschliessend per E-Mail an einen Mitarbeiter von fedpol gemäss den Anweisungen eines anderen Mitarbeiters von fedpol.

392 Unserer Auffassung nach muss Xplain daher im vorliegenden Fall als Auftragsbearbeiter von fedpol bezeichnet werden.

393 Wie die Untersuchung zeigte, war in den Verträgen für ORMA die Auftragsbearbeitung durch Xplain nicht vorgesehen, geschweige denn geregelt. Die zentrale Anforderung von Artikel 10a aDSG scheint somit nicht erfüllt zu sein.[270]

394 Da fedpol diese Auftragsbearbeitung nicht vertraglich geregelt hat, hatte es erst recht keine Möglichkeit, den Ort der Bearbeitung und den möglichen Einsatz von Unterauftragsbearbeitern zu überblicken (Xplain hat Büros im Ausland, die von Tochtergesellschaften in Spanien und Deutschland betrieben werden).[271]

395 Letztendlich handelt es sich in diesem Fall *prima facie* um eine unzulässige Verarbeitung im Sinne von Artikel 7 aDSG, die gegen Artikel 12 Absatz 2 Buchstabe a aDSG in seiner Fassung vom September 2010 verstösst. Keiner der Rechtfertigungsgründe von Artikel 13 aDSG scheint uns in diesem Fall gegeben zu sein.[272]

---

[269] Personendaten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen (Art. 3 Bst. c Ziff. 4 aDSG; Art. 5 Bst. c Ziff. 5 DSG).

[270] Zur Frage der drei *curae* siehe unten Rz. 499 ff.

[271] Vgl. Rz. 214–217 oben.

[272] Als fedpol die Unterstützung dieses externen Anbieters in Anspruch nahm, «handelte es privatrechtlich» im Sinne von Art. 23 aDSG (Art. 40 DSG). fedpol unterlag daher den für Privatpersonen geltenden Bestimmungen des aDSG und nicht den für Bundesorgane geltenden Bestimmungen. Folglich ist die Anforderung einer gesetzlichen Grundlage hier nicht anwendbar (Art. 17 Abs. 1 aDSG für Bundesorgane).

(v) *Technische, organisatorische oder prozesshafte Mängel*

396 Es muss nun untersucht werden, welche Verwaltungsverordnungen in diesem Fall relevant sind und ob es mögliche technische, organisatorische oder prozesshafte Mängel gibt.

397 OA identifizierte unter den bereitgestellten Dokumenten die folgenden Verwaltungsverordnungen:

i. Das Dokument «*Weisung des EJPD über die Einrichtung von Online-Verbindungen und die Erteilung von Zugriffsbewilligungen auf Informatikanwendungen des EJPD (Online-Weisung EJPD)*»[273] vom 30. September 2004 (in Kraft getreten am 1. Oktober 2004) regelt a) die Bedingungen für die Einrichtung einer Internetverbindung zwischen dem EJPD und Organen des Bundes und der Kantone, die den Mitarbeitenden dieser Organe (Benutzerinnen und Benutzern) den Zugang zu einer Informatikanwendung des EJPD ermöglicht, und b) die Bedingungen für die Erteilung einer individuellen Zugangsberechtigung an diese Benutzerinnen und Benutzer, wenn ihnen über diese Internetverbindung Personendaten zugänglich gemacht werden (vgl. Art. 2 Abs. 1 Bst. a und b der Weisung); d. h. ein Zugang für Benutzerinnen und Benutzer ausserhalb der Organe des Bundes und der Kantone ist nicht vorgesehen;

ii. Ein weiteres Dokument «*Weisung des EJPD über die Umsetzung des Datenschutzes und Informationssicherheit (DSIS-Weisung EJPD)*»[274] vom 12. Mai 2011 (in Kraft getreten am 1. Juni 2011) sieht unter Ziffer 22 «Kontrolle und Berichterstattung» Folgendes vor: «*Die Umsetzung von DSIS wird auf der Stufe Departement und in den Verwaltungseinheiten regelmässig kontrolliert, damit Mängel rechtzeitig erkannt und durch geeignete Massnahmen behoben werden können*.»;

iii. Das Dokument «*Handbuch Informatiksicherheit*»[275] von fedpol vom 1. Februar 2003 (Inkrafttreten nicht angegeben) sieht in Abschnitt 4.1.11 «Wartung» Folgendes vor: «*Die Wartung aller Informatik-Systeme des Amtes erfolgt durch den Leistungserbringer ISC-EJPD. Soweit Komponenten vor Ort gewartet werden, sind die Aktionen des externen Dienstleisters zu beaufsichtigen. Vor Weitergabe von Geräten an Externe, sind Informationen des Amts auf diesen zu löschen. Sofern die Informationen nicht vollständig gelöscht werden können, ist der externe Dienstleister vertraglich zur Geheimhaltung zu verpflichten mit dem Hinweis auf zivil-, verwaltungs- und strafrechtliche Konsequenzen bei Verletzung dieser Pflicht. Allenfalls kann zusätzlich eine Konventionalstrafe vereinbart werden.*». Des Weiteren heisst es in Abschnitt 4.3 «Sicherheitsleitsätze»: «*Der Zutritt zu Gebäuden und Räumlichkeiten, der Zugang zu Informatik-Systemen und der Zugriff auf Informatik-Anwendungen und Informationen wird stets nur in dem Umfang gewährt, der für die Aufgabenerfüllung erforderlich ist. Gleichermassen ist jeder Mitarbeiter gefordert, den Zugang zu Informatik-Systemen und Zugriff auf Prozesse oder Informationen unberechtigten Dritten zu verwehren*.»;

iv. Schliesslich das Dokument «*Weisung des Direktors fedpol betreffend Informationssicherheit fedpol*»[276] vom 1. März 2007 (in Kraft getreten am 1. März 2007), in dem es in Abschnitt 4 «E-Mail» heisst: «*Ohne Chiffrierung dürfen generell keine klassifizierten Informationen und keine datenschutzrechtlich geschützten Personendaten elektronisch übermittelt werden, weder innerhalb noch ausserhalb der Bundesverwaltung. Der Versand solcher Informationen muss immer eingeschrieben auf postalischem Weg erfolgen*.»

[273] AUD B03.04.10.934-941.
[274] AUD B03.04.10.1185-1194.
[275] AUD B03.04.10ter.1-24.
[276] AUD B03.04.10bis.1-5.

398 Aus diesen Texten lässt sich ableiten, dass der Zugang zu Personendaten an Bedingungen geknüpft ist, die regelmässig kontrolliert werden müssen. Das ISC-EJPD ist zudem für die Wartung der Informatiksysteme von fedpol zuständig, und es liegt auf der Hand, dass ein externer Dienstleister keinen Zugriff auf «*Informationen des Amtes*» haben darf. Diese Daten müssen grundsätzlich auf Geräten, die an einen externen Dienstleister übergeben werden, gelöscht werden. Wenn sie nicht vollständig gelöscht werden können, muss der Dienstleister zur Geheimhaltung verpflichtet werden, mit Verweis auf die zivilrechtlichen, verwaltungsrechtlichen und strafrechtlichen Folgen einer Verletzung dieser Pflicht. Schliesslich darf der Zugang zu Informatikanwendungen nur in dem Masse gewährt werden, wie es für die Erfüllung der Aufgabe erforderlich ist. Die Mitarbeitenden müssen unbefugten Dritten den Zugang zu Informatiksystemen oder Informationen verweigern.

399 Diese Texte übernehmen somit teilweise den Inhalt der oben erwähnten Datenschutzbestimmungen (Art. 7 Abs. 1 aDSG), insbesondere die Anforderung, Vorkehrungen zu treffen, um eine weitere Verbreitung der Daten zu verhindern.

400 Zwecks Vermeidung von Wiederholungen kann *mutatis mutandis* auf die Analyse der technischen, organisatorischen oder prozessbezogenen Mängel verwiesen werden, die im ersten Fall oben vorgenommen wurde.

e) «Aktiver Transfer»-Fall Nr. 1: Screenshots, die im Rahmen der PAGIRUS-TROVA-Migration gesendet wurden (28. Januar 2016).

401 Dieser Fall muss unter Berücksichtigung des aBPI, der aBinfV, der aISchV und des aDSG in ihrer im Januar 2016 geltenden Fassung analysiert werden.

(i) *Besondere auf PAGIRUS anwendbare Vorschriften*

402 PAGIRUS war hauptsächlich durch die Verordnung über das Personen-, Akten- und Geschäftsverwaltungssystem PAGIRUS des Bundesamtes für Justiz (PAGIRUS-Verordnung)[277] geregelt, die am 1. November 2016[278] aufgehoben wurde, und danach durch die Verordnung über das elektronische Personen-, Akten- und Geschäftsverwaltungssystem (ELPAG-Verordnung).[279]

403 Die PAGIRUS-Verordnung stützte sich auf Artikel 57h Absatz 2 RVOG, der zum Zeitpunkt des Geschehens Folgendes vorsah: «*Zu den Personendaten haben ausschliesslich Mitarbeiterinnen und Mitarbeiter des betreffenden Bundesorgans Zugang, und dies nur soweit sie sie zur Erfüllung ihrer Aufgabe brauchen*».

404 Die Anhänge, die der E-Mail vom 28. Januar 2016 beigefügt waren, enthielten offensichtlich Personendaten. Der Versand dieser Anhänge per E-Mail an den Mitarbeiter von Xplain an seine Adresse [T]@xplain.ch stellt eine Datenbearbeitung dar, die nicht für die Erfüllung der gesetzlichen Aufgaben des BJ erforderlich zu sein scheint. Unserer Auffassung nach war der Versand daher nicht mit Artikel 57h Absatz 2 RVOG vereinbar. Aus der Befragung von G ging ausserdem hervor, dass Xplain nicht für die Migration als solche zuständig war. Xplain war lediglich für die Bereitstellung des Skripts verantwortlich, das die Übertragung der Daten von einer Anwendung zur anderen ermöglichte. Daher waren anonymisierte oder geschwärzte Daten als Teil dieser unterstützenden Tätigkeit ausreichend.[280]

[277] AS 2010 1.
[278] AS 2016 3261.
[279] SR 351.12.
[280] Tonaufnahme der Befragung Nr. 231128-002.

405 Ferner fiel Xplain nicht in eine der Kategorien von Empfängern, an die das BJ PAGIRUS-Daten unter den in der PAGIRUS-Verordnung festgelegten Bedingungen weitergeben konnte.

(ii) *Informationssicherheit*

406 Artikel 13 Absatz 1 der PAGIRUS-Verordnung verwies bezüglich der «Informatiksicherheit» auf die aDSV, die aBinfV 2003 sowie die Richtlinien des IRB vom 27. September 2004 über die Informatiksicherheit in der Bundesverwaltung.

407 Keiner dieser Texte regelte jedoch den Zugriff auf Daten für externe IKT-Leistungserbringer.

408 Der in den vorherigen Fällen erwähnte Artikel 26*a* aBinfV enthielt eine Regelung zum Datenzugriff für externe IKT-Leistungserbringer, trat aber erst nach den Ereignissen am 1. November 2016 in Kraft.[281]

409 Ferner sah Artikel 13 Absatz 2 der PAGIRUS-Verordnung vor, dass das BJ in der in Artikel 2 Absatz 2 erwähnten Verordnung über die Datenbearbeitung die organisatorischen und technischen Massnahmen zur Verhinderung der unbefugten Verarbeitung von Daten festlegt und die Modalitäten der automatischen Aufzeichnung der Datenbearbeitung und des Abrufs von Daten bestimmt.

(iii) *Datenschutz*

410 Unserer Analyse zufolge fallen die Daten von PAGIRUS nicht unter die Ausnahme von Artikel 2 Absatz 2 Buchstabe c aDSG (Stand Januar 2016). Anders formuliert, fand das aDSG und findet nun das DSG auf das PAGIRUS-System des BJ Anwendung.

411 Die als Anhang an die betreffende E-Mail-Adresse gesendeten Dokumente enthalten offensichtlich (besonders schützenswerte) Personendaten.[282] Das BJ muss als «Inhaber der Datensammlung,» im Sinne des aDSG (d. h. als «Verantwortlicher» in der Terminologie des DSG) bezeichnet werden.

412 Wie oben ausgeführt, bestand unserer Auffassung nach keine Notwendigkeit, die in den betreffenden Unterlagen enthaltenen Informationen an Xplain, d. h. einen externen Anbieter, oder an den ebenfalls kopierten externen Berater im Zusammenhang mit der Datenmigration vom PAGIRUS-System an TROVA weiterzugeben.

413 Auf der Grundlage der uns vorliegenden Informationen folgern wir, dass die Rolle von Xplain auf eine unterstützende Funktion im Zusammenhang mit der Migration durch das BJ beschränkt war. In diesem Sinne kann Xplain nicht als Auftragsbearbeiter für diese Leistung bezeichnet werden.

414 Unserer Auffassung nach könnte der Versand dieser Dateien per E-Mail an den Mitarbeiter von Xplain an seine Adresse [T]@xplain.ch somit eine unzulässige Verarbeitung im Sinne von Artikel 7 aDSG darstellen,

[281] AS 2016 3445. Der Inhalt von Art. 26a aBinfV, der von Art. 11 VDTI übernommen wurde, legte die Bedingungen fest, unter denen externe IKT-Leistungserbringer Zugang zu Daten erhalten können, die nicht öffentlich zugänglich sind, nämlich: (i) Es ist zur Erbringung der Leistung erforderlich; (ii) die für die Daten verantwortliche Behörde hat schriftlich zugestimmt und (iii) es wurden angemessene vertragliche, organisatorische und technische Vorkehrungen getroffen, um eine weitere Verbreitung der Daten zu verhindern. Vgl. auch: Pressemitteilung des Bundesrates vom 30. September 2016 «Bundesrat minimiert die Datenweitergabe an externe IKT-Dienstleister beim Bau und Betrieb von Informationssystemen».

[282] Personendaten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen (Art. 3 Bst. c Ziff. 4 aDSG; Art. 5 Bst. c Ziff. 5 DSG).

die *prima facie* gegen Artikel 12 Absatz 2 Buchstabe a aDSG in seiner Fassung vom Januar 2016 verstösst. Keiner der Rechtfertigungsgründe von Artikel 13 aDSG scheint uns in diesem Fall gegeben zu sein.[283]

415 Was Artikel 7 VBNIB betrifft, dessen Inhalt sich seit seinem Inkrafttreten im Jahr 2012 nicht geändert hat, und sofern er anwendbar ist (er trägt den Titel: «Bearbeitung bei technischen Arbeiten»), gestattet er eine Bearbeitung im Zusammenhang mit technischen Arbeiten nur, wenn dies für die Ausführung dieser Arbeiten *erforderlich* ist (Art. 7 Abs. 1 VBNIB). Wie bereits erwähnt, ist die Übermittlung der in den betreffenden Anhängen enthaltenen (besonders schützenswerten) Personendaten an Xplain in diesem Fall nicht erforderlich. Daher könnte auch diese Bestimmung verletzt worden sein.

(iv) *Technische, organisatorische oder prozesshafte Mängel*

416 Es muss nun untersucht werden, welche Verwaltungsverordnungen in diesem Fall relevant sind und ob es mögliche technische, organisatorische oder prozesshafte Mängel gibt.

417 OA identifizierte unter den bereitgestellten Dokumenten die folgende Verwaltungsverordnung, die zum Zeitpunkt des Sachverhalts (Januar 2016) galt: «*Weisung des EJPD über die Umsetzung des Datenschutzes und Informationssicherheit (DSIS-Weisung EJPD)*»[284] vom 12. Mai 2011 (in Kraft getreten am 1. Juni 2011). Sie verweist auf die geltenden Vorschriften über Datenschutz, Informationssicherheit und Informationsschutz (Ziff. 13–16). Ausserdem sieht sie unter Ziffer 22 «Kontrolle und Berichterstattung» Folgendes vor: «*Die Umsetzung von DSIS wird auf der Stufe Departement und in den Verwaltungseinheiten regelmässig kontrolliert, damit Mängel rechtzeitig erkannt und durch geeignete Massnahmen behoben werden können.*»;

418 Aus diesem Text lässt sich ableiten, dass der Zugang zu Personendaten an Bedingungen geknüpft ist, die regelmässig kontrolliert werden müssen. Diese Texte übernehmen somit teilweise den Inhalt der oben erwähnten Datenschutzbestimmungen (Art. 7 Abs. 1 aDSG), insbesondere die Anforderung, Vorkehrungen zu treffen, um eine weitere Verbreitung der Daten zu verhindern.

419 Zwecks Vermeidung von Wiederholungen kann *mutatis mutandis* auf die Analyse der technischen, organisatorischen oder prozesshaften Mängel verwiesen werden, die im ersten Fall oben vorgenommen wurde.

f) «Aktiver Transfer»-Fall Nr. 2: eine Excel-Tabelle mit 156 Patrouillen der Militärpolizei (30. Juli 2020).

(i) *Besondere auf das JORASYS anwendbare Vorschriften*

420 Das Journal- und Rapportsystem der Militärpolizei (JORASYS) basierte zum Zeitpunkt der Ereignisse – und auch heute noch – auf den Artikeln 167a ff. des Bundesgesetzes vom 3. Oktober 2008 über militärische und andere Informationssysteme im VBS (MIG).[285]

421 Das JORASYS dient zur Erfüllung der Aufgaben nach Artikel 100 Absatz 1 MG, insbesondere: a) der Journalführung der Einsatzzentralen des Kommandos Militärpolizei; b) der Rapportierung kriminal- und

[283] Als das BJ die Unterstützung dieses externen Anbieters in Anspruch nahm, «handelte es privatrechtlich» im Sinne von Art. 23 aDSG (Art. 40 DSG). Das BJ unterlag daher den für Privatpersonen geltenden Bestimmungen des aDSG und nicht den für Bundesorgane geltenden Bestimmungen. Folglich ist die Anforderung einer gesetzlichen Grundlage hier nicht anwendbar (Art. 17 Abs. 1 aDSG für Bundesorgane).
[284] AUD B03.04.10.1185-1194.
[285] SR 510.91.

sicherheitspolizeilicher Aufgaben der Berufsformationen des Kommandos Militärpolizei; c) der Beurteilung der militärischen Sicherheitslage; d) dem Eigenschutz der Armee (Art. 167b MIG).

422 Das JORASYS umfasst Daten über Personen, die dem Militärstrafrecht unterliegen, und über Dritte, die mit Vorfällen im Zusammenhang mit der Armee oder mit Angehörigen der Armee verbunden sind (Art. 167c MIG). Die Bereitstellung von Daten wird durch Artikel 167e MIG geregelt, in dem eine Liste von Personen und Stellen aufgeführt ist, die berechtigt sind, Zugang zu den Daten im JORASYS oder Auszüge daraus zu erhalten.

423 Personen, die für die Wartung, Verwaltung und Programmierung zuständig sind, dürfen Daten nur dann verarbeiten, wenn sie für die Erfüllung ihrer jeweiligen Aufgaben absolut notwendig sind und die Datensicherheit gewährleistet ist. Dabei dürfen keine Daten verändert werden (Art. 7 Abs. 2 MIG).

424 Im vorliegenden Fall enthält die Excel-Datei «[redacted].*xls*»[286] offensichtlich Daten über Personen, die dem Militärstrafrecht unterstellt sind. Diese Daten stammen aus dem JORASYS oder sind höchstwahrscheinlich dazu bestimmt, in dieses System eingefügt zu werden. Der Versand dieser Datei per E-Mail an den Mitarbeiter von Xplain über seine Adresse [U]@xplain.ch sowie an die Support-Adresse von Xplain (support@xplain.ch) stellt eine Weitergabe von Daten dar, die nicht mit Artikel 167e MIG vereinbar zu sein scheint. Im Rahmen der Untersuchung konnte nicht festgestellt werden, welche natürlichen Personen zum Zeitpunkt des Vorfalls die an support@xplain.ch gerichteten E-Mails erhielten.

425 Zudem scheint es, dass der Mitarbeiter der Militärpolizei die betreffende Operation alleine durchführen konnte (Hinzufügen von 156 Patrouillen im JORASYS). Wenn er sich an die FUB wandte, geschah dies offenbar, um Zeit zu gewinnen.

426 Bei der Hotline der FUB wurde ein *Incident* eröffnet, doch dies scheint rein formell erfolgt zu sein. Die FUB leitete den Fall umgehend an Xplain weiter, ohne jedoch weitere Schritte zu unternehmen.

427 Unserer Auffassung nach war die Weiterleitung an Xplain durch die FUB daher nicht mit dem MIG vereinbar.

(ii) *Informationssicherheit*

428 Artikel 26*a* aBinfV, der am 1. November 2016[287] in Kraft trat und dessen Inhalt von Artikel 11 VDTI übernommen wurde, legte die Bedingungen fest, unter denen externe IKT-Leistungserbringer Zugang zu Daten erhalten können, die nicht öffentlich zugänglich sind: (i) Es ist zur Erbringung der Leistung erforderlich; (ii) die für die Daten verantwortliche Behörde hat schriftlich zugestimmt und (iii) es wurden angemessene vertragliche, organisatorische und technische Vorkehrungen getroffen, um eine weitere Verbreitung der Daten zu verhindern.

429 Die in der betreffenden Excel-Datei enthaltenen Daten beziehen sich auf Patrouillen der Militärpolizei, die der Öffentlichkeit nicht zugänglich sind. Der Zugang zu diesen Daten durch Xplain als externer Anbieter setzte daher voraus, dass die Bedingungen von Artikel 26*a* aBinfV erfüllt sind.

430 Angesichts der oben genannten Umstände halten wir fest, dass der Versand der Daten per E-Mail durch den Mitarbeiter der FUB an den Mitarbeiter von Xplain nicht notwendig im Sinne von Artikel 26*a* aBinfV war. Es scheint nämlich, dass die Militärpolizei die betreffende Operation (Hinzufügen von 156 Patrouillen im JORASYS) allein hätte durchführen können, doch die Operation wurde von der FUB an

[286] AUD B03.10.05.01.
[287] AS 2016 3445.

Xplain delegiert, nachdem der Mitarbeiter bei der Militärpolizei angegeben hatte, dass die Operation für ihn sehr zeitaufwendig sei.

431 Es muss deshalb nicht untersucht werden, ob die verantwortliche Behörde ihre schriftliche Zustimmung zum Zugang durch Xplain gegeben hatte oder ob Massnahmen ergriffen wurden, um den Zugang Dritter zu den an Xplain übermittelten Daten zu verhindern.

432 Zusammenfassend lässt sich sagen, dass unserer Auffassung nach der Versand der betroffenen Datei per E-Mail an Xplain nicht mit der zum Zeitpunkt des Vorfalls geltenden aBinfV vereinbar zu sein scheint.

(iii) *Klassifizierung der Informationen*

433 Gemäss der vom VBS übernommenen Klassifizierung fallen die im JORASYS enthaltenen Informationen unter die Stufe «VERTRAULICH» im Sinne von Artikel 6 aISchV in der Fassung vom Juli 2020.[288]

434 In Artikel 13 Absätze 1 und 2 aISchV in der Fassung vom Juli 2020 heisst es: «*Die Erstellung, die Bekanntgabe und das Zugänglichmachen klassifizierter Informationen sind auf ein Minimum zu beschränken; dabei sind Lage, Auftrag, Zweck und Zeit zu berücksichtigen. Klassifizierte Informationen dürfen nur jenen Personen bekannt gegeben oder zugänglich gemacht werden, die davon Kenntnis haben müssen*.»

435 Wie oben ausgeführt, bestand unserer Auffassung nach in diesem Zusammenhang keine Notwendigkeit, die in der fraglichen Excel-Datei enthaltenen Informationen an Xplain, d. h. einen externen Anbieter, weiterzugeben.

436 Daher scheint der Versand der Datei per E-Mail an einen Mitarbeiter von Xplain nicht mit der zum Zeitpunkt des Vorfalls geltenden aISchV vereinbar zu sein.

437 Die Tatsache, dass die Excel-Datei nicht mit dem Vermerk «VERTRAULICH» versehen war, scheint zudem nicht mit den Anforderungen der aISchV vereinbar zu sein.

(iv) *Datenschutz*

438 Da das MIG keine spezifischen Bestimmungen enthielt, fand das aDSG und findet nun das DSG auf das JORASYS der Militärpolizei (Art. 1 Abs. 3 MIG) Anwendung.

439 Die Excel-Datei «[redacted]*.xls*» enthält offensichtlich Personendaten. Die Militärpolizei muss als «Inhaber der Datensammlung» im Sinne des aDSG (d. h. als «Verantwortlicher» in der Terminologie des DSG) bezeichnet werden.

440 Wie oben ausgeführt, bestand unserer Auffassung nach in diesem Zusammenhang keine Notwendigkeit, die in der fraglichen Excel-Datei enthaltenen Informationen an Xplain, d. h. einen externen Anbieter, weiterzugeben.

441 Xplain führte *de facto* eine Verarbeitung von Personendaten auf Anweisung der FUB durch. Xplain erhielt nämlich eine Excel-Datei mit persönlichen Daten und erstellte ein Skript im .sql-Format, in das Xplain die gleichen persönlichen Daten einfügte ([redacted].sql»)[289].

[288] Vgl. [redacted] pdf (AUD 03.10.09.223).
[289] AUD B03.10.05.03.

442 Wie die Untersuchung zeigte, war in den Verträgen für das JORASYS die Auftragsbearbeitung durch Xplain nicht vorgesehen, geschweige denn geregelt. Die zentrale Anforderung von Artikel 10a aDSG scheint somit nicht erfüllt zu sein.[290]

443 Artikel 2*a*[bis] MIV (Verordnung über militärische und andere Informationssysteme im VBS), der auch die Auftragsbearbeitung regelt, ist erst am 1. April 2023[291] in Kraft getreten, d. h. nach den hier behandelten Ereignissen.

444 Da die FUB diese Auftragsbearbeitung nicht vertraglich geregelt hat, hatte es erst recht keine Möglichkeit, den Ort der Bearbeitung und den möglichen Einsatz von Unterauftragsbearbeitern zu überblicken (Xplain hat Büros im Ausland, die von Tochtergesellschaften in Spanien und Deutschland betrieben werden).[292]

445 Letztendlich handelt es sich in diesem Fall *prima facie* um eine unzulässige Verarbeitung im Sinne von Artikel 7 aDSG, die gegen Artikel 12 Absatz 2 Buchstabe a aDSG in seiner Fassung vom September 2010 verstösst. Keiner der Rechtfertigungsgründe von Artikel 13 aDSG scheint uns in diesem Fall gegeben zu sein.[293]

446 Was Artikel 7 VBNIB betrifft, dessen Inhalt sich seit seinem Inkrafttreten im Jahr 2012 nicht geändert hat, und sofern er anwendbar ist (er trägt den Titel: «Bearbeitung bei technischen Arbeiten»), gestattet er eine Bearbeitung im Zusammenhang mit technischen Arbeiten nur, wenn dies für die Ausführung dieser Arbeiten *erforderlich* ist (Art. 7 Abs. 1 VBNIB). Wie bereits erwähnt, war die Übermittlung dieser Excel-Datei an Xplain in diesem Fall nicht erforderlich. Daher könnte auch diese Bestimmung verletzt worden sein.

(v) *Technische, organisatorische oder prozesshafte Mängel*

447 Es muss nun untersucht werden, welche Verwaltungsverordnungen in diesem Fall relevant sind und ob es mögliche technische, organisatorische oder prozesshafte Mängel gibt.

448 Unter den vorgelegten Texten identifizierte OA das «*Handbuch IT-Sicherheit VBS*»[294] vom 12. Juli 2011 (Version 3.2). Das 104 Seiten umfassende Dokument enthält zahlreiche Vorschriften, darunter auch zur Organisation der IT-Sicherheit. Insbesondere enthält es einen Abschnitt 6.2.2 über «*Sicherheits-Anforderungen in Aufträgen mit Fremd-Unternehmen (BSE)*». Gemäss Abschnitt 10.7.3.1 muss die Klassifizierung sicher sein («*Sämtliche Daten müssen entsprechend ihrem Schutzbedarf ‹sicher› abgelegt*»). Ferner beschränkt Abschnitt 10.7.4.1. den Zugang zu den Dokumenten des Systems («*System-Dokumentationen dürfen nur Berechtigten zugänglich sein*.»).

449 Zwecks Vermeidung von Wiederholungen kann *mutatis mutandis* auf die Analyse der technischen, organisatorischen oder prozesshaften Mängel verwiesen werden, die im ersten Fall oben vorgenommen wurde.

---

[290] Zur Frage der drei *curae* siehe unten Rz. 499 ff.
[291] AS 2023 133.
[292] Vgl. Rz. 214–217 oben.
[293] Als die FUB die Unterstützung dieses externen Anbieters in Anspruch nahm, «handelte sie privatrechtlich» im Sinne von Artikel 23 aDSG (Art. 40 DSG). Die FUB unterlag daher den für Privatpersonen geltenden Bestimmungen des aDSG und nicht den für Bundesorgane geltenden Bestimmungen. Folglich ist die Anforderung einer gesetzlichen Grundlage hier nicht anwendbar (Art. 17 Abs. 1 aDSG für Bundesorgane).
[294] AUD B03.05.39.

g) «Aktiver Transfer»-Fall Nr. 3: Screenshot eines Ausschnitts einer Anhörung (12. Januar 2018).

450 Die oben aufgeführte Analyse (Buchstabe a) trifft grösstenteils auf den vorliegenden Fall zu. Im Wesentlichen geht es darum, dass ein Mitarbeiter von fedpol (F) am 12. Januar 2018 von seiner Adresse [F]@fedpol.admin.ch aus eine unverschlüsselte E-Mail mit der Bezeichnung «*WG:* [redacted] *(*» an einen Mitarbeiter von Xplain (T) an dessen Adresse [T]@xplain.ch gesendet hat.

451 F informiert T in dieser E-Mail über Probleme bei der Darstellung von Dokumenten, die in ORMA erstellt wurden, und bittet ihn um Unterstützung[295]. Seine E-Mail enthält einen Screenshot des Protokolls einer Anhörung, die offenbar von fedpol durchgeführt wurde. Der Vor- und Nachname der angehörten Person war ebenso zu sehen wie ihre Aussagen (jedoch nicht wörtlich).

452 Zusammenfassend lässt sich sagen, dass die für ORMA geltenden besonderen Vorschriften (insbesondere das BPI) sowie die Bestimmungen zur Informationssicherheit (aBinfV) und zur Klassifizierung von Informationen (aISchV) *prima facie* nicht eingehalten worden zu sein scheinen. Dasselbe gilt für die Datenschutzbestimmungen (aDSG).

453 Die Untersuchung der technischen, organisatorischen oder prozesshaften Mängel, die dazu beigetragen haben, dass dem Mitarbeiter von Xplain die fraglichen Dokumente unter Verletzung der in den vorherigen Abschnitten erörterten Vorschriften zugesandt wurden, wurde bereits weiter oben erläutert, weshalb an dieser Stelle darauf verwiesen wird.

h) «Aktiver Transfer»-Fall Nr. 4: ein im Rahmen einer Supportanfrage übermitteltes Video, in dem Namen/Adressen von Beschuldigten, Zeugen, Anwälten sowie Ermittlern in einem Strafverfahren enthüllt werden (12. Dezember 2014).

454 Die oben aufgeführte Analyse (Buchstabe a) trifft grösstenteils auf den vorliegenden Fall zu. Im Wesentlichen geht es darum, dass ein Mitarbeiter von fedpol (F) am 12. Dezember 2014 von seiner Adresse [F]@fedpol.admin aus eine unverschlüsselte E-Mail mit der Bezeichnung «*Fwd:* [redacted]» an S an dessen Adresse [S]@xplain.ch gesendet hat.

455 Die E-Mail enthielt einen Anhang mit dem Titel «[redacted]*.zip*». Diese komprimierte Datei (.zip) enthielt ihrerseits eine Datei mit der Bezeichnung «[redacted]*.MP4*».[296] Im Wesentlichen handelte es sich um eine 71 Sekunden lange Videoaufnahme, die eine «*Windows-Remoteunterstützung*» wiedergibt, die einem fedpol-Ermittler gewährt worden war. Das Protokoll einer Zeugenbefragung, die von der Bundesanwaltschaft im Rahmen eines Strafverfahrens an fedpol delegiert wurde, ist auf dem Bildschirm zu sehen.

456 Zusammenfassend lässt sich sagen, dass die für ORMA geltenden besonderen Vorschriften (insbesondere das BPI) sowie die Bestimmungen zur Informationssicherheit (aBinfV) und zur Klassifizierung von Informationen (aISchV) *prima facie* nicht eingehalten worden zu sein scheinen. Dasselbe gilt für die Datenschutzbestimmungen (aDSG).

457 Die Untersuchung der technischen, organisatorischen oder prozesshaften Mängel, die dazu beigetragen haben, dass dem Mitarbeiter von Xplain die fraglichen Dokumente unter Verletzung der in den vorherigen

[295] AUD 03.10.02.26-31
[296] AUD B03.10.02.09.

Abschnitten erörterten Vorschriften zugesandt wurden, wurde bereits weiter oben erläutert, weshalb an dieser Stelle darauf verwiesen wird.

i) «Halbautomatischer Transfer»-Fall: die Funktion «Error-Reporting»

458 Die oben beschriebene Analyse gilt im Wesentlichen für die sogenannte Error-Reporting-Funktion.

459 Der oben ausgewählte Fall zur Veranschaulichung dieser Funktion stammt vom 24. Oktober 2016. An diesem Tag stellte M (ein Mitarbeiter des BAZG) Y (einem Mitarbeiter von Xplain, dessen automatische Signatur in der E-Mail-Fusszeile darauf hindeutet, dass er in Deutschland arbeitete) eine .zip-Datei auf dem Server T:EFD\EZV\GWK ZEMIS des Bundes zur Verfügung.

460 Diese komprimierte Datei ist etwa 21 MB gross. Sie enthält Screenshots von Ausweisdokumenten von Personen. Im Wesentlichen sind Name, Vorname, Nationalität und in einem Fall das Passfoto der betreffenden Personen zu sehen.

461 Zusammenfassend lässt sich sagen, dass die für die ZEMIS (Verordnung über das Zentrale Migrationsinformationssystem [ZEMIS-Verordnung][297]) geltenden besonderen Vorschriften sowie die Bestimmungen zur Informationssicherheit (aBinfV) und zur Klassifizierung von Informationen (aISchV) *prima facie* nicht eingehalten worden zu sein scheinen. Dasselbe gilt für die Datenschutzbestimmungen (aDSG).

462 Die Untersuchung der technischen, organisatorischen oder prozesshaften Mängel, die dazu beigetragen haben, dass dem Mitarbeiter von Xplain die fraglichen Dokumente unter Verletzung der in den vorherigen Abschnitten erörterten Vorschriften zugesandt wurden, wurde bereits weiter oben erläutert, weshalb an dieser Stelle darauf verwiesen wird.

B. Hat der Bund seine Pflichten in Bezug auf die Auswahl, Instruktion, Überwachung und Zusammenarbeit mit der Xplain AG erfüllt?

463 Die Fragestellung basiert auf der Prämisse, dass der Bund bei der Auswahl, Instruktion und Überwachung eines externen Dienstleisters oder Lieferanten sowie bei der Zusammenarbeit mit diesem bestimmte Aufgaben wahrnehmen muss.

464 In einem ersten Schritt (Ziff. 1) geht es daher darum, die Gültigkeit dieser Prämisse zu prüfen, bevor wir uns zum vorliegenden Fall äussern (Ziff. 2).

1. Relevante Rechtsnormen

465 Der vorliegende Abschnitt soll einen Überblick über die Rechtsquellen geben, welche die Pflichten der Bundesverwaltung in Bezug auf die Auswahl, Instruktion, Überwachung sowie im Bereich der Zusammenarbeit mit einem externen Dienstleister oder Lieferanten begründen können. Wir behandeln zunächst die Vorschriften des allgemeinen Verwaltungsrechts (*a*), bevor wir uns den speziellen Vorschriften zuwenden (*b*).

[297] SR 142.513.

a) Allgemeines Verwaltungsrecht

(i) *Einführung*

466 Die Komplexität, Fragmentierung und vielfältigen Formen der heutigen Verwaltungsorganisation in der Schweiz machen die Klassifizierung von Verwaltungseinheiten besonders schwierig. In einem Teil der Rechtslehre erfolgt eine dreiteilige Klassifizierung (Zentralverwaltung, dezentralisierte Verwaltung [nur aus Einrichtungen des öffentlichen Rechts bestehend] und Privatpersonen, die mit öffentlichen Aufgaben betraut sind). In einem anderen Teil wird eine zweiteilige Klassifizierung bevorzugt (zentrale und dezentrale Verwaltung, die alle Einrichtungen – unabhängig von ihrer Form und Rechtsnatur – umfasst, die nicht zur zentralen Verwaltung gehören und mit öffentlichen Aufgaben betraut sind).[298]

467 Abgrenzungsfragen stellen sich insbesondere dann, wenn Körperschaften Aufgaben an Personen ausserhalb der Verwaltung vergeben.[299] In diesem Kontext werden insbesondere die Begriffe *Delegation staatlicher Aufgaben* und *administrative Hilfstätigkeiten* unterschieden.

(ii) *Delegation staatlicher Aufgaben und administrative Hilfstätigkeiten*

468 Laut Bundesverfassung kann das Gesetz Verwaltungsaufgaben auf Einrichtungen und Personen des öffentlichen oder privaten Rechts übertragen, die ausserhalb der Bundesverwaltung stehen (Art. 178 Abs. 3 BV). Ein Delegierter ist somit eine Person, die eine *staatliche Aufgabe* auf der Grundlage einer Kompetenzübertragung ausführt.[300]

469 Die Bereitstellung von Gütern oder Dienstleistungen, deren Produktion an sich keine staatliche Aufgabe[301] (d. h. eine Aufgabe der Verwaltung) darstellt, die aber für die Erfüllung solcher Aufgaben erforderlich sind, fällt hingegen unter den Begriff der «*Hilfstätigkeit*» bzw. der «*Bedarfsverwaltung*». Anstatt diese Güter oder Leistungen durch eigene Dienste zu beschaffen, kann die Verwaltung dabei auf Dritte zurückgreifen. Häufig wird von «*Outsourcing*» gesprochen, manchmal auch von Auftragsbearbeitung.[302]

470 Die Unterscheidung zwischen *staatlichen Aufgaben* und *administrativer Hilfstätigkeit* hat insbesondere zur Folge, dass die Bedingungen für die Delegation im ersten Fall gelten (Erfordernis einer gesetzlichen [Art. 178 Abs. 3 BV][303] oder sogar verfassungsrechtlichen Grundlage, öffentliches Interesse, Einhaltung

[298] Thierry Tanquerel, Manuel de droit administratif, 2. Ausgabe, 2018, Rz. 114 und 115a und Verweise.
[299] Thierry Tanquerel, Manuel de droit administratif, 2. Ausgabe, 2018, Rz. 115.
[300] Michael Montavon, Cyberadministration et protection des données, Fribourg 2021, S. 768 f.
[301] Das Konzept der staatlichen Aufgaben ist nicht einheitlich. Es kann jedoch festgehalten werden, dass nach dem Bundesgericht staatliche Aufgaben durch die Verfassung und die Gesetze bestimmt werden und auf einer politischen Entscheidung beruhen (BGE 138 II 134 E. 4.3.1; vgl. ebenfalls Blaise Knapp, L'exécution des tâches publiques fédérales par des tiers, in SBVR Vol. I, 1996, Rz. 3 ff). Einige Autorinnen und Autoren der Rechtslehre schlagen ihrerseits eine umfassendere Definition vor: Zu den staatlichen Aufgaben, bei denen sich die Frage der Auslagerung *a priori* stellen kann, gehören zunächst die Aufgaben, die per Definition ursprünglich nur dem Staat obliegen können: Dies sind alle Aufgaben, die die Ausübung der öffentlichen Gewalt beinhalten. Hinzu kommen alle materiellen Aufgaben, für die der Staat im Rahmen der Verfassung, eines Gesetzes oder einer Verfügung einer öffentlichen Körperschaft oder einer dezentralisierten Einheit im Rahmen eines gesetzlich festgelegten Ermessensspielraums verantwortlich ist. Dies gilt auch für Tätigkeiten, die vom Staat im Rahmen eines Monopols ausgeübt oder vergeben werden, sofern die Auslagerung nicht dazu führt, dass die Tätigkeiten nicht mehr als öffentliches Interesse gelten (Pierre Moor/François Bellanger/Thierry Tanquerel, Droit administratif, Vol. III, 2. Ausgabe, 2018, S. 140).
[302] Pierre Moor/ François Bellanger/Thierry Tanquerel, Droit administratif, Vol. III, 2. Ausgabe, 2018, S. 141 und S. 244 f.
[303] Michael Montavon, Cyberadministration et protection des données, Fribourg 2021, S. 252.

des Spezialitätsvorbehalts und Einrichtung von Aufsichtsbefugnissen [Verpflichtung zur Achtung der Grundrechte gemäss Art. 35 Abs. 2 BV, Art. 187 Abs. 1 a BV])[304], nicht aber im zweiten Fall.

471 Tätigkeiten zur Unterstützung der Verwaltung wie die Beschaffung von Gütern und Dienstleistungen (z. B. Instandhaltung von Büros, Bau von Gebäuden oder Finanzdienstleistungen) fallen gemäss der Rechtslehre unter das Privatrecht.[305]

472 Die Rechtslehre liefert weitere Beispiele für administrative Hilfstätigkeiten: Die Lieferung von Trams, Bussen, Computern, medizinischen Geräten, Büromaterial fällt unter administrative Hilfstätigkeiten, ebenso wie die Bereitstellung von IT- oder Rechtsdienstleistungen oder Bau- oder Wartungsarbeiten (einschliesslich Reinigungsarbeiten) an öffentlichen Infrastrukturen oder Gebäuden. Die Herstellung von Computern oder der Bau von Gebäuden sind daher keine staatlichen Aufgaben, sondern wirtschaftliche Tätigkeiten, welche vom Privatsektor ausgeübt werden und von der Verwaltung zur Erfüllung ihrer Aufgaben benötigt werden. Ein IT-Experte ist ein privater Hilfsdienstleister, der mit der Behebung eines Softwarefehlers in einem von der Verwaltung verwendeten Programm beauftragt ist. Es handelt sich hierbei um administrative Hilfstätigkeiten, welche die Verwaltung ebenso gut durch ihr eigenes Personal hätte ausführen können. Sie entschied sich jedoch dafür, diese auf dem Markt in Anspruch zu nehmen, da sie der Meinung war, dass sie dort auf zufriedenstellende Weise erbracht wird.[306] Ein anderer Autor argumentiert ebenfalls, dass IT-Dienstleistungen von vornherein eine «*Bedarfsverwaltung*» darstellen.[307]

473 Ein Autor hat jedoch kürzlich argumentiert, dass die zunehmende Komplexität dieser Dienstleistungen, die immer wichtigere und strategischere Rolle, die sie für die Funktionsweise und Organisation des Staates spielen, und die damit verbundenen neuen Risiken diese Qualifikation heute zumindest teilweise in Frage stellen. Nach Auffassung dieses Autors geht die Bereitstellung von IT-Dienstleistungen in einigen Fällen über den Rahmen einer Hilfstätigkeit hinaus und kann der Delegation einer echten staatlichen Aufgabe entsprechen, welche die Einhaltung der oben genannten Bedingungen voraussetzt (Erfordernis einer gesetzlichen Grundlage ([Art. 178 Abs. 3 BV]) und die Verpflichtung der Dienstleister, selbst die Grundrechte der betroffenen Personen zu respektieren [vgl. Art. 35 Abs. 2 BV])[308].

(iii) *Administrative Hilfstätigkeiten, die im Prinzip dem Privatrecht unterliegen*

474 Grundsätzlich kann die Auftragsbearbeitung durch ein Bundesorgan auf einem Vertrag basieren; wenn es sich um administrative Hilfstätigkeiten handelt, gelten die Regeln des öffentlichen Beschaffungswesens für die Entstehung der Vertragsbeziehung, während die Beziehung zwischen der Körperschaft und dem privaten Unternehmen, das die Leistungen erbringt, durch das Privatrecht geregelt wird.[309]

475 Das Gesetz erlegt dem Auftragsbearbeiter jedoch bestimmte Pflichten auf, die in der Regel im Vertrag übernommen und präzisiert werden. Hinsichtlich des Schutzes von Personendaten ist der Auftragsbearbeiter verpflichtet, die geeigneten organisatorischen und technischen Massnahmen gemäss Artikel 8 DSG zu ergreifen. Zudem darf er nicht vom festgelegten gesetzlichen Rahmen abweichen und Daten verarbeiten, die das öffentliche Organ nicht selbst verarbeiten darf (vgl. Art. 9 Abs. 1 Bst. a DSG).[310]

---

[304] Pierre Moor/François Bellanger/Thierry Tanquerel, Droit administratif, Vol. III, 2. Ausgabe, 2018, S. 208, S. 210 und S. 245 f.
[305] Téo Genecand, in Benhamou/Cottier (Hrsg.), Petit commentaire LPD, 2023, Rz. 4 ad Art. 40 DSG.
[306] Pierre Moor/François Bellanger/Thierry Tanquerel, Droit administratif, Vol. III, 2. Ausgabe, 2018, S. 141 und S. 245 f.
[307] Rolf H. Weber, Outsourcing von Informatik-Dienstleistungen in der Verwaltung, ZBl 100/1999, S. 97, 102 und 107.
[308] Michael Montavon, Cyberadministration et protection des données, Fribourg 2021, S. 768 f.
[309] Pierre Moor/François Bellanger/Thierry Tanquerel, Droit administratif, Vol. III, 2. Ausgabe, 2018, S. 141 f. und 245.
[310] Michael Montavon, Cyberadministration et protection des données, Fribourg 2021, S. 250.

476 Im IT-Bereich erfolgt die Vertragsqualifizierung anhand der Umstände des Einzelfalls. Verträge über IT-Dienstleistungen sind häufig sogenannte Innominatverträge oder gemischte Verträge. Je nach den Umständen können sie einem Mandatsvertrag, einem Werkvertrag, einem Lizenzvertrag oder sogar einem Kauf- oder Mietvertrag ähneln.[311]

b) Relevante spezielle Vorschriften

477 Unsere untenstehende Analyse (Ziff. 2) berücksichtigt die Vorschriften, die zum Zeitpunkt des Sachverhalts gültig waren und die in aDSG, aISchV, aBinfV, aCyRV und VDTI enthalten sind (siehe die allgemeine Tabelle oben unter Rz. 256).

(i) *Pflicht zur sorgfältigen Auswahl*

478 Die aus Artikel 14 und später 10a aDSG resultierende Pflicht zur sorgfältigen Auswahl des Auftragsbearbeiters (auch «*Processor*» genannt), der Personendaten verarbeitet, wurde weiter oben erörtert, weshalb hier darauf verwiesen wird.[312]

479 Gemäss Artikel 8 aBinfV (in Kraft von 2003 bis 2012), dann Artikel 10 aBinfV (in Kraft von 2012 bis 2021), dann Artikel 14 Absatz 2 aCyRV (in Kraft im Jahr 2020) und schliesslich Artikel 14 Absatz 3 Buchstabe a aCyRV (in Kraft von 2021 bis 2023) sind die Verwaltungseinheiten für die Sicherheit ihrer Informatikschutzobjekte verantwortlich.[313] Sie führen ein Inventar ihrer Informatikschutzobjekte und ergreifen die notwendigen Sicherheitsmassnahmen.

480 Gemäss Artikel 24 Absatz 3 aBinfV («Bezug von IKT-Leistungen bei externen Leistungserbringern»), in Kraft von 2003 bis 2012, wählen die Auftraggeber die Variante mit dem günstigsten Kosten-Nutzen-Risiken-Verhältnis.

481 Gemäss Artikel 26a aBinfV (in Kraft von 2016 bis 2021) und Artikel 11 VDTI (in Kraft seit 2021) können externe IKT-Leistungserbringer Zugang zu Daten erhalten, die nicht öffentlich zugänglich sind, sofern die folgenden Bedingungen erfüllt sind: (a) Es ist zur Erbringung der Leistung erforderlich; b) die für die Daten verantwortliche Behörde hat schriftlich zugestimmt; c) es wurden angemessene vertragliche, organisatorische und technische Vorkehrungen getroffen, um eine weitere Verbreitung der Daten zu verhindern. Daraus ergibt sich unserer Auffassung nach die Pflicht, den jeweiligen Anbieter sorgfältig auszuwählen.

(ii) *Pflicht zur angemessenen Instruktion*

482 Die aus den Artikeln 14 und 10a aDSG resultierende Pflicht zur angemessenen Instruktion des Auftragsbearbeiters, der Personendaten verarbeitet, wurde weiter oben erörtert, weshalb hierauf verwiesen wird.[314]

483 Artikel 8 aBinfV (in Kraft von 2003 bis 2012), Artikel 10 aBinfV (in Kraft von 2012 bis 2021), Artikel 26a aBinfV (in Kraft von 2016 bis 2021) und Artikel 11 VDTI (in Kraft seit 2021), aus denen unserer Auffassung nach eine Pflicht zur sorgfältigen Instruktion eines externen IKT-Leistungserbringers abgeleitet werden kann, wurden oben erläutert, weshalb auch hierauf verwiesen wird.[315]

---

[311] EMILIE JACOT-GUILLARMOD, in Benhamou/Cottier (Hrsg.), Kurzkommentar DSG, 2023, Rz. 9 ad Art. 9 DSG.
[312] Vgl. Rz. 292–300.
[313] Die Formulierung hat sich im Zuge der Überarbeitung der Verordnungen geändert und wir zitieren hier Art. 14 Abs. 3 Bst. a aCyRV, der am 1. April 2021 in Kraft trat.
[314] Vgl. Rz. 292–300.
[315] Vgl. Rz. 308**Fehler! Verweisquelle konnte nicht gefunden werden.**.

484 Gemäss Artikel 25 Absatz 2 aBinfV (in Kraft von 2012 bis 2021) sind bei dem Bezug von Leistungen bei einem externen Leistungserbringer die IKT-Vorgaben integraler Bestandteil der Ausschreibungsunterlagen.

485 Eine entsprechende Regel ergibt sich aus Artikel 14 Absatz 2 Buchstabe d aCyRV (in Kraft im Jahr 2020) bzw. Artikel 14 Absatz 3 Buchstabe d aCyRV (in Kraft von 2021 bis 2023), wonach die Verwaltungseinheiten sicherstellen müssen, dass beim Bezug von Leistungen bei einem externen Leistungserbringer die Informatiksicherheitsvorgaben Teil des Vertragsverhältnisses mit diesem sind.

(iii) *Überwachungspflicht*

486 Die aus Artikel 14 und 10a aDSG resultierende Pflicht zur Überwachung des Auftragsbearbeiters, der Personendaten verarbeitet, wurde weiter oben erörtert, weshalb hierauf verwiesen wird.[316]

487 Artikel 13 aBinfV (in Kraft von 2000 bis 2003) und später Artikel 26 aBinfV (in Kraft von 2003 bis 2012) gaben der Eidgenössischen Finanzkontrolle die Befugnis zur Durchführung von Informatikrevisionen.

488 Gemäss Artikel 25 Absatz 3 aBinfV (in Kraft von 2012 bis 2021) überprüft der Leistungsbezüger beim Bezug von Leistungen bei einem externen Leistungserbringer die Einhaltung der IKT-Vorgaben durch den externen Leistungserbringer in geeigneter Weise.

489 Eine entsprechende Regel ergibt sich aus Artikel 14 Absatz 2 Buchstabe e aCyRV (gültig im Jahr 2020) bzw. Artikel 14 Absatz 3 Buchstabe e aCyRV (gültig von 2021 bis 2023), wonach die Verwaltungseinheiten die Einhaltung der Informatiksicherheitsvorgaben durch die externen Leistungserbringer in geeigneter Weise überprüfen.

2. Im vorliegenden Fall

a) Fehlen allgemeiner Pflichten zur sorgfältigen Auswahl, Instruktion und Überwachung

490 Die vorliegende Untersuchung konzentriert sich auf die Beziehungen des Bundes zu einem privaten Akteur (Xplain). Es ist daher angebracht, die Frage der Dezentralisierung der Verwaltungstätigkeit und die sich daraus möglicherweise ergebenden Bedingungen, insbesondere im Hinblick auf die Überwachungspflicht, kurz zu erörtern.

491 Es wurde vorgebracht, dass der Bereich der Cybersicherheit als ein Bereich der Sicherheit im eigentlichen Sinne betrachtet werden sollte, der nicht oder nur unter sehr strengen Bedingungen an eine private Einrichtung[317] delegiert werden kann: Der Staat würde seine Garantenpflicht (insbesondere: Kontrolle der Ausführung der Aufgaben, staatliche Kontrolle der Einhaltung der Grundrechte) und die endgültige Verantwortung für die öffentliche Sicherheit übernehmen.[318] Unter dieser Annahme würden die von Xplain erbrachten Dienstleistungen strengen Kontrollpflichten unterliegen, was die Schlussfolgerungen der vorliegenden Untersuchung beeinflussen würde.

[316] Vgl. Rz. 292–300.

[317] Nach Auffassung von Autoren ist die Privatisierung ganzer Aufgaben im Bereich der öffentlichen Sicherheit aus verfassungsrechtlicher Sicht nicht zulässig (Michael Guery, La privatisation de la sécurité et ses limites juridiques, SJ 2006 II S. 141, 158 f.; Etienne Poltier, CR BV, Art. 81-SchlB, 2021, Rz. 48 ad Art. 178 BV; siehe auch Rolf H. Weber, Outsourcing von Informatik-Dienstleistungen in der Verwaltung, ZBl 100/1999, S. 97, 100, der jedoch eine Privatisierung nur in einigen Ausnahmefällen [z. B. bei Gewaltanwendung] für ausgeschlossen hält).

[318] Michael Guery, La privatisation de la sécurité et ses limites juridiques, SJ 2006 II S. 141, 158 f.

492 In Anbetracht dessen halten wir nach geltendem Recht fest, dass die mit Xplain vertraglich vereinbarten Aufgaben – insbesondere die Erstellung, Entwicklung oder Wartung von Software sowie der IT-Support – im Prinzip keine staatlichen Aufgaben, sondern administrative Hilfstätigkeiten darstellen. Die von Xplain erbrachten Dienstleistungen und die gelieferten Produkte (Software) müssen als *administrative Hilfstätigkeiten* im gleichen Sinne wie die oben genannten Beispiele aus der Rechtslehre qualifiziert werden[319]. Diese Dienstleistungen und Produkte stellen nämlich an sich keine staatliche Aufgabe dar, deren Delegation – die zudem notwendigerweise einer gesetzlichen Grundlage unterliegen würde – gemäss dem allgemeinen Verwaltungsrecht der Dezentralisierung der Verwaltungstätigkeit automatisch überwacht werden müsste.

493 Infolgedessen sind es die oben zitierten speziellen Vorschriften, welche die Pflichten der direkt betroffenen Einheiten in Bezug auf die Auswahl, die Instruktion und die Überwachung von Xplain begründeten.

b) Anwendung der speziellen Vorschriften

(i) *Wurde die Pflicht zur sorgfältigen Auswahl erfüllt?*

494 In Bezug auf die Informationssicherheit erliess der Informatikrat des Bundes (IRB) am 27. September 2004 Weisungen zur Konkretisierung der Anforderungen der aBinfV. Diese wurden durch die Weisungen des Bundesrates vom 14. August 2013, dann vom 1. Juli 2015 über die IKT-Sicherheit in der Bundesverwaltung und schliesslich durch die Weisungen des Bundesrates vom 16. Januar 2019 über die Informatiksicherheit in der Bundesverwaltung ersetzt.

495 Diese Weisungen sehen alle im Wesentlichen und nebst anderen Regeln vor, dass jedes IKT-Projekt einer «Schutzbedarfsanalyse» unterzogen werden muss. Wenn die Analyse einen hohen Schutzbedarf ergibt, muss ein ISDS-Konzept («Informationssicherheits- und Datenschutzkonzept») erstellt werden.

496 Auf der Grundlage der überprüften Dokumente und der Befragungen, die im Rahmen dieser Administrativuntersuchung durchgeführt wurden, scheint es, dass diese Anforderungen von den direkt betroffenen Einheiten bei jedem IKT-Projekt mit Xplain eingehalten wurden.

497 Unter Berücksichtigung von Artikel 24 Absatz 3 aBinfV (gültig von 2003 bis 2012) sowie Artikel 26a aBinfV (in Kraft von 2016 bis 2021) und Artikel 11 VDTI (in Kraft seit 2021) lässt sich jedoch festhalten, dass die direkt betroffenen Einheiten niemals einen Bericht über die Informationssicherheit bei Xplain angefordert oder gar erhalten haben, bevor sie Vertragsbeziehungen aufnahmen oder verlängerten. Erst nach dem Datenabfluss im Juni 2023 wurde Xplain einer vom Bund in Auftrag gegebenen Prüfung unterzogen, die von mehreren Befragten bestätigt wurde.

498 Das Untersuchungsorgan kommt daher zu dem Schluss, dass der Bund im Rahmen der Zusammenarbeit der direkt betroffenen Einheiten mit Xplain vor dem Datenabfluss im Juni 2023 seine Pflicht zur sorgfältigen Auswahl hinsichtlich der oben genannten Normen der Informationssicherheit teilweise erfüllt hat.

499 In Bezug auf den Schutz von Personendaten haben wir weiter oben einige Fälle (Nr. 4 «ORMA-Extraktion»[320] und Nr. 6 «JORASYS-Patrouillen»[321]) untersucht, in denen Xplain unserer Auffassung nach als Auftragsbearbeiter im Sinne des aDSG und des DSG zu qualifizieren ist. Wir haben ausserdem gesehen,

[319] Rz. 471–472.
[320] Vgl. Abschnitt IV.A.4 oben.
[321] Vgl. Abschnitt IV.A.6 oben.

dass diese Fälle von Auftragsbearbeitung unseres Wissens nicht Gegenstand eines Vertrags waren, entgegen der Anforderung der Artikel 14 und 10a aDSG, die zum Zeitpunkt des Geschehens galten.[322] Es muss daher *a fortiori* festgehalten werden, dass der Bund den Auftragsbearbeiter, der in den betreffenden Fällen mit der Bearbeitung von Personendaten beauftragt wurde, nicht sorgfältig ausgewählt hat.

500 Hinsichtlich des Schutzes von Personendaten kommt das Untersuchungsorgan daher zu dem Schluss, dass der Bund seiner Pflicht zur sorgfältigen Auswahl in den identifizierten Fällen der Auftragsbearbeitung nicht nachgekommen ist.

(ii) *Wurde die Pflicht zur angemessenen Instruktion erfüllt?*

501 Was die Informationssicherheit betrifft, enthalten die an OA übermittelten Verträge alle Verweise auf die Allgemeinen Geschäftsbedingungen des Bundes («AGB») im Informatikbereich, unabhängig davon, ob es sich um die AGB für Kauf und Wartung von Hardware, die AGB für die Beschaffung und die Pflege von Standardsoftware, die AGB für Werkverträge im Informatikbereich und für die Pflege von Individualsoftware, die AGB für Informatikdienstleistungen oder frühere Ausgaben dieser AGB handelt.

502 Die AGB, die im Oktober 2010 und im Januar 2021 veröffentlicht wurden, enthalten eine Verpflichtung zur «Geheimhaltung». Diese sieht insbesondere Folgendes vor:

> *Die Vertragspartner behandeln alle Tatsachen und Informationen vertraulich, die weder offenkundig noch allgemein zugänglich sind. Im Zweifelsfall sind Tatsachen und Informationen vertraulich zu behandeln. Die Parteien verpflichten sich, alle wirtschaftlich zumutbaren sowie technisch und organisatorisch möglichen Vorkehrungen zu treffen, damit vertrauliche Tatsachen und Informationen gegen den Zugang und die Kenntnisnahme durch Unbefugte wirksam geschützt sind. (…)*
>
> *Die Parteien überbinden die Geheimhaltungspflicht auf ihre Mitarbeitenden, Subunternehmer, Unterlieferanten sowie weitere beigezogene Dritte.*

503 Diese Klausel war nicht in den AGB enthalten, die von Juni 1998 bis Oktober 2010 galten.

504 Die im Oktober 2010 und Januar 2021 herausgegebenen AGB enthalten eine Generalklausel zum Datenschutz und zur Datensicherheit:

> *Die Parteien verpflichten sich, die Bestimmungen der schweizerischen Datenschutzgesetzgebung einzuhalten. Sie verpflichten sich, die wirtschaftlich zumutbaren Massnahmen sowie technisch und organisatorisch möglichen Vorkehrungen zu treffen, damit die im Rahmen der Vertragsabwicklung anfallenden Daten gegen unbefugte Kenntnisnahme Dritter geschützt sind.*
>
> *Personendaten dürfen nur für den Zweck und im Umfang, in dem dies für die Erfüllung und Durchführung des Vertrages erforderlich ist, bearbeitet werden. In diesem Umfang und zu diesem Zweck dürfen Personendaten auch an ein mit einer der Vertragsparteien verbundenes Unternehmen im In- oder Ausland weitergegeben werden, sofern die Voraussetzungen gemäss den Bestimmungen der schweizerischen Datenschutzgesetzgebung erfüllt sind.*
>
> *Die Parteien überbinden diese Pflichten auf ihre Mitarbeitenden, Subunternehmer, Unterlieferanten sowie weitere im Hinblick auf die Vertragserfüllung beigezogene Dritte.*

505 Diese Klausel war nicht in den AGB enthalten, die von Juni 1998 bis Oktober 2010 galten.

[322] Aktuell: Art. 9 DSG.

506 Ausserdem enthalten die AGB des Bundes im Informatikbereich keine Klausel über die Pflichten des externen Leistungserbringers in Bezug auf Cyber- oder Informationssicherheit.

507 Die Pflicht, die IKT-Vorgaben (die inzwischen Informatiksicherheitsvorgaben heissen) in die Ausschreibungsunterlagen (gemäss Art. 25 Abs. 2 aBinfV) bzw. in das Vertragsverhältnis (gemäss Art. 14 Abs. 2 Bst. d und später Art. 14 Abs. 3 Bst. d aCyRV) aufzunehmen, wurde teilweise gemäss den Verträgen, die uns von den betroffenen Einheiten zur Verfügung gestellt wurden, eingehalten.

508 Zahlreiche Verträge enthalten diese Vorgaben als Anhänge oder verweisen darauf. In einem Einzelfall wurde in einem Bearbeitungsreglement, das dem Vertrag beigefügt war, darauf verwiesen.[323] Bei der Untersuchung wurde jedoch festgestellt, dass Verträge diese Vorgaben nicht enthielten. Dies gilt insbesondere für fedpol, das diese Vorgaben offenbar nicht in die uns zur Verfügung gestellten Verträge aufgenommen hat, mit Ausnahme des oben genannten Vertrags, der über das Bearbeitungsreglement darauf verweist.[324]

509 Keiner der vor Juli 2020 abgeschlossenen Verträge, die uns vorgelegt wurden, enthält spezifische Klauseln zur Informationssicherheit.

510 Seit der Veröffentlichung der Mustervertragsklauseln der Beschaffungskonferenz des Bundes («BKB») für Cyberrisiken am 1. September 2020 wurde diese Klausel in mehrere, aber nicht in alle Verträge und Zusatzvereinbarungen mit Xplain aufgenommen, die uns von den von der Untersuchung betroffenen Einheiten zur Verfügung gestellt wurden:

	Verträge und Zusatzvereinbarungen[325] nach dem 1. September 2020	*davon mit der Mustervertragsklausel für Cyberrisiken*
EDA	0	*0*
armasuisse	0	*0*
FUB	0	*0*
MP	N/A	*N/A*
NDB	0	*0*
BAZG	3	*0*
BBL	0	*0*
BIT	0	*0*
fedpol	7	*6*
BJ	14	*2*
SEM	0	*0*
ISC-EJPD	0	*0*

511 Das Untersuchungsorgan kommt daher zu dem Schluss, dass der Bund im Rahmen der Zusammenarbeit der direkt betroffenen Einheiten mit Xplain vor dem Datenabfluss im Juni 2023 seine Pflicht zur

[323] Vertrag Nr. [redacted] für die Erbringung von werkvertraglichen Leistungen im Informatikbereich und die Pflege von Individualsoftware (Werkvertrag) (AUD B03.04.10.174).
[324] Vertrag Nr. [redacted] für die Erbringung von werkvertraglichen Leistungen im Informatikbereich und die Pflege von Individualsoftware (Werkvertrag) (AUD B03.04.10.174).
[325] Bestellungen wurden nicht berücksichtigt.

angemessenen Instruktion hinsichtlich der oben genannten Informationssicherheitsvorschriften teilweise erfüllt hat.

512 Hinsichtlich des Schutzes von Personendaten haben wir weiter oben einige Fälle (Nr. 3 «ORMA-Extraktion»[326] und Nr. 5 «JORASYS-Patrouillen»[327]) untersucht, in denen Xplain unserer Auffassung nach als Auftragsbearbeiter im Sinne des aDSG und des DSG zu qualifizieren ist. Wir haben ausserdem gesehen, dass diese Fälle von Auftragsbearbeitung unseres Wissens nicht Gegenstand eines Vertrags waren, entgegen der Anforderung der Artikel 14 und 10a aDSG, die zum Zeitpunkt des Geschehens galten.[328] Es muss daher *a fortiori* festgehalten werden, dass der Bund den Auftragsbearbeiter, der in den betreffenden Fällen mit der Bearbeitung von Personendaten beauftragt wurde, nicht angemessen instruiert hat.

513 Hinsichtlich des Schutzes von Personendaten kommt das Untersuchungsorgan daher zu dem Schluss, dass der Bund seiner Pflicht zur angemessenen Instruktion in den identifizierten Fällen der Auftragsbearbeitung nicht nachgekommen ist.

(iii) *Wurde die Überwachungspflicht erfüllt?*

514 Aus Sicht der Informationssicherheit wurde festgestellt, dass die direkt betroffenen Einheiten niemals einen Bericht über die Informationssicherheit bei Xplain angefordert oder gar erhalten haben.

515 Im Rahmen der Untersuchung wurde zudem im Zusammenhang mit Xplain keine BSE identifiziert.[329]

516 Ebenso konnte im Rahmen der Untersuchung nicht festgestellt werden, dass die direkt betroffenen Einheiten Massnahmen ergriffen hätten, die darauf abzielten, die Einhaltung der IKT-Vorgaben durch Xplain angemessen zu überprüfen (Art. 25 Abs. 3 aBinfV) bzw. angemessen zu überprüfen, ob die Informatiksicherheitsvorgaben von Xplain eingehalten wurden (Art. 14 Abs. 2 Bst. e aCyRV, später Art. 14 Abs. 3 Bst. e aCyRV).

517 Diese Vorgaben sahen insbesondere Folgendes vor: *«Die Leistungserbringer setzen die erforderlichen Sicherheitsmassnahmen beim Betrieb von IKT-Mitteln[330] um , dokumentieren und überprüfen sie. Sie bringen die Ergebnisse den betroffenen Leistungsbezügern in geeigneter Form zur Kenntnis».*

518 Im Rahmen der Untersuchung wurden auch keine Massnahmen der direkt betroffenen Einheiten festgestellt, um zu überprüfen, ob Xplain seinen Tochtergesellschaften in Spanien und Deutschland gemäss den im Oktober 2010 und Januar 2021 herausgegebenen AGB eine Geheimhaltungspflicht auferlegt hat. Die in mehreren Befragungen geäusserte Ansicht, dass die Geschäftsbeziehungen zwischen Xplain und seinen ausländischen Tochtergesellschaften für den Bund nicht relevant seien, kann nicht nachvollzogen werden.

519 Das Untersuchungsorgan kommt daher zu dem Schluss, dass der Bund im Rahmen der Zusammenarbeit der direkt betroffenen Einheiten mit Xplain vor dem Datenabfluss im Juni 2023 seine Überwachungspflicht hinsichtlich der oben genannten Informationssicherheitsvorschriften nicht erfüllt hat.

---

[326] Vgl. Abschnitt IV.A.3 oben.
[327] Vgl. Abschnitt IV.A.6 oben.
[328] Aktuell: Art. 9 DSG.
[329] Vgl. Rz. 359 oben.
[330] In den Richtlinien vom 16. Januar 2019 wird der Begriff «Informatikmittel» verwendet.

520 In Bezug auf den Schutz von Personendaten haben wir weiter oben einige Fälle (Nr. 3 «ORMA-Extraktion»[331] und Nr. 5 «JORASYS-Patrouillen»[332]) untersucht, in denen Xplain unserer Auffassung nach als Auftragsbearbeiter im Sinne des aDSG und des DSG zu qualifizieren ist. Wir haben ausserdem gesehen, dass diese Fälle von Auftragsbearbeitung unseres Wissens nicht Gegenstand eines Vertrags waren, entgegen der Anforderung der Artikel 14 und 10a aDSG, die zum Zeitpunkt des Geschehens galten.[333] Es muss daher *a fortiori* festgehalten werden, dass der Bund den Auftragsbearbeiter, der in den betreffenden Fällen mit der Bearbeitung von Personendaten beauftragt wurde, nicht überwacht hat.

521 Hinsichtlich des Schutzes von Personendaten kommt das Untersuchungsorgan daher zu dem Schluss, dass der Bund seiner Überwachungspflicht in den identifizierten Fällen der Auftragsbearbeitung nicht nachgekommen ist.

VI. ZENTRALE ERKENNTNISSE UND EMPFEHLUNGEN

A. Zentrale Erkenntnisse

1. Wie konnten die produktiven Daten zu Xplain gelangen?

522 Nach Abschluss der Administrativuntersuchung können die tatsächlichen Umstände, die dazu geführt haben, dass produktive Daten von bestimmten Einheiten des Bundes in die IT-Umgebung von Xplain gelangten, wie folgt zusammengefasst werden.

523 Erstens haben Mitarbeiter von Xplain von dem E-Mail-Konto des Bundes, das ihnen im Rahmen der Zusammenarbeit zwischen Xplain und einer betroffenen Einheit bereitgestellt wurde, an ihr E-Mail-Konto bei Xplain oder an das E-Mail-Konto ihrer Kollegen bei Xplain produktive Daten gesendet, die sie von Mitarbeitenden des Bundes erhalten hatten. Zumindest in einem Fall extrahierte ein Mitarbeiter von Xplain höchstwahrscheinlich selbst Daten aus einem Produktionssystem von fedpol, und diese Daten gelangten anschliessend in die IT-Umgebung von Xplain.

524 Zweitens bearbeiteten Mitarbeiter des Bundes, die für die interne IT-Unterstützung zuständig waren, Anfragen von Benutzern, die produktive Daten enthielten, und leiteten diese entweder an Xplain weiter oder stellten sie Xplain auf einem gemeinsam genutzten Server zur Verfügung, ohne die produktiven Daten zuvor zu entfernen, zu pseudonymisieren oder zu schwärzen.

525 Drittens übermittelten Mitarbeiter des Bundes, die an Entwicklungs-, Test- oder Migrationsarbeiten im IT-Bereich beteiligt waren, Xplain produktive Daten im Rahmen dieser Arbeiten.

526 Wir können nicht endgültig ausschliessen, dass es andere Kanäle gab, die dazu geführt haben, dass Produktivdaten des Bundes in der IT-Umgebung von Xplain vorhanden waren. Hinsichtlich der produktiven Daten des Bundes, die nach dem Datenabfluss vom Juni 2023 im Darknet vorhanden waren, scheint die Mehrheit über die in diesem Bericht identifizierten Übermittlungskanäle an Xplain gelangt zu sein. Bei einer Minderheit von Daten konnte der entsprechende Kanal im Rahmen der Untersuchung nicht identifiziert werden. Hingegen konnten im Rahmen der Untersuchung Situationen identifiziert werden, in denen produktive Daten des Bundes in die IT-Umgebung von Xplain gelangten, ohne dass diese Daten im Juni 2023 ins Darknet gelangten.

[331] Vgl. Abschnitt IV.A.3 oben.
[332] Vgl. Abschnitt IV.A.6 oben.
[333] Aktuell: Art. 9 DSG.

2. In welchem Umfang wurden produktive Daten an Xplain übermittelt?

527 Die Fälle, in denen Produktivdaten an Xplain übermittelt wurden, erscheinen isoliert, einerseits auf der Ebene der Korrespondenz zwischen Xplain und den von der Untersuchung betroffenen Verwaltungseinheiten und andererseits auf der Ebene der Korrespondenz zwischen Xplain und jedem Mitarbeiter des Bundes oder jedem Mitarbeiter von Xplain, der mindestens einmal Produktivdaten an Xplain übermittelt hat.

528 Wie die in diesem Bericht untersuchten Fälle zeigen, reicht in Bezug auf Informationssicherheit und Datenschutz jedoch potenziell eine einzige Weitergabe an einen Dritten aus:

- um die Informationssicherheit und den Datenschutz zu gefährden;
- damit grosse Datenmengen in die Hände eines Dritten gelangen;
- damit besonders schützenswerte oder klassifizierte Daten in die Hände eines Dritten gelangen.

3. Welche Mängel bestanden in Bezug auf Organisation, Prozesse oder Technik?

529 Im Rahmen der Administrativuntersuchung wurden im Wesentlichen folgende Mängel festgestellt.

530 Erstens, ein Prozessmangel: Angestellte des Bundes und Angestellte eines externen Lieferanten (Xplain) konnten Daten aus den Produktionssystemen des Bundes extrahieren und per E-Mail an Xplain senden, ohne dass es offensichtlich einen Prozess für diese Schritte gab und insbesondere ohne, dass das Vier-Augen-Prinzip bei jedem Schritt beachtet wurde.

531 Zweitens, ein Mangel in technischer Hinsicht: Es gab keine technischen Massnahmen, die die oben genannten Extraktionen von Produktivdaten oder das Versenden von Produktivdaten per E-Mail an einen externen Anbieter verhinderten (z. B. automatische Blockierung, wenn eine Extraktion oder ein Versand bestimmte vordefinierte Kriterien erfüllt, z. B. in Bezug auf Benutzergruppen, Volumen, Metadaten oder Dateityp).

532 Drittens zeigen die in diesem Bericht beschriebenen Fälle ein Defizit in Bezug auf die Ausbildung und die Sensibilisierung der Personen auf, die innerhalb des Bundes Daten aus den fraglichen Systemen bearbeiten. Zudem haben einige Einheiten nicht bemerkt, dass die von Xplain entwickelten Anwendungen potenziell zu einem Abfluss produktiver Daten im Rahmen von Support-Anfragen führen können. Obwohl eine Einheit dies im Jahr 2020 erkannt hat, scheint die Information nicht zwischen den direkt betroffenen Einheiten zirkuliert zu haben.

4. Wurden die Pflichten in Bezug auf Auswahl, Instruktion und Überwachung eingehalten?

533 Die mit Xplain vertraglich vereinbarten Aufgaben – insbesondere die Erstellung, Entwicklung oder Wartung von Software sowie der IT-Support – sind unserer Auffassung nach keine staatlichen Aufgaben, sondern administrative Hilfstätigkeiten. In Bezug auf das allgemeine Verwaltungsrecht stellt das Untersuchungsorgan daher fest, dass der Bund in seiner Zusammenarbeit mit Xplain nicht die Bedingungen für die Delegation staatlicher Aufgaben erfüllen musste.

534 Aus Sicht der Informationssicherheit kommt das Untersuchungsorgan zu dem Schluss, dass der Bund in den Beziehungen der direkt betroffenen Einheiten zu Xplain vor dem Datenabfluss im Juni 2023 seine Pflichten, sorgfältig auszuwählen und angemessen zu instruieren, teilweise erfüllt hat. Die Überwachungspflicht wurde in diesem Zusammenhang hingegen nicht erfüllt.

535 Aus Sicht des Datenschutzes kommt das Untersuchungsorgan zu dem Schluss, dass der Bund in den identifizierten Fällen der Bearbeitung von Personendaten durch Xplain als Auftragsbearbeiter seine

Pflichten zur sorgfältigen Auswahl, zur angemessenen Instruktion und zur Überwachung nicht erfüllt hat.[334]

5. In welchem Zusammenhang stehen die Übermittlung produktiver Daten an Xplain und die Verletzung der Pflicht zur sorgfältigen Auswahl, angemessenen Instruktion und Überwachung?

536 Die Fälle der Weitergabe produktiver Daten an Xplain und die von der Untersuchungsbehörde festgestellten Verstösse gegen die Pflicht zur sorgfältigen Auswahl, angemessenen Instruktion und Überwachung seitens des Bundes fanden vor dem nachfolgend zusammengefassten Hintergrund statt. Unserer Auffassung nach haben mehrere Faktoren diese Fälle von Datenübermittlungen und Verstössen begünstigt, jedoch nicht verursacht.

a) Lücken im Umgang mit Cyberbedrohungen durch Dritte

537 Die Einbeziehung externer Leistungserbringer stellt in mindestens zweifacher Hinsicht eine Herausforderung im Hinblick auf die Informationssicherheit dar.

538 Einerseits geht es um die Sicherheit innerhalb der Lieferkette («*supply chain security*»)[335]. Der Begriff bezieht sich auf die Sicherheit von Informatikmitteln[336] (insbesondere Software), die von Dritten entwickelt und von einem Unternehmen oder einer Behörde erworben werden.[337] Die meisten Software-Produkte werden nicht von Grund auf und komplett neu geschrieben.[338] Bei der Software-Entwicklung werden häufig bereits bestehende Bibliotheken oder *Open-Source-Code* integriert.[339] Dies führt dazu, dass mit diesen Bestandteilen unabsichtlich auch enthaltene Schwachstellen integriert und verbreitet werden.[340]

539 Bei einem Cyberangriff *über* die Lieferkette wird zunächst eine Drittperson attackiert und dann versucht, über eine weitere Drittperson an das Unternehmen oder die Behörde zu gelangen.[341] «*Vorstellbar sind auch Angriffe auf Soft- oder Hardware während des Herstellungsprozesses. Entsprechend wird das Produkt dann mit einer Schwachstelle, einer Hintertür oder mit vorinstallierter Schadsoftware ausgeliefert.*»[342] Schliesslich kann die Lieferkette auch durch punktuelle Störungen unterbrochen werden (Angriff *auf* die Lieferkette).[343]

540 Nach Abschluss der Untersuchung haben wir keine Hinweise gefunden oder erhalten, dass diese Risiken im Fall von Xplain eingetreten sind.[344] Jedenfalls bezog sich die Administrativuntersuchung nicht auf die

[334] Vgl. Rz. 494–521 oben.
[335] Siehe zur Veranschaulichung im Fall der USA: Abschnitt 4 der Executive Order on Improving the Nation's Cybersecurity, 12. Mai 2021.
[336] Art. 5 Bst. a ISG (in Kraft seit dem 1. Januar 2014).
[337] Im weiteren Sinne umfasst die Sicherheit der Lieferkette auch die Sicherheit der Informatikmittel, die eine Bundeseinheit entwickelt oder erwirbt und anderen Bundeseinheiten zur Verfügung stellt.
[338] NCSC, Informationssicherheit, Halbjahresbericht 2021/II, S. 10. [Anm. d. Übers.: Abweichungen von der französischen Fassung sind auf Abweichungen bei der Übersetzung des Halbjahresberichts zurückzuführen]
[339] *Ibidem*.
[340] *Ibidem*.
[341] NCSC, Informationssicherheit, Halbjahresbericht 2021/II, S. 7; vgl. auch Fisseler/Siegmund/Mörstedt, Unterschätzte Risiken durch Lieferanten, digma 2018 S. 120, 122.
[342] NCSC, Informationssicherheit, Halbjahresbericht 2021/II, S. 7.
[343] *Ibidem*.
[344] Siehe diesbezüglich die Aussagen des Bundesbeauftragten für Cybersicherheit von Anfang Juli 2023 (nachzulesen u. a. auf Watson.ch, *Xplain-Hack war laut Bund kein gezielter Angriff auf den Bund*, 5. Juli 2023).

Umstände, unter denen Xplain im Juni 2023 Opfer des Datenabflusses wurde. Die Administrativuntersuchung hat sich dagegen auf den Bund konzentriert.

541 Andererseits wirft die Einbeziehung externer Leistungserbringer die allgemeinere Frage nach der Handhabung von Cyberbedrohungen durch Dritte («*third party cyber risk management*») auf. Diese Frage ist im vorliegenden Fall zentral. Das Management von Cyberbedrohungen durch Dritte ist der systematische Prozess der Identifizierung, Analyse, Bewertung und Bewältigung von Cyberbedrohungen, die von Dritten ausgehen, mit denen eine Organisation bestimmte Daten teilt.[345]

542 Die Untersuchung ergab, dass die Informationssicherheit von den Einheiten, die von der Untersuchung betroffen waren, in einigen Fällen bis etwa 2019 oder 2020 und in anderen Fällen bis zum Datenabfluss bei Xplain im Jahr 2023, als ein vorwiegend internes Problem wahrgenommen wurde (die Systeme des Bundes müssen sicher/resilient gegenüber Cyberbedrohungen sein) und dass die Risiken, die von Dritten ausgehen, im Allgemeinen unterschätzt wurden, unabhängig davon, ob es sich um das Risiko eines Angriffs über die Lieferkette oder die Risiken im Zusammenhang mit der gemeinsamen Nutzung von Daten mit einem externen Leistungserbringer handelt. Insbesondere wurden die Risiken im Zusammenhang mit der Einbeziehung eines Softwareanbieters, im Gegensatz zu einem Anbieter von Cloud-Diensten, unterschätzt.

b) Unklarheiten bezüglich der Verantwortlichkeiten für die Informationssicherheit

543 Die vom Untersuchungsorgan durchgeführten Befragungen offenbarten Unsicherheiten und sogar widersprüchliche Positionen hinsichtlich der Verteilung der Verantwortlichkeiten im Bereich der Informationssicherheit. Bei den meisten Befragungen wurde die Frage gestellt, wer (welche Einheit oder sogar welche Person innerhalb einer Einheit) für die Informationssicherheit bei der Inanspruchnahme von Dienstleistungen von einem externen Leistungserbringer (i) während eines Ausschreibungsverfahrens, (ii) während Vertragsverhandlungen und eines Vertragsabschlusses und (iii) im Laufe des Vertragsverhältnisses verantwortlich sei.

544 Beim Vergleich der Antworten zeigt sich ein teilweise unterschiedliches Verständnis in Bezug auf die Verantwortlichkeiten zwischen – je nach Situation – (i) der zentralen Beschaffungsstelle im Sinne von Artikel 9 Org-VöB, (ii) der Verwaltungseinheit, die als Bedarfsstelle im Sinne von Artikel 3 Buchstabe b Org-VöB auftritt, (iii) der Abteilung, der diese Einheit angehört, (iv) dem ISC-EJPD, (v) dem BIT oder sogar (vi) zwischen einzelnen Mitarbeitenden derselben Abteilung.

545 Aufgrund des fehlenden einheitlichen Verständnisses bezüglich der Verantwortlichkeiten besteht die Gefahr negativer Kompetenzkonflikte.

c) Unzureichende Ressourcen im Bereich der Informationssicherheit

546 In der Nationalen Cyberstrategie (NCS; April 2023) heisst es: «*Die Schweiz nutzt die Chancen der Digitalisierung und mindert Cyberbedrohungen und deren Auswirkungen durch geeignete Schutzmassnahmen. Sie gehört zu den weltweit führenden Wissens-, Bildungs- und Innovationsstandorten in der Cybersicherheit. Die Handlungsfähigkeit und die Integrität ihrer Bevölkerung, ihrer Wirtschaft, ihrer*

[345] Aus verschiedenen Quellen abgeleitete Definition: Bericht des Bundesrates «Produktesicherheit und Supply Chain Risk Management in den Bereichen Cybersicherheit und Cyberdefence», 24.11.2021, S. 8; Judith H. Germano, Third-Party Cyber Risk & Corporate Responsability, NYU Center for Cybersecurity, 2017; Ponemon Institute, Data Risk in the Third-Party Ecosystem: Third Annual Study, November 2018, S. 2.

Behörden und der in der Schweiz ansässigen internationalen Organisationen gegenüber Cyberbedrohungen sind gewährleistet.»[346]

547 Gemäss dem erläuternden Bericht des VBS vom 24. August 2022 über das Ausführungsrecht zum ISG ist es nicht möglich, eine absolute Informationssicherheit zu erreichen.[347] Angesichts der Cyberbedrohungen geht es darum, die Wahrscheinlichkeit eines Cybervorfalls und, falls er eintritt, dessen Folgen durch geeignete Schutzmassnahmen zu verringern.

548 Mit anderen Worten, wie mehrere Befragte anmerkten, ist Informationssicherheit mit Kosten verbunden, deren Höhe letztlich von politischen Entscheidungen über die Ressourcenverteilung abhängt.

549 Aus den von OA durchgeführten Befragungen ergab sich jedoch die Tendenz, dass bis zum Datenabfluss bei Xplain im Juni 2023 die Ressourcen für die Informationssicherheit in den direkt betroffenen Einheiten insgesamt unzureichend waren.

550 Die Funktion des Informatiksicherheitsbeauftragten der Verwaltungseinheiten («ISBO»)[348] ist ein Beispiel für diese Feststellung. Diese Funktion war im Rahmen der Informationssicherheitsarchitektur des Bundes unter dem bis zum 31. Dezember 2023 geltenden Recht zentral. Sie ist es immer noch, mit einer neuen Bezeichnung[349], unter der Schirmherrschaft des ISG und der ISV.

551 Zum Zeitpunkt der Befragungen im November/Dezember 2023 und gemäss den Aussagen der zu diesem Thema befragten Personen wurden folgende Feststellungen gemacht:

- Bei fedpol war der ISBO überlastet, aber zwei zusätzliche Stellen waren beantragt oder ausgeschrieben worden.
- Im BJ machte die Funktion des ISBO nur etwa 10 % des Pflichtenhefts einer einzigen Person aus, was absolut unzureichend war.
- Im BAZG wurde die Funktion des ISBO von zwei Personen ausgeübt, was ausreichend war. Eine Erhöhung dieser Zahl war geplant, wenn Ressourcen in anderen Funktionen frei werden würden.
- Im Kommando Operationen, dem die Militärpolizei unterstellt ist, wurde die Funktion des ISBO von einer Person ausgeübt, was ausreichend war, aber angesichts der Strategie Digitale Bundesverwaltung in Zukunft sicherlich nicht mehr der Fall sein wird.
- Im SEM war die Funktion des ISBO mit einer Person besetzt, was gerade ausreichend war. Im Hinblick auf die bevorstehenden Gesetzesänderungen dürfte diese jedoch ausgeweitet werden.

552 Diese Erkenntnisse in Bezug auf die ISBO wurden der Koordinationsstelle Mitte Dezember 2023 mitgeteilt und es scheint, dass in der Zwischenzeit in den oben genannten Einheiten Massnahmen ergriffen wurden, um die Ressourcen für die derzeitige Funktion des Informationssicherheitsbeauftragten der Verwaltungseinheiten zu erhöhen.

d) Abhängigkeit der direkt betroffenen Einheiten von Xplain

553 Die Untersuchung zeigte im Allgemeinen eine Abhängigkeit der direkt betroffenen Einheiten von Xplain in den von der Untersuchung abgedeckten Jahren.

[346] Nationale Cyberstrategie NCS, April 2023, S. 11.
[347] Erläuternder Bericht des VBS zum Ausführungsrecht zum Informationssicherheitsgesetz, 24. August 2022, GS-VBS-251.2-35/1/6/8, S. 5.
[348] Art. 13 Abs. 5 und 14 aCyRV.
[349] Informationssicherheitsbeauftragte der Verwaltungseinheiten (Art. 37 ISV).

554 Im Wesentlichen gab es nach ihrer Analyse keine Alternative zu Xplain.[350] Die Tatsache, dass der Bund nicht über das geistige Eigentum an den von Xplain gelieferten Anwendungen verfügte, wird regelmässig in den Formularen erwähnt, wodurch eine freihändige Vergabe begründet wird.[351] Dasselbe gilt für das Argument, dass ein Wechsel des Anbieters grundsätzlich einen Wechsel des Systems bedeuten würde, was zu technischen Schwierigkeiten, unverhältnismässigen Kosten und Verzögerungen führen würde.[352] Weitere Argumente sind das fehlende Wissen anderer Anbieter in den Tätigkeitsbereichen der Einheiten im Vergleich zu Xplain,[353] fehlende Ressourcen in den Einheiten, beispielsweise für die Schulung der Mitarbeitenden in Bezug auf das neue System[354], sowie die zusätzlichen Kosten und die zusätzliche Zeit, die eine neue Ausschreibung mit sich bringen würde.[355]

555 Zur Veranschaulichung zeigt die folgende Grafik, wie das BAZG verschiedene Risiken im Zusammenhang mit einem Wechsel von Xplain zu einem neuen Anbieter nach Wahrscheinlichkeit und Ausmass des potenziellen Schadens gewichtet hat:[356]

[350] Siehe beispielsweise: [redacted] (AUD 03.10.09.64-77); [redacted] (AUD 03.10.09.84-106); [redacted] (AUD 03.10.09.59-62); [redacted] (AUD 03.10.09.79-82) [redacted] (AUD 03.10.09.108-148). [redacted] (AUD 03.10.09.34-45). [redacted] (AUD 03.10.09.47-57). [redacted] (AUD 03.10.09.25-28); [redacted] (AUD 03.10.09.30-32). [redacted] (AUD 03.10.09.18-23). [redacted] (AUD 03.10.09.1-4); [redacted] (AUD 03.10.09.6-16).

[351] [redacted] (AUD 03.10.09.64-77); [redacted] (AUD 03.10.09.59-62). [redacted] (AUD 03.10.09.25-28); [redacted] (AUD 03.10.09.30-32). [redacted] (AUD 03.10.09.1-4); [redacted] (AUD 03.10.09.6-16).

[352] [redacted] (AUD 03.10.09.64-77); [redacted] (AUD 03.10.09.59-62); [redacted] (AUD 03.10.09.79-82). [redacted] (AUD 03.10.09.34-45). [redacted] (AUD 03.10.09.47-57). [redacted] (AUD 03.10.09.25-28); [redacted] (AUD 03.10.09.30-32). [redacted] (AUD 03.10.09.18-23). [redacted] (AUD 03.10.09.1-4).

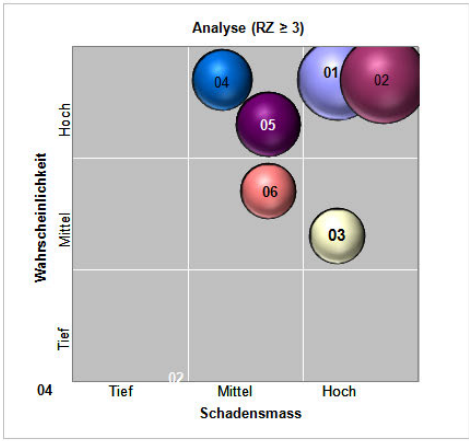
[353] [redacted] (AUD 03.10.09.64-77); [redacted] (AUD 03.10.09.59-62); [redacted] (AUD 03.10.09.34-45). [redacted] (AUD 03.10.09.18-23). [redacted] (AUD 03.10.09.1-4).

[354] [redacted] (AUD 03.10.09.18-23).

[355] [redacted] (AUD 03.10.09.64-77); [redacted] (AUD 03.10.09.59-62). [redacted] (AUD 03.10.09.34-45). [redacted] (AUD 03.10.09.18-23). [redacted] (AUD 03.10.09.1-4).

[356] Auszug aus EneXs Mobile: [redacted] (AUD 03.10.09.18-23). Das Untersuchungsorgan hat keine unterzeichnete Version dieses Dokuments ermittelt. Dass es sich dabei um eine endgültige Fassung handelt, steht jedoch ausser Zweifel. Diese Tabelle ist nämlich in einem Dokument enthalten, das einer internen E-Mail des BBL von Juni 2018 angehängt war und in der sie als «final» dargestellt wird (AUD 03.10.09.305).

Hauptrisiken



	Auswahl
01 Technik Die technische Trennung mit zwei Anbieter würde zu nicht tragbaren Projektaufwänden führen	01
02 Budget Das Projektbudget würde wesentlich überschritten und wäre nicht tragbar	02
03 Wissen Die Kenntnisse der Konzeptphase müssten mit einem neuen Lieferanten neu Aufgebaut werden und können zum Teil nicht vermittelt werden.	03
04 Mehrkosten Die Kosten für eine Ausschreibung sind nicht geplant und würden nicht zur Verfügung stehen	04
05 Zeit Die Umsetzung mit einem neuen Lieferanten könnte nicht in der geplanten Zeit erfolgen.	05
06 Ressourcen Eine alternative Lösung würde erneut zusätzliche interne Ressourcen binden, welche nicht vorgesehen sind und verfügbar wären.	06

556 Die Befragungen und die Auswertung der uns vorliegenden E-Mail-Korrespondenz legen nahe, dass die Abhängigkeit von Xplain zumindest von einigen Einheiten erkannt wurde. Die Konsequenzen, die sich aus der Feststellung der Abhängigkeit von diesem externen Anbieter ergeben würden, waren jedoch nicht offensichtlich.

557 Ein Entwurf eines internen Berichts von fedpol mit der Bezeichnung «*IKT-Beschaffungen fedpol PVS (Polizeisysteme im Bereich Bundeskriminalpolizei) – Aktuelle Situation*» vom 26. Juli 2010 ist in dieser Hinsicht aufschlussreich.[357] Laut der Titelseite wurde dieser Entwurf von einem externen Berater von fedpol verfasst und von einem *Integrationsmanager* bei fedpol überprüft. Anschliessend fügte der Leiter der Sektion Polizeisysteme II von fedpol den Kommentar ein, der nach dem Pfeil aufgeführt ist:[358]

> Ausgehend von vorliegenden Liefer- und Dienstleistungsverträgen wird die Abhängigkeit von einer Lieferfirma augenfällig. Dies könnte für fedpol nicht nur beschaffungsrechtlich zunehmend problematisch sein (rechtskonforme Begründung) - sonder auch in einem höheren Risiko resultieren. ← **eine Abhängigkeit ist in jedem Fall und immer gegeben**. heute würde ich nicht wagen zu beurteilen, welche Abhängigkeit, die vom ISC oder die von Xplain problematischer ist. Der Bund hat viele solche Abhängigkeiten, weil sie schlicht weg nicht wegbedungen werden können (Oracle, Microsoft, HP, etc.). Wird die Anwendung ORMA durch eine andere ersetzt, so entsteht mit dem neuen Anbieter umgehend wieder ein gleiches Abhängigkeitspotenzial. Andererseits ist wirtschaftlich kaum vertretbar, dass auf dem Markt existierende Standardsoftware beim Bund nachgebaut werden. Dies selbst dann nicht, wenn der Markt für Standardsoftware im Polizeiumfeld nicht sehr gross ist.
> Ich bitte beim Überarbeiten dieses Abschnittes meine Anmerkungen zu berücksichtigen. ¶

e) <u>Hauptsächlich auf Vertrauen basierende Zusammenarbeit</u>

558 Die Analyse der uns vorliegenden Exchange-Daten zeigt, dass die Zusammenarbeit zwischen Xplain und den direkt betroffenen Einheiten sowie dem ISC-EJPD von einem begrenzten Kreis von Xplain-Mitarbeitenden (insgesamt etwa 20; in der Regel zwischen zwei und fünf pro Projekt) ausgeübt

[357] [redacted] (AUD 03.10.09.84-106).
[358] Das Untersuchungsorgan konnte keine endgültige und unterzeichnete Version dieses Dokuments ermitteln.

wurde, die in direktem Kontakt mit einem relativ kleinen Kreis von Mitarbeitenden der direkt betroffenen Einheiten und des ISC-EJPD (in der Regel zwischen einer und drei Personen pro Projekt) standen.

559 Einige dieser Personen haben über einen Zeitraum von mehreren Jahren im Rahmen von Entwicklungsprojekten, mit denen Xplain beauftragt wurde, oder im Rahmen der von Xplain geleisteten Supportarbeit eng zusammengearbeitet. Die meisten dieser Mitarbeitenden von Xplain waren im Rahmen eines «*Onboarding*» beschäftigt, d. h. sie verfügten über einen Laptop, ein Benutzerkonto und ein E-Mail-Postfach des Bundes. Die Mitarbeitenden der direkt betroffenen Einheiten und des ISC-EJPD duzten sich in Bezug auf diesen externen Anbieter praktisch ausnahmslos. Der E-Mail-Verkehr war von der häufigen Verwendung von Spitznamen geprägt.

560 Ferner trat ein Mitarbeiter des SEM, der 2011 als Schlüsselperson in einem Vertrag genannt wurde, Ende Mai 2023[359] im Zusammenhang mit Xplain in den Ausstand mit der Begründung, dass sich zwischen ihm und einem der Gründer von Xplain während der Zusammenarbeit mit seiner Einheit eine Freundschaft entwickelt habe und dass sein Sohn bei Xplain seine Lehre absolviere.[360] Es scheint zudem, dass eine Person bei Xplain angestellt war und in einigen Verträgen mit fedpol als Schlüsselperson genannt wurde[361], bevor sie bei fedpol angestellt wurde und in Verträgen mit Xplain als Schlüsselperson genannt wurde.[362] Im Fall eines Mitarbeiters von fedpol legten Elemente, die zufällig vom Untersuchungsorgan entdeckt wurden, nahe, dass gewisse Privilegien bei Verwaltungsratsmitgliedern von Xplain angefragt wurden.[363]

561 Die Korrespondenz zwischen den Mitarbeitern von Xplain und den betreffenden Mitarbeitern des Bundes vermittelt letztlich den Eindruck einer Zusammenarbeit, die hauptsächlich auf Vertrauen beruht; in diesem Zusammenhang wiesen einige Befragte darauf hin, dass die betreffenden Mitarbeiter von Xplain eine Personensicherheitsprüfung (PSP) bestanden hatten, dass sie sich verpflichtet hatten, die Informatiksicherheitsvorgaben einzuhalten, und dass sie daher im Wesentlichen denselben Regeln unterworfen waren wie die Mitarbeitenden des Bundes.

562 Obwohl im Rahmen der Untersuchung mehrere Sicherheitserklärungen von Xplain-Mitarbeitenden sowie Verpflichtungen zur Einhaltung der Informatiksicherheitsvorgaben identifiziert wurden, konnte nicht bestätigt werden, dass diese Erklärungen und Verpflichtungen systematisch von allen Xplain-Mitarbeitenden, die im Rahmen eines «*Onboarding*» beschäftigt waren, unterzeichnet wurden.

563 Andererseits handelte es sich bei den Mitarbeitenden von Xplain immer noch um Mitarbeitende eines externen Anbieters.

[359] AUD B03.04.08.48.
[360] AUD B03.04.08.67.
[361] AUD B03.04.10.237; AUD B03.04.10.208.
[362] AUD B03.04.10.383; AUD B03.04.10.715.
[363] Diese Anfragen beziehen sich auf mögliche Vergünstigungen, die Verwaltungsratsmitglieder von Xplain zugestanden haben sollen, um Tickets für Fussballspiele oder einen Flug von Bern nach Madrid zu Vorzugspreisen zu erwerben. In einem Fall scheint dieser Mitarbeitende von fedpol ein Verwaltungsratsmitglied von Xplain um eine potenzielle Jobmöglichkeit innerhalb von Xplain für ein Familienmitglied ersucht zu haben. OA informierte die Koordinationsstelle am 28. Februar 2024 darüber (vgl. Rz. 29 oben; AUD 01.04.23 ; B01.04.01 ; B01.04.02 ; B01.04.03 ; B01.04.04).

B. Empfehlungen

1. Organisatorische Empfehlungen

564 Im Laufe der Administrativuntersuchung, die zwischen dem 1. September 2023 und dem 28. März 2024 stattfand, fanden in der Organisation des Bundes im Bereich der Informationssicherheit grosse Veränderungen statt.

565 Das ISG und die ISV traten am 1. Januar 2024 nach einem Prozess in Kraft, der mit der Botschaft des Bundesrates vom Februar 2017 eingeleitet worden war.[364]

566 Seit dem 1. Januar 2024[365] verfügt der Bund über drei neue Verwaltungseinheiten innerhalb des VBS: das Staatssekretariat für Sicherheitspolitik (SEPOS), das Kommando Cyber (Kdo Cy) und das Bundesamt für Cybersicherheit (BACS). Das BACS folgt auf das NCSC und das Kdo Cy auf die FUB.

567 Die organisatorischen Empfehlungen müssen daher die Organisation berücksichtigen, die am 1. Januar 2024 geschaffen wurde.

568 Nach Auffassung des Untersuchungsorgans stellen die Ergebnisse der vorliegenden Administrativuntersuchung die folgenden *Grundsätze* des ISG und der ISV nicht in Frage:

i. Die dem ISG unterliegenden Behörden sorgen in ihrem Zuständigkeitsbereich dafür, dass die Informationssicherheit nach dem Stand von Wissenschaft und Technik organisiert, umgesetzt und überprüft wird.[366]

ii. Die Verwaltungseinheiten sind für den Schutz der Informationen, die sie bearbeiten oder deren Bearbeitung sie in Auftrag geben, sowie die Sicherheit der Informatikmittel, die sie selber betreiben oder durch Dritte betreiben lassen, verantwortlich.[367]

569 Das Untersuchungsorgan ist jedoch der Ansicht, dass diese grundsätzliche Verantwortung der Verwaltungseinheiten in mehrfacher Hinsicht abgeschwächt werden sollte.

570 Durch die Komplexität der Informationssicherheit und das Erfordernis der Effizienz ist es unserer Auffassung nach notwendig, die Nutzung des vorhandenen Wissens und der vorhandenen (personellen und technischen) Mittel im Bereich der Informationssicherheit zu optimieren, bevor zusätzliche Mittel in Betracht gezogen werden.

571 Die im Rahmen dieser Untersuchung durchgeführten Befragungen haben ergeben, dass dieses Wissen und diese Mittel vor dem 31. Dezember 2023 *im Wesentlichen* bei den internen IKT-Leistungserbringern (BIT, FUB, Informatikeinheit des EDA, ISC-EJPD) und beim NCSC vorhanden waren.

572 Die Untersuchung ergab, dass die anderen von der Untersuchung betroffenen Verwaltungseinheiten über ungleiche Kompetenzen und Mittel im Bereich der Informationssicherheit verfügten, die jedoch in jedem Fall weniger umfangreich waren als die der oben genannten internen Leistungserbringer und des NCSC.

573 Ausserdem und in Anlehnung an diese Erkenntnis stellt das Untersuchungsorgan fest, dass im derzeitigen System des ISG und der ISV die *Verantwortung* und das *Wissen* im Bereich der Informationssicherheit – zumindest teilweise – nicht aufeinander abgestimmt sind. Die Befragungen im Rahmen dieser

[364] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953.
[365] AS 2023 746.
[366] Art. 7 ISG; Art. 3 ISV.
[367] Art. 4 Abs. 1 ISV.

Administrativuntersuchung ergaben eine Diskrepanz zwischen (i) der Verantwortung der Verwaltungseinheiten gemäss Artikel 4 ISV und (ii) den verfügbaren Informationen zur Gewährleistung der Informationssicherheit (und damit zur Wahrnehmung der Verantwortung, die ihnen durch Art. 4 ISV übertragen wurde).

574 Es ist richtig, dass Artikel 30 Absatz 2 ISV vorsieht, dass internen IKT-Leistungserbringer den Verwaltungseinheiten die Informationen zur Verfügung stellen, die sie zur Gewährleistung der Informationssicherheit benötigen. Die Tatsache, dass diese Regelung überhaupt vorhanden ist, bestätigt die in den Befragungen gemachte Feststellung, dass die internen IKT-Leistungserbringer über Informationen verfügen, welche die Verwaltungseinheiten *nicht haben* und die sie daher an sie weitergeben müssen. Das Untersuchungsorgan ist jedoch der Ansicht, dass dieses erweiterte Wissen mit einer erweiterten Verantwortung einhergehen sollte. Um diese Empfehlung in die Praxis umsetzen zu können, sind Massnahmen erforderlich, die über den Rahmen dieser Administrativuntersuchung hinausgehen.

575 Schliesslich ergab die Untersuchung, dass, nachdem eine Verwaltungseinheit eine Funktion («*Error-Reporting*») identifiziert hatte, die potenziell zu einem Abfluss produktiver Daten im Rahmen von Support-Anfragen hätte führen können, die Information offenbar nicht zwischen den direkt betroffenen Einheiten zirkulierte. Dies macht unserer Auffassung nach die Risiken der Dezentralisierung in Bezug auf die Informationssicherheit deutlich.

576 Diese Feststellungen führen zu den folgenden Empfehlungen.

Empfehlungen:

1. Die Verantwortung der internen IKT-Leistungserbringer in Bezug auf die Informationssicherheit sollte erweitert werden, wenn diese für die Leistungsbezügerinnen und-bezüger Informatikmittel betreiben oder Informationen bearbeiten.

2. Die Zentralisierung der Kompetenzen im Bereich der Informationssicherheit des Bundes sollte ausgebaut werden:

   a) Dem SEPOS sollte die Verantwortung für die Steuerung und Überwachung der Informationssicherheit des Bundes übertragen werden, die derzeit bei den Departementen liegt (vgl. Art. 39 ISV).

   b) Dem SEPOS sollten Delegierte zugeteilt werden, die der Weisungsbefugnis des SEPOS unterstehen und in die Verwaltungseinheiten sowie Departemente entsandt werden, um ein Gleichgewicht zu schaffen zwischen (i) der Zentralisierung der Kompetenzen und der Mittel im Bereich der Informationssicherheit sowie (ii) der Notwendigkeit, die individuellen Besonderheiten und Bedürfnisse der Verwaltungseinheiten und Departemente zu berücksichtigen.

3. Das SEPOS und das BACS sollten die Verteilung ihrer jeweiligen Rolle im Hinblick auf Artikel 8 Absatz 2, Artikel 10 Absatz 3, Artikel 21 Absatz 2 Buchstabe a und Artikel 43 Absatz 2 ISV schnell und klar festlegen.

2. Inhaltliche Empfehlungen

577 Die aus dieser Administrativuntersuchung gewonnenen Erkenntnisse erfordern unserer Ansicht nach auch inhaltliche Empfehlungen.

578 Der Bundesrat hielt in der Botschaft zum ISG 2017 Folgendes fest: «*Die Sicherheit beim Einsatz von Informatikmitteln wird oft als technische Angelegenheit betrachtet. Dies trifft nur am Rande zu: Die überwiegende Mehrheit der Sicherheitsvorkehrungen im Informatikbereich sind organisatorischer Natur.*»[368] Auch die meisten unserer Empfehlungen sind dieser Art.

579 Die folgende Empfehlungen technischer Natur sind technologieneutral.

Empfehlungen:

1. Den Behörden und Organisationen, die dem ISG und dem DSG unterstellt sind, sollten ausreichende Ressourcen zur Erfüllung ihrer Aufgaben im Bereich der Informationssicherheit und des Datenschutzes zur Verfügung gestellt werden.

2. Jede Verwaltungseinheit muss ihre externen Leistungserbringer kennen und das SEPOS muss die Identität und Kritikalität aller externen Leistungserbringer kennen.

3. Die Informationssicherheits- und Datenschutzkultur muss gestärkt werden (Sensibilisierung und Schulung), insbesondere bei den Personen, die mit der Bearbeitung von Daten aus den Produktionssystemen des Bundes beauftragt sind.

4. Das Verbot, produktive Daten an externe Leistungserbringer zu *transferieren*, sollte klar und deutlich kommuniziert werden.

5. Die Tatsache, dass eine natürliche Person ein externer Leistungserbringer oder ein Mitarbeiter oder Organ eines externen Leistungserbringers ist, sollte dem Bundespersonal gegenüber unmittelbar erkennbar gemacht werden.

6. Der *Zugriff* externer Leistungserbringer auf produktive Daten, sei es vor Ort oder aus der Ferne, sollte auf ein Minimum reduziert, streng geregelt und kontrolliert werden (Etablierung schriftlich dokumentierter Prozesse, die einheitlich sind, regelmässig überprüft werden und auf dem Vier-Augen-Prinzip und nicht auf Vertrauen basieren).

7. Die Löschung produktiver Daten, die in der Vergangenheit aktuellen oder früheren externen Leistungserbringern des Bundes zur Verfügung gestellt wurden, muss systematisch verlangt und anschliessend überprüft werden (einschliesslich Archive).

8. Datenbearbeitungen im Ausland durch externe Leistungserbringer müssen identifiziert und gegebenenfalls geregelt werden.

9. Anwendungen sollten Sicherheit und Datenschutz ab der Planung («privacy and security by design») und Benutzerfreundlichkeit («user friendliness») miteinander vereinbaren.

[368] Botschaft zum Bundesgesetz über die Informationssicherheit vom 22. Februar 2017, BBl 2017 2953 2979.

10. Die Einführung technischer Beschränkungen zur Verhinderung von Transfers von produktiven Daten sollte, je nach Kritikalität der betreffenden Daten, für bestimmte Situationen in Betracht gezogen werden.

* * *