Bearbeitungsreglement[1]

für
die Applikation

EDÖB - Office

vom Dez. 2014

(Version 2.3)

Gemäss Art. 21 der Verordnung zum Bundesgesetz über den Datenschutz
(VDSG; SR 235.11)

Die Unterzeichnenden haben das Reglement am Ende der Projektplanungsphasen nach HERMES zur Kenntnis genommen und sind mit dem Inhalt einverstanden. Das Bearbeitungsreglement muss bei Änderungen des Systems nachgeführt werden. Aus diesem Grunde ist es sinnvoll, kleinere Korrekturen am Anfang des Dokumentes (Reglementsänderungen) nachzuführen. Bei umfassenderen Änderungen ist es empfehlenswert, ein neues Bearbeitungsreglement mit einer neuen Version zu erstellen. Es ist sinnvoll, das Reglement während der Betriebsphase regelmässig einzusehen.

Unterschriften:

Datenschutzberater / -verantwortlicher Verantwortliches Organ

[1] Aus Sicherheitsgründen werden in diesem veröffentlichten Bearbeitungsreglement nicht alle Informationen aufgeführt.

Inhaltsverzeichnis

Abkürzungen

BAR	Bundesarchiv
BIT	Bundesamt für Informatik und Telekommunikation
BK	Bundeskanzlei
BGer	Bundesgericht
BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (SR 152.3)
BV	Bundesverwaltung
BVGer	Bundesverwaltungsgericht
DSG	Bundesgesetz über den Datenschutz (SR 235.1)
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
E-Mail	Elektronisches Mail
FAX	Telefax
GEWA	Datenverarbeitungssystem für die Bekämpfung der Geldwäscherei, des organisierten Verbrechens und der Terrorismusfinanzierung
ISIS	Informationssystem Innere Sicherheit
JANUS	Informationssystem der Bundeskriminalpolizei
KZL	Kanzlei beim EDÖB
MA	MitarbeiterInnen
ÖB	Öffentlichkeitsberater
Org.	Organisation
SB	SachbearbeiterInnen
SIS	Schengener Informationssystem
VDSG	Verordnung zum Bundesgesetz über den Datenschutz (SR 235.11)

Reglementsänderungen

Wann: (Datum)	Was (kurze Umschreibung der Änderung / Kontrollen)	Wer
07.09.2004	2 Schnittstellenbeschreibung (Beziehungen EDÖB ⇔ BV) 2.2 Organigramm des EDÖB angepasst 2.3 Verantwortlichkeiten nachgeführt 5.2 Ablauf Dossierarchivierung angepasst (nicht archivwürdige Dossiers, Übergabe Diskette an BAR) 10 Anpassen Datenfelder (Word ⇒ OLE, Volltextsuche noch besser umschrieben) 13 Konfiguration der Informatikmittel (diverse Nachführungen)	Sche
2011	Vollständige Überarbeitung Bei der Überarbeitung des Reglements haben wir erkannt, dass bei der Authentisierung der Einsatz eines USB-Sticks mit passwortgeschützten Schlüsselpaaren nicht mehr ganz dem Stand der Technik entspricht. Zukünftig sollen entsprechende Smartcards / -Tokens mit Lesegeräten der entsprechenden Güteklassen eingesetzt werden. Zusätzlich sind auch die Zugriffe von Personen mit erhöhten Systemprivilegien (bspw. Admin) auf dem System revisionssicher und pseudonym zu protokollieren. Die oben aufgeführten Anforderungen gelten für das neue System, weil das bestehende abgelöst wird.	Sche
Dez. 2013	8.2 Ablauf Dossierarchivierung EDÖB / BAR Diverse bessere Umschreibungen bei den Bemerkungen 12.2 Zugriffskontrolle Neue Zwei-Faktor-Authentifizierung am Bundesclient	Sche
April 2014	1.-3. und 5.-7. eingefügt (von Anhang 1 übertragen) und Nummerierung angepasst; Präzisierungen und Aktualisierungen in 18, 19 und 20	JS / Sche
Dez. 2014	Organigramm angepasst (Seite 13) Anpassung der EDÖB-Office Version 2.0.2 (Seite 32) Dateien der Anwendung angepasst (Seite 33) Druckerlokalitäten besser bezeichnet (Seite 35) Angaben zur Hardware nachgeführt (Seite 36)	Sche

1. Name und Adresse des verantwortlichen Bundesorgans

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
Feldeggweg 1
3003 Bern

2. Name und vollständige Bezeichnung der Datensammlung

EDÖB-Office

3. Rechtsgrundlage und Zweck der Datensammlung

Insbesondere die folgenden Gesetze gelten als Grundlage für das System (Datensammlung / Anwendung) EDÖB-Office:

- Regierungs- und Verwaltungsorganisationsgesetz (RVOG; SR172.10) Art. 57h
- Verordnung zum Bundesgesetz über den Datenschutz (VDSG; SR 235.11) Art. 32 Abs. 2
- Archivierungsgesetz (BGA; SR 152.1)

Die Datensammlung dient der Verwaltung von Geschäften/Dossiers.

4. Ausgangslage

Aufgrund der Nicht-Jahr 2000 Fähigkeit des Registratursystems CORES, welches vom Eidg. Datenschutz- und Öffentlichkeitsbeauftragten eingesetzt wurde, sah man sich gezwungen, ein neues System zu evaluieren, welches es dem EDÖB erlaubt, seine Tätigkeiten weiterhin mit den notwendigen EDV-technischen Sachmitteln zu unterstützen. Aufgrund dessen wurde ein Projekt gemäss HERMES (Handbuch für die Führung und Abwicklung von Informatikprojekten in der Bundesverwaltung) gestartet. Hauptzielsetzung des zukünftigen Systems EDÖB-Office soll die effiziente, effektive und sichere Bearbeitung der Dossiers beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) sein. Grundsätzlich sollen möglichst alle Dateien bzw. Dokumente beim EDÖB mit diesem System erstellt oder bearbeitet werden. Die Anforderungen an das System waren, die folgenden Bereiche zu unterstützen (Soll-Vorgaben):

- Dokumentenverwaltung
- Registratur
- Planung
- Statistik
- Steuerung

In den Projektplanungsphasen wurde darauf geachtet, dass ein Mitarbeiter in der Projektorganisation Einsitz nimmt, der sich für die Datenschutz- und Datensicherheitsbelange im Projekt einsetzt und dafür auch die notwendige Zeit zur Verfügung hat. Das zukünftige System wird besonders schützenswerte Personendaten beinhalten und ist somit der höchsten Schutzstufe (3) zuzuordnen. Eine gute Systemverfügbarkeit ist wünschenswert. Bei einem mehrtägigen Ausfall der Anwendung könnte dennoch ein minimaler Betrieb beim EDÖB aufrechterhalten werden. Aus Sicht des Datenschutzes und der Datensicherheit wurden namentlich die folgenden Kriterien festgehalten:

- Es ist eine Prozessanalyse durchzuführen und zu dokumentieren.
- Die Daten sind bei der Übertragung als auch bei der Speicherung (inkl. Sicherungsbänder) zu chiffrieren.
- Es ist dafür zu sorgen, dass nur diejenigen Personenkreise auf die Daten zugreifen können, welche diese für die Aufgabenerfüllung benötigen.
- Neben Benutzeridentifikation und Passwort ist noch eine weitere Absicherung mit Hilfe von Besitz (bspw. Chipkarte / Diskette / USB-Stick) oder einem biometrischen Verfahren vorzusehen.
- Namentlich Änderungen bzw. Mutationen von Zugriffsberechtigungen, Applikations- und Systemänderungen sowie Wartungsarbeiten müssen weitmöglichst pseudonymisiert und revisionsfähig protokolliert werden.
- Die Protokolle sind regelmässig möglichst mit einem Tool auszuwerten.

Das Pflichtenheft wurde Informatikfirmen zugestellt, die eine Lösung anbieten konnten. Insbesondere aufgrund der Unterstützung gewisser Produkte, als auch der umfassenden Implementierung der geforderten Datensicherheitsmassnahmen, wurde 1999 die Lösung der Firma X gewählt.

5. Kategorien der bearbeiteten Personendaten

Adresse, Identität, ein- und ausgehende Sachgeschäfte, Dossiernummer, Datum der Aufnahme, Schlüsselwörter.

6. Kategorien der Empfänger der Daten

Bundesarchiv, Bundesverwaltungsgericht, betroffene Behörden und Personen (natürliche oder juristische Personen).

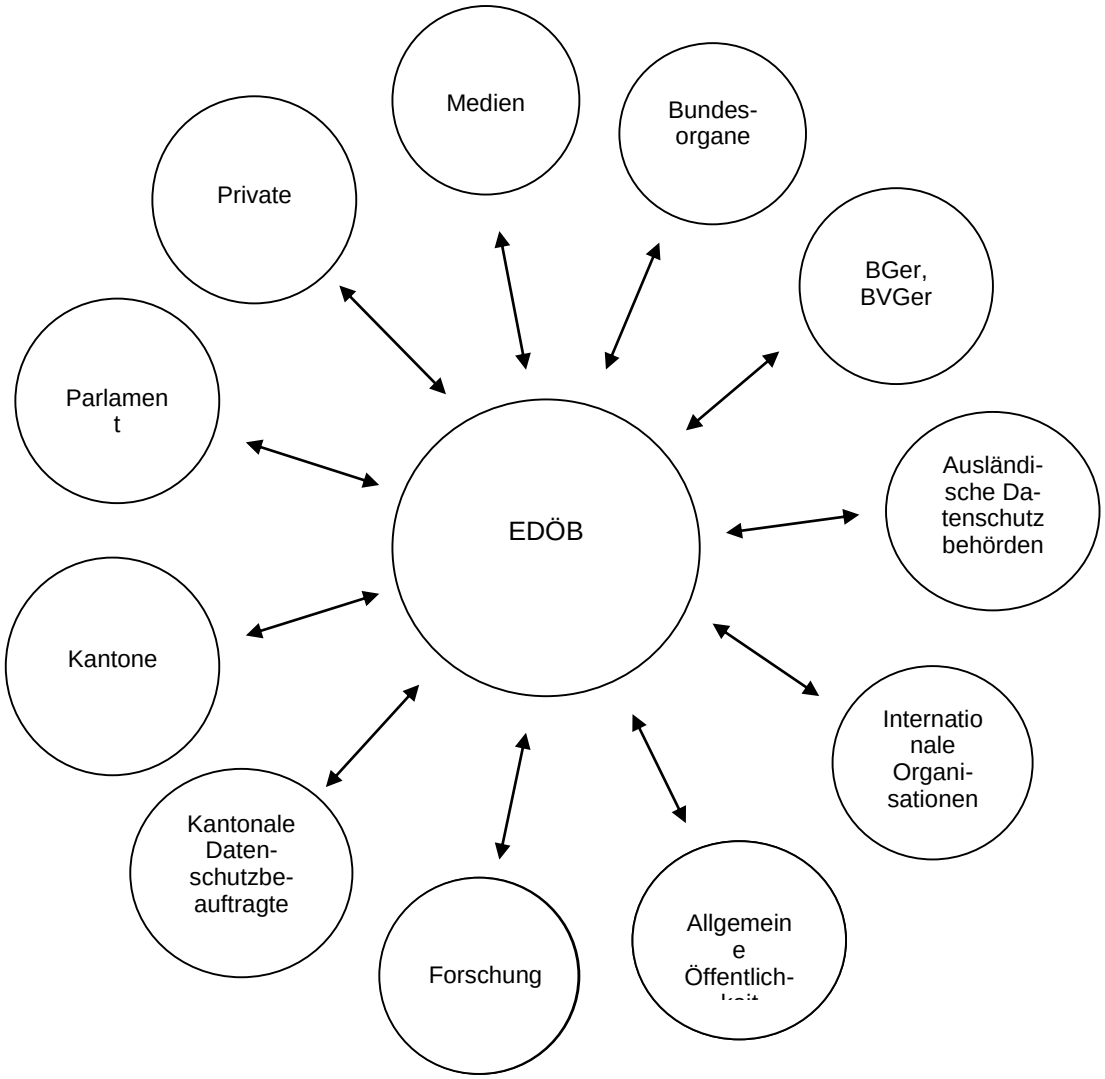
7. Kategorien der an der Datensammlung Beteiligten

Keine.

8. Dokumentation, der vom System betroffenen Organisationseinheiten (EDÖB-Umsystem)

- **Aufgrund des Datenschutzgesetzes (DSG)**

BGer = Bundesgericht
BVGer = Bundesverwaltungsgericht



Schnittstellenbeschreibung des Datenflusses vom EDÖB zu den Umsystemen:

Von	Nach	Zweck	Datenart[2]	Periodizität	Auslöser	Medium[3]
Private[4]	EDÖB	Antwort auf Datenschutzfragen Antworten auf Empfehlung EDÖB		Bei Anfragen (dauernd) Nach Erstellung einer Empfehlung	Private natürliche oder juristische Personen Empfehlung	
EDÖB	Private	Informieren, Datenschutzberatung Erlässt Empfehlung	Stellungnahmen (Tätigkeitsbericht, Leitfäden, Merkblätter)	Jährlich, bei wichtigen Vorkommnissen Bei Nichtbefolgung von Vorgaben des EDÖB	Stichdaten, wichtige Vorkommnisse	Papier mit Unterschrift
Medien	EDÖB	Anfragen von Medien zu Fragen des Datenschutzes		Bei Anfragen oder besonderen Vorkommnissen im Datenschutzbereich	Medien, besondere Vorkommnisse	
EDÖB	Medien	Information der Öffentlichkeit	Tätigkeitsbericht	Jährlicher Stellungnahmen bei besonderen Vorkommnissen	Gesetzliche Vorgaben Besondere Vorkommnisse	Pressecommuniques
Bundesorgane[5]	EDÖB	Antwort auf Datenschutzfragen Datenschutzkonforme Gesetzgebung Datenschutzkonforme (EDV-)Systemgestaltung Antworten auf Empfehlung des EDÖB	 Gesetzes- und Verordnungsentwürfe Projektanträge, Bearbeitungsreglemente	regelmässig Bei Anfragen zu Gesetzgebungsarbeiten, Ämterkonsultationen Bei sensit. EDV Projekten in der BV (im Einzelfall und wenn Datenschutzberater der Org. Einheit an uns gelangt) Nach Erstellung einer Empfehlung	Bundesorgane Bundesorgane Neues EDV-Projekt muss in der Bundesverwaltung angemeldet werden (Art. 20 Abs. 2 VDSG) Empfehlung	 Meist Papierform mit Unterschrift

[2] Ist normalerweise Freitext, wo möglich wird dieser konkretisiert.
[3] Das Medium kann je nach Kommunikationsmöglichkeiten folgende Form aufweisen: Telefon, Papier, FAX, E-Mail, Intra-, Internet, Sitzungen. Wo möglich erfolgt eine Konkretisierung.
[4] Private sind natürliche oder juristische Personen, welche Personendaten im Umfeld des Privatrechts bearbeiten
[5] Bundesorgane sind Behörden und Dienststellen des Bundes sowie Personen, wenn sie öffentliche Aufgaben des Bundes wahrnehmen (bspw. Krankenkassen im obligat. Teil der Krankenversicherung / öffentliches Recht).

Von	Nach	Zweck	Datenart[6]	Periodizität	Auslöser	Medium[7]
EDÖB	Bundes-organe	Informieren, Daten-schutzberatung	Stellungnah-men, (mit Ver-weis auf Leit-fäden, Merk-blätter, Tätig-keitsberichte)	Antworten auf Anfragen	Anfragesteller Bundesorgane	
		Datenschutzkon-forme Gesetzge-bung	Stellungnah-men	Regelmässig bei Gesetzgebungs-fragen und Ämter-konsultationen	Gesetzge - bungs– und Ämterkonsulta-tionsverfahren	Stellung-nahme in Papierform mit Unter-schrift
		Datenschutzkon-forme (EDV-) Sy-stemgestaltung	Nachfassen beim Projekt-antrag oder aufgrund des Bearbeitungs-reglements	Im Einzelfall, bei unklaren oder sen sitiven EDV-Projektanträgen, bei der Zustellung eines Bearbei-tungsreglements. Anfrage von Da-tenschutzberatern	Projektantrag in der Bundesver-waltung Zugestelltes Be-arbeitungsregle-ment, Daten-schutzberater	
		Erlässt Empfeh-lung		Bei Nichtbefolgun von Vorgaben des EDÖB		Papier mit Unterschrift
BGer, BVGer	EDÖB	Beantragen Stel-lungnahme zu Da-tenschutzfragen		Bei Anfragen	Gerichte	Papier mit Unterschrift
		Klageantwort des Beklagten wird zugestellt		Nach dem Ein-reichen der Kla-ge des EDÖB	Gerichtsfall	Papier mit Unterschrift
		Gegenerklärung des Beklagten wird zugestellt Duplik		Nach der Replik des EDÖB		Papier mit Unterschrift
		Informiert über Gerichtsentscheide		Nach Gerichts-verhandlungen		Papier mit Unterschrift
EDÖB	BGer, BVGer	Stellungnahmen zu Datenschutzfragen		Bei Anfragen	Anfragende	Papier mit Unterschrift
		Klage beim Gericht einreichen		Bei Nichtbefol-gung einer Emp-fehlung	EDÖB	Papier mit Unterschrift
		Erwiderung auf Klageantwort (Replik)		Nach Klageant-wort des beklag-ten	Beklagter	Papier mit Unterschrift
Ausländische Datenschutz-behörden	EDÖB	Informationsaus-tausch Feststellen ob Da-tenschutz gleich-wertig ist		Mehrmals jährlich	Dossiers, Sit-zungen und Ver-anstaltungen Anfragende	
EDÖB	Ausländi-sche Daten-schutzbe-hörden	Informationsaus-tausch Feststellen ob Da-tenschutz gleich-wertig ist		Mehrmals jährlich	Dossiers, Sit-zungen und Veranstaltungen Anfragende	

[6] Ist normalerweise Freitext, wo möglich wird dieser konkretisiert.

[6] Das Medium kann je nach Kommunikationsmöglichkeiten folgende Form aufweisen: Telefon, Papier, FAX, E-Mail, Intra-, Internet, Sitzungen. Wo möglich erfolgt eine Konkretisierung.

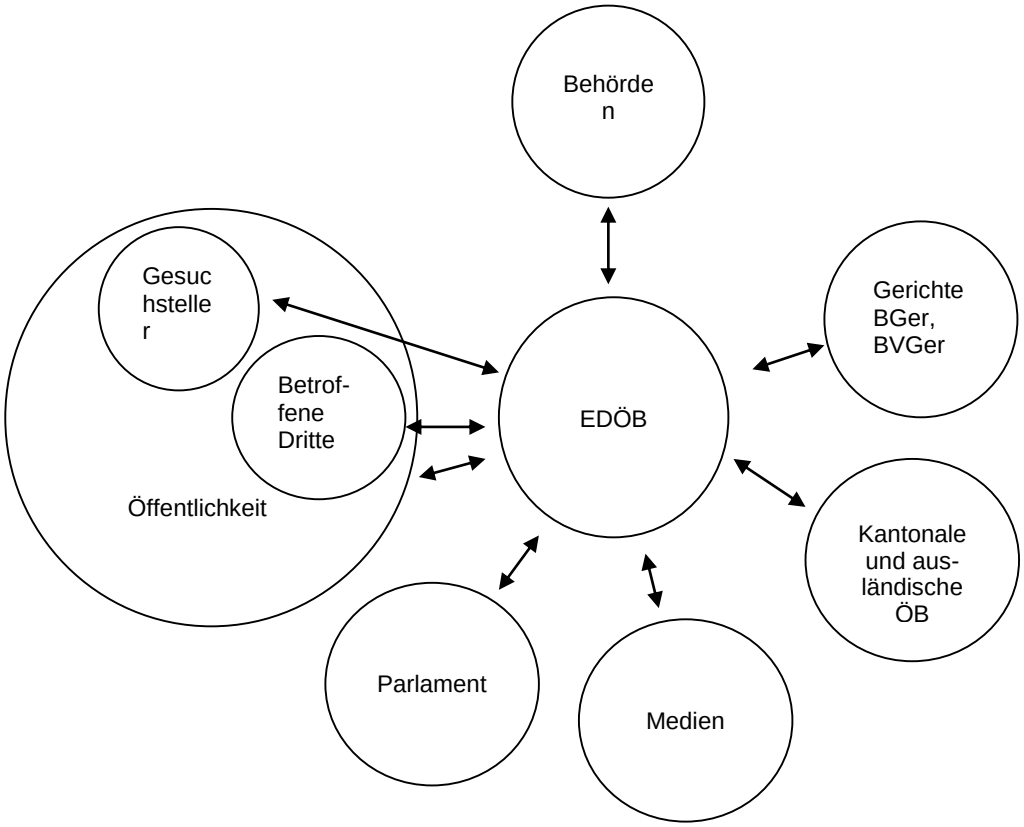
Von	Nach	Zweck	Datenart[8]	Periodizität	Auslöser	Medium[9]
Internationale, Organisationen (OECD, Europarat)	EDÖB	Informationsaustausch Teilnahme in Arbeitsgruppen, Kommissionen, ...		Regelmässig	Beidseitig	
EDÖB	Internationale Organisationen (OECD, Europarat)	Informationsaustausch Teilnahme in Arbeitsgruppen, Kommissionen, ...		Regelmässig	Beidseitig	
Allgemeine Öffentlichkeit	EDÖB	Anfragen aus dem Ausland zu Datenschutzfragen		Mehrmals jährlich	Anfragende	
EDÖB	Allgemeine Öffentlichkeit	Beantwortung der Anfrage Information der Öffentlichkeit		Mehrmals jährlich Regelmässig	Anfragende EDÖB	
Forschung	EDÖB	Anfragen zu Forschungsvorhaben		Regelmässig	Forschungsstellen	
EDÖB	Forschung	Antwort zu Forschungsanfragen		Regelmässig	Forschungsstellen	
Kantonale Datenschutz beauftragte	EDÖB	Zusammenarbeit im Rahmen der CH-Vereinigung der Datenschutzbeauftragten. Wenn für Anfrage nicht zuständig, weiterl. an EDÖB		Regelmässige Zusammenkünfte Bei Anfrage	Vorgesehene Sitzungen und deren Traktanden Anfragende	
EDÖB	Kantonale Datenschutzbeauftragte	Zusammenarbeit im Rahmen der CH-Vereinigung der Datenschutzbeauftragten. Wenn für Anfrage nicht zuständig, weiterleiten an Kantonalen DSB		Regelmässige Zusammenkünfte Bei Anfrage	Vorgesehene Sitzungen und deren Traktanden Anfragende	
Kantone	EDÖB	Anfrage von kantonalen Stellen		Bei Anfragen	Kantonale Stelle	
EDÖB	Kantone	Informieren, Beraten		Bei Anfragen	Kantonale Stelle	
Parlament	EDÖB	Informieren, beraten		Bei Anfragen zum Datenschutz Gesetzgebungsarbeiten	Parlamentarische Kommissionen, Parlamentarier	Papier mit Unterschrift
EDÖB	Parlament	Beraten, informieren		Bei Anfragen zum Datenschutz Gesetzgebungsarbeiten	Parlamentarische Kommissionen, Parlamentarier	Papier mit Unterschrift

[8] Ist normalerweise Freitext, wo möglich wird dieser konkretisiert.

[6] Das Medium kann je nach Kommunikationsmöglichkeiten folgende Form aufweisen: Telefon, Papier, FAX, E-Mail, Intra-, Internet, Sitzungen. Wo möglich erfolgt eine Konkretisierung.

- **Aufgrund des Öffentlichkeitsgesetzes (BGÖ)**

Behörden[10]
BGer = Bundesgericht
BVGer = Bundesverwaltungsgericht
EDÖB = Eidg. Datenschutz- und Öffentlichkeitsbeauftragter
ÖB = Öffentlichkeitsberater



Schnittstellenbeschreibung des Datenflusses vom EDÖB zu den Umsystemen:

Von	**Nach**	**Zweck**	**Datenart[11]**	**Periodizität**	**Auslöser**	**Medium[12]**
Gesuchsteller	EDÖB[13]	*Stellt Gesuch um Zugang zu Dokumenten des EDÖB (gemäss Art. 10 BGÖ)*		*Bei Zugangsgesuch*	*Zugangsgesuchsteller*	Telefon, E-Mail[14]
		Stellt Schlichtungsantrag (Art. 13 BGÖ)		Bei Antragstellung	Schlichtungsantragssteller	E-Mail

[10] In der vorliegen Dokumentation versteht man darunter die (siehe auch Art. 2 BGÖ; SR 152.3):
- Bundesverwaltung;
- Organisationen und Personen des öffentlichen oder privaten Rechts, die nicht der Bundesverwaltung angehören, soweit sie Erlasse oder erstinstanzliche Verfügungen Im Sinne von Art. 5 des Bundesgesetzes vom 20. Dezember 1968 über die Verwaltungsverfahren (Verwaltungsverfahrensgesetz) erlassen;
- Parlamentsdienste.

[11] Wenn nichts anderes festgehalten ist, handelt es sich um Freitext (z.T. konkretisiert).

[12] Beim Medium handelt es sich um Papier mit Unterschrift; sofern auch andere Medien verwendet werden, sind diese zusätzlich aufgeführt.

[13] Der EDÖB ist in den ersten vier Zeilen (je oberster Bereich / *in kursiv festgehalten*) der Schnittstellenbeschreibung als Behörde zu betrachten, welche die Zugangsgesuche für die von ihm bearbeiteten Dokumente entgegennimmt. Bei Verweigerung, Einschränkung oder Aufschub des Zugangsgesuchs führt der EDÖB kein Schlichtungsverfahren durch und erlässt keine Empfehlung, sondern direkt eine Verfügung, die dann erstinstanzlich vom BVGer beurteilt werden muss.

[14] Sensitive Daten, wie besonders schützenswerte Personendaten oder Persönlichkeitsprofile, dürfen nur dann via E-Mail übertragen werden, wenn dem Stand der Technik entsprechende Verschlüsselungsverfahren eingesetzt werden.

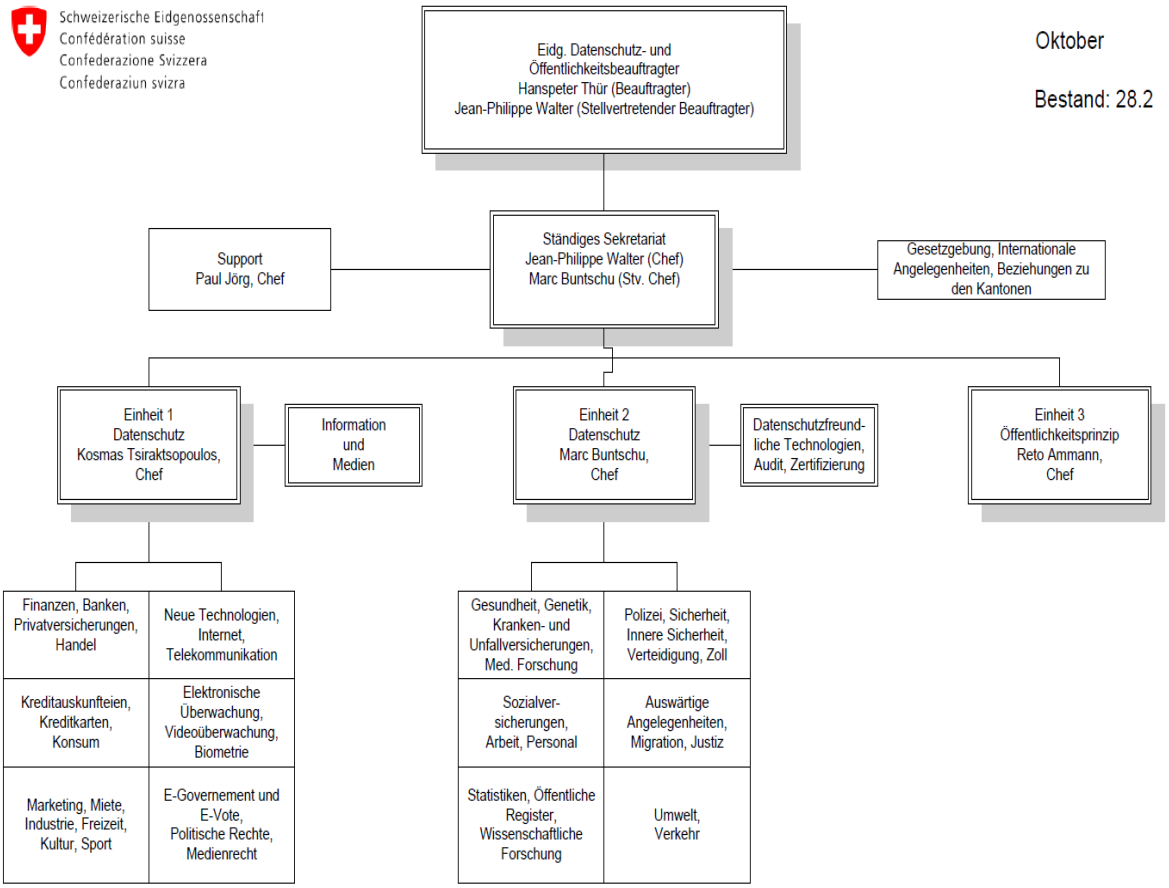
Von	Nach	Zweck	Datenart	Periodizität	Auslöser	Medium
EDÖB	Gesuchsteller	*EDÖB gibt Gesuchsteller Antwort, ob der Zugang zu den Dokumenten gewährt wird*		*Nach Zugangsgesuch*	*Zugangsgesuchsteller*	E-Mail
		Durchführung des Schlichtungsverfahrens und teilt Endergebnis mit		Nach der Durchführung der Schlichtung	Schlichtungsantragsteller	E-Mail
		EDÖB stellt Empfehlung aus		Sofern bei der Schlichtung keine Einigung erzielt wurde	Diejenigen, welche die Schlichtung nicht akzeptieren	
Betroffene Dritte	EDÖB	*Geben dem EDÖB bekannt, ob sie mit der Zugangsgewährung einverstanden sind*		*Wenn bei einem Zugangsgesuch die Personendaten der Betroffenen nicht anonymisiert werden können*	*Zugangsgesuchsteller*	E-Mail
		Geben dem EDÖB im Rahmen des Schlichtungsverfahrens bekannt, ob sie mit der Zugangsgewährung einverstanden sind		Wenn bei einem Zugangsgesuch die Personendaten der Betroffenen nicht anonymisiert werden können	Schlichtungsantragsteller	E-Mail
		Stellt / Stellen Schlichtungsantrag		Bei Schlichtungsantragsstellung	Schlichtungsantragsteller	E-Mail
EDÖB	Betroffene Dritte	*Anhörung der Betroffenen, die in den Dokumenten aufgeführt sind, ob sie mit dem Zugangsgewährung einverstanden sind*		*Nach einem Gesuch um Zugang zu den jeweiligen Dokumenten*	*Zugangsgesuchsteller*	E-Mail
		Durchführung des Schlichtungsverfahrens und teilt Endergebnis mit		Nach der Durchführung der Schlichtung	Schlichtungsantragsteller	
		EDÖB stellt Empfehlung aus		Sofern bei der Schlichtung keine Einigung erzielt wird	Die, welche die Schlichtung nicht akzeptieren	

Von	Nach	Zweck	Datenart	Periodizität	Auslöser	Medium
Behörde	EDÖB	Anfragen zum Öffentlichkeitsgesetz		Bei Anfragen	Behörde	Telefon, E-Mail
		EDÖB erhält Dokumentation und Stellungnahme der Behörde während dem Schlichtungsverfahren		Innert 20 Tagen nach Empfang der Empfehlung	Behörde	Telefon, E-Mail
		Wenn nicht einverstanden mit der Empfehlung des EDÖB, erlässt die Behörde eine Verfügung (Kopie an EDÖB)				
		Teilt dem EDÖB - die Anzahl der Gesuche mit - die Anzahl der angenommenen Gesuche und der ganz oder teilw. abgelehnten Gesuche mit - Der Gesamtbetrag der einverlangten Gebühren mit	Statistik	1 x jährlich	Behörde	E-Mail
EDÖB	Behörde	Antwort auf Anfragen zum Öffentlichkeitsgesetz		Bei Anfragen	Behörde	Telefon, E-Mail
		Durchführung des Schlichtungsverfahrens und teilt Ergebnis mit		Nach Durchführung von Schlichtungen	Schlichtungsantragsteller	
		EDÖB stellt Empfehlung aus		Sofern bei der Schlichtung keine Einigung erzielt wird	Diejenigen, welche die Schlichtung nicht akzeptieren	
Gerichte BVGer[15] BGer[16]	EDÖB	Geben die Urteile dem EDÖB bekannt		Nach Gerichtsentscheiden	Gerichte	
EDÖB	Gerichte BVGer BGer	Erstellt Stellungnahmen zu Anfragen von Gerichten		Bei Anfragen	Gerichte	
Kantonale und ausländische ÖB	EDÖB	Gegenseitiger Informationsaustausch				Telefon, E-Mail
EDÖB	Kantonale und ausländische ÖB	Gegenseitiger Informationsaustausch				Telefon, E-Mail
Öffentlichkeit	EDÖB	Anfrage zum Öffentlichkeitsgesetz		Regelmässig		Telefon, E-Mail
EDÖB	Öffentlichkeit	Information der Öffentlichkeit		Regelmässig		Telefon, E-Mail
		Beratung bei Anfragen		Regelmässig		
Medien	EDÖB	Beantwortung von Anfragen		Bei Anfragen oder besonderen Vorkommnissen im Öffentlichkeitsbereich	Medien, besondere Vorkommnisse	Telefon, E-Mail

[15] Bundesverwaltungsgericht (1. Instanz).
[16] Bundesgericht (letzte Instanz).

Von	Nach	Zweck	Datenart	Periodizität	Auslöser	Medium
EDÖB	Medien	Information der Öffentlichkeit	Tätigkeits-bericht	Jährlich Stellungnahme bei besonderen Vor-kommnissen	Gesetzliche Vorgaben Besondere Vorkommnisse	 Telefon, E-Mail
Parlament	EDÖB	Informieren, beraten		Bei Anfragen zum Öffentlichkeits-gesetz	Parlamentari-sche Kommis-sionen, Parlamentarier	Telefon, E-Mail
EDÖB	Parlament	Beraten, informieren		Bei Anfragen zum Öffentlichkeits-gesetz	Parlamentari-sche Kommis-sionen, Parlamentarier	Telefon, E-Mail

8.1. Organigramm des EDÖB



Das System EDÖB-Office wird von allen rund 30 (Teilzeit-) MitarbeiterInnen des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten benutzt.
Es besteht ein Informatikforum (IFE) EDÖB, deren Mitglieder in den Einheiten 1 und 2 vertreten sind. Im Forum werden u. a. technische und organisatorische Fragen analysiert und die Resultate der Geschäftsleitung unterbreitet.

8.2. Verantwortlichkeiten

Der EDÖB bestimmt als Leistungsbezüger die Anforderungen für die EDÖB Domäne.
Verantwortlich für die „Client-Applikation“ sowie die Administration der SQL-DB (Server) ist BY und sein Stellvertreter SP. Für die restliche Informatik ist ein externes Organ als Leistungserbringer zuständig.
JP nimmt beim EDÖB die Funktion als Superuser war.

8.3. Weitere wichtige Anwendungen beim EDÖB mit Schnittstellen zum EDÖB-Office

- Mit der Web-Applikation Datareg wird das Register der Datensammlungen geführt. Mit Hilfe dieser Anwendung können bereits angemeldete Datensammlungen gesucht, nachgeführt sowie neue Datensammlungen angemeldet werden.
- Die Website www.edoeb.admin.ch beinhaltet die Publikationen des EDÖB für die Öffentlichkeit, welche meist mit Hilfe des EDÖB-Office erstellt wurden.

9. Auflisten der Unterlagen über die Planung, Realisierung und den Betrieb der Datensammlung

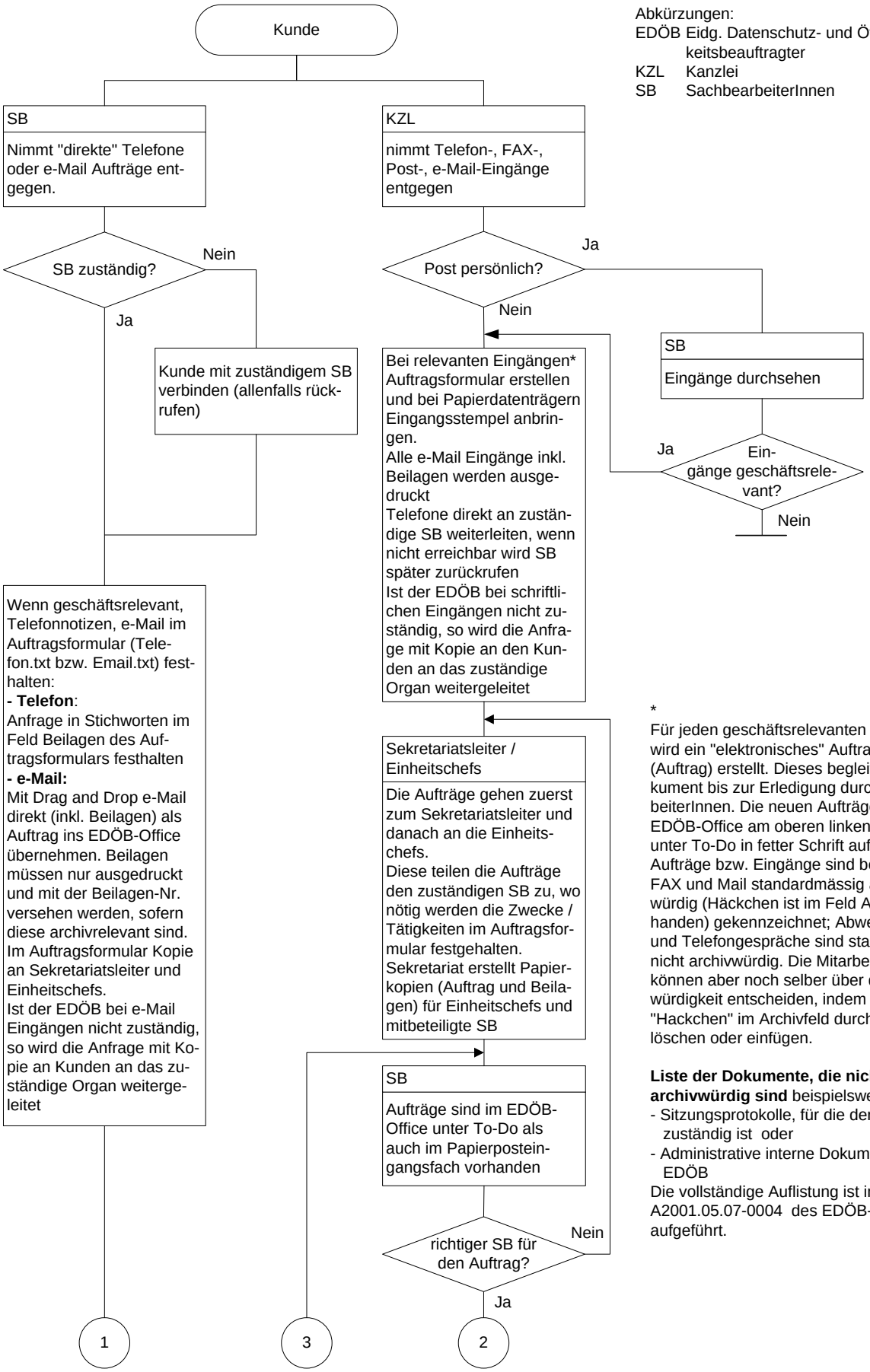
Planung:
Es wurde ein Projektantrag, eine Vorstudie, ein Konzept sowie ein Pflichtenheft gemäss HERMES erstellt. Dies ist ein Standard für die Führung und Abwicklung von Informatik-Projekten in der Bundesverwaltung.
Realisierung:
Die Realisierung bzw. Programmierung wurde an eine externe Firma vergeben. Die Realisierung erfolgte aufgrund eines Pflichtenhefts.
Betrieb:
Benutzerhandbuch (online abrufbar), Anwendungshandbuch (Ordner BY), Systemhandbuch, vorliegendes Bearbeitungsreglement

10. Anmeldung der Datensammlung beim EDÖB "Register der Datensammlung"

Siehe Anhang 1.

11. Abläufe

11.1. Ablauf Administration EDÖB



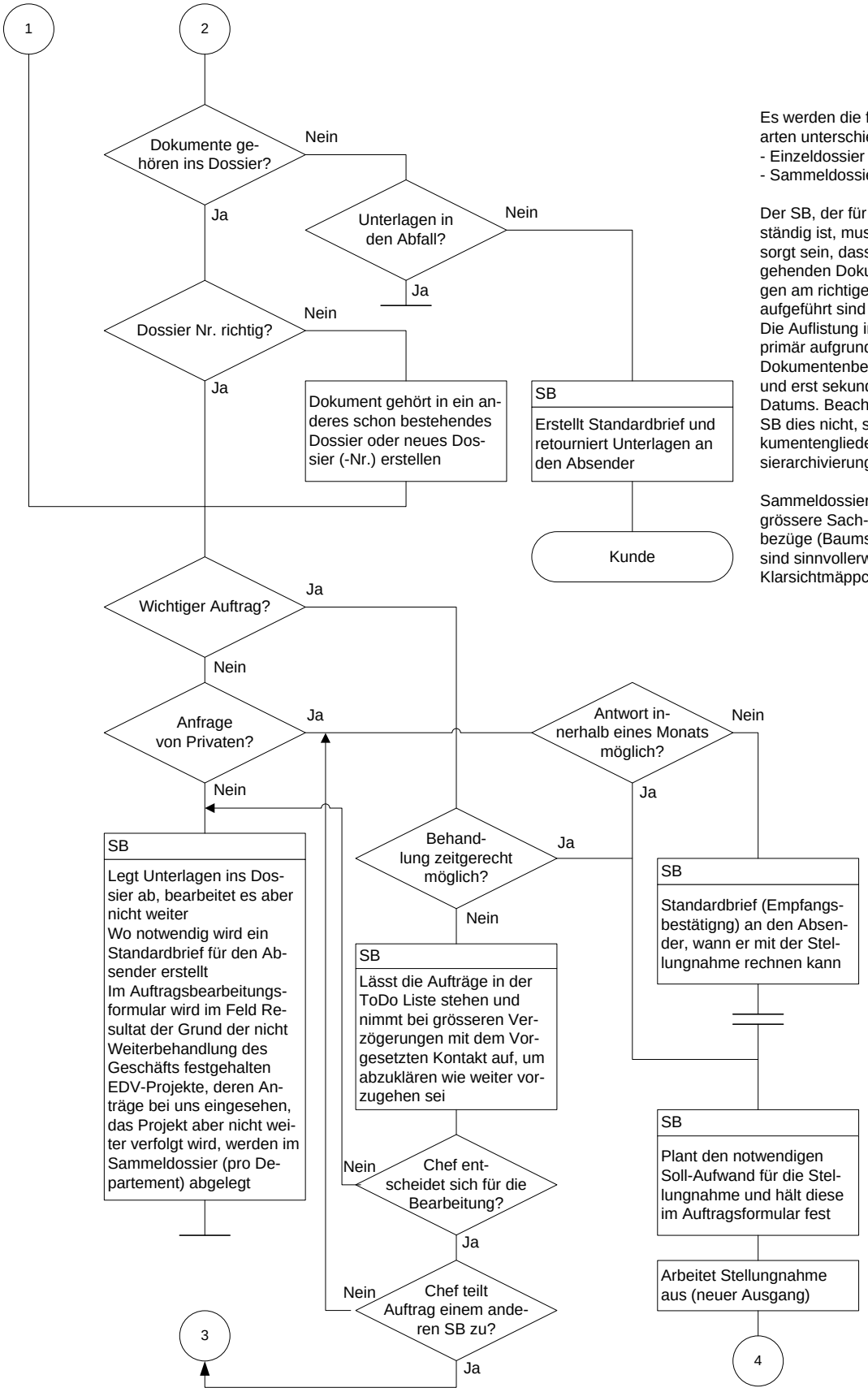
Bemerkungen:

Abkürzungen:
EDÖB Eidg. Datenschutz- und Öffentlichkeitsbeauftragter
KZL Kanzlei
SB SachbearbeiterInnen

*
Für jeden geschäftsrelevanten Eingang wird ein "elektronisches" Auftragsformular (Auftrag) erstellt. Dieses begleitet das Dokument bis zur Erledigung durch die MitarbeiterInnen. Die neuen Aufträge sind im EDÖB-Office am oberen linken Bildrand unter To-Do in fetter Schrift aufgeführt. Aufträge bzw. Eingänge sind bei der Post, FAX und Mail standardmässig als archivwürdig (Häckchen ist im Feld Archiv vorhanden) gekennzeichnet; Abwesenheiten und Telefongespräche sind standardmässig nicht archivwürdig. Die MitarbeiterInnen können aber noch selber über die Archivwürdigkeit entscheiden, indem sie das "Hackchen" im Archivfeld durch Anklicken löschen oder einfügen.

Liste der Dokumente, die nicht archivwürdig sind beispielsweise
- Sitzungsprotokolle, für die der EDÖB nicht zuständig ist oder
- Administrative interne Dokumente des EDÖB

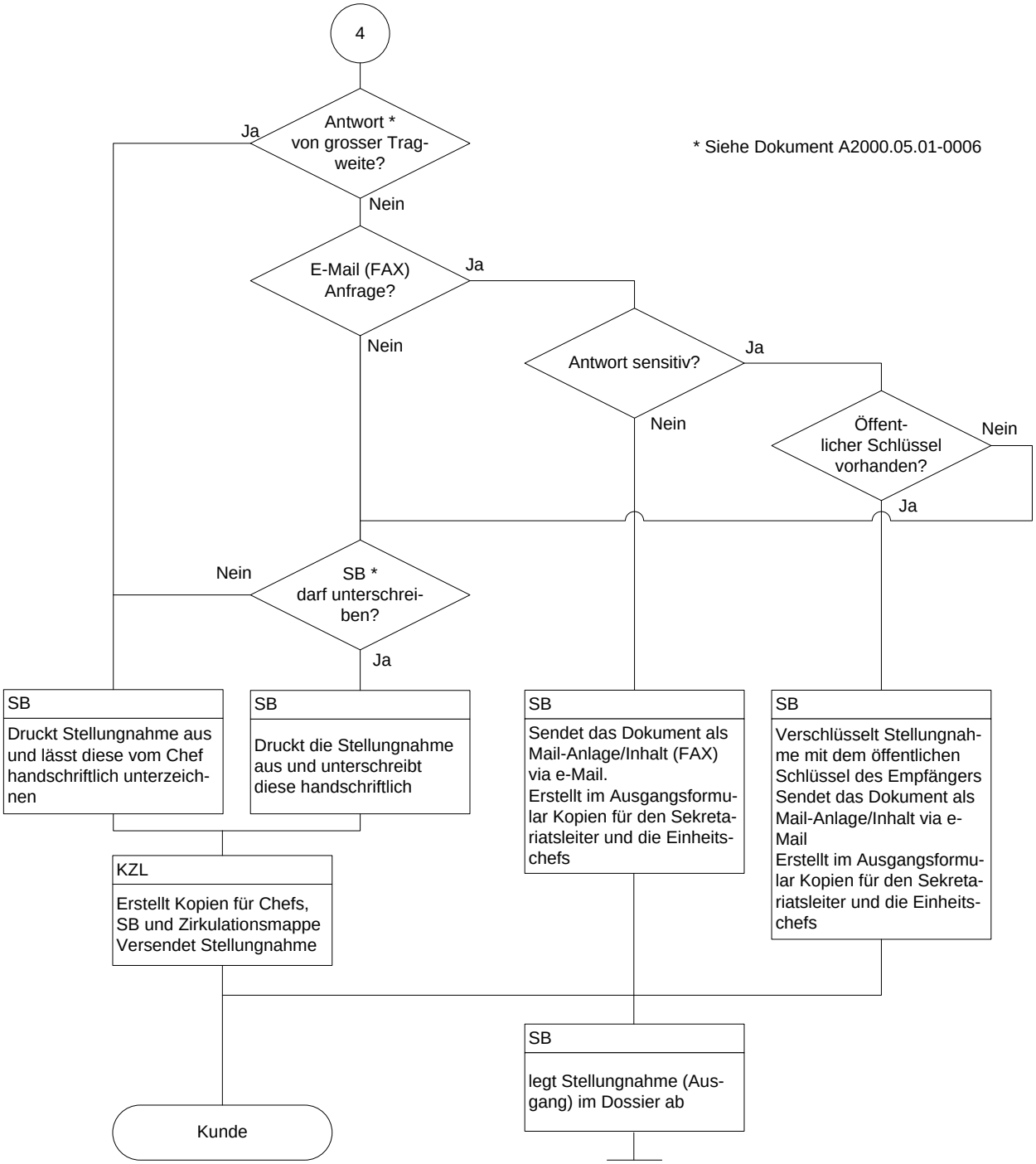
Die vollständige Auflistung ist im Dokument A2001.05.07-0004 des EDÖB-Offices aufgeführt.



Es werden die folgenden Dossierarten unterschieden:
- Einzeldossier
- Sammeldossier

Der SB, der für die Dossiers zuständig ist, muss immer dafür besorgt sein, dass die ein- und ausgehenden Dokumente sachbezogen am richtigen Ort im Dossier aufgeführt sind (Drag und Drop). Die Auflistung im Dossier erfolgt primär aufgrund des Sach- bzw. Dokumentenbezugs (Baumstruktur) und erst sekundär aufgrund des Datums. Beachtet der zuständige SB dies nicht, so muss er die Dokumentengliederung bei der Dossierarchivierung vornehmen.

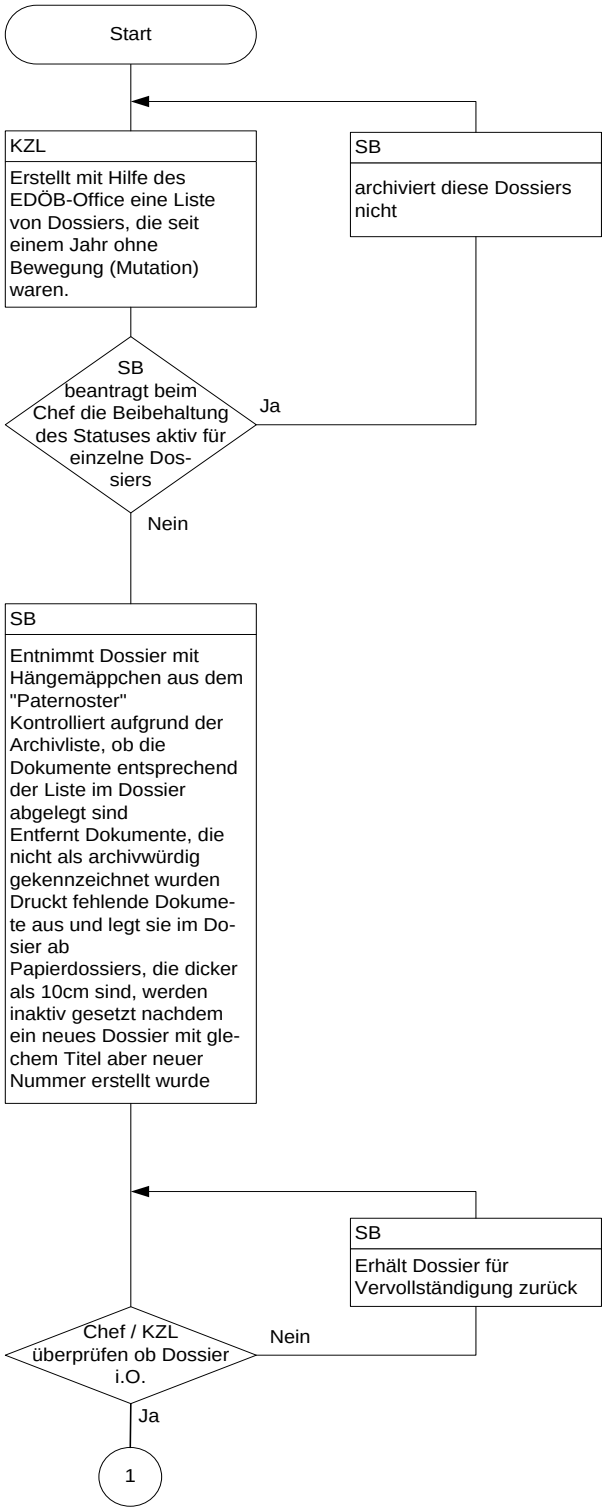
Sammeldossiers, die mehrere grössere Sach- bzw. Dokumentenbezüge (Baumstrukturen) haben, sind sinnvollerweise mit Hilfe von Klarsichtmäppchen zu unterteilen



Nach dem Unterschreiben oder dem Versenden des Dokuments ist das Kästchen erledigt auf dem Ausgangsformular (-Bildschirm) zu aktivieren. Das Dokument ist danach schreibgeschützt. Für wichtige Ausgänge wird das Kästchen Zirkulations-Mappe (Z-Mappe) aktiviert. Alle Ausgänge (Stellungnahmen), welche den EDÖB in Papierform verlassen, werden als Kopie in die Z-Mappe gelegt; mit Ausnahme der Stellungnahmen zu den Einsichtsgesuchen für die Datensammlung ISIS sowie die Prüfungsverfahren für die Datensammlungen JANUS, GEWA und SIS. Ausgänge, die für den Tätigkeitsbericht oder Publikationen vorgesehen sind, können durch Aktivierung des Kästchens für Publikation markiert werden. Ist der Auftrag abgeschlossen, so werden die IST-Stunden im Auftragsformular festgehalten und der Auftrag als erledigt gekennzeichnet.

Bemerkung zum Versenden der e-Mails
Versendet man das Dokument als Anhang, so entspricht die Formatierung beim Empfänger der e-Mail, der die Anlage öffnet, dem ursprünglichen Dokument. Dies hat allerdings den Nachteil, dass auch Daten versendet werden, die im Dokument selber nicht direkt erkennbar sind, aber bspw. durch einen Editor sichtbar gemacht werden können. Es ist sehr wichtig, dass keine Dokumente ungewollt als Anhang versendet werden, die im Word mit EXTRAS / ÄNDERUNGEN VERFOLGEN erstellt wurden, sonst kann der Empfänger die Änderungen bzw. den ursprünglichen Inhalt lesen.
Beim Versenden der Dokumente mit Mail Inhalt werden nur diejenigen Daten versendet, die am Bildschirm ersichtlich sind. Dieses Vorgehen hat allerdings den Nachteil, dass ein grosser Teil der Formatierung des Worddokuments nicht mehr vorhanden ist.

11.2. Ablauf Dossierarchivierung EDÖB / BAR



Bemerkungen

Abkürzungen:

BAR	Bundesarchiv
EDÖB	Eidg.Datenschutz- und Öffentlichkeitsbeauftragter
KZL	Kanzlei
SB	SachbearbeiterInnen

Grundsätzlich werden die Dokumente in den Dossiers sachbezogen bzw. dokumentenbezogen (Baumstruktur) und erst in zweiter Linie chronologisch nach Datum geordnet.
Der zuständige Sachbearbeiter ist für die Ordnung verantwortlich.

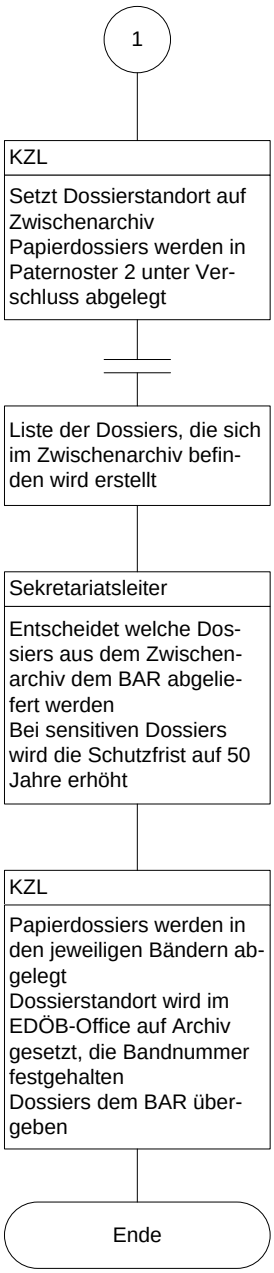
Die Archivliste des Dossiers führt alle Notizen (N) und die nicht archivwürdigen Aufträge (E) mit Punkten gekennzeichnet auf Bsp.: N ....., wenn diese bei der Erste-lung als nicht archivwürdig bezeichnet wurden. Diese sind - sofern sie in Papierform abgelegt sind - aus dem Dossier zu entfernen. Dokumente, die beim Eingang irrtümlich als archivrelevant registriert wurden, können mit Kugekschrei-ber auf der Liste durcgestricen werden und sind danach aus dem Dossier zu entfernen.

Büroklammern / Heftklammern (Bostitches), die verschie-dene Dokumente umfassen, sind zu entfernen. Die Doku-mente sind entsprechend der Reihenfolge der Archivliste im Dossier abzulegen

Es existiert eine Liste von Dokumenten, die gemäss BAR nicht archivwürdig sind, diese kann dem Dokument A2001.05.07-0004 des EDÖB-Office entnommen werden. Solche Eingänge bzw. Dokumente oder Notizen sind auch aus den Papierdossiers zu entfernen

Vor der Inaktivsetzung des Dossiers sind Verweise von der alten zur neuen Dossier-Nr. und umgekehrt festzuhalten. Der Dossiertitel, der gleich bleibt, ist fortlaufend zu numerieren

Nicht archivwürdige Dossiers müssen vom Vorgesetzten ebenfalls als solche betrachtet werden, dann kann der D-tenbank-Admin diese Dossiers auf elektronisch setzen und der SB kann diese danach löschen



Im Zwischenarchiv haben die SB keinen direkten Zugriff auf die Dossiers.
Die Schutzfrist ist mit 30 Jahren festgehalten. Bei besonders schützenswerten Personendaten oder Persönlichkeitsprofilen ist eine Schutzfrist von 50 Jahren vorzusehen (siehe Archivierungsgesetz BGA, SR 152.1 / 3. Abschnitt)

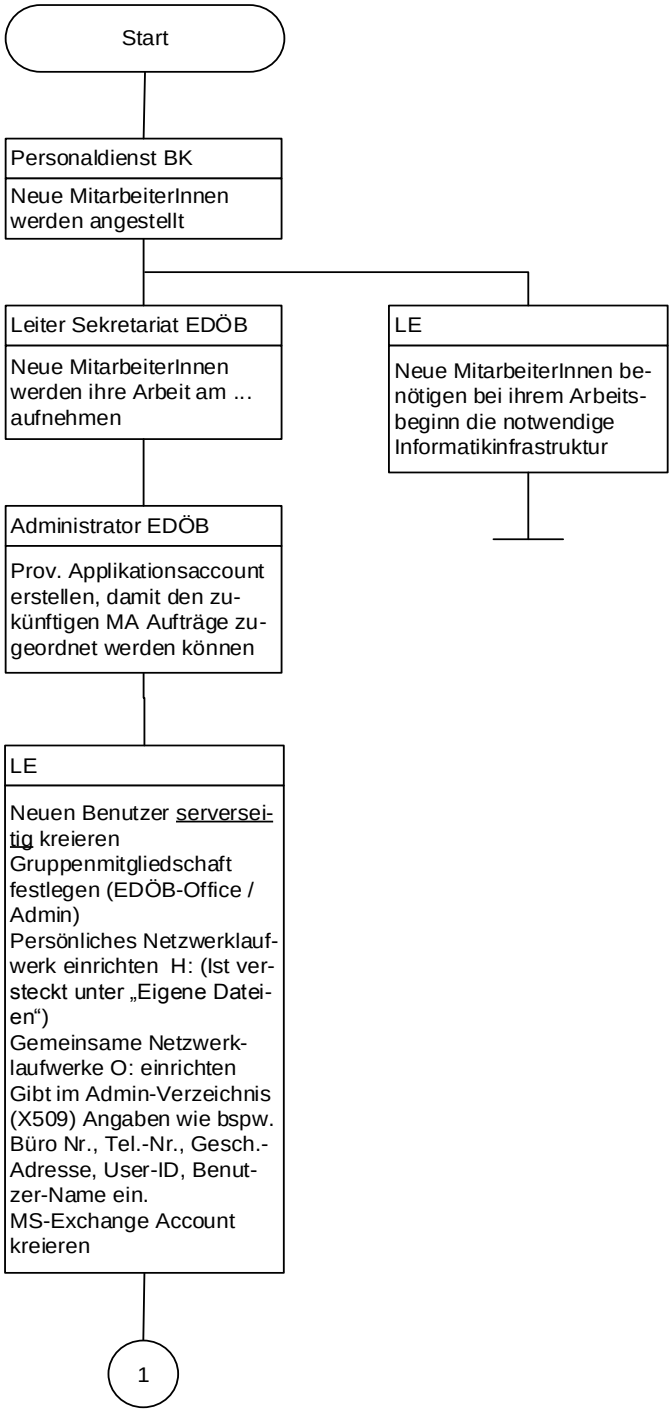
Bei der Archivierung der Dossiers erfolgt eine physikalische Löschung der Datenfelder „Zweck“, „Resultat“ sowie der „Ausgänge (OLE-Dokument wie Word, Excel, ...)“. Die restlichen Daten (Randdaten) verbleiben noch fünf Jahre im System und werden danach automatisch von einem SQL-Job physikalisch gelöscht.

Dem BAR wird neben den Papierakten noch ein e-Mail zugestellt, welches folgende Daten beinhaltet:
Dossiernummer (Aktenzeichen), Dossiertitel (Aktenbetreff), Dauer der Dossierführung (von bis), Bandnummer, Schutzfrist der zu archivierenden Dossiers.

Sobald auf Archiv gesetzt wird, werden die Inhalte im EDÖB-Office gelöscht.
Bei den Aufträgen ist dies: Beilage, Zweck, Resultat
Bei den Ausgängen und den Notizen: Alle OLE-Dokumente wie Word, Excel, Visio, … .
Die Randdaten bleiben noch 5 Jahre im System gespeichert, danach werden auch diese physikalisch gelöscht.

Dossierbeschaffung beim BAR
Für die Anforderung von archivierten Dossiers beim BAR, ist der KZL die Dossier-Nummer mitzuteilen.
Die KZL beantragt beim BAR mit Hilfe der folgenden Daten das Dossier:
- Ablieferungsnummer
- Dossiertitel (Aktenbetreff)
- Dossiernummer (Aktenzeichen)
- Band-Nummer

11.3. Ein- und Austritte der MitarbeiterInnen beim EDÖB

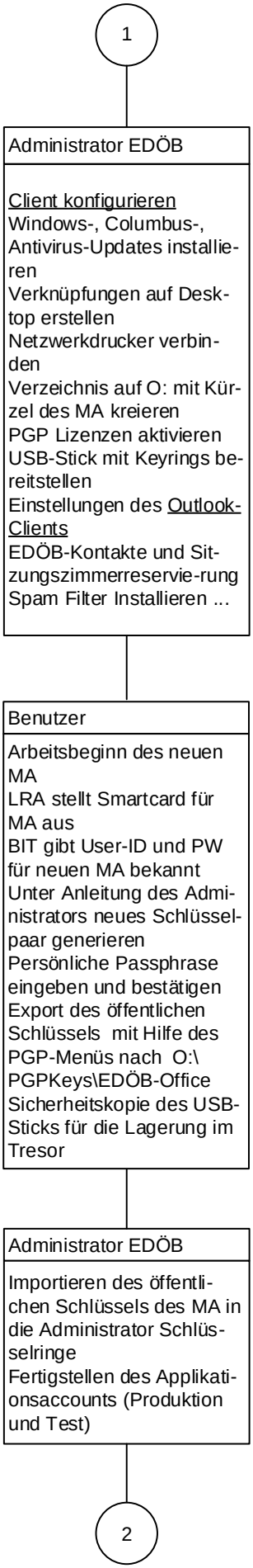


Bemerkungen:

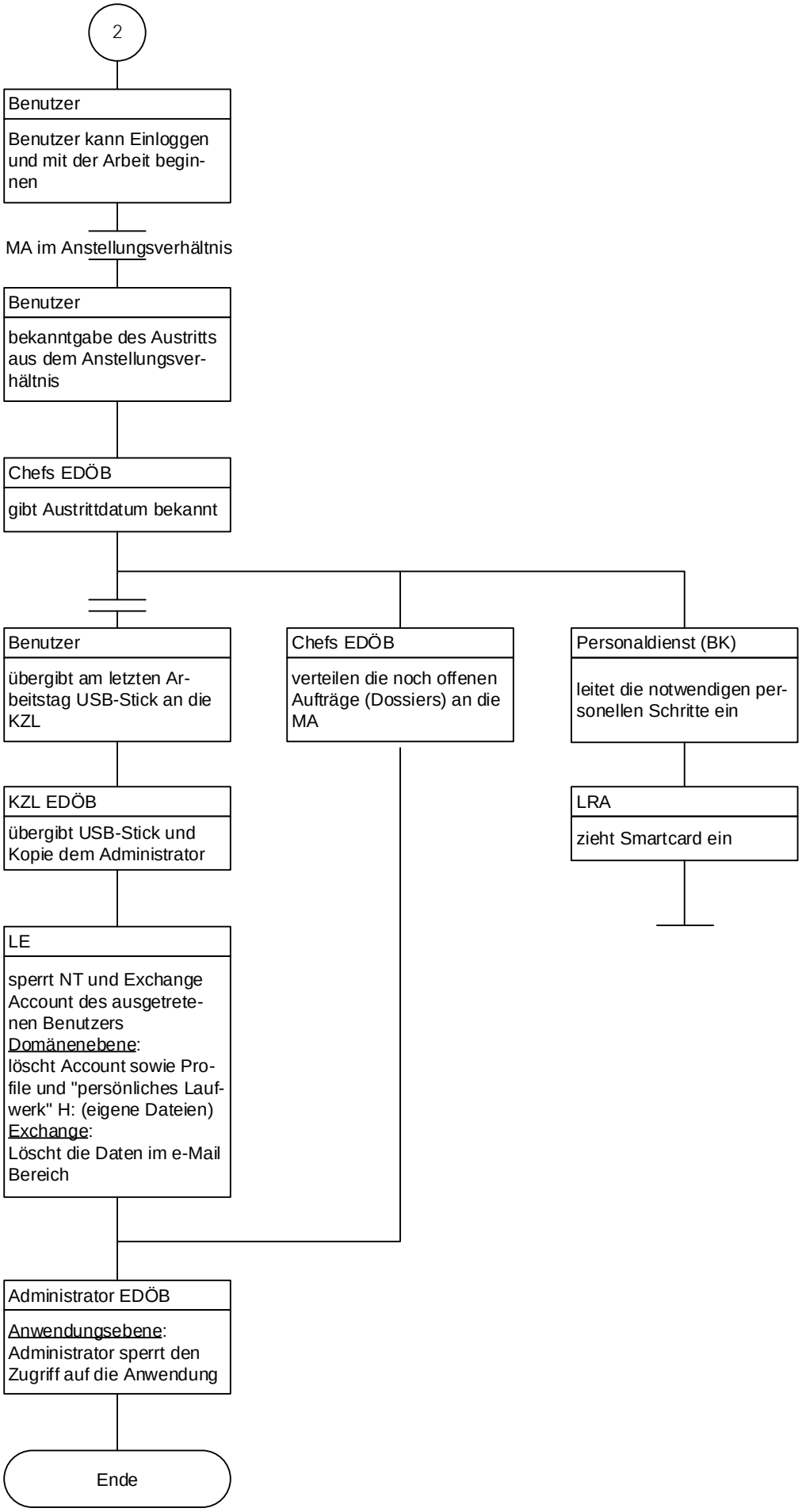
LE Leistungserbringer

KZL Kanzlei

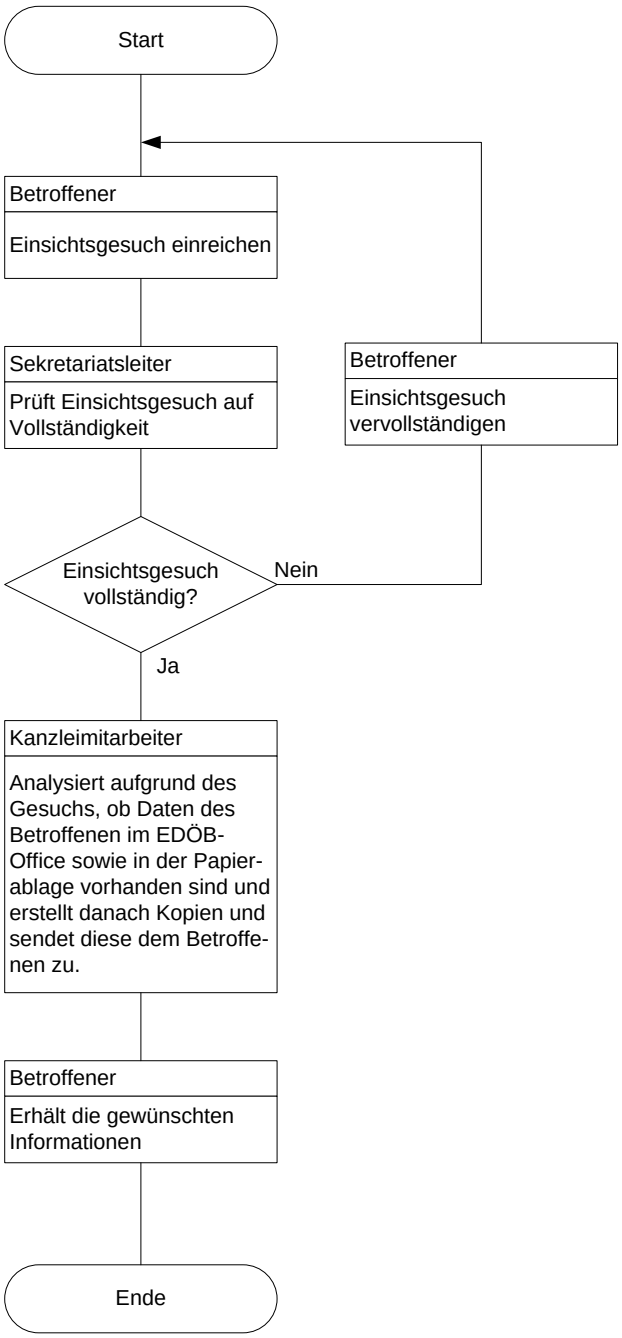
LRA Local Register Authority



Der Account „Test“ wird insb. auch dafür verwendet, dass sich der neue MA ins EDÖB-Office einarbeiten kann.

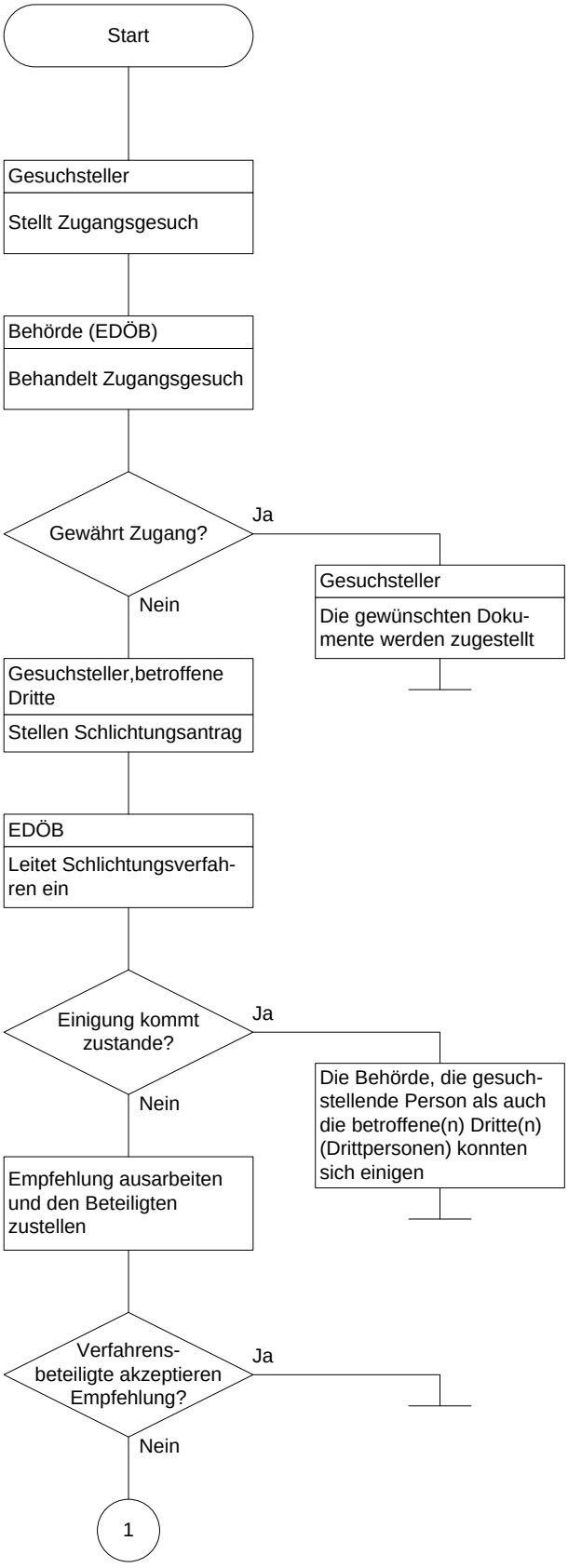

2
Benutzer
Benutzer kann Einloggen und mit der Arbeit beginnen
MA im Anstellungsverhältnis
Benutzer
bekanntgabe des Austritts aus dem Anstellungsverhältnis
Chefs EDÖB
gibt Austrittdatum bekannt
Benutzer
übergibt am letzten Arbeitstag USB-Stick an die KZL
Chefs EDÖB
verteilen die noch offenen Aufträge (Dossiers) an die MA
Personaldienst (BK)
leitet die notwendigen personellen Schritte ein
KZL EDÖB
übergibt USB-Stick und Kopie dem Administrator
LRA
zieht Smartcard ein
LE
sperrt NT und Exchange Account des ausgetretenen Benutzers
Domänenebene:
löscht Account sowie Profile und "persönliches Laufwerk" H: (eigene Dateien)
Exchange:
Löscht die Daten im e-Mail Bereich
Administrator EDÖB
Anwendungsebene:
Administrator sperrt den Zugriff auf die Anwendung
Ende

11.4. Auskunftsrecht beim EDÖB wahrnehmen



In den meisten Fällen gehen die Betroffenen irrtümlich davon aus, dass sie beim EDÖB Auskunft über alle Datensammlungen der Ämter der Bundesverwaltung verlangen können. Wir machend die Betroffenen dann darauf aufmerksam, dass sie das Auskunftsgesuch an die jeweiligen Ämter richten müssen.
(Standardbrief A2008.07.11-0002)

11.5. Zugang zu amtlichen Dokumenten gemäss dem Öffentlichkeitsgesetz (BGÖ)



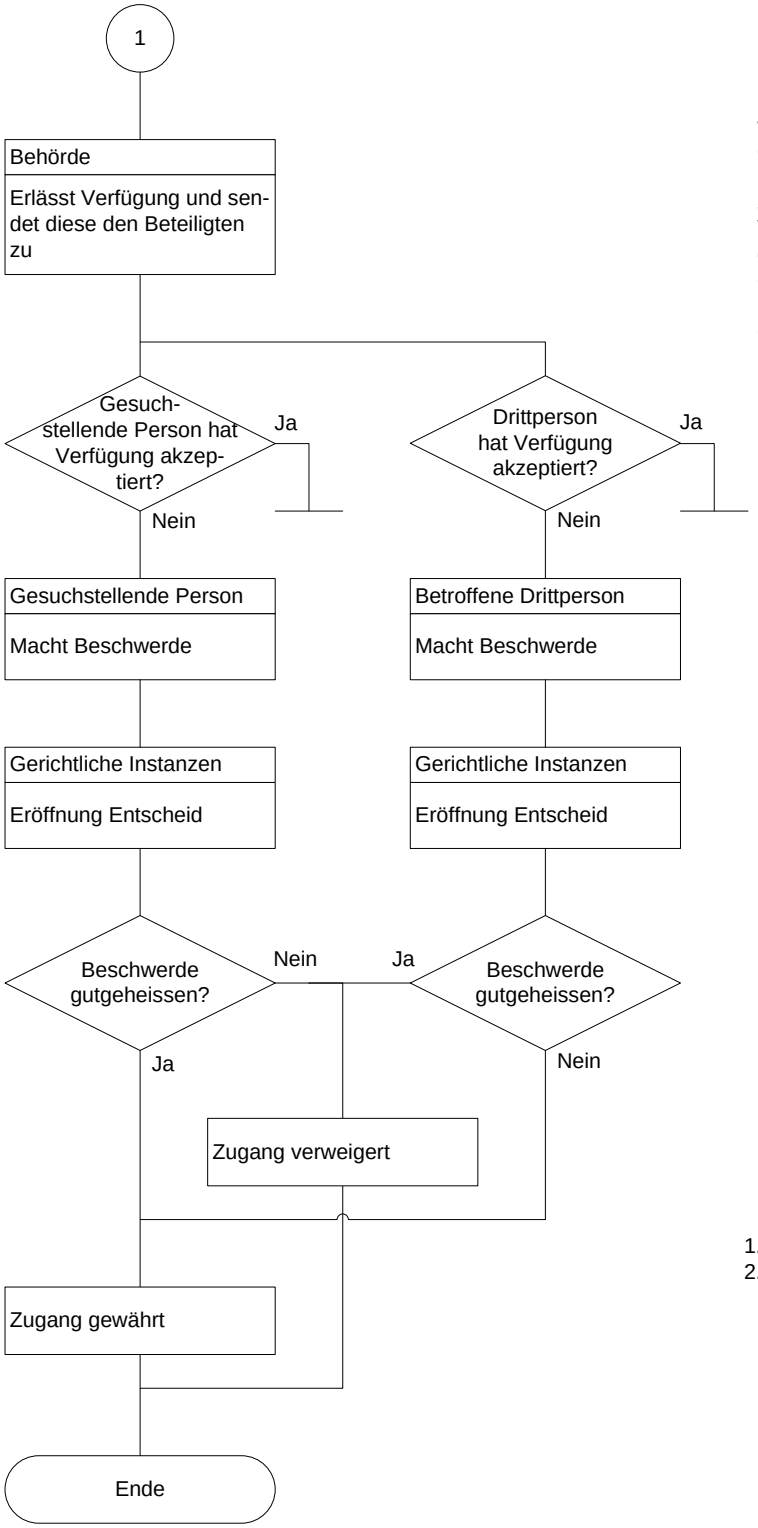
Bemerkungen

Zugang zu amtlichen Dokumenten

Der EDÖB ist dann als „Behörde“ und nicht als Öffentlichkeitsbeauftragter zu betrachten, wenn bei ihm ein Zugangsgesuch eingeht. Wird man sich in diesem Fall nicht einig über die Dokumentenherausgabe, so kann der EDÖB kein Schlichtungsverfahren durchführen und auch keine Empfehlung erlassen. In einem solchen Fall erlässt der EDÖB direkt eine Verfügung, die dann erstinstanzlich vom BVGer beurteilt werden muss.

Betroffene Dritte (Drittpersonen), sind solche Personen, die im einzusehenden Dokument bestimmbar sind und nicht anonymisiert werden können.

Einigung bedeutet:
- Behörde gewährt ganz, teilweise oder keinen Zugang; und
- Gesuchstellende Person ist einverstanden mit einer Beschränkung, dem Aufschub oder der Verweigerung des Zugangs; und
- Betroffene Drittperson erklärt sich mit der Zugänglichmachung ihrer Personendaten einverstanden



Eine **Verfügung** kann von der **gesuchstellenden Person und von der Drittperson verlangt** werden, wenn:
die **Behörde in Übereinstimmung mit der Empfehlung** das Recht auf Zugang einschränkt, aufschiebt oder verweigert
Von Amtes wegen, wenn die **Behörde entgegen der Empfehlung:**
- das Recht auf Zugang einschränken, aufschieben oder verweigern will; oder
- den Zugang zu einem Dokument, das Personendaten Dritter enthält, gewähren will

1. Instanz Bundesverwaltungsgericht BVGer
2. letzte Instanz Bundesgericht BGE

12. Das für den Datenschutz und die Datensicherheit verantwortliche Organ

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter.

13. Die Herkunft der Daten

Die Daten (inkl. Personendaten) stammen von den Organen, die in Kapitel 8 zur Dokumentation des EDÖB-Umsystems aufgeführt sind.

14. Die Zwecke, für welche die Daten regelmässig bekannt gegeben werden

In unserem Fall besteht nur eine fallbezogene Bekanntgabe von Personendaten für die Beratung, Information und Kontrolle von Anliegen des Datenschutz- oder des Öffentlichkeitsgesetzes.

15. Die Kontrollverfahren und insbesondere die technischen und organisatorischen Massnahmen

15.1. Kontrollverfahren

- In den Projektplanungs- und Realisierungsphasen wurde analysiert, inwiefern Sicherheitsvorgaben berücksichtigt bzw. umgesetzt wurden.
- Aus den dokumentierten Prozessen (siehe Abschnitt 11, Abläufe) geht hervor, wie die Aufgabenerfüllung mit Hilfe des EDÖB-Office Systems beim EDÖB abläuft. Eine transparente Darstellung der Aufgabenerfüllung von der Erhebung bzw. der Bearbeitung der Daten bis zu deren Archivierung oder Löschung ist damit gewährleistet.
- Stichprobenweise wird kontrolliert, ob die Büros bei längerer Abwesenheit abgeschlossen sind.
- Eine Überprüfung der Sicherheitsmassnahmen im EDV-Umfeld wurde zusätzlich durch externe Sachverständige vorgenommen (Unterlagen sind beim EDÖB vorhanden).
- Bei Austritten von MitarbeiterInnen wird der Zugriff auf die Anwendung gesperrt und der Zugriffs-USB-Stick von der Kanzlei des EDÖB eingezogen. Diese übergibt den Zugriffs-USB-Stick als auch dessen Kopie dem Applikationsverantwortlichen.

15.2. Technische und organisatorische Massnahmen

Zugangskontrolle

Der Zutritt zum Gebäude, in dem der EDÖB seine Büros hat, ist mit einem Badge gesichert. Ein Besucher kann beim Eingang mit Hilfe des installierten Telefons Kontakt mit den im Gebäude befindlichen Personen aufnehmen. Danach wird der Besucher beim Eingang abgeholt. Abends und bei längeren Pausen sind die Bürotüren abzuschliessen.
Zutritt zu den Räumlichkeiten, in denen sich die Papierdossiers befinden, haben alle Mitarbeiter des EDÖB. Der Zugang zum Paternoster, in denen sich die Papierdossiers befinden, ist nur mit einem Schlüssel möglich. Die Identifikation des Dossierstandorts im Paternoster erfolgt mit Hilfe des EDÖB-Office Systems.
Der Server befindet sich in einem externen Rechenzentrum. In diesem sind entsprechende Sicherheitsmassnahmen umgesetzt, die aus Sicherheitsgründen in diesem veröffentlichtem Bearbeitungsreglement nicht aufgeführt werden.

Datenträgerkontrolle

Bei den Datenträgern können wir grundsätzlich zwischen den “elektronischen“ Datenträgern im Rechenzentrum (RZ) und denjenigen bei den Clients unterscheiden.
Im RZ befinden sich Taperoboter als auch Diskspeichersysteme für die Backups. Aus Sicherheitsgründen bleiben die Sicherheitskassetten (Bänder) immer im Taperoboter. Durch Mehrfachauslegung ist ein allfälliger Datenverlust rekonstruierbar. Der Backup der Daten des EDÖB-Office ist wie folgt realisiert:

Periodizität	Backup-Art	Aufbewahrungsfrist
Monatlich	Vollsicherung	3 Monate
Wöchentlich	Vollsicherung	3 Wochen
Täglich	Inkrementelle Sicherung	7 Tage

Die Bandstation (High End Tapedrive) verifiziert nach dem Schreiben auf das Band, ob die Daten lesbar sind. Erfolgt keine Fehlermeldung so kann man davon ausgehen, dass die Daten richtig kopiert wurden.
Für die kontrollierte Entsorgung namentlich von Festplatten ist im BIT der Bereich „Bereitstellung und Support 4 (BSSU4)“ zuständig. Detailliertere Angaben dazu sind unten im Abschnitt Speicherkontrolle aufgeführt.
Auf der Clientseite (Computerarbeitsplatz) benötigen wir einen USB-Stick, auf denen sich die Schlüsselringe für die Chiffrierung befinden. Dieser USB-Stick wird bei längerer Abwesenheit (nachts, Wochenende) unter Verschluss aufbewahrt. Eine Kopie dieser Sticks der MitarbeiterInnen befindet sich in einem verschlossenen Briefumschlag an einem sicheren Ort.
Die ein- und ausgehenden Dokumente werden in den Dossiers in einem abschliessbaren Raum in einem abschliessbaren Behältnis gelagert. Sehr sensitive Dokumente oder Dossiers werden an einem speziellen Ort gelagert.
Dossiers, die sich am Arbeitsplatz befinden, müssen, sofern diese sensitiven Inhalt haben, nachts oder am Wochenende unter Verschluss aufbewahrt werden.
Für die Vernichtung von sensitiven Dokumenten, steht beim EDÖB ein Papiershredder zur Verfügung.

Transportkontrolle

Sensitive Stellungnahmen oder Informationen dürfen nicht in unchiffrierter Form mit Hilfe der elektronischen Post (E-Mail) oder dem Telefax versendet werden.
Im EDÖB-Office System sind die sensitiven Datenfelder bei der Übertragung (Client – Server) dem Stand der Technik entsprechend, verschlüsselt (Algorithmen CAST-128 und AES-256). Die Stellungnahmen an Dritte erfolgen in den meisten Fällen mit Hilfe der Briefpost in verschlossenen Kuverts (siehe auch Ablauf Administration EDÖB). In den folgenden Fällen werden die Briefe eingeschrieben versendet:

- wenn man sicher sein muss, dass der Empfänger die Stellungnahme erhalten hat
- beim Zustellen von Empfehlungen des EDÖB
- beim Weiterzug von Empfehlungen an die Departemente und die Bundeskanzlei
- Zustellung von Stellungnahmen für Gerichte oder Untersuchungsbehörden
- z. T. beim indirekten Auskunftsrecht
- z. T. beim Nachfassen, wenn Fristen nicht eingehalten wurden.

Wird eine Stellungnahme mit Hilfe der E-Mail zum Empfänger übertragen, so haben die Mitarbeiter/Innen dafür zu sorgen, dass die verborgenen Daten im Dokument gelöscht werden (In Word-03 bspw. : Datei / Remove Hidden Data).

Bekanntgabekontrolle

Aufgrund der Anschrift, die sich auf jeder Stellungnahme befindet, ist jeder Datenempfänger ausserhalb der Organisationseinheit EDÖB bestimmbar. Diese Angaben sind sowohl in Papierform als auch im System EDÖB-Office vorhanden.

Speicherkontrolle[17]

Der Grossteil der Daten ist auf den Festplatten in chiffrierter Form gespeichert. Neben dem produktiven System besteht noch ein Testsystem, welches eine separate Anwendung (EDÖB-Office) als auch eine logisch getrennte Datenbank (SQL) bzw. Datenbasis beinhaltet. Auf diesem System können die neuen Versionen oder Anpassungen zuerst ausgetestet werden. Erst wenn die Tests den Anforderungen entsprochen haben, wird die neue Version oder Anwendung auf dem produktiven System installiert (siehe auch Abschnitt 19 Konfiguration der Informatikmittel).
Beim Auswechseln von Datenspeichern (Festplatten) oder beim Ersatz von Computern (PC und Server) ist dafür zu sorgen, dass insb. die nicht chiffrierten Daten sowie der freie Speicherplatz vollständig physisch gelöscht werden. Dazu kann bspw. ein Tool mit den beiden Funktionen “unwiderherstellbar löschen“ und “freien Speicherplatz löschen“ verwendet werden. Ist der Zugriff auf die Festplatten bzw. Datenspeicher wegen Defekten am System nicht mehr möglich, so sind die Speicher oder das System fachgerecht zu entsorgen. Die Systeme sind grundsätzlich so zu vernichten, dass auf die gespeicherten interpretierbaren Daten nicht mehr zugegriffen werden kann**.** Das BIT bietet mit dem Bereich „Bereitstellung und Support 4 (BSSU4)“ eine Stelle an, die

[17] Siehe auch Abschnitt 19 “Konfiguration der Informatikmittel“.

defekte Systeme oder Datenträger entgegen nimmt. Die Servicetechniker (Supporter), welche die jeweiligen Systeme oder Datenträger entgegennehmen bzw. austauschen, übergeben die defekten Geräte der oben aufgeführten Organisationseinheit. BSSU4 bewahrt die defekten Geräte unter Verschluss auf und übergibt diese danach einer externen Firma zur fachgerechten Entsorgung. Diese Firma ist u. a. ISO 9001 und 14001 zertifiziert.
Durch das regelmässige Update von Betriebssystemen und Anwendungen werden Angriffe durch Malware minimiert. Der Zugang zu bekannten Malwaredomains und unbekannten IP Adressen ist auf der Proxy Infrastruktur des zuständigen Amtes gesperrt.
Die Festplatte des Kopiergerätes / Druckers wird jede Nacht physikalisch gelöscht, so dass nicht über eine längere Zeit nachvollzogen werden kann, wer wann was ausgedruckt / kopiert hat.

Benutzerkontrolle

Der Zugang zum EDÖB-Office System über Kommunikationsverbindungen ist gegenüber Fremdnetzen (Internet, kantonale Netze, ...) mit Firewalls geschützt. Es erfolgt eine Authentifizierung an der Domäne mit Smartcard und PIN und eine Weitere mit Benutzerkennung und Passwort sowie dem Einsatz eines USB-Sticks für den Zugang zum EDÖB-Office System.

Zugriffskontrolle[18]

Zwei-Faktor-Authentifizierung am Bundesclient.
Die Zugriffe auf Applikations-, Datenbank- und Betriebssystemebene sind im Bereich “Konfiguration der Informatikmittel“ detailliert aufgeführt.

Eingabekontrolle[19]

Die Nachvollziehbarkeit der Eingaben ist durch die Anwendung selbst gewährleistet. Auf Anwendungsstufe wird das Erstellungs- als auch das letzte Änderungsdatum sowie die Zeit festgehalten. Die wichtigen Informationen sind auf Papier festgehalten und handschriftlich unterzeichnet. Aus diesem Grund erübrigt sich eine umfassende Protokollierung im EDV-System.

16. Die Beschreibung der Datenfelder und die zugriffsberechtigten Organisationseinheiten

In der Folge werden nur die Datenfelder aufgeführt, die nicht technischer Art sind und von den MitarbeiterInnen beim EDÖB insb. im Zusammenhang mit dem EDÖB-Office benutzt werden. Zusätzlich bestehen noch Datenfelder, die für das Systemmanagement verwendet werden, die unten ebenfalls nicht aufgeführt sind. Den vollständigen Datenkatalog kann man dem Entity-Relationship-Model im Anwendungshandbuch entnehmen. Der Zugriff auf die unten aufgeführten Daten erfolgt aufgrund der Zugriffssteuerung, welche im Abschnitt “Konfiguration der Informatikmittel (Abschnitt 19)“ aufgeführt ist.

- Die Chefs haben auf alle Datenfelder und alle gespeicherten Dokumente online Zugriff
- Die MitarbeiterInnen haben auf alle EDÖB- und ihre persönlich verschlüsselten Dokumente online Zugriff
- Die MitarbeiterInnen, die zusätzlich für das indirekte Auskunftsrecht oder das Öffentlichkeitsprinzip (BGÖ) zuständig sind, haben auch auf die Dokumente ihrer Zuständigkeitsbereiche online Zugriff.

Feldname	Beschreibung
(Auftrag)	
Woher	Umschreibt Kommunikationsmittel, wie das Dokument bei uns eingetroffen ist, sowie die Auslösung eines internen Auftrags als auch der Absender der Anfrage
Verantwortlicher	Zeigt an, wer für den Auftrag zuständig ist
Wohin	Aus Liste auswählen, was mit dem Eingang/Auftrag geschehen soll
Auftragsnummer	Wird vom System vergeben (Bsp. E1999.05.16-0012)
Dossiernummer	System generiert automatisch bei der Erstellung eines neuen Dossiers die Dossier-Nr. (Jahr+fortlaufende Nr. Bsp. 1999-01167)
Dossiertitel	Auftrag wird kurz im Titel umschrieben bspw. Projekt XYZ
Betreff	Der Inhalt des Auftrags/Eingangs wird kurz umschrieben

[18] Siehe auch Abschnitt 19 “Konfiguration der Informatikmittel“.
[19] Siehe auch Abschnitt 19 “Konfiguration der Informatikmittel“.

Beilagen	Umschreibt Art und Anzahl der Beilagen / Kopie von eing. E-Mails
Kopie an	MitarbeiterInnen des EDÖB können Kopien „zugestellt“ werden
Neu	Sendet den überarbeiteten Auftrag wieder an die (bereits bestehenden) Empfänger „Kopie an“
Veranlasst durch	Kürzel der MA, welche Kopien veranlasst haben, wird angezeigt
Übermittelt von	Wenn Briefe bspw. von anderen, für die Frage nicht zuständige Organe an uns weitergeleitet werden, so wird dieses Organ festgehalten
Schreibberechtigung an	Wer hat neben der verantwortlichen Person auch noch Schreibberechtigung für diesen Auftrag
Zweck/Tätigkeiten	Ziel des Auftrags wird umschrieben sowie die Tätigkeiten, damit das Ziel erreicht werden kann
Resultat/Folgerng	Die Folgerungen aus dem Auftrag können festgehalten werden
Produkt	Aus einer Liste ist ein Produkt auszuwählen, welches am ehesten dem Auftrag zugeordnet werden kann
Sachgebiet	Auswahl des Sachgebiets, welches am besten das Dossier umschreibt
Frist	Auftrag kann vom Chef speziell vergeben werden. Die Prioritäten beinhalten Standardwerte für die Frist (siehe folgende Zeile)
Priorität	Auftrag ist in folgender Zeit zu erledigen: A ≤ 30 Tage; B ≤ 60 Tage; C ≤ 90 Tage; D = AdActa; E = Abwesenheit
Behandlungsdatum	Geplantes Behandlungsdatum des Auftrags
Soll-Dauer	Geplante Dauer für die Erledigung des Auftrags
Ist-Dauer	Dauer die benötigt wurde, um den Auftrag zu erledigen
Erledigt	Durch Aktivieren des Feldes wird der Auftrag als erledigt markiert
Archiv	Dieses Feld muss aktiviert sein, wenn der Auftrag archivwürdig ist
Abwesenheit	Sitzung intern/extern, Ferien, ..., inkl. Dauer
Schlüssel	Wahl bzw. Schlüssel der für die Datenbearbeitung verwendet wird
(Anhang)	
Dossiernummer	Jahr der Dossiererstellung mit Nummer (Bsp. 1999-01167)
Reaktion auf	Auftrags-Nr. wird angezeigt, aufgrund dessen man reagiert bzw. eine Stellungnahme ausarbeitet (EJJJJ.MM.TT-4stell.-Nr.)
Verantwortlich	Verantwortlicher für den Anhang
Geändert	Wer hat wann die letzte Änderung durchgeführt
Dossiertitel	Bezeichnung des Inhalts des Dossiers
Betreff	Betreff des Anhangs
OLE- Dokument	Anhang, welcher im Word geschrieben wurde
Kopie an	Hält fest, wer eine Kopie des Anhangs erhalten hat
Schreibberechtigung	Hält fest, wer für die Erstellung des Anhangs Schreibberechtigung hatte
Schlüssel	Wahl bzw. Schlüssel der bei der Anhangerstellung verwendet wurde
Erledigt	Anhang wird durch die Aktivierung dieses Feldes schreibgeschützt
(Dossier)	
Dossiernummer	Jahr der Dossiererstellung mit Nummer (Bsp. 1999-01167)
Dossiertitel	Bezeichnung des Inhalts des Dossiers
Verantwortlicher	Verantwortliche(r) Mitarbeiter/In für das Dossier
Org. Einheit	Organisationseinheit, aufgrund derer das Dossier geführt wird
Sachgebiet	Auswahl des Sachgebiets, welches am besten das Dossier umschreibt
Verweise	Verweis auf andere „ähnliche“ Dossiers
Beteiligte	Festhalten von anderen Personen, die am Dossier beteiligt sind
Kategorie	Auswahl der Kategorie, welche am besten das Dossier umschreibt
Status	Status des Dossiers (Aktiv, Inaktiv, Archiviert)
Schreibberechtigung an	Schreibberechtigung für das Dossier kann auch für andere MitarbeiterInnen vergeben werden
Standort	Standort des Dossiers (letzte Phase) ist aufgeführt
Geändert	Datum der letzten Änderung im Dossier
“Inhalt“	Ist eigentlich kein Feld, sondern ein Fenster, welches den Inhalt des Dossiers mit den Aufträgen, Ausgängen und Notizen sowie deren Verknüpfungen auflistet

(Ausgang)	
Dossiernummer	Jahr der Dossiererstellung mit Nummer (Bsp. 1999-01167)
Reaktion auf	Auftrags-Nr. wird angezeigt, aufgrund dessen man reagiert bzw. eine Stellungnahme ausarbeitet (EJJJJ.MM.TT-4stell.-Nr.)
Verantwortlicher	Verantwortlicher für den Ausgang
Geändert	Wer hat wann die letzte Änderung durchgeführt
Wohin	Auswahl von Brief, Mail-Inhalt / Anlage (in Verb. mit Empfänger)
Dossiertitel	Bezeichnung des Inhalts des Dossiers
Empfänger	Adresse des Empfängers des Ausgangs bzw. der Stellungnahme
Ausgangsnummer	Wird automatisch vom System generiert (AJJJJ.MM.TT–4stell.-Nr.)
Gesendet	Gibt Datum und Zeit an, an dem das Dokument dem Postausgang im MS-Outlook übergeben wurde
Betreff	Ausgangsbetreff wird festgehalten
OLE- Dokument	Dokument wird angezeigt, kann durch Doppelklick geöffnet werden
Kopie an	Hält fest, wer eine Kopie des Ausgangs erhalten hat
Neu	Sendet den überarbeiteten Ausgang wieder an die (bereits bestehenden) Empfänger „Kopie an“
Für Publikation	Ausgang für den Tätigkeitsbericht vorsehen
Z-Mappe	Ausgang (Dokument) soll in der Zirkulationsmappe erscheinen
Erledigt	Dokument ist durch die Aktivierung dieses Feldes schreibgeschützt
Schreibberechtigung	Hält fest, wer für die Erstellung des Ausgangs Schreibberechtigung hatte
Schlüssel	Wahl bzw. Schlüssel, der bei der Ausgangerstell. verwendet wurde
(Notizen)	
Notiznummer	Wird bei der Erstellung vergeben (NJJJJ.MM.TT- fortlaufenden Nr.)
Dossiernummer	Jahr der Dossiererstellung mit Nummer (Bsp. 1999-01167)
Reaktion auf	Auftrags-Nr. wird angezeigt, aufgrund dessen man reagiert bzw. eine Stellungnahme ausarbeitet (EJJJJ.MM.TT-4stell.-Nr.)
Verantwortlich	Verantwortlicher für den Ausgang
Geändert	Wer hat wann die letzte Änderung durchgeführt
Dossiertitel	Bezeichnung des Inhalts des Dossiers
Betreff	Betreff der Notiz
OLE- Dokument	Notiz, welche im Word geschrieben wurde
Kopie an	Hält fest, wer eine Kopie des Ausgangs erhalten hat
Neu	Sendet das überarbeitete Dokument wieder an die (bereits bestehenden) Empfänger „Kopie an“
Schreibberechtigung	Hält fest, wer für die Erstellung der Notiz Schreibberechtigung hatte
Schlüssel	Wahl bzw. Schlüssel, der bei der Notizerstellung verwendet wurde
Erledigt	Notiz wird durch die Aktivierung dieses Feldes schreibgeschützt
(Adresse)	
Kurzname	Abkürzung der Namen (inkl. Firmennamen und Vornamen (Max. 7 Stellen des Namens und eine Stelle des Vornamens)
Art	Liste, aus der man bspw. Privatperson, Firma, ... auswählen kann
Status	Werden Adressen während dreier Jahre nicht mehr benutzt, so setzt die KZL diese auf inaktiv. Fünf Jahre später löscht die Applikation diese inaktiven Adressen physisch.
Adresse	Adresse von Absender und Empfänger
Erstellt	Person, welche die Adresse erstellt hat sowie Datum und Zeit
Letzte Änderung	Person, welche die Adresse zuletzt geändert hat sowie Datum u. Zeit
Sprache	Sprache in der die Adresse festgehalten wurde
Telefon	Telefonnummer von Absender und Empfänger (soweit vorhanden)
Telefax	Telefaxnummer von Absender und Empfänger (soweit vorhanden)
Email	E-Mail Adresse von Absender und Empfänger (soweit vorhanden)
Versand	Feld für die Auswahl von Gruppen für den Versand von Infos
(Volltextsuche)	

(Standortliste) **(Archivliste)**	Eine Volltextsuche mit Verknüpfungsmöglichkeiten (und, oder, und nicht) ist in den Worddokumenten (EDÖB-Schlüssel) möglich. Im Weiteren wird in den Feldern Dossiertitel und Betreff als auch in den Aufträgen in den Feldern Beilage, Zweck und Resultat gesucht werden Unter anderem durch Eingabe der Dossiernummer oder des Mitarbeiterkürzels (alle, Ablage, Zwischenarchiv, Archiv, gelöscht (Dossier nicht archivwürdig)) kann festgestellt werden, an welchem Ort sich ein Dossier befindet Unter anderem durch Eingabe der Dossiernummer oder des Mitarbeiterkürzels oder der Phase (alle, Ablage, Zwischenarchiv, Archiv) kann festgestellt werden, an welchem Ort sich ein Dossier befindet. Durch aktivieren eines Dossiers kann der "archivierbare" Inhalt des Dossiers angezeigt werden

Die oben in kursiver Form aufgeführten Datenfelder sowie das Feld, welches die Dokumentennummern beinhaltet, auf welche das entsprechende Wort des Indexes zeigt, werden in chiffrierter Form bearbeitet.

In Anhang 2 finden Sie die drei wichtigsten Bildschirmmasken "Auftrag, Dossier und Ausgang" aufgeführt.

17. Art und Umfang des Zugriffs der Benutzer der Datensammlung

Mit dem System kann nach den folgenden Kriterien (Arten) bzw. Datenfeldern gesucht werden:

- nach Adressen
  Kurzname der Adresse
- Versand
  Dient der Identifikation von Adressgruppen, wie z. B. Datenschutzberater, Medien, ...
- Dossier
  Dossier-Nr., SB, Kategorie, Sachgebiet, Dossiertitel, Org.-Einheit, Status des Dossiers
- Aufträge
  Datum (von-bis), Auftrags-Nr., Absender, SB, Betreff, Produkt, Status des Auftrags, Art
- Ausgänge
  Datum (von-bis), Ausgangs-Nr., Dossier-Nr., Empfänger, SB, Betreff, Produkt, Status des Ausgangs, Publikation, Art
- Notizen
  Datum (von-bis), Notiz-Nr., Dossier-Nr., SB, Betreff, Status der Notiz, Art
- Volltext
  Suche nach Dokumenten mit Verknüpfungsmöglichkeiten (und, oder, und nicht)

Weitere Angaben zu den Zugriffsregelungen sind unter Abschnitt 19 "Konfiguration der Informatikmittel" aufgeführt.

18. Die Datenbearbeitungsverfahren, insbesondere die Verfahren bei der Berichtigung, Sperrung, Anonymisierung, Speicherung, Aufbewahrung, Archivierung oder Vernichtung der Daten

Die Datenbearbeitungsverfahren sind zum grossen Teil eingangs in den Ablaufschemen aufgeführt. In der Folge gehen wir noch spezifisch auf die obigen, im Titel festgehaltenen, Verfahren ein.
Berichtigung (Sperrung, Vermerk): Aufgrund des Systems kann der Betroffene jederzeit seine Anregungen oder Vermerke (bspw. In Form von Stellungnahmen) in die Datensammlung einbringen.
Normalerweise gelangen keine Personendaten an Dritte. Ausnahmen bestehen für die Weitergabe von Daten an Untersuchungsbehörden oder wenn z. B. kantonale Datenschutzbeauftragte für Anfragen zuständig sind. Eine Sperrung der Daten spielt in der vorliegenden Anwendung, wenn überhaupt nur eine begrenzte Rolle.

Anonymisierung (Pseudonymisierung) der Daten:
Bei Veröffentlichungen werden die Daten weitmöglichst anonymisiert, soweit nicht ein überwiegendes öffentliches Interesse für eine Nichtanonymisierung besteht.

Speicherung / Aufbewahrung / Archivierung / Vernichtung der Daten:
Erfolgt während einer Zeitdauer von einem Jahr keine Bewegung im Dossier, so wird dieses für die Archivierung vorgeschlagen. Die Beibehaltung des Dossiers kann mit Einverständnis des Chefs um ein weiteres Jahr verlängert werden. Die Dossiers werden vom zuständigen Sachbearbeiter bereinigt und für die Archivierung bereitgestellt. Die Randdaten werden noch fünf Jahre im EDÖB-Office gespeichert, bevor diese gelöscht werden. Siehe auch Ablauf Dossierarchivierung EDÖB /BAR, Abschnitt 11.2.

Die betroffene Person kann ihr Berichtigungs-, Vernichtungs- und Sperrecht beim EDÖB geltend machen. Falls der EDÖB dem Gesuch der betroffenen Person nicht oder nur teilweise stattgibt, teilt er ihr dies in einer Verfügung mit.

19. Die Konfiguration der Informatikmittel

Die Grafik und ein Teil der Beschreibung wird aus Sicherheitsgründen im veröffentlichten Reglement nicht aufgeführt.

19.1. Anwendung

EDÖB-Office
EDÖB-Office Version 2.0.2 (Visual Basic Runtime). Der EDÖB ist im Besitz des Source-Codes dieser Anwendung. Diese verwendet Verschlüsselungswerkzeuge und MS-Office als Büroautomationstools.

Kurze Umschreibung der Anwendung
Die Anwendung ist ein System, welches alle geschäftsrelevanten Eingänge (Anfragen von Kunden) als auch unsere Stellungnahmen (Ausgänge) oder Notizen im Dossier ablegt. Alle Datenbestände werden automatisch und verständlich nummeriert. So hat beispielsweise der dritte Eingang (Auftrag) vom 17. November 2000 folgende Nummerierung (E2000.11.17-0003). Zusammengehörende Dokumente sind im elektronischen Dossier verkettet (Baumstruktur). So gehört z. B. zu einem Eingang (E) ein Ausgang (A) und oder eine Notiz (N) usw. (siehe Anhang 2, Bildschirmmaske “Dossier“). Zusätzlich kann im Auftrag die Zeit geplant werden. Anfangs trägt man die Soll-Zeit ein und nach Erledigung des Auftrags die benötigte Ist-Zeit. Im Weiteren kann der EDÖB eine Statistik erstellen, in der festgehalten wird, für welche Produkte und Sachgebiete wie viel Zeit aufgewendet wurde.

Rollen:	Die Anwendung unterstützt die folgenden 4 Rollen: Kanzlei (KZL), Chefs, Administratoren und SachbearbeiterInnen (SB).
Login:	Nur mit Besitz des USB-Sticks möglich, auf der sich die Schlüssel für die Ver- bzw. Entschlüsselung befinden und unter Eingabe der Passphrase, die mindestens 10 Zeichen lang sein muss. Die Passphrase ist namentlich so zu gestalten, dass Gross- und Kleinschreibung als auch Sonderzeichen verwendet werden.
Berechtigungen:	Man kann anderen MitarbeiterInnen eine Schreiberechtigung für das Dokument vergeben
Schreibschutz:	Ist das Dokument vervollständigt und versendet, so kann mit Hilfe des Befehls erledigt ein Schreibschutz gesetzt werden.
Löschen:	Fehlerhafte Aufträge oder Dokumente werden nur logisch gelöscht. Nach einem Jahr erfolgt die physische Löschung. Tempörare-Dateien werden physisch mit wipe gelöscht (löschen und überschreiben).

Die Anwendung besteht aus den folgenden Dateien; diese befinden sich in den beiden folgenden Verzeichnissen:

Dateiname	Dateibeschreibung
C:\Programme\EDSB\EDSB.exe	Applikation EDÖB
C:\Programme\EDSB\EDSB.chm	Hilfedatei
C:\Programme\EDSB\EdsbData.dll	Programmbibliothek für die Anwendung
C:\Programme\EDSB\SumatraPDF.exe	Portable PDF Viewer
C:\Programme\redemption\Redemption.dll	Wrapper für Outlook
C:\Windows\SYSTEM32\NSDPGP3.dll	Wrapper für PGP

Die Verschlüsselungstechnik funktioniert wie folgt:
Intern: Die Dokumente bzw. Datenfelder werden mit dem symmetrischen 256 Bit AES bzw. ältere Daten mit dem CAST-128 Algorithmus verschlüsselt (verborgener Dokumentenschlüssel).
Extern: 2048 Bit asymmetrische Diffie-Hellman (DH) Algorithmus Verschlüsselung. Der Dokumentenschlüssel ist mit dem öffentlichen Schlüssel der Zielverschlüsselungsgruppe (bspw. EDÖB-Schlüssel) verschlüsselt. Mit Hilfe des privaten Schlüssels, welcher mit der Passphrase geschützt ist, kann jedes Mitglied der entsprechenden Verschlüsselungsgruppe den verborgenen Dokumentenschlüssel für die Entschlüsselung aktivieren.

Zugriffssteuerung (Ver- und Entschlüsselung):
Jeder Benutzer benötigt für das Arbeiten mit der Applikation EDÖB-Office ein Schlüsselpaar des persönlichen und des EDÖB-Schlüssels. Für die herkömmliche Aufgabenerfüllung werden die Daten mit dem öffentlichen EDÖB-Schlüssel verschlüsselt. Alle MitarbeiterInnen des EDÖB können diese Daten mit dem privaten Schlüssel des EDÖB-Schlüssels entschlüsseln und somit einsehen. Mit dem persönlichen Schlüsselpaar können die MitarbeiterInnen Daten bearbeiten, die zusätzlich nur von den Chefschlüsseln einsehbar sind. Die mit den Chefschlüsseln bearbeiteten Daten, können nur mit Hilfe der Chefschlüssel eingesehen werden. Im Weiteren existieren noch Gruppenschlüssel für das indirekte Auskunftsrecht und das Öffentlichkeitsprinzip (BGÖ), diese werden von zwei kleineren Gruppe von MitarbeiterInnen benötigt.

Grafische Darstellung der Verschlüsselungsgruppen (Zugriffe):

<table>
<tr><td colspan="4">Chefschlüsselpaar</td></tr>
<tr><td>Gruppenschlüssel-paar für das Öffen-tlichkeitsgesetz (BGÖ)</td><td>Guppenschlüssel-paar für das indi-rekte Auskunfts-recht</td><td>EDÖB-Schlüsselpaar</td><td>Persönliches Schlüsselpaar</td></tr>
</table>

Mit Hilfe des Chefschlüssels hat man Zugang zu allen Informationen, die mit einem der oben aufgeführten Schlüssel verschlüsselt wurde.
Mit dem EDÖB-Schlüsselpaar, den alle MitarbeiterInnen beim EDÖB zur Verfügung haben, sind rund 95% der gespeicherten Daten einsehbar.

Die folgenden Schlüsselringe bestehen:
MitarbeiterInnen welche zur EDÖB-Gruppe gehören (der Grossteil der MA beim EDÖB)

	Privater Schlüssel	Öffentlicher Schlüssel
Persönlicher Schlüssel des MA	Ja (Passphrase notwendig)	Ja
EDÖB Schlüssel	Ja	Ja
Chef Schlüssel	Nein	Ja
Drucker Schlüssel	Nein	Ja

Für den privaten Schlüssel des EDÖB-Schlüsselpaares müssen die MitarbeiterInnen keine explizite Passphrase eingeben. Die Passphrase für den privaten Schlüssel des EDÖB-Schlüsselpaares ist in der Mitarbeiter-Tabelle der Datenbank gespeichert. Diese ist mit dem öffentlichen Schlüssel des persönlichen Schlüsselpaares der MitarbeiterInnen verschlüsselt. Beim Einloggen ins EDÖB-Office geben die MitarbeiterInnen die Passphrase für den privaten Schlüssel des persönlichen Schlüsselpaares ein.

Grundsätzlich haben alle MitarbeiterInnen des EDÖB mindestens zwei asymmetrische Schlüsselpaare (persönliches und EDÖB Schlüsselpaar) im EDÖB-Office zur Verfügung (USB-Stick).
Asymmetrische Schlüsselpaare beinhalten einen öffentlichen und einen privaten Schlüssel. Mit dem öffentlichen Schlüssel verschlüsselt man die Daten und mit dem privaten Schlüssel kann man diese wieder entschlüsseln. Der Zugriff auf den privaten Schlüssel wird durch ein Passwort (Passphrase) geschützt.

MitarbeiterInnen des EDÖB, welche zusätzlich zu einer speziellen Gruppe mit Gruppenschlüssel gehören:

	Privater Schlüssel	Öffentlicher Schlüssel
Persönlicher Schlüssel des MA	Ja (Passphrase notwendig)	Ja
EDÖB Schlüssel	Ja	Ja
Gruppenschlüssel	Ja (Passphrase notwendig)	Ja
Chef Schlüssel	Nein	Ja
Drucker Schlüssel	Nein	Ja

MitarbeiterInnen des EDÖB, die eine Cheffunktion inne haben:

	Privater Schlüssel	Öffentlicher Schlüssel
Persönlicher Schlüssel des MA	Ja (Passphrase notwendig)	Ja
EDÖB Schlüssel	Ja	Ja
Chef Schlüssel	Ja (Passphrase notwendig)	Ja
Drucker Schlüssel	Nein	Ja

MitarbeiterInnen, die Administratorenfunktionen der Anwendung wahrnehmen:

	Privater Schlüssel	Öffentlicher Schlüssel
Persönlicher Schlüssel des MA	Ja (Passphrase notwendig)	Ja
Schlüssel anderer MA	Nein	Ja
EDÖB Schlüssel	Ja (Passphrase notwendig)	Ja
Schlüssel anderer Gruppen	Nein	Nein
Chef Schlüssel	Nein	Ja
Drucker Schlüssel	(Ja Passphrase notwendig)	Ja
Service Schlüssel	(Ja Passphrase notwendig)	Ja

Beim Booten des Druckerservers wird die Passphrase von der lokalen Registry eingelesen und dekodiert. Der Service Schlüssel wird für die Indexerstellung der DB benötigt. Dies geschieht auf einem anderen virtuellen Server.

Index:
Der Index für die Freitextsuche im Dokument konnte aufgrund der zu grossen Leistungsbeeinträchtigung nicht vollständig chiffriert werden. Nur die Dokumentennummer, nicht aber die Wörter, die auf diese Nummern zeigen, können chiffriert werden. Sobald man in der Anwendung speichern wählt, wird das Dokument vom Client zum Server übertragen. Dies erfolgt indem das Dokument mit dem öffentlichen EDÖB-Schlüssel chiffriert wird. Sobald das Dokument auf dem Server gespeichert ist, holt der Indexserver bzw. –Prozess (polling) dieses Dokument, entschlüsselt es mit dem privaten EDÖB-Schlüssel und indexiert das Dokument. Es werden nur die wichtigen Wörter indexiert. Es besteht eine viersprachige rubbish-Liste, die firmenintern aufgebaut wurde. Die Indexierung erfolgt nur für die EDÖB-Gruppe (siehe dazu unter Zugriffskontrolle), nicht aber für die Gruppen Chef, Persönlich, Auskunftsrecht oder BGÖ, sonst hätte man die Möglichkeit Dokumentennummern aufzudecken, auf die man keinen Zugriff haben darf.

Ausdrucken:
Es bestehen drei Printserver, die es erlauben, die Daten bis vor den Drucker in chiffrierter Form zu übertragen. Beim Ausdrucken wird das Dokument mit dem öffentlichen Printkey verschlüsselt. Sobald im Datenbankserver ein Dokument zum Ausdrucken bereit ist, holt der Printserver (polling) dieses Dokument ab und entschlüsselt es mit dem privaten Printkey. Danach wird das Dokument über die USB-Schnittstelle auf den Drucker ausgegeben.
Druckaufträge an die Netzwerkdrucker, die nicht aus dem EDÖB-Office stammen, sind nicht verschlüsselt. Für die Entschlüsselung der übermittelten Druckaufträge aus dem EDÖB-Office bestehen die folgenden beiden Druckerserver:

Druckerserver für die Entschlüsselung der Dokumente aus dem EDÖB-Office	Standort der Drucker, Druckerbezeichung
Printserver01 (cbef05xft1024)	Networkprinter01, Raum 03.013, Korridor 3. Stock; HP Laserjet P4015x
Printserver02 (cbef05xft1023)	Networkprinter02, Raum 02.015, 2. Stock; HP Laserjet P4015x
Kein Printserver / keine Datenverschlüsselung / darf nicht für das Ausdrucken von sensitiven Informationen verwendet werden	Netzwerkprinter 03, Farbdrucker des Kopiergerätes im Raum 02.015, 2. Stock (XEROX)
Printserver03 (cbef05xft1009); ist zugleich Arbeitsplatzgerät eines MA's	Netzwerkprinter 04, Kanzlei 2.Stock, Raum 02.001, HP Laserjet P2055d

19.2. Netzwerk

Beim Netzwerkprotokoll handelt es sich um TCP/IP. Die sensitiven Daten werden von jedem EDÖB-Office Client von und zum Server verschlüsselt übertragen.

19.3. Datenbank

- Die MS-SQL-Server Datenbanken befinden sich auf dem virtuellen Server des externen Organs. Dieser hat die Bezeichnung XYZ. Diese Datenbanken haben die folgenden Bezeichnungen: EDSB, ZDATA[20], EDSBtest, ZdataTest.
- Integrität bei Mutationen:
  Die Datenbank ist in der höheren Normalform um dies zu gewährleisten
- Nachvollziehbarkeit:
  Die Eingriffe der DB-Administratoren werden nicht vollständig protokolliert. Dies ist nicht optimal, weil die Nachvollziehbarkeit in diesem Bereich nicht gewährleistet ist. Allerdings haben nur zwei Personen DB-Administratorenrechte (Admin und Stellvertreter).
- Vertraulichkeit:
  Spezielle Datenbank-Accounts bestehen keine. Die Identifikation und Authentifikation wird auf der EDÖB-Domänenebene geregelt. Mit Hilfe der SQL-GRANT's erfolgt die Zugriffsregelung (vererbt von der globalen Domänengruppe) auf Tabellenebene; dabei werden die folgenden zwei DB-Rollen unterschieden:
- EDÖBADMIN entspricht den DB-Administratoren
- EDÖBOFFICE entspricht den Zugriffen, welche die Mitarbeiter des EDÖB bei ihrer "normalen" Aufgabenerfüllung (Rollen) wahrnehmen (Chefs, KZL, SB).
- Batches / Jobs, die auf dem SQL Server ausgeführt werden:

Name Batches/Jobs	Beschreibung
Autom. Erledigung der Zirkulations-Mappe	Die Z-Mappe beinhaltet die wichtigen Dokumente, die vom EDÖB versendet wurden. Diese Dokumente werden allen Mitarbeitern des EDÖB periodisch zur Kenntnis gebracht (Papier und elektr. Form). Davon ausgenommen sind die Stellungnahmen zu den Einsichtgesuchen für die Datensammlung ISIS sowie die Prüfungsverfahren für die Datensammlungen JANUS, GEWA und SIS. Nach einem Monat wird die elektr. Form gelöscht. (Start jeden Morgen 06:00)
Phys. Löschen Daten	Physisches Löschen der vor einem Jahr logische gelöschten Daten (Start jeden ersten Montag im Monat 12:00)
Phys. Löschen der 5-jährigen Archivdaten	Die dossierbeschreibenden Daten (Randdaten) der archivierten Dossiers werden nach fünf Jahren physikalisch gelöscht. (***Momentan inaktiv***)
EDSBtest backup (1)	Erstellt DB-Backup der Testdatenbank (Start nur wenn bspw. auf Einzeldaten –dokumente zurückgegriffen werden muss)
EDSBtest overwrite (2)	Überschreibt die Testumgebung mit dem gewünschten Backup der Produktion. Damit können die gewünschten Dokumente zurück ins System kopiert werden, ohne den Produktionsbetrieb zu belasten.

[20] Metadaten "rein" für die EDÖB-Office Anwendung.

	(Start dito wie backup (1)
EDSBtest restore (3)	Wieder Herstellen der Testumgebung (Restore der Testdaten) auf der Testdatenbank (Start dito wie backup (1)

19.4. Betriebssystem / SW

Gewisse Teile werden aus Sicherheitsgründen im vorliegenden veröffentlichten Reglement nicht aufgeführt.

Benutzerverwaltung:

- Auf der Stufe Betriebssystem erfolgt das Einloggen mit Hilfe der Smartcard und der Eingabe der PIN (zwei Faktor Authentifikation / 2FA). Das jeweilige Zertifikat für die Authentifikation ist drei Jahre gültig. Im Weiteren befindet sich auf der Karte noch ein Verschlüsselungs- als auch ein Signaturzertifikat. Nach zehn fehlerhaften Eingaben der PIN wird die Smartcard gesperrt. Die Zertifikate werden in der Folge revoziert. Die Karte ist mit neuen Zertifikaten zu erstellen.
- Einige Leitungsmitglieder können über einen abgesicherten Zugang (RAS) von extern auf das EDÖB-Office zugreifen (inkl. 2FA).
- Im Weiteren können einige Personen mit Hilfe der Outlook Web Applikation (OWA) und einem Browser auf e-Mail, Kalender, Kontakte, Aufgaben (Outlook) zugreifen. Dies allerdings nur mit Hilfe eine SMS Codes auf das jeweilige Smartphone (ebenfalls 2FA).
- Das Einloggen in die Applikation EDÖB-Office erfolgt mit Hilfe eines USB-Sticks sowie der Eingabe der Benutzeridentifikation und der Passphrase.
- Angestrebt wird die SSO-Unterstützung. Diese ist aber momentan noch nicht realisierbar.

Zusätzlich erfolgt die Verwaltung aufgrund der folgenden Benutzergruppen:

Bezeichnung	**Beschreibung (Rollen)**	**Wer**
ADMINISTRATION	Systemadministratoren	Administrator und Stellvertreter
EDSBOFFICE	Chefs, KZL, SachbearbeiterInnen	Rund 30 Personen
EDSBADMIN	Datenbankadministratoren	Administrator und Stellvertreter

Dabei sind u.a. die folgenden Normen einzuhalten:

- Richtlinien für die Benutzung des Geschäftsverwaltungssystems EDÖB-Office.
- Reglement für die Benutzung der Informations- und Kommunikationstechnolgie des EDÖB.
- Weisung Informatiksicherheit in der Bundesverwaltung WIsB, Anhang 1)

19.5. Hardware

Host bzw. Server
Hardware: (Infrastructure as a service)

Client
Hardware: Laptop: 2,7 GHz, 4 GB, 130 GB
Desktop: 3 GHz, 4 GB, 250 GB

Printserver
Hardware: 2 Stück; 3 GHz, 4 GB, 250 GB

Netzwerk: Cisco Catalyst 3750 (V2 Series, PoE-24), 100BaseT. Weitergehende Angaben bestehen, werden aber nicht veröffentlicht.

20. Das Verfahren zur Ausübung des Auskunftsrechts

Die Betroffenen können ihr Einsichtsrecht (Auskunftsrecht) wahrnehmen, indem sie sich in schriftlicher Form unter Beilage einer Kopie eines Personalausweises an folgende Adresse wenden:

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragtenbeauftragter
Sekretariatsleiter
Feldeggweg 1
3003 Bern

Wenn der Eidgenössische Datenschutz- und Öffentlichkeistbeauftragte das Auskunftsrecht beschränkt, so teilt er dies innerhalb von 30 Tagen der betroffenen Person in einer Verfügung schriftlich mit.

Siehe auch den Ablauf im Abschnitt 11.4 „Auskunftsrecht beim EDÖB wahrnehmen“.

21. Anhänge

Anhang 1 Ordentliche Anmeldung der Datensammlung

Name und Adresse des verantwortlichen Bundesorgans

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragtenbeauftragter
Feldeggweg 1
3003 Bern

Name und vollständige Bezeichnung der Datensammlung

EDÖB-Office

Das Organ, bei dem das Auskunftsrecht geltend gemacht werden kann

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragtenbeauftragter
Sekretariatsleiter
Herrn Jean-Philippe Walter
Feldeggweg 1
3003 Bern

Rechtsgrundlagen und Zweck der Datensammlung

Art. 32 Verordnung zum Bundesgesetz über den Datenschutz (VDSG); SR 235.11
Art. 57h Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 (RVOG); SR 172.010

Verwaltung von Geschäften/Dossiers

Kategorien der bearbeiteten Personendaten

Adresse, Identität, ein- und ausgehende Sachgeschäfte, Dossiernummer, Datum der Aufnahme, Schlüsselwörter

Kategorien der Empfänger der Daten

Bundesarchiv, Bundesverwaltungsgericht, betroffene Behörden und Personen (natürliche oder juristische Personen)

*Kategorien der an der Datensammlung Beteiligten, das heisst Dritte, die Daten in eine Datensamm*lung eingeben und verändern dürfen

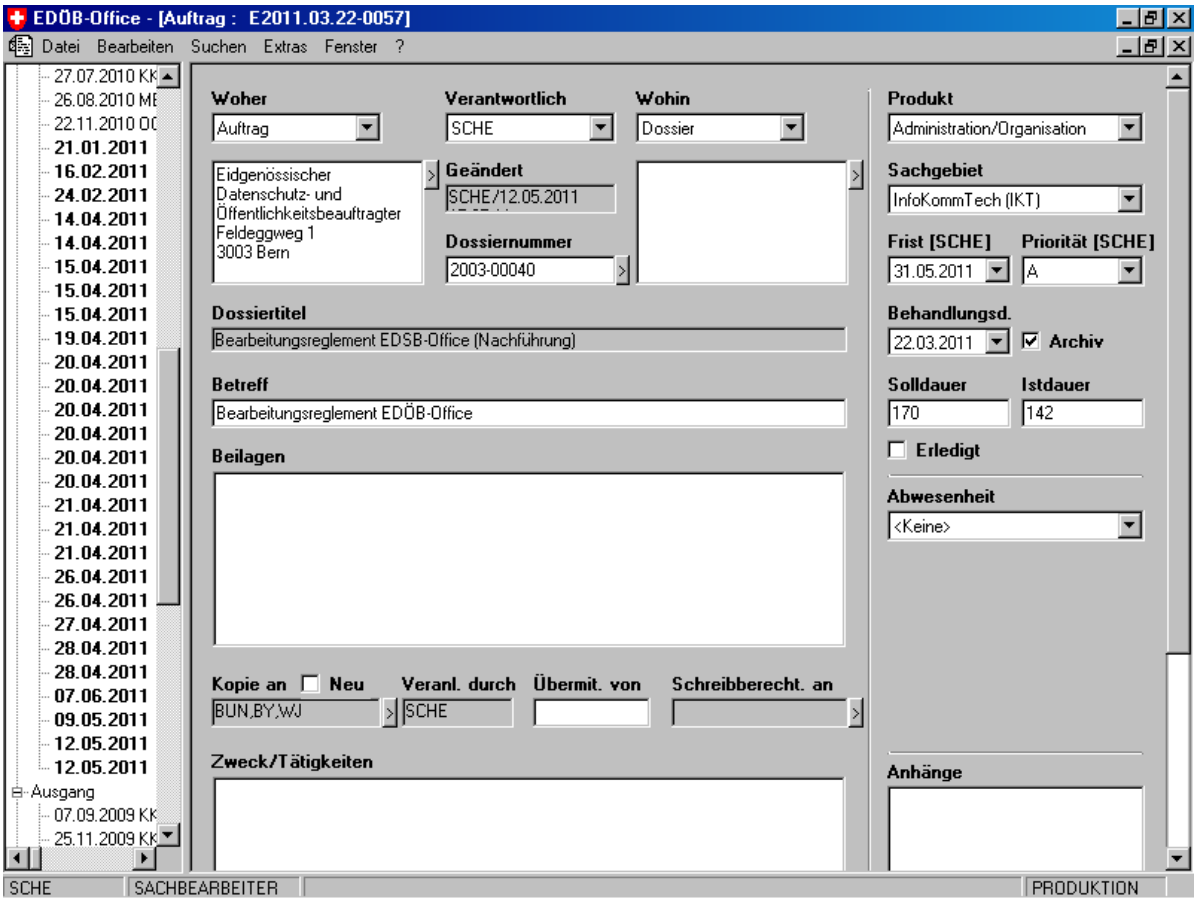
- keine -

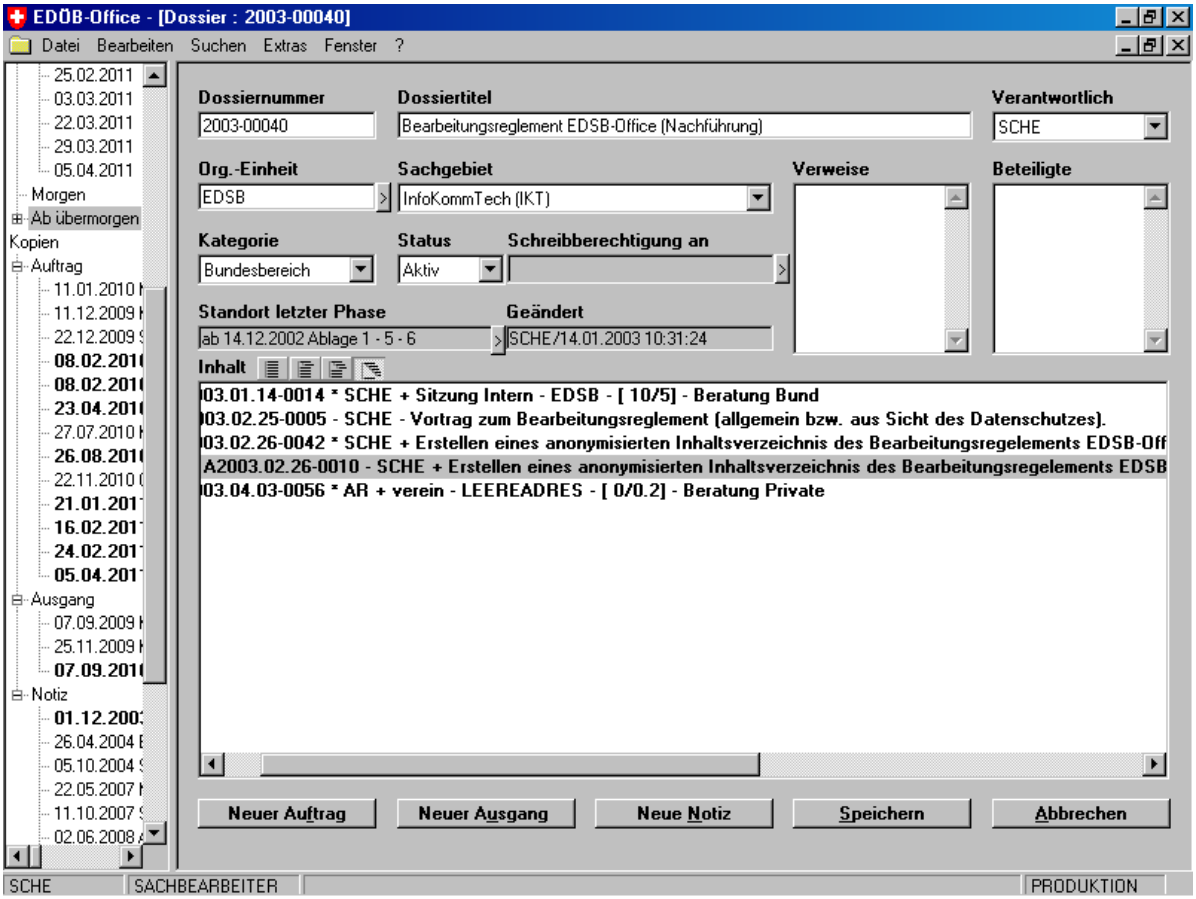
Kreis und ungefähre Anzahl der betroffenen Personen

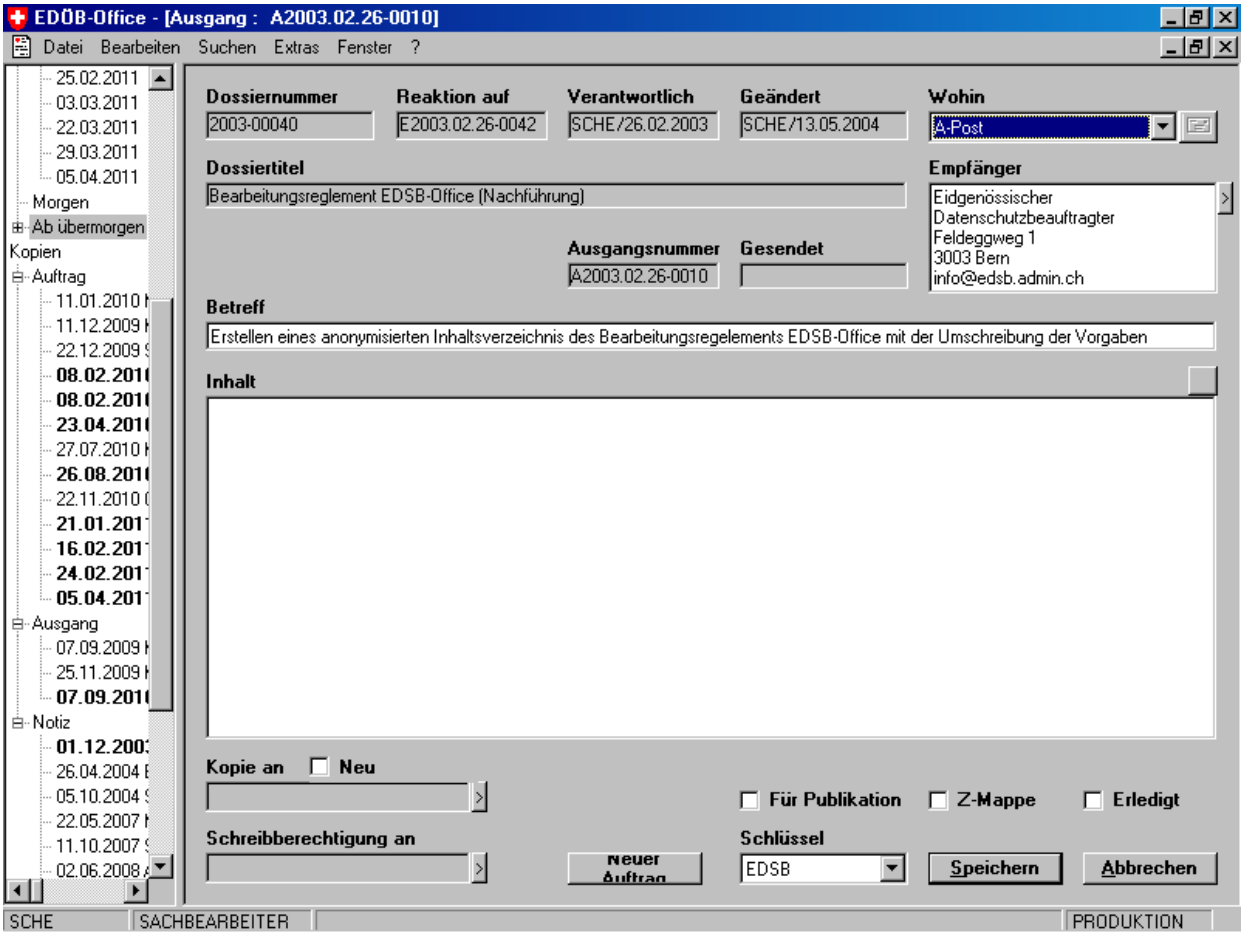
Natürliche, juristische Personen, Behörden, welche schriftlich mit dem Eidg. Datenschutz- und Öffentlichkeitsbeauftragten-Beauftragten verkehren

Datareg-Nummer: 200200029

Anhang 2 Drei wichtige Bildschirmmasken der Anwendung






EDÖB-Office - [Ausgang : A2003.02.26-0010]
Datei Bearbeiten Suchen Extras Fenster ?
25.02.2011
03.03.2011
22.03.2011
29.03.2011
05.04.2011
Morgen
Ab übermorgen
Kopien
Auftrag
Ausgang
Notiz
Dossiernummer
2003-00040
Reaktion auf
E2003.02.26-0042
Verantwortlich
SCHE/26.02.2003
Geändert
SCHE/13.05.2004
Wohin
A-Post
Dossiertitel
Bearbeitungsreglement EDSB-Office (Nachführung)
Empfänger
Eidgenössischer
Datenschutzbeauftragter
Feldeggweg 1
3003 Bern
info@edsb.admin.ch
Ausgangsnummer
A2003.02.26-0010
Gesendet
Betreff
Erstellen eines anonymisierten Inhaltsverzeichnis des Bearbeitungsregelements EDSB-Office mit der Umschreibung der Vorgaben
Inhalt
Kopie an
Neu
Für Publikation
Z-Mappe
Erledigt
Schreibberechtigung an
Neuer Auftrag
Schlüssel
EDSB
Speichern
Abbrechen
SCHE
SACHBEARBEITER
PRODUKTION