Ort, Datum Mustervorlage V2.0

Organisationsvorschriften (OV)

[Verwaltungseinheit]

Version [2.0]

|  |  |
| --- | --- |
| **Kontakte / Ansprechpersonen** | |
| Fragen rund um die GEVER-Anwendung | Super User |
| Fragen zur Informationsbewirtschaftung | CC INFORMATIONSMANAGEMENT |
| Fragen und Kommentare zum vorliegenden Dokument | OV-Verantwortliche |

Inhaltsverzeichnis

[1 Ziel und Zweck der Organisationsvorschriften 3](#_Toc177469386)

[2 Grundsätze 4](#_Toc177469387)

[2.1 Bearbeiten von Informationen 4](#_Toc177469388)

[2.2 Ordnungssystem *[Verwaltungseinheit]* 4](#_Toc177469389)

[2.3 Zugriffe, Informationsschutz, Datenschutz 5](#_Toc177469390)

[2.4 Dossiers, Dokumente, Titelvorgaben 5](#_Toc177469391)

[2.5 Anpassungen der Organisationsvorschriften 6](#_Toc177469392)

[3 Ablauforganisation: Life Cycle Management 7](#_Toc177469393)

[3.1 Bewirtschaftung im Lifecycle 7](#_Toc177469394)

[3.2 Eröffnen 7](#_Toc177469395)

[3.3 Bearbeiten 8](#_Toc177469396)

[3.4 Abschliessen 9](#_Toc177469397)

[3.5 Aussondern 10](#_Toc177469398)

[3.6 Aufbewahren, Löschen/Vernichten 10](#_Toc177469399)

[3.7 Archivieren 10](#_Toc177469400)

[3.8 Nutzen 10](#_Toc177469401)

[3.9 Controlling 11](#_Toc177469402)

[4 Aufbauorganisation: Verantwortlichkeiten und Rollen 12](#_Toc177469403)

[4.1 Organisationsspezifische Rollen 12](#_Toc177469404)

[4.2 Technische Rollen 14](#_Toc177469405)

[5 Inkraftsetzung 16](#_Toc177469406)

[Anhänge *[Detailregelungen und Spezifizierungen]* 17](#_Toc177469407)

[Anhang 1 Aktualisierungs- und Änderungskontrolle 17](#_Toc177469408)

[Anhang 2 Begriffe 17](#_Toc177469409)

[Anhang 3 Abkürzungen 19](#_Toc177469410)

[Anhang 4 Rollenverteilung 19](#_Toc177469411)

[Anhang 5 Negativliste 20](#_Toc177469412)

[Anhang 6 Scanning-Anweisungen 21](#_Toc177469413)

[Anhang 7 Liste juristisch relevanter Unterlagen 22](#_Toc177469414)

[Anhang 8 Liste der autorisierten Systeme und Ablagen 23](#_Toc177469415)

[Anhang 9 Liste der Unterlagen mit eingeschränktem Zugriff 25](#_Toc177469416)

[Anhang 10 Anweisungen zum Dossierabschluss für Dossierverantwortliche 26](#_Toc177469417)

[Anhang 11 Anweisungen zur Aussonderung für das *[CC INFORMATIONSMANAGEMENT]* 27](#_Toc177469418)

[Anhang 12 Anweisung zum Umgang mit klassifizierten und datenschutzrelevanten Informationen und Verschlüsselung 29](#_Toc177469419)

[Anhang 13 Anweisung zur Nutzung von Kollaborationstools und temporären Ablagen 31](#_Toc177469420)

[*[Optional: Anhang 14 Liste der Zusatzkomponenten]* 31](#_Toc177469421)

Hinweise zu Zweck und Nutzung der Muster-Organisationsvorschriften (Muster-OV)

Dieses Dokument dient als Muster für Organisationsvorschriften (OV). Es unterstützt die Verwaltungseinheiten (VE) [[1]](#footnote-1) der Bundesverwaltung. bei der Erstellung und Überarbeitung ihrer Organisationsvorschriften (OV). OV regeln das gesamte Informationsmanagement einer VE.

Das Erstellen und Führen der OV liegt in der Verantwortung der VE.[[2]](#footnote-2)

Die Muster-OV führen alle zu regelnden Aspekte auf. Sie enthalten die allgemeinen Vorgaben zum Informationsmanagement Bund und verweisen auf ***[zu ergänzende Inhalte]***. Teilweise sind ***[Empfehlungen]*** für detaillierte Regelungen formuliert, die sich als Best Practice etabliert haben. Optional zu ergänzende Inhalte sind entsprechend gekennzeichnet ***[Optional: Beispiel]***.

Die Muster-OV müssen der spezifischen Situation der VE angepasst werden. Die VE ist frei, Passagen umzuformulieren oder zu ergänzen. Zu beachten ist, dass die aufgeführten Bereiche vollständig geregelt und die rechtlichen Vorgaben (Stufe Bund und ggf. Stufe Departement) eingehalten werden müssen.

Die OV der VE der Bundesverwaltung werden dem Schweizerischen Bundesarchiv (BAR) zur formellen Prüfung eingereicht. Negativlisten müssen vom BAR geprüft und genehmigt werden.

# Ziel und Zweck der Organisationsvorschriften

Die Organisationsvorschriften (OV) dienen als Grundlage für das gesamte Informationsmanagement der ***[Verwaltungseinheit VE]****.* Sie sind für alle Mitarbeitenden der ***[VE]*** verbindlich. ***[Ev. präzisieren: Dies schliesst ein: Standorte, Arbeitsorte, externe Mitarbeitende, …]***

Die OV regeln die Bearbeitung aller Informationen, die im Rahmen der Verwaltungstätigkeit empfangen oder erstellt werden. Die OV beschreiben, gestützt auf rechtliche Vorgaben sowie technische Normen und Standards,[[3]](#footnote-3) die Organisation des Informationsmanagements und die Umsetzung der Anforderungen an eine systematische Aktenführung.

Das Informationsmanagement umfasst das standardisierte Geschäftsverwaltungssystem (GEVER-System) sowie alle weiteren autorisierten Systeme und Ablagen (digital und physisch),[[4]](#footnote-4) in denen geschäftsrelevante Informationen bewirtschaftet werden. Ziel ist eine transparente und nachvollziehbare Geschäftstätigkeit sowie eine effiziente Geschäftsabwicklung.

Ein geregeltes Informationsmanagement ermöglicht der ***[VE]***:

* in laufenden Geschäften die Übersicht zu wahren und deren Koordination zu gewährleisten;
* sich selbst und dem Bundesrat Rechenschaft abzulegen (Planung, Controlling, Aufsicht);
* Berechtigten wie dem Parlament oder Dritten Rechenschaft über ihre geschäftlichen Aktivitäten abzulegen (z. B. aufgrund eines Akteneinsichtsrechts von Betroffenen);
* die Umsetzung der rechtlichen Vorgaben wie des Bundesgesetzes über das Öffentlichkeitsprinzip BGÖ, des Datenschutzgesetzes DSG und der dazugehörigen Verordnung DSV, des Informationssicherheitsgesetzes ISG und der Informationssicherheitsverordnung ISV) zu gewährleisten.

# Grundsätze

## Bearbeiten von Informationen

Grundsätzlich werden alle geschäftsrelevanten Informationen digital bearbeitet. Die digitale Bearbeitung erfolgt standardmässig in Dossiers im GEVER-System. Massgeblich ist ***[seit ….]*** das digitale Dossier.[[5]](#footnote-5)

Alle geschäftsrelevanten Unterlagen müssen registriert und abgelegt werden. Unterlagen, die für den Nachweis der Verwaltungstätigkeit nicht relevant sind, müssen nicht registriert werden. Nicht geschäftsrelevante Unterlagentypen sind abschliessend in der Negativliste aufgeführt (siehe ***[*Anhang *5]***).

Für spezifische Aufgaben können autorisierte Systeme und Ablagen ausserhalb des GEVER-Systems eingesetzt werden.[[6]](#footnote-6) Diese Systeme und Ablagen müssen ins Informationsmanagement eingebettet sein, um die Vorgaben an ein geregeltes Informationsmanagement gemäss Absatz 1 der OV ***[*VE*]*** zu erfüllen. Autorisierte Systeme und Ablagen ausserhalb des GEVER-Systems sind abschliessend im ***[Anhang 8]*** aufgelistet.

Für die Zusammenarbeit können Kollaborationstools genutzt werden.[[7]](#footnote-7) Geschäftsrelevante Informationen, die in Kollaborationstools bearbeitet werden, müssen laufend im GEVER-System ***[bzw. in den dafür vorgesehenen autorisierten Systemen und Ablagen]*** abgelegt werden. Je nach Schutzniveau dürfen Informationen nicht oder nur eingeschränkt in Kollaborationstools bearbeitet werden. Die eingesetzten Tools sind in ***[Anhang 8]*** abschliessend aufgeführt. Die Nutzung von Kollaborationstools wird in ***[Anhang 13]*** geregelt.

Mitarbeitende und Vorgesetzte sind gemeinsam für die korrekte und vollständige Ablage der Geschäfte in Ihrem Zuständigkeitsbereich verantwortlich.

## Ordnungssystem *[Verwaltungseinheit]*

Das Ordnungssystem (OS) ist die massgebende Struktur für die Verwaltung und Bearbeitung aller geschäftsrelevanten Informationen. Es ist aufgabenorientiert aufgebaut und umfasst alle Aufgaben der ***[VE]***, unabhängig davon, ob sie im GEVER-System oder ausserhalb davon bearbeitet werden. Ebenso enthält das OS Metadaten, welche die Bewirtschaftung der Informationen regeln.

Bei Anpassungsbedarf am OS gilt folgendes Vorgehen:

* Mitarbeitende melden Anpassungsbedarfdem ***[CC INFORMATIONSMANAGEMENT jeweils per Ende Q1 und Ende Q3]***.
* Das ***[CC INFORMATIONSMANAGEMENT]*** sammelt eingereichten Anpassungswünsche und prüft deren Konformität mit den Vorgaben und dem bestehenden OS ***[VE]***.[[8]](#footnote-8)
* Das ***[CC INFORMATIONSMANAGEMENT]*** führt eine OS-Aktualisierung durch und lässt die Anpassungen vom Bundesarchiv (BAR) genehmigen.Die Anpassung und Genehmigung des OS erfolgt in der Webapplikation StrucTool des BAR.
* Die genehmigten Anpassungen werden im GEVER-System umgesetzt.

## Zugriffe, Informationsschutz, Datenschutz

Das Zugriffskonzept der ***[VE]*** sieht eine offene Informationskultur vor. Grundsätzlich haben alle Mitarbeitenden der ***[VE]*** Zugriff auf sämtliche Informationen. Verschlüsselung und eingeschränkte Zugriffe werden zurückhaltend eingesetzt (vgl. ***[Anhang 9]***).

Rubriken im OS, unter denen Geschäfte anfallen, die klassifizierte Dokumente nach ISG/ISV,[[9]](#footnote-9) Personendaten gemäss DSG oder Daten juristischer Personen enthalten,[[10]](#footnote-10) sind in den Metadaten entsprechend zu kennzeichnen. Sie sind gemäss ihres Schutzniveaus mit geeigneten Mechanismen je Ablage zu schützen und der Zugriff auf sie ist technisch einzuschränken (vgl. ***[Anhang 9]***).

Dokumente, die als *GEHEIM* klassifiziert sind, dürfen im GEVER System weder abgelegt noch bearbeitet werden. Die Ablage und Bearbeitung dürfen nur in dafür vorgesehenen Systemen erfolgen.

Die federführenden Organisationseinheiten (OE) sind für die Umsetzung dieser Vorgaben verantwortlich.

## Dossiers, Dokumente, Titelvorgaben

Im GEVER-System ***[und weiteren autorisierten Systemen und Ablagen]*** werden Geschäfte bewirtschaftet. Alle relevanten Informationen zu einem Geschäft werden als Einheit bewirtschaftet und grundsätzlich in Form von Dossiers abgelegt. Es gilt das Prinzip 1 Dossier = 1 Geschäft. Die Einheit «Geschäft» oder «Dossier» bleibt über die gesamte Bewirtschaftung im Lifecycle (Kap. 3) bestehen.[[11]](#footnote-11) Sie bezieht sich auf:

* im GEVER-System bearbeitete Informationen;
* Informationen in autorisierten Systemen und Ablagen, die als Dossiers strukturiert abgelegt werden;
* Informationen in autorisierten Systemen und Ablagen, die als Geschäfte mit Anfang und Abschluss bewirtschaftet werden.

Ein Dossier kann Subdossiers umfassen und enthält Aufzeichnungen wie Dokumente oder Daten.

Für Titel bis auf ***[Stufe Dossier/Subdossier/Dokument]*** gelten folgende Regeln:

* aussagekräftige Bezeichnung, kurze Angaben zum Geschäft;
* Datum in der Form ***[jjjj-tt-mm]***,z. B. bei Protokollen;
* Sprache: ***[Landessprache oder Englisch]***.Ausnahmen können mit dem ***[CC INFORMATIONSMANAGEMENT]*** abgesprochen werden;
* Abkürzungen und Akronyme müssen aufgeschlüsselt sein (in runder Klammer), ausgenommen sind Abkürzungen, die in den ***[Landessprache]*** Standardwörterbüchern enthalten sind (z. B. DUDEN);
* sind im Titel und bzw. oder im Inhalt Personennamen in Kombination mit besonders schützenswerten Personendaten erfasst, müssen auch die Metadaten bezüglich DSG angepasst werden;
* Enthalten Titel Informationen, welche dem Informations- oder Datenschutz unterstehen, dürfen diese nur für autorisierte Personen einsehbar sein.

Fachbereichsspezifische Regelungen sind zugelassen, sofern sie diesem Grundsatz nicht widersprechen. Sie sind der ***[OV-Verantwortlichen]*** mitzuteilen und werden in die OV integriert.

## Anpassungen der Organisationsvorschriften

Die Organisationsvorschriften (OV) werden jährlich ***[jeweils Ende Q3]*** durch den/die ***[OV-Verantwortliche/n]*** auf Anpassungsbedarf hin überprüft.

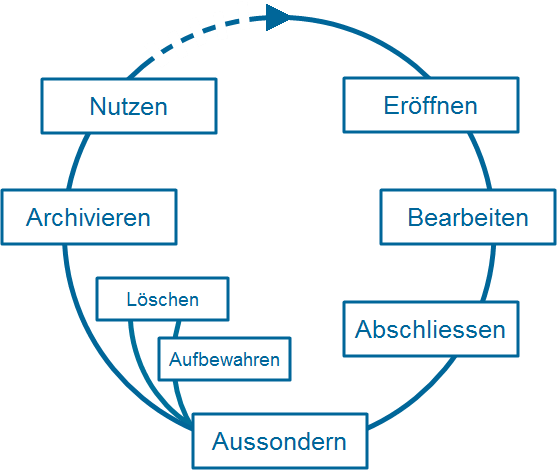
Allfällige Änderungs- oder Ergänzungsvorschläge der Mitarbeitenden sind erwünscht und bis zu diesem Termin direkt an den/die ***[OV-Verantwortliche/n]*** zu richten. Ergänzende bereichsspezifische Vorgaben, z.B. für die Bewirtschaftung oder Bearbeitungsvorschriften für autorisierte Systeme und Ablagen sind der OV-Verantwortlichen ebenfalls bis zu diesem Termin mitzuteilen. Diese werden als Anhang/Link in die OV aufgenommen.

Anträge zu Anpassungen der OV werden durch den/die ***[OV-Verantwortliche/n]*** an die Geschäftsleitung gestellt und von dieser verabschiedet.

Zur Einhaltung der OV führt ***[das CC INFORMATIONSMANAGEMENT]*** jährlich ein Controlling durch (siehe ***[Kap. 3.8]***).

# Ablauforganisation: Life Cycle Management

## Bewirtschaftung im Lifecycle



Der Lifecycle von Informationen

Geschäftsrelevante Informationen müssen so bewirtschaftet werden, dass sie während ihres gesamten Lifecycles (von der Entstehung bis zur Aufbewahrung, Archivierung oder Löschung) jederzeit zur Verfügung stehen.

Die nachfolgenden Regelungen gelten für die Bewirtschaftung von Informationen im GEVER-System sowie für alle Systeme und Ablagen, in denen Geschäfte, bzw. Dossiers gemäss der Definition unter 2.4 bewirtschaftet werden. Ohne zusätzliche oder anderweitige Vorgaben (OV-Anhänge, Bearbeitungsvorschriften) gelten sie für alle Bereiche ***[Standorte /Aussenstellen],*** Systeme / Ablagen und alle geschäftsrelevanten Informationen der ***[VE]***.

Wo Informationen ausserhalb eines Geschäftszusammenhangs bewirtschaftet werden (z.B. unstrukturierte Daten, Datensammlungen) gelten die nachfolgenden Regelungen im Grundsatz. Spezifische Vorgaben müssen in den Bearbeitungsvorschriften der jeweiligen Systeme und Ablagen festgehalten werden (siehe Anhänge ***[8 und 13]***).

## Eröffnen

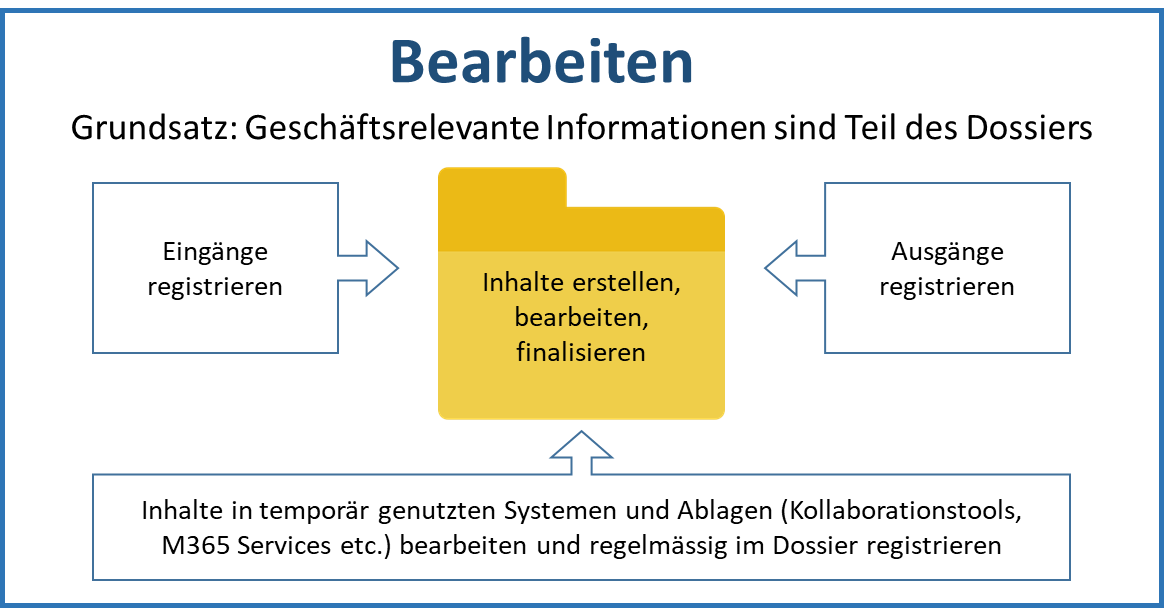
Ein neues Geschäft führt im Grundsatz zur Eröffnung eines neuen Dossiers. Ohne anderweitige Vorgaben wird das neue Dossier im GEVER-System eröffnet. Dies gilt auch für Geschäfte, die temporär oder teilweise ausserhalb des GEVER-Systems bearbeitet werden. Dossiers werden auf Antrag der Mitarbeitenden durch das ***[CC INFORMATIONSMANAGEMENT]*** eröffnet. Das ***[CC INFORMATIONSMANAGEMENT]*** prüft bei der Dossiereröffnung die korrekte Eingliederung ins Ordnungssystem (OS), eventuelle Redundanzen, die Verständlichkeit und die Regelkonformität des Dossiertitels (siehe Kap. 2.4).[[12]](#footnote-12)

Mit der Eröffnung der Dossiers werden die Metadaten von der Ordnungsposition automatisch auf das Dossier übertragen. Individuelle Anpassungen müssen mit der Dossierbestellung beim ***[CC INFORMATIONSMANAGEMENT]*** beantragt werden.

Subdossiers können anschliessend von den Mitarbeitenden selber eröffnet und verwaltet werden, möglich sind maximal ***[drei]*** Unterstufen.

Für Geschäfte, die vollständig ausserhalb des GEVER-Systems bewirtschaftet werden, gilt entsprechend, dass die Eröffnung des Geschäfts im betroffenen System nachvollziehbar dokumentiert ist und die erforderlichen Metadaten für die Bewirtschaftung angelegt sind.

## Bearbeiten

Die Bearbeitung umfasst alle Aktivitäten im Rahmen der Umsetzung der Geschäfte. Die Mitarbeitenden sind dafür verantwortlich, geschäftsrelevante Informationen korrekt zu registrieren und zu bearbeiten.

### Eingänge bearbeiten

Geschäftsrelevante Eingänge werden registriert. Dies gilt für sämtliche Formate und Medien.[[13]](#footnote-13) Eingänge zu Geschäften mit einem Dossier im GEVER-System werden im GEVER-System registriert. Eingänge zu Geschäften ohne Dossier im GEVER-System werden im zuständigen autorisierten System oder in der zuständigen autorisierten Ablage registriert.

Registrieren bedeutet, Unterlagen einem Geschäft zuzuordnen, mit Metadaten zu versehen (Betreff, Absender, Eingangsdatum usw.) und ins Ordnungssystem (OS) zu integrieren.[[14]](#footnote-14) ***[Anhänge werden separat registriert]***. Der Bezug zwischen Dokumenten (z. B. E-Mail und Anhängen) muss dabei im Titel erkennbar sein. Im GEVER-System werden bei der Registrierung die Metadaten des Dossiers automatisch auf die darunter liegenden Objekte übertragen.

Auf der Negativliste (***[Anhang 5]***) aufgeführte Unterlagentypen müssen nicht registriert werden.

|  |  |
| --- | --- |
| **Digitale Eingänge** | E-Mails an unpersönliche ***[VE]***-Adressen werden von den dafür zuständigen Mitarbeitenden an die zuständige Person oder Stelle weitergeleitet. Die zuständige Person registriert die E-Mail im GEVER-System bzw. im zuständigen System / in der zuständigen Ablage.  E-Mails, welche direkt bei den Mitarbeitenden eingehen, ([vorname.name@amt.admin.ch](mailto:vorname.name@amt.admin.ch)), werden durch diese registriert. |
| **Physische  Eingänge** | Beim zentralen Posteingang werden physische Eingänge durch das ***[CC INFORMATIONSMANAGEMENT]*** digitalisiert,registriert und/oder zugeteilt. Das konkrete Vorgehen wird in Anhang ***[6]*** beschrieben. |

### Geschäfte bearbeiten

Die Mitarbeitenden der ***[VE]*** bearbeiten Dokumente vom Entwurf bis zur finalen Version grundsätzlich im betreffenden Dossier. Temporär können für die Bearbeitung andere autorisierte Systeme / Ablagen oder Kollaborationstools genutzt werden. Hierbei sind die Vorgaben zu deren Nutzung zu beachten, insbesondere für sensitive Informationen. Sämtliche geschäftsrelevante Informationen werden laufend ins Dossier im GEVER-System bzw. in die dafür vorgesehenen Systeme/Ablagen überführt (siehe ***[Anhang 13]***).

Externe Beteiligte aus der Bundesverwaltung (BVerw) und Dritte können im Grundsatz für jene Bereiche oder Inhalte berechtigt werden, die Sie für die Erledigung ihrer Arbeit oder ihres Mandats benötigen. Dies gilt für das GEVER-System sowie für weitere autorisierte Systeme und Ablagen. Einzelheiten sind in den entsprechenden Bearbeitungsvorschriften festgehalten (siehe ***[Anhang 8]***).

Die Verschlüsselung von Informationen und der Umgang mit klassifizierten oder datenschutzrelevanten Unterlagen richtet sich nach dem ISG/der ISV, dem DSG und der GEVER-Verordnung. Anweisungen dazu sind in ***[Anhang 12]*** und in ***[Kapitel 2.3]***.

### Ausgänge bearbeiten

Die zuständigen Mitarbeitenden versenden Informationen (digital oder physisch) im Rahmen der Geschäftsbearbeitung.Bei Ausgängen, für die gemäss Unterschriftenregelung der VE die Leitung verantwortlich ist, wird die ***[digitale]*** Unterschrift der Leitung eingeholt. Versände werden im Dossier registriert.

Ausgedruckte und von Hand unterschriebene Ausgänge werden ***[zusätzlich digital signiert und nicht wieder eingescannt] /*** ***[durch die Registratur eingescannt]***. Ausnahmen sind beim ***[CC INFORMATIONSMANAGEMENT]*** zu beantragen.

## Abschliessen

Wenn das Geschäft abgeschlossen ist, wird das zugehörige Dossier abgeschlossen.

Der Dossierabschluss besteht aus den Schritten «Bereinigung» (inhaltliche Bereinigung durch die/den Mitarbeitende/n) und «Abschluss» (technischer Abschluss im System inkl. Konvertierung in archivtaugliche Formate durch das ***[CC INFORMATIONSMANAGEMENT]***).

Die Anweisungen zum Dossierabschluss sind in ***[Anhang 10]*** festgehalten.

Für Geschäfte, die vollständig ausserhalb des GEVER-Systems bewirtschaftet werden, gilt entsprechend, dass der Abschluss des Geschäfts nachvollziehbar dokumentiert ist und die inhaltliche Bereinigung sowie die erforderlichen technischen Arbeitsschritte vollzogen sind.[[15]](#footnote-15)

## Aussondern

Die Aussonderung markiert den Zeitpunkt, an dem abgeschlossene Dossiers aus einem System oder einer Ablage entfernt werden. Die Zuständigkeit hierfür liegt beim ***[CC INFORMATIONSMANAGEMENT]***.

Eine Aussonderung abgeschlossener Dossiers aus dem GEVER-System oder aus autorisierten Systemen und Ablagen betrifft:

* **archivwürdige Dossiers** ***[nach Ablauf der im OS hinterlegten Aussonderungsfrist]***: Ablieferung an das BAR, anschliessend Löschung;
* **nicht archivwürdige Dossiers ohne Aufbewahrungsfrist bzw. nach Ablauf der Aufbewahrungsfrist:** Löschung.

Die detaillierten Anweisungen zur Aussonderung sind in ***[Anhang 11]*** festgehalten.

## Aufbewahren, Löschen/Vernichten

Alle als nicht archivwürdig bewerteten Informationen werden bis zum Ablauf der hinterlegten Aufbewahrungsfrist aufbewahrt. Für die Aufbewahrung sowie die Sicherung der Zuverlässigkeit, Authentizität, Integrität und Benutzbarkeit der Informationen ist nach Dossierabschluss das ***[CC INFORMATIONSMANAGEMENT]*** zuständig.

Dossiers aus dem GEVER-System verbleiben bis zum Ablauf der Aufbewahrungsfrist im GEVER-System. Ohne anderweitige Vorgaben gilt dasselbe auch für Informationen aus Systemen und Ablagen ausserhalb des GEVER-Systems.

Die nicht archivwürdig bewerteten Informationen müssen nach Ablauf ihrer Aufbewahrungsfrist gelöscht werden. Die Löschung/Vernichtung wird in jedem Fall protokolliert.

Das detaillierte Vorgehen wird in ***[Anhang 11]*** erläutert.

## Archivieren

**Digitale archivwürdige Unterlagen** (sowohl aus dem GEVER-System als auch aus anderen Systemen und Ablagen) werden dem BAR gemäss dessen Vorgaben als SIP (Submission Information Package) abgeliefert.

Das ***[CC INFORMATIONSMANAGEMENT]*** ist für die Ablieferung und alle dazugehörigen Arbeitsschritte verantwortlich.

**Analoge archivwürdige Unterlagen** werden gemäss den Vorgaben des BAR aufbereitet und abgeliefert.

Kopien von abgelieferten Unterlagen (physisch und digital) werden gelöscht/vernichtet. Die Löschung/Vernichtung wird in jedem Fall protokolliert.

Das detaillierte Vorgehen wird in ***[Anhang 11]*** erläutert.

## Nutzen

Der Zugang zu Informationen, die zur Archivierung an das Bundesarchiv (BAR) abgeliefert wurden, richtet sich nach den Bestimmungen des Bundesgesetzes über die Archivierung (BGA) sowie den entsprechenden Ausführungserlassen.

Die Bestellung abgelieferter Unterlagen erfolgt online ([www.recherche.bar.admin.ch](http://www.recherche.bar.admin.ch)). Die Regulierung des Zugangs zu Unterlagen ***[in Schutzfrist]*** der ***[VE]***geschieht mittels entsprechender Rollen (siehe Kap. 4). ***[Unterlagen ohne Schutzfrist werden von der federführenden Stelle direkt bestellt.]***

Die federführende Stelle fordert die Unterlagen ***[in Schutzfrist]*** bei der ***[zuständigen Stelle der VE]*** an.[[16]](#footnote-16) Die ***[zuständige Stelle der VE*]** hat die Rolle «Abliefernde Stelle» im Online-Zugang BAR inne und bestellt die Unterlagen über den Online-Zugang beim BAR. Die Bereitstellung schon digital vorhandener Unterlagen erfolgt grundsätzlich online per Download über [www.recherche.bar.admin.ch](http://www.recherche.bar.admin.ch). Die Digitalisate müssen nach Gebrauch gelöscht werden und können, falls später wieder benötigt, neu heruntergeladen werden.[[17]](#footnote-17) ***[Das CC INFORMATIONSMANAGEMENT kontrolliert periodisch, ob die Digitalisate gelöscht wurden.]***

Wenn analoge Unterlagen bestellt werden, werden diese vom BAR nach Möglichkeit digitalisiert. Diese stehen dann zum Download bereit. Bei einer analogen Bereitstellung ist sowohl eine Verwaltungsausleihe als auch eine Konsultation vor Ort im Lesesaal des BAR möglich. Ausgeliehene Unterlagen dürfen nicht verändert werden. Die Rückgabe der physischen Unterlagen ans BAR wird kontrolliert.

Einsichtsgesuche von Dritten für Unterlagen der VE und ihrer Vorgängerinnen, welche noch einer Schutzfrist unterliegen, leitet das BAR ***[der zuständigen Stelle/des Rechtsdienstes der VE]*** zur Prüfung weiter.[[18]](#footnote-18)

## Controlling

Das Controlling zur Einhaltung der OV wird jeweils ***[Ende Q4]*** durch ***[das CC INFORMATIONSMANAGEMENT]*** durchgeführt.

***[Das CC INFORMATIONSMANAGEMENT]*** ist berechtigt, zu Controlling-Zwecken Abfragen im GEVER-System und weiteren autorisierten Systemen und Ablagen durchzuführen, bzw. durchführen zu lassen und diese nach vorgängig festgelegten Kriterien auszuwerten.

Das Controlling wird ***[im Q1]*** mittels Controllingbericht an die GL rapportiert. Im Controllingbericht werden Ziele und Methoden des Controllings sowie dessen Resultate dargelegt. Auch werden im Controllingbericht allfällige Massnahmen für die Optimierung vorgeschlagen. Die Umsetzung dieser Massnahmen wird durch die GL beschlossen und durch ***[das CC INFORMATIONSMANAGEMENT]*** koordiniert.

# Aufbauorganisation: Verantwortlichkeiten und Rollen

Die Mitarbeitenden der ***[VE]*** haben aufgrund ihrer verschiedenen Funktionen verschiedene Verantwortlichkeiten im Informationsmanagement. Diese werden anhand von Rollen definiert und beschrieben. Verantwortlichkeiten und Rollen können sowohl organisatorischer Natur sein als auch technischer (verbunden mit entsprechenden Rechten im GEVER-System oder in anderen Systemen und Ablagen) ***[vgl. Anhang 8]***. Die Rollenverteilung ist in ***[Anhang 4]*** festgehalten.

Mitarbeitende haben jeweils eine oder mehrere organisationsspezifische Rolle(n) sowie eine oder mehrere technische Rolle(n) inne.

## Organisationsspezifische Rollen

|  |  |
| --- | --- |
| Direktion | Erlässt die Organisationsvorschriften OV. |
| Geschäftsleitung | Legt die Informationen mit eingeschränkten Zugriffsrechten fest. |
| OV-Verantwortliche/r | Ist verantwortlich für den Unterhalt der OV (inkl. Anhängen) und die Kontrolle ihrer Umsetzung durch die Mitarbeitenden der ***[VE]***.Erstattet der GL regelmässig Bericht und gibt Empfehlungen ab für das Controlling. Kommuniziert Änderungsanträge.Führt in Zusammenarbeit mit dem ***[das CC INFORMATIONSMANAGEMENT]*** Schulungen zu den OV durch. |
| Linienvorgesetzte/r | Ist verantwortlich für die Umsetzung der OV im eigenen Zuständigkeitsbereich (inkl. allfällige OE-spezifische Anhänge).  Meldet neue Mitarbeitende (inkl. Rollen) zur Erfassung im GEVER-System und weiteren Systemen / Ablagen und allfällige Änderungen an das ***[das CC INFORMATIONSMANAGEMENT]***.  Gibt nach Austritt eines Mitarbeitenden dessen Personal- und ggf. Zielvereinbarungsdossier in Abschluss. |
| Mitarbeitende/r | Ist verantwortlich für die Einhaltung der OV.  Jeder Mitarbeitende der ***[VE]*** wird beim Eintritt durch das ***[CC INFORMATIONSMANAGEMENT]*** im GEVER-System erfasst. Mutationen werden vom ***[CC INFORMATIONSMANAGEMENT]*** festgehalten.  Jede/r Mitarbeitende wird einer Organisationseinheit (OE) zugewiesen und erhält eine oder mehrere Rollen. |
| Super User/in GEVER-System[[19]](#footnote-19) | Ist die erste Ansprechperson für alle Benutzenden zur täglichen Bedienung des GEVER-Systems. Kann der/die Super User/in nicht weiterhelfen oder gilt es, ein technisches Problem zu beheben, wendet er/sie sich an das ***[CC INFORMATIONSMANAGEMENT]***. |
| CC INFORMATIONSMANAGEMENT | «CC INFORMATIONSMANAGEMENT» steht für Kompetenzzentrum Informationsmanagement und fasst verschiedene Rollen und Verantwortlichkeiten zusammen. Diese umfassen: Betreuung des GEVER-Systems (verbunden mit technischen Rollen im System), Betreuung OS, Betreuung / Koordination OV, Betreuung / Koordination autorisierter Systeme und Ablagen, Verwaltung des Lifecycles von der Eröffnung von Geschäften bis zur Ablieferung und Wiedernutzung von Informationen. |
| Sekretariat (CC INFORMATIONSMANAGEMENT) | Verwaltet den zentralen Posteingang der ***[VE]***.  Ist zuständig für das Lifecycle Management der Unterlagen (inkl. Dossier- eröffnung und -wiedereröffnung, Abschluss, Aussonderung und Ablieferung der Dossiers) im GEVER-System ***[und ggf. weiteren autorisierten Systemen und Ablagen der VE]***.  Arbeitet mit dem/der Anwendungsverantwortlichen GEVER und den (Anwendungs-)Verantwortlichen weiterer autorisierter Systeme und Ablagen zusammen, um ein korrektes und effizientes Lifecycle-Management sämtlicher Informationen der ***[VE]*** sicherzustellen.  Betreut die Papierablage(n) (inkl. Ausleihkontrolle) und weitere autorisierte Ablagen (gemäss ***[Anhang 8]***). |
| OS-Verantwortliche/r (CC-INFORMATIONSMANAGEMENT) | Ist für die Pflege und Aktualisierung des Ordnungssystems (OS) der ***[VE]*** zuständig. Sammelt und prüft Änderungsanträge am OS. Ist zuständig für OS-Prozesse in StrucTool und die Zusammenarbeit mit dem BAR rund um die Erarbeitung und dokumentiert diese schriftlich in StrucTool (siehe auch unter 2.2). |
| GEVER-Support (CC-INFORMATIONSMANAGEMENT) | Führt Aus- und Weiterbildungen zur Verwendung des GEVER-Systems durch. Stellt den Support aller Benutzenden sicher (Second Level Support) und nimmt an den Sitzungen der Super User Group ***[VE]*** teil. |
| Anwendungsverantwortliche/r GEVER-System (CC-INFORMATIONSMANAGEMENT) | Unterhält das GEVER-System von der Gestaltung über die Pflege bis hin zur Aktualisierung. Verantwortlich für die Planung, die Beantragung und die Überwachung aller Aktivitäten, welche notwendig sind, um das GEVER-System zu nutzen und den sich ändernden Bedürfnissen und Rahmenbedingungen anzupassen. Ist verantwortlich für Betrieb und Weiterentwicklung des GEVER-Systems.  Leitet die Sitzungen der Super User Group ***[VE]***.  Vertritt die ***[VE]*** in (departementalen) GEVER-Arbeitsgruppen und -gremien.  Ist für die Adressverwaltung ***[und das Prozessdesign]*** im GEVER-System verantwortlich.  Plant und koordiniert die jährliche Aussonderung.  Arbeitet mit den Anwendungsverantwortlichen autorisierter Systeme und Ablagen der ***[VE]*** zusammen, um organisatorische und technische Schnittstellen zum GEVER-System zu koordinieren.  Ist in Zusammenarbeit mit dem/der OV-Verantwortlichen für das Controlling verantwortlich (zur Verfügung stellen von Suchabfragen, Erfahrungswerten aus dem täglichen Betrieb etc.). |
| Anwendungsverantwortliche autorisierte Systeme und Ablagen (CC-INFORMATIONSMANAGEMENT)[[20]](#footnote-20) | Verantwortlich für Gestaltung, Pflege, Betrieb und Weiterentwicklung des jeweiligen Systems / der jeweiligen Ablage.  Arbeiten mit dem/der Anwendungsverantwortlichen GEVER, den Anwendungsverantwortlichen weiterer autorisierter Systeme und Ablagen sowie den Zuständigen aus dem ***[CC-INFORMATIONSMANAGEMENT]*** zusammen. So stellen sie die technischen und organisatorischen Schnittstellen und das Lifecycle-Management sicher.  Stellt dem/der OV-Verantwortlichen die erforderlichen Informationen für das Controlling zur Verfügung (z.B. Suchabfragen im System).  Spezifische Aufgaben und Verantwortlichkeiten gemäss jeweiligen Bearbeitungsvorschriften ***[Anhang 8]***. |
| Öffentlichkeitsbeauftragte/r | Empfängt, bearbeitet und beantwortet BGÖ-Anfragen.  Pflegt die Metadaten von Unterlagen im GEVER-System betreffend BGÖ-Status und Zugänglichkeit nach BGÖ, DSG/DSV und ISG/ISV gemäss der Weisung zum BGÖ des ***[Departements vom tt.mm.jjjj]***. |

## Technische Rollen

### GEVER System[[21]](#footnote-21)

|  |  |
| --- | --- |
| Sachbearbeiter/in | Standardrolle für Mitarbeitende im GEVER-System.  Beantragt Dossiers für neue Geschäfte beim ***[CC INFORMATIONSMANAGEMENT]***.  Erfasst (registriert) und bearbeitet die geschäftsrelevanten Unterlagen im GEVER-System.  Stellt seine Stellvertretung durch Vergabe von Stellvertreter-Rechten im GEVER-System sicher. |
| Registrator/in | Alle Mitarbeitenden des ***[CC INFORMATIONSMANAGEMENT]*** besitzen diese Rolle, um ihre fachspezifischen Aufgaben zu erledigen (vgl. Kap. 4.1, Beschreibung ***[CC INFORMATIONSMANAGEMENT]***). |
| GEVER Administrator/in Amt | Ist in Zusammenarbeit mit dem Anwendungsverantwortlichen zuständig für den Kontakt mit dem Leistungserbringer.  Ist verantwortlich für die Betreuung und die Koordination der technischen und organisatorischen Aufgaben rund um das GEVER-System.  Führt die Administration des GEVER-Systems, pflegt das OS und die Vorlagen, kann im Bedarfsfall Stellvertretungen einrichten.  Die Rolle GEVER Administrator Amt können nur Mitarbeitende des ***[CC INFORMATIONSMANAGEMENT]*** innehaben. |
| Systemadministrator/in Leistungserbringer | Erbringt die technische Administration des GEVER-Systems gemäss dem Service Level Agreement (SLA) mit der ***[VE]***. |

### StrucTool[[22]](#footnote-22)

|  |  |
| --- | --- |
| Benutzer BV (BVerw)[[23]](#footnote-23) StrucTool | Kann in StrucTool Strukturen erstellen und bearbeiten sowie analoge Ablieferungen bearbeiten. Teil des ***[CC INFORMATIONSMANAGEMENT]***.  Die Rolle «Benutzer BV» wird durch den/die Inhaber/in der «Rolle Admin BV StrucTool» berechtigt. |
| Admin BV (BVerw) StrucTool | Ist verantwortlich für die Nutzung und Verwaltung von StrucTool innerhalb der ***[VE]***. Berechtigt die Rolle «Benutzer BV» und meldet Mutationen dem BAR. Kann wie die Rolle «Benutzer BV» in StrucTool Strukturen erstellen und bearbeiten sowie analoge Ablieferungen bearbeiten. Teil des ***[CC INFORMATIONSMANAGEMENT]***.  Die Rolle «Admin BV» wird nach vorgängiger Schulung durch das BAR berechtigt. |

### Online-Zugang BAR

|  |  |
| --- | --- |
| Abliefernde Stelle Online-Zugang BAR | Fachspezifische Rolle für den Online-Zugang des BAR.[[24]](#footnote-24) ist berechtigt, in sämtliche abgelieferte Unterlagen der ***[VE]*** Einsicht zu nehmen. Das betrifft insbesondere auch Unterlagen, die noch einer Schutzfrist gemäss Art. 9, 11 oder 12 BGA unterliegen. Enthalten diese Unterlagen Personendaten, ist eine Einsicht nur aus bestimmten Gründen zulässig (Art. 14 Abs. 2 BGA).  Die Rolle «Abliefernde Stelle» wird von der Rolle «Verantwortliche/r Amtsausleihen» berechtigt, Mutationen meldet die Rolle «Verantwortliche/r Amtsausleihen» der ***[VE]*** dem BAR (benutzer-admin@bar.admin.ch). |
| Verantwortliche/r Amtsausleihen Online-Zugang BAR | Bestellt die Person mit der Rolle «Abliefernde Stelle» Unterlagen von ***[VE]***, die noch einer Schutzfrist unterliegen, wird der/die «Verantwortliche Amtsausleihen» automatisch per E-Mail über diesen Vorgang informiert. Ist für die Einsicht eine Begründung nötig, wird diese ebenfalls gemeldet.  Die Erstmeldung der Rolle «Verantwortliche/r Amtsausleihen erfolgt durch ein GL-Mitglied der ***[VE]*** an das BAR. Mutationen werden durch die Rolle «Verantwortliche/r Amtsausleihen» gemeldet (benutzer-admin@bar.admin.ch). |

### Weitere Systeme und Ablagen

***[Die Verantwortlichkeiten für weitere Systeme und Ablagen sind in Anhang 8aufgeführt und in den entsprechenden Bearbeitungsvorschriften geregelt.]***

# Inkraftsetzung

Diese Weisungen treten auf den ***[tt.mm.jjjj]*** in Kraft und ersetzen alle früheren diesbezüglichen Bestimmungen.

***[VE]***

Unterschrift

Vorname Name, Direktor/in

# Anhänge *[Detailregelungen und Spezifizierungen]*

Anhang 1 Aktualisierungs- und Änderungskontrolle

Aktualisierungskontrolle

|  |  |
| --- | --- |
| Überprüfungsrhythmus | Weisung jährlich, Anhänge laufend, mindestens aber halbjährlich |
| Federführung | ***[OV-Verantwortliche]*** |

Änderungskontrolle

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Datum** | **Name oder Rolle** | **Bemerkungen (geändert, geprüft, genehmigt)** |
| 0.1 |  |  |  |
|  |  |  |  |

Anhang 2 Begriffe[[25]](#footnote-25)

Informationen

Übergreifende Bezeichnung für Daten, Dokumente, Aufzeichnungen, Unterlagen, Dossiers, Geschäfte. Verweist auf jegliche Inhalte unabhängig vom Umfang, Medium und Kontext sowie vom Ablage- bzw. Speicherort.

Unterlagen, auch Aufzeichnungen

Alle aufgezeichneten Informationen, unabhängig vom Informationsträger, sowie alle Hilfsmittel und ergänzenden Daten, die für das Verständnis dieser Informationen und deren Nutzung notwendig sind.

Dokument

Als Einheit zu behandelnde, aufgezeichnete Information, unabhängig vom Informationsträger.

Daten

Isolierte oder isolierbare Einheiten, welche maschinell bearbeitet und analysiert werden können. Beispiele sind: Messdaten (z. B. Wetterdaten, Geodaten, Verkehrsmessungen), Forschungsdaten, Erhebungsdaten, Finanzdaten, Registerdaten, Personendaten.

Dossier

Als Dossier gilt die Gesamtheit (Kollektiv) der Unterlagen zu einem Geschäft. Grundsätzlich entspricht ein Dossier einem Geschäft. Die Dossierbildung erfolgt auf der Grundlage des Ordnungssystems (OS).

Geschäft

Die Bearbeitung der Amtsaufgaben erfolgt mehrheitlich in Form von Geschäften. Das einzelne Geschäft umfasst den Geschäftsprozess (z. B. Steuerung, Bearbeitung) und die dazugehörenden Unterlagen sowie deren Eingliederung in das dafür geschaffene Ordnungssystem (OS). Die Gesamtheit der während der Laufzeit eines Geschäfts registrierten Unterlagen und die Prozessinformationen erlauben es, die Geschäftstätigkeit zuverlässig nachzuweisen.

GEVER-System

Als Geschäftsverwaltungssystem gilt ein Informatiksystem, das im Sinne von Artikel 57*h* RVOG der Abwicklung von Geschäftsprozessen sowie der Verwaltung von Dokumenten, einschliesslich der Korrespondenz, dient. Die Verwaltungseinheiten der zentralen Bundesverwaltung nutzen das vom IKT Standarddienst GEVER bereitgestellte Geschäftsverwaltungssystem Acta Nova (standardisiertes GEVER-System).

Autorisierte Systeme und Ablagen

Die Bezeichnung «Systeme und Ablagen» umfasst sämtliche zur Erfüllung eines Aufgabenkomplexes genutzten technischen und/oder organisatorischen und/oder anderer Mittel. Dies schliesst ein: Geschäftsverwaltungssysteme, Fachanwendungen, Datenbanken, physische Ablagen, Kollaborationstools etc., unabhängig davon, ob Informationen darin temporär oder dauerhaft bewirtschaftet werden.

«Autorisiert» umfasst:

* das standardisierte GEVER-System;
* Elektronische Systeme und Ablagen, welche die Voraussetzungen von Art. 3 und Art. 4 der GEVER-Verordnung erfüllen;
* Physische Ablagen, welche die Voraussetzungen gemäss GEVER-Verordnung Art. 5 erfüllen.

Sämtliche in der Verwaltungseinheit für die Bewirtschaftung geschäftsrelevanter Informationen genutzter Systeme und Ablagen müssen «autorisiert» sein.

Ordnungssystem

Das Ordnungssystem (OS) bildet alle Aufgaben der ***[VE]*** ab und ermöglicht damit einen Überblick über alle Aufgabenbereiche. Es stellt die Grundlage dar für die Registrierung der Unterlagen bzw. die Dossierbildung.

**Bearbeiten**

Ohne spezifischen Kontext steht der Begriff für jeden Umgang mit Informationen, z.B. beschaffen, lesen, verändern, versenden, löschen, aufbewahren.[[26]](#footnote-26)

**Organisationseinheiten**

Eine Organisationseinheit (OE) ist ein Teil einer Verwaltungseinheit (VE). Es kann sich dabei um eine Abteilung, Sektion oder Gruppe handeln.

**[weitere Begriffe]**

Anhang 3 Abkürzungen

|  |  |
| --- | --- |
| BAR | Schweizerisches Bundesarchiv |
| BGA | Bundesgesetz über die Archivierung |
| BGÖ | Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung |
| BVerw | Bundesverwaltung |
| CC Informationsmanagement | Kompetenzzentrum GEVER |
| DSG, DSV | Bundesgesetz über den Datenschutz, Datenschutzverordnung |
| GEVER-System | Standardisiertes Geschäftsverwaltungssystem (Acta Nova) |
| ISG, ISV | Informationssicherheitsgesetz, Informationssicherheitsverordnung |
| OS | Ordnungssystem |
| OV | Organisationsvorschriften |
| VE | Verwaltungseinheit |
| OE | Organisationseinheit |
| ***[w.A.]*** | ***[weitere Abkürzungen]*** |

Anhang 4 Rollenverteilung

Der nachfolgende Anhang listet die Rollenverteilung für sämtliche in Kapitel 4 beschriebenen Rollen auf. Die Rollenverteilung für autorisierte Systeme und Ablagen sind gemäss den Angaben in Kap.4 in den entsprechenden Bearbeitungsvorschriften ***[vgl. Anhang 8]*** ersichtlich.[[27]](#footnote-27)

|  |  |
| --- | --- |
| **Organisatorische Rollen:** | |
| OV-Verantwortliche/r | *[Name, Vorname, OE]* |
| Super User/in GEVER-System | *[Name, Vorname, OE]*  *[Name, Vorname, OE]* |
| Sekretariat (CC INFORMATIONSMANAGEMENT) | *[Name, Vorname, OE]*  *[Name, Vorname, OE]* |
| OS-Verantwortliche/r (CC INFORMATIONSMANAGEMENT) | *[Name, Vorname, OE]* |
| GEVER-Support (CC-INFORMATIONSMANAGEMENT) | *[Name, Vorname, OE]* |
| Anwendungsverantwortliche/r GEVER-System (CC-INFORMATIONSMANAGEMENT) | *[Name, Vorname, OE]* |
| Anwendungsverantwortliche/r *[System/Ablage]* | *[Name, Vorname, OE]* |
| Anwendungsverantwortliche/r *[System/Ablage]* | *[Name, Vorname, OE]* |
| Öffentlichkeitsbeauftragte/r | *[Name, Vorname, OE]* |
| GEVER Administrator/in Amt | *[Name, Vorname, OE]* |
| OV-Verantwortliche/r | *[Name, Vorname, OE]* |
| Öffentlichkeitsbeauftragte/r | *[Name, Vorname, OE]* |
| GEVER-System Registrator/in | *[Name, Vorname, OE]*  *[Name, Vorname, OE]* |
| GEVER-System Administrator/in *[Verwaltungseinheit]* | *[Name, Vorname, OE]*  *[Name, Vorname, OE]* |
| GEVER-System Systemadministrator/in Leistungserbringer | *[Name, Vorname, OE, VE]* |
| StrucTool Benutzer BV | *[Name, Vorname, OE]*  *[Name, Vorname, OE]* |
| StrucTool Admin BV | *[Name, Vorname, OE]* |
| Online-Zugang BAR Abliefernde Stelle | *[Name, Vorname, OE]* |
| Online-Zugang BAR Verantwortliche/r Amtsausleihen | *[Name, Vorname, OE]* |
| *[…]* | *[Name, Vorname, OE]* |

Anhang 5 Negativliste

Die Negativliste[[28]](#footnote-28) umfasst alle **Typen von Unterlagen**, die nicht geschäftsrelevant sind und demzufolge nicht registriert werden müssen. Sie gilt für alle Medien, für die Ablage und Bewirtschaftung im GEVER-System sowie in sämtlichen weiteren autorisierten Systemen und Ablagen.[[29]](#footnote-29)

***Hier folgt die Auflistung der genannten Dokumenttypen. Beispiele finden Sie im*** [***Merkblatt Negativliste***](https://www.bar.admin.ch/dam/bar/de/dokumente/kundeninformation/merkblatt_negativliste.pdf.download.pdf/merkblatt_negativliste.pdf) ***des BAR.***

***Die Negativliste von Verwaltungseinheiten (VE) der Bundesverwaltung muss dem Bundesarchiv zur Genehmigung eingereicht werden.***

Anhang 6 Scanning-Anweisungen

Die Scanning-Anweisungen regeln, wie das Scanning physischer Dokumente durchgeführt wird. Wo nicht anders vermerkt, gelten diese Vorgaben unabhängig davon, ob die eingescannten Dokumente anschliessend im GEVER-System oder in anderen autorisierten Systemen und Ablagen registriert und bewirtschaftet werden.

Grundsätze

* Alle geschäftsrelevanten physischen Unterlagen werden im ***[CC INFORMATIONSMANAGEMENT]*** zentral als PDF/A-Dateien eingescannt.
* Die Zeitspanne von der Postöffnung bis zum Einscannen sollte möglichst gering gehalten werden.
* Als ***[„persönlich“]***, ***[„vertraulich“]***, oder ***[an den Personaldienst]*** adressierte sowie als VERTRAULICH oder GEHEIM klassifizierte Post wird direkt und ungeöffnet den jeweiligen Adressaten zugestellt.[[30]](#footnote-30)
* Bei sensitiven Informationen gelten zusätzlich die Vorgaben in ***[Anhang 12]***.

Vorgehen und Qualitätssicherung Scanning

1. Briefe und allfällige Beilagen werden separat gescannt. Dies ermöglicht, dass Brief und Beilage(n) separat registriert und somit unabhängig voneinander zugänglich, suchbar und wieder verwendbar werden. Die Zusammengehörigkeit wird mittels Metadaten oder mittels Titel dokumentiert.[[31]](#footnote-31)
2. Alle Unterlagen werden beidseitig und gerade gescannt.
3. Die Reihenfolge beim Scanning ist so einzuhalten, wie die Unterlagen eingetroffen sind.
4. Es wird kontrolliert, ob sämtliche Elemente vorhanden und gut lesbar sind. Informationen dürfen nicht von anderen Unterlagen (z. B. Post-it) abgedeckt sein.

Nicht oder nur teilweise scannbare Medien

Physische Dokumente bis und mit Format ***[A4]*** und ***[100]*** Blatt werden eingescannt. Bei umfangreicheren Dokumentationen wird die erste Seite gescannt. Grössere Formate und nicht scannbare Medien werden durch die Erfassung eines Stellvertreter-Dokuments (Metadaten und Angaben zur Ablage bzw. zum Standort) im Master-Dossier ***[im GEVER-System]*** erschlossen. Diese Unterlagen werden der zuständigen Stelle zusätzlich in physischer Form weitergeleitet. Die zuständige Stelle ist dafür verantwortlich, dass für die physischen Unterlagen nur die entsprechenden autorisierten Ablagen und Systeme gemäss ***[Anhang 8]***. genutzt werden. Ein Standortwechsel wird in den Metadaten des Stellvertreter-Dokuments nachgetragen.

Registrierung / Zuteilung

Die Zuteilung der erfassten Eingangspost erfolgt gemäss folgenden Kriterien:

* Unpersönliche Post – OE nicht erkennbar: ***[Leitung Stab]***
* Unpersönliche Post – OE erkennbar: Direkt an die OE oder die zuständigen Mitarbeitenden
* Persönlich adressierte Post: Direkte Zustellung.[[32]](#footnote-32)
* Irrtümlich geöffnete oder falsch adressierte (Vermerk «persönlich» fehlt) VERTRAULICH klassifizierte Post ist gemäss den Vorgaben ISG/ISV zu verpacken, zu adressieren und dem/der Empfänger/in direkt zuzustellen.

Spezifische Anliegen von OE bezüglich Scanning und Digitalisierung können an das ***[CC INFORMATIONSMANAGEMENT]*** gerichtet werden.

Aufbewahrung

Nach dem Einscannen und Registrieren werden physische Posteingänge im ***[CC INFORMATIONSMANAGEMENT]*** in Tagesmappen gesammelt und nach 3 Monaten vernichtet.[[33]](#footnote-33) Ausnahmen: Nicht oder nur teilweise scannbare Medien (siehe weiter oben) sowie Unterlagen gemäss ***[Anhang 7]***.

Anhang 7 Liste juristisch relevanter Unterlagen

Juristisch relevante Unterlagen werden sowohl in Papier- als auch in digitaler Form aufbewahrt.[[34]](#footnote-34) Die Aufbewahrung erfolgt beim ***[CC INFORMATIONSMANAGEMENT]*** in der Ablage ***[Juristisch relevante Unterlagen]*** (***[vgl. Anhang 8]***). und kann dort bei Bedarf angefordert werden (Ausnahme: Staatsverträge/Abkommen[[35]](#footnote-35)). Die Aussonderung, Ablieferung bzw. Vernichtung wird in den ***[Anhängen 10 und 11]*** beschrieben. Als juristisch relevante Unterlagen gelten folgende Unterlagentypen:

* Verträge mit Dienstleistungsanbietern (sofern handschriftlich signiert)
* Anonyme Schreiben
* Drohbriefe
* Staatsverträge
* ***[…]***
* ***[…]***

Juristisch relevante Unterlagen, die Teil archivwürdig bewerteter Aufgaben sind, werden immer in digitaler Form abgeliefert. Die Ablieferung erfolgt im Rahmen der Ablieferung des entsprechenden digitalen Dossiers. Physisch vorliegende Unterlagen werden nach der Ablieferung als Doublette verstanden und nach Abschluss der Ablieferung vernichtet. Wo es rechtlich notwendig ist, die analogen Unterlagen zu archivieren, kann eine zusätzliche Ablieferung der juristisch relevanten Unterlagen in physischer Form erfolgen. Auch hier erfolgt die Ablieferung des vollständigen Dossiers in digitaler Form, die juristisch relevanten Unterlagen werden zusätzlich physisch aus der Separatablage abgeliefert gemäss den Vorgaben des BAR zur Ablieferung von Mischablagen.

Anhang 8 Liste der autorisierten Systeme und Ablagen

Die Amtsablage besteht aus der Gesamtheit aller autorisierten Systeme und Ablagen (temporär und dauerhaft; digital und physisch). Neben den autorisierten dürfen keine weiteren Systeme und Ablagen genutzt werden.

Physische Ablagen

Physische Unterlagen, die aus rechtlichen und/oder organisatorischen Gründen aufzubewahren sind, werden in folgenden Ablagen abgelegt und vom ***[CC INFORMATIONSMANAGEMENT]*** betreut. Der Zugang ist zu Bürozeiten bzw. nach Vereinbarung möglich.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.** | **Name Ablage** | **Standort** | **Zuständigkeit/StV.** | **Bemerkungen** |
| 1 | Tagesmappen Posteingänge | ***[EG, Büro XXX]*** | ***[CC INFORMATIONSMANAGEMENT]*** | Vernichtung 3 Monate nach Eingang |
| 2 | Juristisch relevante Unterlagen ***[vgl. Anhang 7]*** | ***[EG, Büro YYY]*** | ***[CC INFORMATIONSMANAGEMENT]*** | Vernichtung nach Aufbewahrungsfrist bzw. Ablieferung BAR |
| 3 | Nicht scannbare Unterlagen *[vgl. Anhang 7]* | *[1. Stock, Büro ZZZ]* | *[CC INFORMATIONSMANAGEMENT]* | Vernichtung nach Aufbewahrungsfrist bzw. Ablieferung BAR |

Digitale Systeme und Ablagen

Digitale Informationen werden in den folgenden autorisierten Systemen und Ablagen temporär oder dauerhaft bewirtschaftet. Es gelten die Vorgaben der GEVER-Verordnung für die temporäre oder dauerhafte Bewirtschaftung von Informationen.[[36]](#footnote-36) Die aufgeführten Systeme und Ablagen (ausgenommen das standardisierte GEVER-System 1) werden im Ordnungssystem (OS) in den Metadaten der betroffenen OS-Positionen aufgeführt.

Datensammlungen müssen dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet werden.[[37]](#footnote-37)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Nr.** | **Bezeichnung** | **Einsatzgebiet/Zweck** | **Beschreibung Inhalt /Struktur /Mischablage** | **Lifecycle (ständige bzw. temporäre Ablage)** | **Zuständigkeit** | **OS-Position** | **Bearbeitungsreglement (Link)** |
| 1 | Acta Nova | Elektronische Geschäftsverwaltung / gesamtes OS | OS, Dossiers | Ständige Ablage, Eröffnung bis Ablieferung | [CC INFORMATIONSMANAGEMENT] | Gesamtes OS | ***[Link]*** |
| 2 | SAP | Finanzen |  |  |  |  | ***[Link]*** |
| 3 | SAP | Personal |  |  |  |  | ***[Link]*** |
| 4 | SAP | IKS |  |  |  |  | ***[Link]*** |
| 5 | SAP | Immobilien |  |  |  |  | ***[Link]*** |
| 6 | SAP | Controlling |  |  |  |  | ***[Link]*** |

Anhang 9 Liste der Unterlagen mit eingeschränktem Zugriff

Grundsätzlich haben alle Mitarbeitende Schreib- und Leserechte im GEVER-System. Für weitere autorisierte Systeme und Ablagen gelten die Zugriffskonzepte gemäss ***[Bearbeitungsvorschriften, siehe Anhang 8]***. Ausnahmen sind in den Metadaten hinterlegt, im Ordnungssystem (OS) auf Stufe Rubrik und/oder im Dossier. Unter folgenden Rubriken im OS sind die Zugriffe eingeschränkt:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | ART DES ZUGRIFFS | Leiter | Bereich sensitiv | GRUPPEN GEMÄSS ORGANIGRAMM | Amtsleitung | Ressortleitung | Dienstleitung | Sachbearbeitende | WEITERE GRUPPEN | Controlling & Finanzen | cc informationsmanagement | Sicherheitsbeauftragte |  |  |
| Ordnungsposition Rubriktitel | Begründung |
| 033.11  Unterlagen zur Amtsführung | - | X | X | - | - | - | - | X | - | Handlungsfähigkeit Amtsleitung |
| 033.12  Unterlagen zur Ressortleitung | - | X | X | X | - | - | - | X | - | Handlungsfähigkeit Ressortleitung |
| 033.211  Unterlagen zur Dienstleitung | - | X | X | X | X | - | - | X | - | Handlungsfähigkeit Dienstleitung |
| 033.212  Personalbeurteilungen und Zielvereinbarungen | X | - | X | X | X | X | - | - | - | Gesetzlicher Rahmen |
| 033.31  Unterlagen zu GL-Sitzungen | - | X | X | X | - | - | - | X | - | Handlungsfähigkeit Geschäftsleitung |
| 145.01  Dienstleistungsverträge | - | X | X | X | - | - | X | X | - | Wahrung des Geschäftsgeheimnisses |
| 152  Ereignisvorbereitung und -bewältigung, Grundlagen | - | X | X | - | - | - | - | - | X | Sicherheitsbestimmungen |

Anhang 10 Anweisungen zum Dossierabschluss für Dossierverantwortliche

Die Anweisungen zum Dossierabschluss gelten im Grundsatz für alle Geschäfte, die in Dossiers bewirtschaftet werden (gemäss Kap. 2.4). Sie gelten für Dossiers im GEVER-System sowie für Dossiers in weiteren Systemen und Ablagen, sofern hier keine spezifischen Regelungen bestehen.[[38]](#footnote-38)

Die jeweils federführenden Mitarbeitenden für ein Geschäft sind dossierverantwortlich und zuständig für die Bereinigung und den Abschluss der Dossiers. Bei Abwesenheit oder Austritt der federführenden Mitarbeitenden geht die Dossierverantwortung an die zuständigen Vorgesetzten.

Die Dossierbereinigung und der Dossierabschluss sollten möglichst zeitnah nach Abschluss eines Geschäfts erfolgen. Jahresdossiers werden jeweils bis ***[Ende Januar des Folgejahres]*** abgeschlossen. Zielvereinbarungsdossiers sollen nach dem Austritt eines Mitarbeitenden abgeschlossen werden. Übrige Dossiers werden bis spätestens ***[3 Monate]*** nach Geschäftsabschluss abgeschlossen.

Das ***[CC INFORMATIONSMANAGEMENT]*** prüft regelmässig ***[alle 6 Monate, jeweils im Mai und November]***,ob Dossiers abgeschlossen werden können. Dabei werden die Dossiers hinsichtlich ihres letzten Aktenzuwachses überprüft. Liegt dieser länger als ***[zwei]*** Jahre zurück, wird mit den federführenden Mitarbeitenden bzw. Dossierverantwortlichen der Organisationseinheit (OE) Kontakt aufgenommen, damit das Dossier abgeschlossen werden kann.

Dossierbereinigung

Wenn ein Geschäft abgeschlossen ist, bereinigt die/der zuständige Mitarbeitende der federführenden OE die zugehörigen Dossiers. Dazu gehören:

* offene Geschäftsvorfälle abschliessen;
* Überprüfung der Inhalte auf Vollständigkeit, Löschen von Doubletten;
* Überprüfung der Metadaten, ob diese vollständig und korrekt vergeben sind;
* Verweise auf andere autorisierte Ablagen prüfen;
* Konvertierung in archivtaugliche Formate;[[39]](#footnote-39)
* Leere Dossiers/Subdossiers löschen.

Anschliessend wird das Geschäft vom Mitarbeitenden zum Dossierabschluss weitergeben.

Dossierabschluss

Das ***[CC INFORMATIONSMANAGEMENT]*** führt anschliessend mit dem Dossierabschluss die folgenden Arbeiten durch:

* Metadaten stichprobenweise kontrollieren, evtl. korrigieren und ergänzen;
* Validierung und Konvertierung in archivtaugliche Formate auslösen;
* Dossierabschluss im System auslösen.

Während das Dossier beim ***[CC INFORMATIONSMANAGEMENT]*** in Abschluss ist, können die Mitarbeitenden im System nicht mehr darauf zugreifen. Nach Abschluss im System ist ein Zugriff im Lesemodus wieder möglich. Um den Zeitraum zwischen dem Geschäftsabschluss durch die Dossierverantwortlichen und dem Dossierabschluss im System so kurz wie möglich zu halten, überprüft das ***[CC INFORMATIONSMANAGEMENT]*** jeweils ***[per Monatsende]***, ob Dossiers in Abschluss gegeben worden sind.

Einmal abgeschlossene Dossiers können nicht mehr ergänzt oder weitergeführt werden. Wird ein Geschäft nach Dossierabschluss weitergeführt, muss ein neues Dossier eröffnet werden.

Anhang 11 Anweisungen zur Aussonderung für das *[CC INFORMATIONSMANAGEMENT]*

Die Anweisungen zur Aussonderung gelten im Grundsatz für alle Informationen, die als Geschäfte bzw. Dossiers bewirtschaftet werden (gemäss Kap. 2.4). Sie gelten für Dossiers im GEVER-System sowie für Dossiers in weiteren Systemen und Ablagen, sofern hier keine spezifischen Regelungen bestehen.[[40]](#footnote-40) Für die Aussonderung von Informationen ausserhalb der Definition von Geschäften/Dossiers unter 2.4 müssen in den Bearbeitungsvorschriften der jeweiligen Systeme/Ablagen spezifische Vorgaben erarbeitet werden.

Das ***[CC INFORMATIONSMANAGEMENT]*** ist verantwortlich für die Aussonderung. Es prüft ***[jährlich, jeweils im Januar]*** gemeinsam mit den zuständigen OE die Systeme und Ablagen dahingehend, ob Unterlagen ausgesondert werden können. Für Dossiers mit beschränkter Zugriffsberechtigung (z. B. Zielvereinbarungsdossiers) wird eine Person aus der Registratur für den Zugriff berechtigt, damit sie die Aussonderung dieser Dossiers durchführen kann.

Aufbewahrung und Löschung

Nicht archivwürdig bewertete Dossiers werden in der ***[VE] für die Dauer der hinterlegten Aufbewahrungsfrist aufbewahrt.*** Die Aufbewahrungsfrist beginnt mit dem letzten Aktenzuwachs eines Dossiers zu laufen.

Die Aufbewahrung erfolgt im GEVER-System bzw. in den Systemen oder Ablagen, in denen die Dossiers gemäss Vorgaben geführt wurden. Nach Ablauf der Aufbewahrungsfrist werden sie durch das ***[CC INFORMATIONSMANAGEMENT bzw. den/die Verantwortlichen autorisierte Systeme und Ablagen]*** periodisch gelöscht.

Die Löschung erfolgt in der Regel im Rahmen der Aussonderung. Im Falle von nicht archivwürdigen Unterlagen, die gemäss DSG besonders schützenswert sind, erfolgt diese Löschung zwingend, sobald die Unterlagen für den Zweck, für den sie erstellt worden sind, nicht mehr benötigt werden. Jede Löschung wird durch ein Löschprotokoll dokumentiert.

Für die Löschung nimmt das ***[CC INFORMATIONSMANAGEMENT]*** die folgenden Arbeitsschritte vor:

* Zusammenstellen der zu löschenden Dossiers und Ausfüllen des Löschprotokolls. ***[Genehmigung durch die Direktion VE]***.
* Löschen der Primärdaten im System (nach dem Vier-Augenprinzip). Dokumentation im Löschprotokoll. Die dazugehörigen Metadaten werden nicht gelöscht, diese dienen als Findmittel für die gelöschten Primärdaten. Bei datenschutzrelevanten Unterlagen: Löschung von Primär- und Metadaten gemäss den Vorgaben DSG.
* Allfällige physisch vorhandene Unterlagen kontrolliert vernichten, Dokumentation im Löschprotokoll.[[41]](#footnote-41)
* Löschprotokoll unterzeichnen, im GEVER-System registrieren und dem BAR zur Kenntnis zustellen (an [anbieten.abliefern@bar.admin.ch](mailto:anbieten.abliefern@bar.admin.ch)).

Das Löschprotokoll[[42]](#footnote-42) enthält auf Stufe Rubrik oder auf der betreffenden tieferen Stufe im Mindesten folgende Informationen:

* Datum und Uhrzeit der Löschung;
* Verantwortliche und durchführende Person(en)/Benutzer (inkl. Rollen/Funktionen);
* Anzahl gelöschter Dossiers/Datensätze;
* Aktenzeichen und Name Ordnungsposition (gemäss Registraturplan/OS ***[VE]***) sowie Titel und Entstehungszeitraum jener Dossiers, deren Daten gelöscht wurden;
* Allenfalls einen inhaltlichen Hinweis zu den Dossiers/Datensätzen, welche gelöscht wurden.

Ablieferung ans BAR zur Archivierung

Archivwürdig bewertete digitale Dossiers müssen dem BAR nach Ablauf der Aussonderungsfrist zur Archivierung abgeliefert werden.[[43]](#footnote-43) Dabei nimmt das ***[CC INFORMATIONSMANAGEMENT]*** die folgenden Arbeitsschritte vor:

* Ablieferung beim BAR anmelden über [anbieten.abliefern@bar.admin.ch](mailto:anbieten.abliefern@bar.admin.ch) (mit Angaben zum Zeitraum, den betroffenen Rubriken sowie dem ungefähren Umfang der abzuliefernden Unterlagen/Daten).
* Erstellung eines SIP (Submission Information Package) gemäss den Vorgaben BAR.[[44]](#footnote-44) Bei Dossiers aus dem GEVER-System kann das SIP automatisch über die Ablieferungsschnittstelle BAR erstellt werden. Bei Dossiers aus Systemen und Ablagen ausserhalb des GEVER-Systems erfolgt das Vorgehen nach Absprache mit dem BAR.
* Übermittlung der SIP an das BAR.

Das BAR bestätigt den Erhalt des SIP, prüft dessen Qualität und archiviert die Daten. Anschliessend erhält das ***[CC INFORMATIONSMANAGEMENT]*** vom BAR eine Archivierungsbestätigung. Nun nimmt das ***[CC INFORMATIONSMANAGEMENT]*** die folgenden Schritte vor:

* Prüfung der Bestätigung BAR (Ablieferungsverzeichnis).
* Löschung der archivwürdig bewerteten Primärdaten der abgelieferten Unterlagen im System (nach dem Vier-Augenprinzip) und Dokumentation mittels Löschprotokoll (Details siehe oben unter «Aufbewahrung und Löschung»). Die dazugehörigen Metadaten werden nicht gelöscht, diese dienen als Findmittel für die gelöschten Primärdaten. Bei datenschutzrelevanten Unterlagen: Löschung von Primär- und Metadaten gemäss den Vorgaben DSG.
* Löschprotokoll (Inhalte siehe oben) im GEVER-System registrieren und dem BAR zustellen.

Die Ablieferung von archivwürdig bewerteten Informationen, die nicht als Geschäfte oder Dossiers gemäss 2.4 geführt werden (z.B. Daten aus Datenbanken), erfolgt nach Absprache mit dem BAR.

Archivwürdig bewertete physische Dossiers werden gemäss den Vorgaben BAR aufbereitet, verzeichnet und abgeliefert.[[45]](#footnote-45)

Zum Umgang mit Handakten und Privatarchiven von Magistratspersonen und Topkader siehe die entsprechenden Merkblätter des BAR.[[46]](#footnote-46)

Der Zugriff für Dritte auf archivierte Unterlagen wird anhand von Schutzfristen geregelt. Die ordentliche Schutzfrist für archivwürdige Unterlagen beträgt 30 Jahre gemäss Art. 9 BGA.[[47]](#footnote-47) Falls davon abweichende, besondere Schutzfristen gemäss Art. 11 oder Art. 12 BGA angewendet werden sollen, müssen diese durch die abliefernde Stelle mit vorliegendem Formular dem BAR gemeldet und begründet werden.[[48]](#footnote-48)

Anhang 12 Anweisung zum Umgang mit klassifizierten und datenschutzrelevanten Informationen und Verschlüsselung

Informationen, welche dem Informations- oder Datenschutz unterstehen (dieser Status ist in den Metadaten ersichtlich), dürfen nur für autorisierte Personen einsehbar und bearbeitbar sein.[[49]](#footnote-49) Dies gilt unabhängig davon, wo die Informationen bewirtschaftet werden (im GEVER-System, in Fachanwendungen, physischen Ablagen etc.).

Dies bedeutet insbesondere:

* Versand und Zugang erfolgen ausschliesslich mit entsprechenden Zugriffsrechten und gemäss Vorgaben ISG/ISV, respektive DSG (z. B. Verschlüsselung).
* Der Zugriff durch eine/n Stellvertreter/in oder Nachfolger/in muss sichergestellt sein für den Fall, dass der/die Berechtigte keinen Zugang (mehr) hat, z. B. infolge Austritts oder Krankheit.
* Die Informationen dürfen auch während kurzer Abwesenheiten oder Pausen nicht offen auf Bildschirmen oder Schreibtischen belassen werden. Unterlagen müssen unverzüglich vom Kopierer/Drucker geholt werden. Das Drucken und Kopieren ist nur mit zugelassenen Druckern und Verfahren gestattet.
* Ablage und Speicherung ist nur in autorisierten Systemen und Ablagen zulässig, deren ISDS[[50]](#footnote-50)-Konzept dies erlaubt. Physische Unterlagen müssen abschliessbar vor dem Zugriff Unberechtigter geschützt werden.

Die Schutzwürdigkeit und der Verteiler klassifizierter Informationen müssen durch die autorisierten Personen laufend ***[mindestens alle fünf Jahre]*** überprüft und allenfalls angepasst werden.

Auch klassifizierte (INTERN, VERTRAULICH, GEHEIM gemäss ISG/ISV) und datenschutzrechtliche Informationen müssen im Falle der Archivwürdigkeit dem BAR abgeliefert werden.

Verschlüsselung

Die Verschlüsselung von Informationen sollte auf ein Minimum beschränkt werden, damit die langfristige Benutzbarkeit und Bewirtschaftung gewährleistet wird. Die Verschlüsselung erfolgt gemäss Verschlüsselungskonzept GEVER oder gemäss ISDS-Konzept der entsprechenden Ablage.

Im Folgenden wird detailliert beschrieben, **was** verschlüsselt werden muss bzw. darf, **wer** verschlüsseln darf und **wann** entschlüsselt werden muss bzw. kann sowie wer entschlüsseln muss bzw. kann:

* Informationen, die gemäss ISG/ISV als ***[INTERN]*** klassifiziert sind oder andere schutzwürdige Informationen (z.B. «Personendaten» nach DSG, Ausschreibungsunterlagen WTO) dürfen für die Übermittlung verschlüsselt werden. Deren Speicherung im (GEVER-)System erfolgt jedoch unverschlüsselt.[[51]](#footnote-51) Verschlüsselte E-Mails werden entschlüsselt und anschliessend unverschlüsselt abgelegt.
* Informationen, die gemäss ISG/ISV als ***[VERTRAULICH]*** klassifiziert sind sowie Informationen, die aus Sicht Datenschutz mit «enthält besonders schützenswerte Personendaten» bewertet sind, müssen verschlüsselt abgespeichert und verschlüsselt versendet werden. Verschlüsselte E-Mails werden entschlüsselt und neu verschlüsselt abgelegt. In Dossiers mit eingeschränktem Zugriff werden E-Mails unverschlüsselt abgelegt.
* Informationen bis und mit Stufe ***[VERTRAULICH]*** dürfen im GEVER-System abgelegt werden, [GEHEIM] klassifizierte Informationen sind in einem dezidierten System abzulegen und werden dort ebenfalls verschlüsselt. Eine allfällige Übermittlung von ***[GEHEIM]*** klassifizierte Informationen darf nur persönlich erfolgen (kein E-Mail-Versand).
* [Der/die zuständige Mitarbeitende] ist befugt, klassifizierte Informationen zu verschlüsseln.

Bei einer Änderung des Klassifikationsstatus oder bei Entklassifizierung oder vor der Registrierung (ausgenommen ***[GEHEIME und VERTRAULICHE]*** Informationen) müssen die entsprechenden Informationen ***[von den zuständigen Mitarbeitenden]*** entschlüsselt und die zugehörigen Metadaten entsprechend angepasst werden.

Das BAR akzeptiert in geeigneter Weise verschlüsselte Dokumente im SIP aus GEVER.[[52]](#footnote-52) VERTRAULICH klassifizierte Dossiers und Dossiers mit besonders schützenswerten Personendaten können somit verschlüsselt an das BAR abgeliefert werden. Dossiers mit verschlüsselten Informationen müssen in separaten SIP abgeliefert werden.

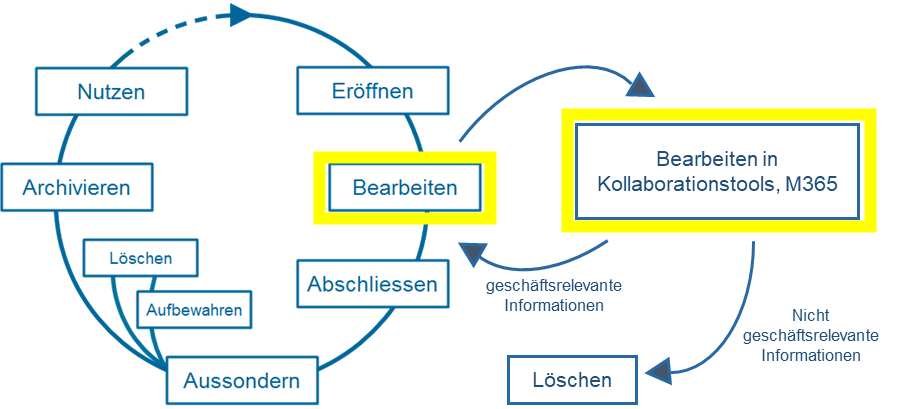
Vor der Ablieferung müssen die zuständigen Mitarbeitenden des BAR in der Verschlüsselungsrolle ergänzt werden, damit die Dokumente im BAR entschlüsselt werden können.

Aufgrund der Vorgaben Artikel 25 ISG/ISV und um den Aufwand in Grenzen zu halten, muss vor der Ablieferung geprüft werden, ob die Klassifikation VERTRAULICH noch angemessen ist.

Anhang 13 Anweisung zur Nutzung von Kollaborationstools und temporären Ablagen

Kollaborationstools inkl. M365 Services gelten als temporäre Ablagen.[[53]](#footnote-53) Dies bedeutet, dass geschäftsrelevante Informationen aus solchen Tools und Ablagen regelmässig, spätestens jedoch nach Abschluss der Arbeiten ins GEVER-System (bzw. in die dafür vorgesehene ständige Ablage) überführt werden müssen.

GEVER-System bzw. Ständige Ablage temporäre Ablage

M365 Services

Geschäftsrelevante Informationen dürfen grundsätzlich temporär mit M365 Services bearbeitet werden. Nach Abschluss der Arbeiten müssen diese im Dossier im GEVER-System bzw. im dafür vorgesehenen System abgelegt werden.[[54]](#footnote-54) Einschränkungen gelten insbesondere für sensible Informationen gemäss DSG und ISG.

Auf Ebene Departement und Verwaltungseinheit sind konkrete Vorgaben zur Nutzung von M365 definiert.[[55]](#footnote-55) Diese betreffen insbesondere:

* Schutzbedarf der Informationen der ***[VE]***,Klassifizierung nach ISG und DSG und Zuordnung der Labels;
* Nutzung der einzelnen Services (Varianten Cloud und on premise), Zweck, Geschäftstypen, Zusammenarbeit;
* Lifecycle-Management, u.a. Eröffnung / Bearbeitung, Art und Häufigkeit der Sicherung und Rückführung ins Geschäftsdossier im GEVER-System bzw. im betroffenen System / in der betroffenen Ablage;
* Zuständigkeiten, Verantwortlichkeiten und Controlling.

***[ggf. Confluence, Jira, weitere]***

*[Optional: Anhang 14 Liste der Zusatzkomponenten]*

1. Einschliesslich zentraler und dezentraler Bundesverwaltung, Parlamentsdienste, weitere Behörden des Bundes und Organisationen, die Bundesaufgaben wahrnehmen gemäss Regierungs- und Verwaltungsorganisationsgesetz RVOG Art. 2 Abs. 4. Siehe auch Bundesgesetz über die Archivierung BGA, Abschnitt 1, Art.1 sowie Regierungs- und Verwaltungsorganisationsverordnung (RVOV), Anhang 1. [↑](#footnote-ref-1)
2. Regierungs- und Verwaltungsorganisationsgesetz RVOG (SR **172.010**), Art. 22, Abs. 1. [↑](#footnote-ref-2)
3. Regierungs- und Verwaltungsorganisationsgesetz RVOG (SR **172.010**), Archivierungsgesetz BGA (SR **152.1)**, Datenschutzgesetz DSG (SR **235.1**) sowie Datenschutzverordnung DSV (SR **235.11**), Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung BGÖ (SR **152.3**), Informationssicherheitsgesetz ISG (SR **128**) und Informationssicherheitsverordnung ISV (SR **128.1**), Schweizerisches Zivilgesetzbuch ZGB (SR **210**), Obligationenrecht OR SR **220**), Geschäftsbücherverordnung GebüV (SR **221.431**), GEVER-Verordnung (SR **172.010.441**), GEVER Standards: A290, I017, E018, Einsatzrichtlinien Microsoft E031 etc. ***[ggf. weitere Grundlagen, z.B. departementale Vorgaben ergänzen]*** [↑](#footnote-ref-3)
4. Autorisiert bedeutet: Elektronische Systeme neben dem standardisierten GEVER erfüllen die Voraussetzungen von Art. 3 und Art. 4 der GEVER-Verordnung. Physische Ablagen erfüllen die Voraussetzungen gemäss GEVER-Verordnung Art. 5 bzw. … Dies schliesst ein: Fachanwendungen, Datenbanken, Kollaborationstools, M365 Services u.a., in denen Informationen temporär oder dauerhaft gespeichert werden. [↑](#footnote-ref-4)
5. Gemäss GEVER-Verordnung, Art.2. Physische Ablagen sind grundsätzlich nicht erlaubt. Ausnahmen werden in ***[Anhang 8]*** abschliessend aufgelistet. Siehe auch ***[Anhänge 6 und 7]***. [↑](#footnote-ref-5)
6. Gemäss GEVER-Verordnung Art. 3 und 4. [↑](#footnote-ref-6)
7. Die Bearbeitung von geschäftsrelevanten Informationen in Kollaborationstools unterliegt entsprechenden Bestimmungen von Bundesverwaltung, ***[Departement]*** und ***[Verwaltungseinheit]***. Einsatzrichtlinien Microsoft E031. [↑](#footnote-ref-7)
8. Z.B. Aufgabenprinzip, Aussagekraft und Abgrenzbarkeit Titel, einheitliche Systematik. Gemäss den Vorgaben von GEVER Bund bzw. den Vorgaben des BAR. [↑](#footnote-ref-8)
9. Art. 13 Informationssicherheitsgesetz (ISG, SR 128) und Art. 18 ff. Informationssicherheitsverordnung (ISV, SR 128.1) Die Klassifizierungsstufen gemäss ISG / ISV sind INTERN, VERTRAULICH und GEHEIM. [↑](#footnote-ref-9)
10. Siehe Art. 5 DSG und Art. 57h ff. RVOG. [↑](#footnote-ref-10)
11. Der Zeitpunkt, wann alle relevanten Informationen effektiv zu einem Dossier zusammengeführt werden, kann in autorisierten Systemen und Ablagen ausserhalb des GEVER-Systems variieren und wird in den entsprechenden Bearbeitungsreglementen geregelt (***[Anhang 8]****).* [↑](#footnote-ref-11)
12. ***[Optional: Eine Liste der möglichen Zusatzkomponenten im GEVER-System findet sich im [Anhang 14]. Noch nicht vorhandene Zusatzkomponenten können beim [CC INFORMATIONSMANAGEMENT] via [Administrativen Auftrag im GEVER-System] beantragt werden.]*** [↑](#footnote-ref-12)
13. E-Mails, Faxe, Telefonnotizen sowie Beilagen (Mikrofichen, Mikrofilme, Tonspuren, CDs, Videos, Fotos, Bilder etc.). [↑](#footnote-ref-13)
14. Auch wenn Unterlagen in autorisierten Systemen / Ablagen ausserhalb des GEVER-Systems bewirtschaftet werden, erfolgt die Zuordnung zu einer Aufgabe im OS. [↑](#footnote-ref-14)
15. Es sind jeweils die spezifischen Bearbeitungsvorschriften gemäss ***[Anhang 8]*** beizuziehen. [↑](#footnote-ref-15)
16. Organisatorisch ist zu regeln, ob alle Unterlagen zentral in der VE bestellt werden oder nur Unterlagen in Schutzfrist. Technisch ist nur die Bestellung von Unterlagen in Schutzfrist gebunden an die Rolle «Abliefernde Stelle». Frei zugängliche Unterlagen können die federführenden Stellen auch selbst bestellen. [↑](#footnote-ref-16)
17. Gemäss Art. 12 der Weisungen über die Anbietepflicht und die Ablieferung von Unterlagen an das Bundesarchiv WAA vom 28. September 1999 dürfen von abgelieferten Unterlagen grundsätzlich keine Kopien in der abliefernden Stelle verbleiben respektive wieder in das GEVER-System integriert werden. [↑](#footnote-ref-17)
18. Nach der Prüfung kommuniziert das BAR den Entscheid ***[VE]*** gegenüber dem Gesuchsteller/der Gesuchstellerin. [↑](#footnote-ref-18)
19. Die Rolle von Super-User/innen weiterer autorisierter Systeme und Ablagen wird in deren spezifischen Bearbeitungsvorschriften ***[siehe Anhang 8]*** beschrieben. [↑](#footnote-ref-19)
20. Unter Kap. 4 sind zusammenfassend übergreifende, koordinierende Aufgaben und Rollen bezüglich der autorisierten Systeme und Ablagen festgehalten. Die spezifischen Rollen und Aufgaben werden in den Bearbeitungsvorschriften der jeweiligen Systeme und Ablagen geführt (siehe ***[Anhang 8]***). [↑](#footnote-ref-20)
21. Siehe auch das Systemkonzept GEVER. [↑](#footnote-ref-21)
22. Die Webapplikation StrucTool des BAR dient dazu, das OS der VE und weitere Strukturen (autorisierte Ablagen, Fachanwendungen) inkl. Metadaten und Bewertung zu erstellen, zu aktualisieren und zu verwalten. Zudem werden über StrucTool analoge Ablieferungen bearbeitet. [↑](#footnote-ref-22)
23. BV = Bundesverwaltung (BVerw). [↑](#footnote-ref-23)
24. Das BAR empfiehlt, dass mehrere Personen in der VE diese Rolle innehaben (Stellvertretung und Gewährleistung des Zugangs während Abwesenheiten). Die Rolle ist personengebunden, jedoch nicht an eine Stelle. Oft wird sie von Mitarbeitenden des CC Informationsmanagements bzw. der Registratur oder des Archivdiensts wahrgenommen. Zudem haben meistens auch die Juristen und Juristinnen, welche Einsichtsgesuche prüfen, die Rolle «Abliefernde Stelle». So können sie betroffene Dossiers selbst bestellen und herunterladen/konsultieren. [↑](#footnote-ref-24)
25. Die Definitionen richten sich nach der Terminologiedatenbank der Bundesverwaltung Termdat, für die OV relevanten rechtlichen Grundlagen sowie dem Gebrauch in den vorliegenden OV. [↑](#footnote-ref-25)
26. Gemäss Erläuterungen zur GEVER-Verordnung, Artikel 1, Absatz 2. [↑](#footnote-ref-26)
27. Die organisatorische Struktur und OE-Zugehörigkeit können dem aktuellen Organigramm ***[VE]*** im ***[Intranet]*** entnommen werden. [↑](#footnote-ref-27)
28. Für weitere Informationen zur Negativliste siehe das separate [Merkblatt Negativliste](https://www.bar.admin.ch/dam/bar/de/dokumente/kundeninformation/merkblatt_negativliste.pdf.download.pdf/merkblatt_negativliste.pdf) des BAR. [↑](#footnote-ref-28)
29. Gemäss GEVER-Verordnung Art. 3 und 4. [↑](#footnote-ref-29)
30. Siehe [Post (admin.ch)](https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeitsbereich/kommunikations--und-informationsmittel/brief--und-elektronische-post.html) auf der Webseite des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). [↑](#footnote-ref-30)
31. Erfolgt je nach System unterschiedlich. Im GEVER-System automatisch über «Objekt Eingang». Doppelablage vermeiden. [↑](#footnote-ref-31)
32. Als persönliche Post gelten mit „privat“, „persönlich“ oder „eigenhändig“ adressierte Unterlagen. Das blosse Voranstellen des Namens genügt nicht, um zu zeigen, dass die Post einem Mitarbeitenden als Privatperson zugestellt wird. Stellt der Mitarbeitende nach Öffnen des Briefs fest, dass die als „privat“ gekennzeichnete Post geschäftsrelevant ist, muss er sie dem ***[CC INFORMATIONSMANAGEMENT]*** zum Einscannen geben. Siehe auch das „Merkblatt private/persönliche Post“ von GEVER Bund auf der Website der Bundeskanzlei: [Merkblatt private/persönliche Post](https://www.bk.admin.ch/dam/bk/de/dokumente/gever/Merkblaetter/merkblatt_privatepersoenlichepost.pdf.download.pdf/merkblatt_privatepersoenlichepost.pdf). [↑](#footnote-ref-32)
33. GEVER-Verordnung, 2. Abschnitt, Art. 5. [↑](#footnote-ref-33)
34. Siehe auch GEVER-Verordnung Art. 5 Abs. 3b. [↑](#footnote-ref-34)
35. Siehe Art. 4 Absatz 3 der Archivierungsverordnung VBGA und Art. 4 Absatz 1 der Weisungen über die Anbietepflicht und die Ablieferung an das Bundesarchiv WAA. Die physische Version von Staatsverträgen, internationalen Abkommen und anderen Instrumenten der internationalen Zusammenarbeit werden unmittelbar nach ihrer Ausfertigung bzw. Unterzeichnung dem BAR (bei Staatsverträgen via Direktion für Völkerrecht) abgeben. [↑](#footnote-ref-35)
36. Dauerhafte Bewirtschaftung: GEVER-Verordnung Artikel 3, temporäre Bewirtschaftung: GEVER-Verordnung Artikel 4. [↑](#footnote-ref-36)
37. Dies kann unter [17.11.2022 - Datensammlung anmelden - Verzeichnisse melden (DataReg) (admin.ch)](https://www.edoeb.admin.ch/edoeb/de/home/kurzmeldungen/2022/20221117_datareg.html) vorgenommen werden. [↑](#footnote-ref-37)
38. Gemäss ***[Anhang 8]*** und dort verlinkten Bearbeitungsvorschriften. [↑](#footnote-ref-38)
39. Im GEVER-System: Von Formaten ohne hinterlegten Konvertierungspfad. Siehe auch GEVER-Wiki: unterstützte Dateiformate 🡪 Spalte Konvertierung [Unterstützte Dateiformate - GEVER-Wiki Bund Public - ISCeco-Wiki (admin.ch)](https://services.isceco.admin.ch/confluence-pr/pages/viewpage.action?pageId=88932987). [↑](#footnote-ref-39)
40. Gemäss ***[Anhang 8]*** und dort verlinkten Bearbeitungsvorschriften. [↑](#footnote-ref-40)
41. Gemäss ***[Anhang 7 und 8]***. [↑](#footnote-ref-41)
42. Siehe das [Merkblatt Löschprotokoll](https://www.bar.admin.ch/dam/bar/de/dokumente/kundeninformation/Merkblatt%20L%C3%B6schprotokoll.pdf.download.pdf/Merkblatt_L%C3%B6schprotokoll_-_d.pdf) des BAR. [↑](#footnote-ref-42)
43. Aussonderungsfrist gemäss BGA: Archivwürdig bewertete Dossiers müssen dem BAR abgeliefert werden, wenn Sie in der Verwaltungseinheit nicht mehr ständig benötigt werden. [↑](#footnote-ref-43)
44. Siehe die Webseite des BAR unter: <https://www.bar.admin.ch/bar/de/home/archivierung/ablieferung/digitale-unterlagen.html>. [↑](#footnote-ref-44)
45. Siehe Webseite des BAR unter: <https://www.bar.admin.ch/bar/de/home/archivierung/ablieferung/analoge-unterlagen.html>. [↑](#footnote-ref-45)
46. Siehe das [Merkblatt Handakten und Privatarchive für Magistratspersonen der Bundesverwaltung](https://www.bar.admin.ch/dam/bar/de/dokumente/kundeninformation/merkblatt_handaktenundprivatarchivefuermagistratspersonenderbund.pdf.download.pdf/merkblatt_handaktenundprivatarchivefuermagistratspersonenderbund.pdf) und [Merkblatt Handakten und Privatarchive für Topkader der Bundesverwaltung](https://www.bar.admin.ch/dam/bar/de/dokumente/kundeninformation/merkblatt_handaktenundprivatarchivefuertopkaderderbundesverwaltu.pdf.download.pdf/merkblatt_handaktenundprivatarchivefuertopkaderderbundesverwaltu.pdf) des BAR. [↑](#footnote-ref-46)
47. Art. 9. Abs. 1 des Archivierungsgesetzes BGA. [↑](#footnote-ref-47)
48. Art. 5 Abs. 2 Weisungen über die Anbietepflicht und die Ablieferung von Unterlagen an das Bundesarchiv WAA. Für den Zugriff der VE auf die eigenen Unterlagen siehe Kapitel 3.8 Nutzen. [↑](#footnote-ref-48)
49. Gemäss ISG /ISV und DSG sowie Nachfolgeerlasse. [↑](#footnote-ref-49)
50. ISDS = Informationssicherheit und Datenschutz. [↑](#footnote-ref-50)
51. Vgl. Bearbeitungsvorschriften in ***[Anhang 8]***, ISG/ISV sowie Weisungen des Bereichs Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei (BK) zur Informatiksicherheit. [↑](#footnote-ref-51)
52. Für die Ablieferung verschlüsselter Informationen aus anderen Systemen und Ablagen sind die Ablieferungsmodalitäten in den entsprechenden Bearbeitungsvorschriften zu konsultieren bzw. ist die Ablieferung fallspezifisch zu klären. [↑](#footnote-ref-52)
53. Gemäss GEVER-Verordnung Art 4. [↑](#footnote-ref-53)
54. Siehe Einsatzrichtlinien Microsoft E031. [↑](#footnote-ref-54)
55. ***[Link Vorgaben Departement], [Link Vorgaben VE]***. [↑](#footnote-ref-55)