

Richtlinien für den Datenschutz innerhalb der ECAP

Inhalt

Einführung	1
Datenspeicherung, -veränderung und -nutzung	2
Datentypen	2
Zugangsarten und Mitarbeiterrollen	3
Bekanntgabe der Daten an Dritte	4
Einfache Personendaten	4
Besondere Personendaten	4
Nicht personenbezogene Daten	5
Zusammenfassung der Arbeitsanweisungen	6

Einführung

Diese Richtlinien legen die allgemeinen Anweisungen für die Speicherung, die Pflege und die Erhaltung der Daten innerhalb der ECAP fest. Sie berücksichtigen alle geltenden gesetzlichen Bestimmungen¹ und sie müssen in den Regionalstellen unter Einhaltung der Anweisungen der zuständigen Behörden oder Auftraggeber umgesetzt werden. Diese Anweisungen müssen als Ergänzung und Erweiterung dieses Dokumentes betrachtet werden.

Eventuelle regionale Anpassungen sollen begründet werden und müssen die gleiche Datensicherheit garantieren.

Die Richtlinien dienen zur Erreichung folgender Ziele:

- Garantie des Schutzes der persönlichen «sensiblen» Daten vor internen und externen Angriffen und vor Missbrauch
- Effizienz in der Kursverwaltung und -durchführung
- Berücksichtigung der Bedürfnisse und der Interessen der Teilnehmenden
- Berücksichtigung der Bedürfnisse der Auftraggeber und/oder der subventionierenden Stellen (z.B. Berichterstattung, usw.).

Allgemeine Massnahmen

Bei ECAP werden generell folgende organisatorische und technische Massnahmen umgesetzt:

- Es ist den Mitarbeitenden nicht zugelassen personenbezogenen Daten auf Geräte zu speichern, die nicht der ECAP gehören
- Alle Mitarbeitenden nehmen diese Richtlinien und eventuelle zusätzliche Anweisungen sämtlicher Auftraggeber zum Datenschutz zur Kenntnis und verpflichten sich, sie einzuhalten

¹ Revidiertes Bundesgesetz über den Datenschutz revDSG (Gültig ab 1.09.2023), Verordnung über den Datenschutz DSV (31.08.2022), ev. kantonale Datenschutzgesetze und Verordnungen, Weisungen und Verordnungen von SECO, SEM und SBFJ

- Alle Server sowohl der ECAP als auch ihrer Partner befinden sich in der Schweiz
- Die Transaktionen werden protokolliert
- Der Zugang zu personenbezogenen Daten ist personalisiert, Rollen basiert und Passwort gesichert
- Eine Auswertung der aktiven Benutzer und ihrer Berechtigungen steht im System zur Verfügung (Rollen-Audit)
- Benutzer können gezwungen werden, das Passwort neu zu setzen
- Unsichere Passwörter werden vom System nicht zugelassen
- Eine Zwei-Faktor Authentifizierung steht zur Verfügung
- Von ECAP implementierte Webseiten verfügen über einen Hinweis mit Link auf Datenschutz-Richtlinien und die Verwendung von Cookies.

Datenspeicherung, -veränderung und -nutzung

Die Daten, die von der ECAP gespeichert und aufbewahrt werden, dienen nur der Organisation und der Verwaltung der eigenen Aktivitäten unter Vorbehalt eventueller Vorgaben der Auftraggeber. Sie können nicht gesammelt werden, ohne dass die Betroffenen davon Kenntnis haben, und können nicht für andere Zwecke verwendet werden. Alle Mitarbeitenden verpflichten sich, Daten, auf die sie Zugriff haben, nur für die Erfüllung der eigenen Aufgaben zu verwenden.

Die Erhebung und Speicherung von Daten erfolgt nach drei Prinzipien²

- Berechtigte Personen haben nur auf diejenigen Personendaten Zugriff, die sie zur Erfüllung ihrer Aufgaben benötigen (Zugriffskontrolle)
- Nur berechtigte Personen haben Zugang zu den Räumlichkeiten und Anlagen, in denen Personendaten bearbeitet werden (Zugangskontrolle)
- Unbefugte Personen haben keinen Zugang zu den Daten sowie zu Datenbearbeitungssystemen oder zu Mitteln zur Datenübertragung (Benutzerkontrolle).

Die nicht-Einhaltung dieser Grundprinzipien oder der Anweisungen, die in diesem Papier enthalten sind, wird als mangelhaftes Verhalten betrachtet, gilt als Grund für die Kündigung des Arbeitsverhältnisses gemäss Art. 12 des GAV und kann in schwerwiegenden Fällen zu einer Anzeige bei den Strafbehörden führen.

Datentypen

Es wird zwischen folgenden Datentypen unterschieden:

Kursdaten
○ Kursstart und -ende ○ Präsenzlisten ○ Kursjournal ○ Konzept, Ausschreibung, Zielgruppe, Ziele, Inhalte usw.
Personaldaten
○ Kursadministrative Daten: Dozentenbuchungen und -einsätze; Termine und Honorare ○ Personen- und lohn- und versicherungsbezogene Daten

² Art. 3.1 DSV

Daten der Teilnehmenden
○ Kursadministrative Daten: Personalien, Anmeldungen usw. ○ Personen- und kursbezogene Daten: Lebensläufe, Prüfungsergebnisse, Noten, Zertifikate usw.
Kontaktdaten
○ Personalien von Kontaktpersonen, Auftraggebern und zuweisenden Stellen
Buchhaltung
○ Finanzbuchhaltung ○ Lohnbuchhaltung ○ Debitoren und Kreditoren
Korrespondenz
○ Eingehende und ausgehende E-Mail ○ Eingehende und ausgehende Briefe
Nicht personenbezogene Arbeitsunterlagen
○ Kurskonzepte ○ Kurspläne ○ Formulare ○ usw.

Zugangsarten und Mitarbeiterrollen

Es sind verschiedene Zugriffsarten auf die Daten vorgesehen aufgrund von sieben verschiedenen Kategorien von Mitarbeitenden:

1. GL – Geschäftsleitung
2. RL – Regionalstellenleitungen
3. BL – Bereichsleitungen
4. S – Sekretariatsangestellte
5. KL – Kursleitende
6. Adm - Administration
7. IT-Support Abteilung

Kategorie	Aufgaben
GL	• verabschiedet die Richtlinien und überwacht deren Umsetzung • bestimmt der/die Datenschutzbeauftragte/r • erteilt und verwaltet die Zugangsrechte zu den Datenbanken Tocco und Abacus • entscheidet in Zweifelsfällen
RL	• sind zuständig für die nötigen organisatorischen, logistischen und infrastrukturellen Voraussetzungen und Massnahmen zur Umsetzung der Richtlinien in ihrem Kompetenzbereich • überwachen die Umsetzung der Richtlinien seitens ihrer Mitarbeitende • erteilen Aufträge an die IT-Support Abteilung • melden Probleme und Engpässe • sind gegenüber der GL rechenschaftspflichtig

BL, S und KL	• setzen die Richtlinien in ihren Kompetenzbereichen um • melden Probleme und Engpässe • sind gegenüber den RL rechenschaftspflichtig
Adm.	• setzt die Richtlinien in ihren Kompetenzbereichen um
IT-Support	• ist verantwortlich für die Bereitstellung der nötigen IT-Infrastruktur inkl. ECAP-Plattform und Lizenzen • bereitet Login, Profile und kollektive und individuelle Arbeitsbereiche in Absprache mit der GL und den RL vor und garantiert die Geheimhaltung der Informationen • überwacht die Umsetzung der Richtlinien und meldet den RL und der GL ev. unkorrekte Handlungen • unterstützt die Mitarbeitenden bei der Lösung von Problemen • stellt das Löschen der Daten nach der entsprechenden Aufbewahrungsfrist sicher • ist gegenüber der GL rechenschaftspflichtig
Daten-schutzbe-auftragte/r	• überwacht die Umsetzung dieser Richtlinien, sowie der Anweisungen der Auftraggebende • ist der Anlaufpunkt für alle, die Informationen über gespeicherte Daten und deren Verwendung benötigen.

Bekanntgabe der Daten an Dritte

Einfache Personendaten

Grundsätzlich werden Daten nur für die eigenen Aktivitäten gespeichert und nicht an Dritte bekanntgegeben.

Es können einfache Personendaten (administrative und kursbezogene Informationen) an Institutionen oder Auftraggeber bekanntgegeben werden, wenn

- eine gesetzliche oder vertragliche³ Bestimmung dazu verpflichtet
- dies zur Erfüllung einer gesetzlichen oder vertraglichen Aufgabe erforderlich ist.
In diesen Fällen müssen die betroffenen Personen im Voraus informiert werden, dass eine Bekanntgabe der Daten möglich oder vorgesehen ist.
- das im Voraus mit den betroffenen Personen ausdrücklich vereinbart worden ist⁴ und die Daten anonymisiert werden.

Besondere Personendaten

Besondere Personendaten werden nur an Behörden bekanntgegeben, wenn sie schriftlich verlangt werden und

- ein Gesetz ausdrücklich dazu verpflichtet
- wenn dies nicht ausdrücklich im spezifischen Mandat bzw. Leistungsauftrag ausgeschlossen ist
- dies zur Erfüllung einer in einem Gesetz klar umschriebenen Aufgabe zwingend notwendig ist

³ Z.B. eine Leistungsvereinbarung, eine Kostengutsprache oder eine Zuweisung einer Behörde sollen auch als Vertrag wahrgenommen werden.

⁴ Z.B. für Forschungszwecke.

- im Einzelfall die betroffene Person ausdrücklich zugestimmt hat oder falls sie dazu nicht in der Lage ist, die Bekanntgabe in ihrem Interesse liegt und ihre Zustimmung in gutem Treu und Glauben vorausgesetzt werden kann.

Um zu entscheiden, ob Personendaten bekannt gegeben werden sollen oder können, wird die Checkliste des Datenschutzbeauftragten des Kantons Basel-Stadt⁵ als Hilfsinstrument benützt. In den Zweifelsfällen entscheidet die Geschäftsleitung.

Nicht personenbezogene Daten

Es werden grundsätzlich nur statistische und abrechnungstechnische Informationen über die ECAP-Aktivitäten bekanntgeben. Informationen oder Unterlagen, die dem Copyright unterstehen und/oder innerhalb der Arbeitstätigkeit bei ECAP oder in deren Auftrag gesammelt und gespeichert worden sind, können nicht ohne Einverständnis der Geschäftsleitung an Dritte weitergeleitet werden. Es können keine Daten an Dritte bekanntgegeben werden, die der ECAP direkt oder indirekt schaden können.

⁵ Siehe <https://www.dsb.bs.ch/handreichungen/checkliste-bekanntgabe.html>

Zusammenfassung der Arbeitsanweisungen

Beschreibung	Speichermedium u. -ort	Speicherdauer ⁶	Wer hat Zugang	Datenschutz
1. Kursdaten				
1.1 Präsenzlisten	1.1.1 Die Präsenzlisten sind in der Regel elektronisch erfasst und die Informationen bleiben in der Datenbank Tocco gespeichert	Uneingeschränkt	➤ GL, Adm: uneingeschränkt ➤ S, BL, RL: uneingeschränkt, Filter auf die eigenen Kurse ➤ KL: nur für ihre laufenden Kurse	Passwortgeschütztes individuelles Login mit unterschiedlichen Rollen
	1.1.2 Ev. Unterlagen im Papierformat werden in den Archiven der Regionalstellen gespeichert. Nach 10 Jahren sollen sie ins ECAP-Archiv transferiert werden	Uneingeschränkt	➤ S, BL, RL: uneingeschränkt ➤ KL: nur für ihre laufenden Kurse	Geschlossene Räume bzw. Schränke mit Zugang nur für Berechtigte
1.2 Kursjournal⁷	1.2.1 Es wird elektronisch auf den ECAP-Servern ⁸ gespeichert	10 Jahre	➤ S, BL, RL: eingeschränkt auf die eigene Regionalstelle	Passwortgeschütztes individuelles Login.
	1.2.2 Ev. Unterlagen im Papierformat werden in den Archiven der Regionalstellen gespeichert. Nach 10 Jahren sollen sie ins ECAP-Archiv transferiert werden	Uneingeschränkt	➤ S, BL, RL: uneingeschränkt ➤ KL: nur für ihre Kurse	Geschlossene Räume bzw. Schränke mit Zugang nur für Berechtigte
1.3 Konzepte	1.3.1 Sie werden auf den ECAP-Servern gespeichert	Uneingeschränkt	➤ BL, RL, GL: uneingeschränkt	Passwortgeschütztes individuelles Login

⁶ Bei den Angaben zur Dauer der Datenspeicherung handelt es sich um eine allgemeine Angabe, die gültig ist, wenn es keine spezifischen Anweisungen von den Auftraggebern oder den Subventionsbehörden gibt.

⁷ Die Kursjournale enthalten keine personenbezogenen Daten.

⁸ Alle Server sowohl der ECAP als auch ihrer Partner befinden sich in der Schweiz.

2. Personaldaten				
2.1 Kursadministrative Daten ➤ Personalien ➤ Unterrichtspensum ➤ Anstellungsdauer ➤ Einsatzplan ➤ Qualifikation	2.1.1 Die Informationen werden ausschliesslich in den Datenbanken tocco und Abacus gespeichert	Uneingeschränkt	➤ GL, Adm: uneingeschränkt ➤ S, BL, RL: eingeschränkt auf die eigene Regionalstelle und die eigene Kompetenzbereiche	Passwortgeschütztes individuelles Login mit unterschiedlichen Benutzerrollen
	2.1.2 Ev. Unterlagen im Papierformat werden in den Archiven der Regionalstellen gespeichert. Nach 10 Jahren werden alle Informationen vernichtet.	10 Jahre	➤ S, BL, RL: eingeschränkt auf die eigene Regionalstelle und die eigene Kompetenzbereiche	Geschlossene Räume bzw. Schränke mit Zugang nur für Berechtigte
2.2 Persönliche lohn- u. versicherungsbezogene Daten: ➤ Bankverbindung ➤ Alle für die Lohnzahlung nötigen Informationen ➤ Alle von den Sozialversicherungen verlangte Informationen	2.2.1 Die Informationen werden ausschliesslich in der Datenbank Abacus und auf dem Server der Administration gespeichert	Uneingeschränkt	➤ GL, Adm	Passwortgeschütztes individuelles Login mit unterschiedlichen Benutzerrollen
	2.2.2 Die Unterlagen im Papierformat werden im Archiv der Adm aufbewahrt	10 Jahre nach Ende des Arbeitsverhältnisses	➤ GL, Adm	Geschlossene Räume mit Zugang nur für Berechtigte
2.3 Personaldossier ➤ Bewerbungsunterlagen ➤ Arbeitsverträge ➤ MAG, Verwarnungen usw. ➤ Zeugnisse ➤ MAG	2.3.1 Die elektronische Unterlagen werden im Arbeitsordner der Regionalstellenleitung und auf dem Server der Administration gespeichert	Arbeitsordner der RL: Bis zu Ende des Arbeitsverhältnisses Server der Administration: 10 Jahre nach Ende des Arbeitsverhältnisses	➤ RL: eingeschränkt auf die eigene Regionalstelle ➤ GL, Adm: Uneingeschränkt	Passwortgeschütztes individuelles Login
	2.3.2 Die Unterlagen im Papierformat werden in geschlossenen Schränken im Büro der Regionalstellenleitung und im Archiv der Administration aufbewahrt	Büro der RL: Bis zu Ende des Arbeitsverhältnisses Archiv der Administration: 10 Jahre nach Ende des Arbeitsverhältnisses	➤ RL: eingeschränkt auf die eigene Regionalstelle ➤ GL, Adm: Uneingeschränkt	Geschlossene Räume bzw. Schränke mit Zugang nur für Berechtigte

3. TN-Daten

3.1 Kursadministrative Daten:

- Personenangaben
- Adresse (Korrespondenz u. Rechnung)
- Telefon und E-Mail
- Nationalitäten
- Sprachen
- Ev. Aufenthaltsbewilligung
- Einstufungen, Lernergebnisse und Kursbestätigungen
- Kontaktpersonen
- Korrespondenz mit den zuweisenden Stellen
- Ev. Marketinginformationen
- Ev. Reduktionsunterlagen
- usw.

Es werden nur die Daten gespeichert, die nötig sind für

- die Kursdurchführung u. -verwaltung
- die Erstellung und die ev. Zweitaustellung von Zertifikaten und Bestätigungen
- die Berichterstattung und die Abrechnung gegenüber zuweisenden und/oder subventionierenden Stellen
- die Vereinfachung von zukünftigen weiteren Anmeldungen.

Es ist strikt verboten, Informationen über Religionszugehörigkeit und/oder politische Meinungen zu sammeln und zu speichern.

3.1.1 Die Informationen werden **elektronisch** ausschliesslich in der Datenbank Tocco gespeichert

3.1.2 Die Unterlagen im Papierformat werden in den Archiven der Regionalstellen gespeichert.
Nach 10 Jahren werden alle Informationen vernichtet

3.1.3 Alle weiteren Unterlagen, die für die Berichterstattung bzw. die Erstellung der Abrechnungen benötigt werden, werden bis zum Ende des Abrechnungsverfahrens auf den Servern der Regionalstellen gespeichert

Uneingeschränkt

10 Jahre

Bis Ende des Abrechnungsverfahrens.
Nach Ende des Abrechnungsverfahrens werden die Daten ohne Zugangsmöglichkeiten archiviert und für 5 Jahren aufbewahrt

- GL, Adm: uneingeschränkt
- S, BL, RL: eingeschränkt auf die eigene Regionalstelle und die eigene Kompetenzbereiche

- S, BL, RL: eingeschränkt auf die eigene Regionalstelle und die eigene Kompetenzbereiche

- S, BL, RL: während der Berichterstattungs- u. Abrechnungsphase, eingeschränkt auf die eigene Regionalstelle und die eigenen Kompetenzbereiche
- Nach der Archivierung können die Daten nur von den IT-Supportern wieder zugänglich gemacht werden

Passwortgeschütztes individuelles Login mit unterschiedlichen Benutzerrollen

Geschlossene Räume bzw. Schränke mit Zugang nur für Berechtigte

Passwortgeschütztes individuelles Login mit unterschiedlichen Benutzerrollen

3.2 Persönliche «kursbezogene» Daten Lebenslauf und alle anderen persönlichen Informationen, die während der Kursdurchführung behandelt werden (z.B. Standortbestimmungskurse, usw.). Die persönlichen Daten werden grundsätzlich nur elektronisch gespeichert. Ev. Unterlagen in Papierform werden entweder den TN abgegeben oder sofort nach Kursende vernichtet. Während der Kursdauer werden sie in den geschlossenen «Aktenschränken» der KL aufbewahrt.	3.2.1 Variante 1 → tiefe bis mittlere Sensibilität der Daten und keine intensive Arbeit der TN am PC Die Daten werden in dem für den Kurs reservierten Arbeitsbereich auf dem ECAP-Cloud u./o. auf der ECAP-Plattform gespeichert	Bis Kursende. Am Ende der Kurse werden die Daten ohne Zugangsmöglichkeiten entweder gelöscht oder archiviert⁹	➤ KL während der Kursdauer ➤ BL während der Berichterstattungs- u. Abrechnungsphase ➤ Nach der Archivierung können die Daten nur von den IT-Supportern wieder zugänglich gemacht werden	Passwortgeschütztes individuelles Login
	3.2.2 Variante 2 → Mittlere bis hohe Sensibilität der Daten oder intensive Arbeit der TN am PC. Die Daten werden in den für die einzelnen TN reservierten Arbeitsbereich auf dem ECAP-Cloud u./o. auf der ECAP-Plattform gespeichert	Bis Kursende. Am Ende der Kurse werden die Daten ohne Zugangsmöglichkeiten entweder gelöscht oder archiviert	➤ KL während der Kursdauer ➤ Nach der Archivierung können die Daten nur von der IT-Abteilung wieder zugänglich gemacht werden	Passwortgeschütztes individuelles Login und eigenes Profil
	3.2.3 Variante 3 → Es ist kein Server vorhanden. Die TN arbeiten mit persönlichem USB-Stick	Bis Kursende	➤ KL	Alle auf einem PC in den ECAP-Kursräumen gespeicherten Informationen werden automatisch gelöscht, wenn das Gerät ausgeschaltet wird. Die KL sollen am Ende jedes Kurstages sicherstellen, dass TN ihre Dateien auf eigenem USB-Stick speichern.

⁹ Gemäss Anweisungen des Auftraggebers.

4. Kontaktdaten				
4.1 Nicht sensible <u>Informationen über die Kontakte</u> bzw. externe Personen und Institutionen, mit denen wir zusammenarbeiten: ➤ Personalien ➤ Kommunikationsinformationen ➤ Rechnungswesen ➤ usw.	4.1.1 Die Informationen bleiben in der Datenbank Tocco gespeichert	Uneingeschränkt	➤ GL, Adm: uneingeschränkt ➤ S, BL, RL: eingeschränkt auf die eigene Regionalstelle und die eigene Kompetenzbereiche	Passwortgeschütztes individuelles Login mit unterschiedlichen Rollen.
5. Buchhaltung				
5.1 Finanz- und Lohnbuchhaltung	5.1.1 Die Informationen werden ausschliesslich in der Datenbank Abacus auf dem Server der zentralen Administration gespeichert	Uneingeschränkt	➤ GL, Adm	Passwortgeschütztes individuelles Login
5.2 Kreditorenbuchhaltung	5.2.1 Die Informationen werden ausschliesslich in der Datenbank Abacus auf dem Server der zentralen Administration gespeichert	Uneingeschränkt	➤ GL, Adm: Uneingeschränkt ➤ Visumverantwortliche: eingeschränkt auf die eigene Regionalstelle	Passwortgeschütztes individuelles Login
6. Korrespondenz				
6.1 E-Mail	6.1.1 E-Mail mit persönlichen Daten der TN können nur mit ECAP-Mailadressen der Mitarbeitende auf Microsoft-Exchange-Server gesendet, empfangen und gespeichert werden. E-Mails mit persönlichen und sensiblen Daten, werden ge-	Uneingeschränkt. Private E-Mails müssen bei Austritt gelöscht werden. Geschäftliche E-Mails werden archiviert. E-Mails, die persönliche und sensible Daten der TN enthalten (siehe 3.2), werden für den mit dem Auftraggeber vereinbarten Zeitraum gespeichert.	➤ Jede/r MitarbeiterIn hat Zugang nur auf die ihm/ihr zugewiesenen Mailadressen. ➤ Nach der Archivierung können die Daten nur von den IT-Supportern wieder zugänglich gemacht werden.	Passwortgeschütztes individuelles Login

	mäss Anweisungen des Auftraggebers bzw. der zuweisenden Stelle verwaltet ¹⁰			
6.2 Briefe	6.2.1 Die Korrespondenz auf Papier wird in geschlossenen Schränken und in den Archiven der Regionalstellen aufbewahrt	10 Jahre Nach 10 Jahren wird sie ins ECAP-Archiv transferiert	➤ GL, Adm: uneingeschränkt ➤ S, BL, RL: eingeschränkt auf die eigene Regionalstelle	Geschlossene Schränke oder Räume
7. Nicht personenbezogene Unterlagen				
7.1 Laufende Arbeitsunterlagen ➤ Interne Arbeitsunterlagen ➤ Berichte ➤ Entwürfe Sitzungsunterlagen ➤ Protokolle ➤ usw.	7.1.1 Die gemeinsamen elektronischen Versionen der laufenden Arbeitsunterlagen werden auf den ECAP-Servern (o. im Microsoft Teams) mit der entsprechenden Struktur gespeichert	Uneingeschränkt	➤ Alle MA haben Zugang nur auf die ihrer Funktion entsprechenden Unterlagen	Passwortgeschütztes individuelles Login mit unterschiedlichen Benutzerrollen
	7.1.2 Ev. Papierversionen der gemeinsamen Unterlagen werden in den Archiven der Regionalstellen gespeichert	10 Jahre Nach 10 Jahren werden sie ins Archiv der Stiftung transferiert	➤ GL, Adm: uneingeschränkt ➤ S, BL, RL: Eingeschränkt auf die eigene Regionalstelle	Geschlossene Räume oder Schränke mit Zugang nur für Berechtigte
	7.1.3 Persönliche elektronische Arbeitsunterlagen werden in den eigenen persönlichen Profilen auf dem Server der Regionalstellen (o. im Microsoft Teams) gespeichert	Anstellungsdauer Nach Ende der Anstellung werden die Unterlagen archiviert	➤ Jede/r MA hat nur auf die eigenen Daten Zugriff.	Passwortgeschütztes individuelles Login

Die Geschäftsleitung

Guglielmo Bozzolini, Giuliana Tedesco-Manca

Zürich, im Juli 2023

¹⁰ Z.B. mit IncaMail