

Richtlinien für den Datenschutz innerhalb der ECAP

Inhalt

Einführung	1
Allgemeine Massnahmen	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

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

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 SBFI

- Alle Mitarbeitenden nehmen diese Richtlinien und eventuelle zusätzliche Anweisungen sämtlicher Auftraggeber zum Datenschutz zur Kenntnis und verpflichten sich, sie einzuhalten
- 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
<ul style="list-style-type: none">○ Kursstart und -ende○ Präsenzlisten○ Kursjournal○ Konzept, Ausschreibung, Zielgruppe, Ziele, Inhalte usw.
Personaldaten
<ul style="list-style-type: none">○ Kursadministrative Daten: Dozentenbuchungen und -einsätze; Termine und Honorare○ Personen- und lohn- und versicherungsbezogene Daten

² Art. 3.1 DSV

Daten der Teilnehmenden
<ul style="list-style-type: none"> ○ Kursadministrative Daten: Personalien, Anmeldungen usw. ○ Personen- und kursbezogene Daten: Lebensläufe, Prüfungsergebnisse, Noten, Zertifikate usw.
Kontaktdaten
<ul style="list-style-type: none"> ○ Personalien von Kontaktpersonen, Auftraggebern und zuweisenden Stellen
Buchhaltung
<ul style="list-style-type: none"> ○ Finanzbuchhaltung ○ Lohnbuchhaltung ○ Debitoren und Kreditoren
Korrespondenz
<ul style="list-style-type: none"> ○ Eingehende und ausgehende E-Mail ○ Eingehende und ausgehende Briefe
Nicht personenbezogene Arbeitsunterlagen
<ul style="list-style-type: none"> ○ 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

	<ul style="list-style-type: none"> • sind gegenüber der GL rechenschaftspflichtig
BL, S und KL	<ul style="list-style-type: none"> • setzen die Richtlinien in ihren Kompetenzbereichen um • melden Probleme und Engpässe • sind gegenüber den RL rechenschaftspflichtig
Adm.	<ul style="list-style-type: none"> • setzt die Richtlinien in ihren Kompetenzbereichen um
IT-Support	<ul style="list-style-type: none"> • 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
Datenschutzbeauftragte/r	<ul style="list-style-type: none"> • 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

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

⁴ Z.B. für Forschungszwecke.

- dies zur Erfüllung einer in einem Gesetz klar umschriebenen Aufgabe zwingend notwendig ist
- 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 benutzt. 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.

Zürich, im Juli 2023

Die Geschäftsleitung

Guglielmo Bozzolini, Giuliana Tedesco-Manca

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