

Linee guida per la protezione dei dati all'interno dell'ECAP

Indice dei contenuti

Introduzione	1
Misure generali	1
Salvataggio, modifica e uso dei dati.....	2
Tipi di dati.....	2
Tipi di accesso e ruoli dei/delle collaboratori/trici.....	3
Comunicazione dei dati a terzi.....	4
Semplici dati sulle persone	4
Dati personali particolari	4
Dati non personali	5
Sintesi delle procedure operative	6

Introduzione

Queste linee guida definiscono le direttive generali per il salvataggio, la cura e l'archiviazione dei dati all'interno di ECAP. Esse tengono conto di tutte le disposizioni legali vigenti in materia ¹ e devono essere applicate nei centri regionali in conformità con le disposizioni delle autorità di competenza, che sono da considerarsi un'integrazione ed estensione del presente documento.

Eventuali adattamenti regionali devono essere motivati e garantire la stessa sicurezza dei dati.

Le linee guida mirano a raggiungere i seguenti obiettivi:

- Garantire la protezione di dati personali 'sensibili' da attacchi interni ed esterni e da un uso improprio degli stessi
- Garantire l'efficienza nella gestione e realizzazione del corso
- Tenere conto dei bisogni e degli interessi dei/delle partecipanti
- Tenere conto delle esigenze dei committenti e/o degli enti finanziatori (per es. rapporti, ecc.).

Misure generali

All'ECAP vengono generalmente applicate le seguenti misure organizzative e tecniche:

- I/Le dipendenti non sono autorizzati/e a memorizzare dati personali su dispositivi che non appartengono all'ECAP
- Tutti/e i/le dipendenti prendono atto di queste linee guida e delle eventuali istruzioni aggiuntive dei committenti in materia di protezione dei dati e si impegnano a rispettarle
- Tutti i server di ECAP e dei suoi partner si trovano in Svizzera

¹ Legge federale revisionata sulla protezione dei dati revLPD (valida dal 1.09.2023), Ordinanza sulla protezione dei dati OLPD (31.08.2022), ev. leggi e ordinanze cantonali sulla protezione dei dati, direttive e ordinanze di SECO, SEM e SEFRI.

- Tutte le operazioni vengono protocollate
- L'accesso ai dati personali è personalizzato, differenziato a seconda dei ruoli e protetto da password
- Una valutazione degli utenti attivi e delle loro autorizzazioni è disponibile nel sistema (audit dei ruoli)
- Gli utenti possono essere obbligati a reimpostare la password
- Le password non sicure non sono ammesse dal sistema
- È disponibile l'autenticazione a due fattori
- Le pagine web implementate da ECAP presentano un avviso con un link alle politiche di protezione dei dati e all'uso dei cookie.

Salvataggio, modifica e uso dei dati

I dati archiviati e conservati da ECAP sono utilizzati esclusivamente per l'organizzazione e la gestione delle proprie attività, fatti salvi gli obblighi imposti dai committenti. I dati non possono essere raccolti senza che gli interessati ne siano a conoscenza e non possono essere utilizzati per altri scopi. Tutti i/le dipendenti si impegnano a utilizzare i dati a cui hanno accesso solo per lo svolgimento delle proprie funzioni.

La raccolta e l'archiviazione dei dati si basa su tre principi:²

- Le persone autorizzate hanno accesso solo ai dati personali di cui hanno bisogno per svolgere i loro compiti (controllo degli accessi).
- Solo le persone autorizzate hanno accesso ai locali e alle strutture in cui vengono trattati i dati personali (controllo degli accessi)
- Le persone non autorizzate non hanno accesso ai dati o ai sistemi di elaborazione o ai mezzi di trasmissione dei dati (controllo degli utenti).

L'inosservanza di questi principi fondamentali o delle istruzioni contenute nel presente documento sarà valutata come un comportamento scorretto, costituirà motivo di risoluzione del rapporto di lavoro ai sensi dell'art. 12 del CCL e, nei casi più gravi, potrà comportare una denuncia alle autorità penali.

Tipi di dati

Vengono distinti i seguenti tipi di dati:

Dati del corso
○ Data di inizio e di fine ○ Liste di presenza ○ Diari del corso ○ Progetto, bando, gruppo target, obiettivi, contenuti, ecc.
Dati personali
○ Dati amministrativi del corso: prenotazioni e incarichi dei docenti; calendari del corso e stipendi ○ Dati personali rilevanti per il salario e le assicurazioni

² Art. 3.1 LPD

Dati dei/delle partecipanti
○ Dati amministrativi del corso: dati personali, iscrizioni, ecc. ○ Dati personali legati al corso: curriculum vitae, risultati di esami, voti, certificati, ecc.
Dati di contatto
○ Dati personali di persone di contatto e committenti
Contabilità
○ Contabilità finanziaria ○ Contabilità del personale ○ Debitori e creditori
Corrispondenza
○ E-Mail in entrata e in uscita ○ Corrispondenza in entrata e in uscita
Documenti di lavoro senza riferimenti alla persona
○ Progetto del corso ○ Programmi del corso ○ Moduli ○ ecc.

Tipi di accesso e ruoli dei/delle collaboratori/trici

Sono previsti diversi tipi di accesso ai dati sulla base di sette diverse categorie di collaboratori e collaboratrici:

1. DN – Direzione
2. DC – Direttore/-trice di centro
3. RS – Responsabile di settore
4. S – Personale di segreteria
5. I – Insegnanti
6. Amm. - Amministrazione
7. IT-Support

Categoria	Compiti
DN	• Approva le linee guida e ne controlla l'applicazione • Determina la persona responsabile della protezione dei dati • Assegna e gestisce i diritti di accesso alle banche dati Tocco e Abacus • Decide in caso di dubbio
DC	• Hanno il compito di garantire le condizioni organizzative, logistiche e infrastrutturali necessarie all'applicazione delle linee guida nel loro ambito di competenza • Monitorano l'applicazione delle linee guida da parte dei loro collaboratori e collaboratrici • Impartiscono incarichi agli IT-Supporter • Segnalano problemi e difficoltà • Rendono conto alla DN
RS, S e I	• Applicano le linee guida nel loro ambito di competenze

Amm.	• Segnalano problemi e difficoltà • Rendono conto ai DC
	• Applica le linee guida nel suo ambito di competenze
IT-Support	• Ha il compito di fornire l'infrastruttura informatica necessaria, incl. piattaforma ECAP e licenze • Prepara login, profili e aree di lavoro collettive e individuali di concerto con i/le DC e garantisce la riservatezza delle informazioni. • Monitora l'applicazione delle linee guida e informa il/la DC e la DN in caso di eventuali scorrettezze • Aiuta i collaboratori e le collaboratrici a risolvere i problemi • Garantisce la cancellazione dei dati al termine del periodo di archiviazione stabilito • Rende conto alla DN
	• monitora l'applicazione di queste linee guida e delle direttive del commit-tente • è l'interlocutore di riferimento per chiunque abbia bisogno di informazioni sui dati memorizzati e sul loro utilizzo.
Responsabile protezione dati	

Comunicazione dei dati a terzi

Semplici dati sulle persone

In linea di principio, i dati vengono raccolti solo per la realizzazione delle proprie attività e non vengono divulgati a terzi.

Semplici dati sulle persone (informazioni amministrative e riferite al corso) possono essere comunicati a istituzioni o a enti committenti, se

- vige una disposizione legale o contrattuale³
- è necessario per soddisfare un obbligo legale o contrattuale.

In questi casi le persone interessate devono essere informate per tempo, che è possibile o prevista una comunicazione dei dati.

- Ciò è stato esplicitamente concordato in anticipo con le persone interessate⁴ e i dati vengono anonimizzati.

Dati personali particolari

Dati personali particolari vengono comunicati solo alle autorità, se richieste per iscritto e

- una legge lo impone espressamente
- se ciò non è esplicitamente escluso nel mandato specifico o nel contratto di prestazione
- ciò è assolutamente necessario per adempiere ad un compito chiaramente definito dalla legge
- in casi particolari la persona interessata abbia espressamente acconsentito o, nel caso in cui non sia in grado di farlo, si ritenga sia nel suo interesse comunicare i suoi dati e il suo consenso sia in buona fede presunto.

³ Per es. un contratto di prestazione, un'approvazione dei costi o un'assegnazione da parte di un'autorità devono essere percepiti come un contratto.

⁴ Per es. per motivi di ricerca.

Per decidere se e in quali casi i dati personali debbano o possano essere trasmessi, si userà come ausilio la check-list del delegato della protezione dei dati del Cantone Basilea-Città ⁵. In casi dubbi decide la Direzione.

Dati non personali

In sostanza vengono divulgate solo informazioni statistiche sulle attività dell'ECAP e dati tecnici di rendicontazione. Informazioni o documentazioni soggette a Copyright e/o che siano state raccolte e salvate nell'ambito dell'attività lavorativa presso ECAP, o su suo incarico, non possono essere inoltrate a terzi senza il consenso della Direzione. Non possono essere comunicate a terzi informazioni che danneggino ECAP direttamente o indirettamente.

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

Sintesi delle procedure operative

Descrizione	Supporto e luogo di salvataggio dei dati	Durata del salvataggio ⁶	Chi ha accesso	Protezione dati
1. Dati del corso				
1.1 Liste presenza	1.1.1 Le liste di presenza generalmente vengono compilate elettronicamente e le informazioni restano salvate nella banca dati tocco	Illimitata	➤ DN, Amm: illimitato ➤ S, RS, DC: filtro sui propri corsi ➤ I: solo per i loro corsi correnti	Login individuale protetto da password con diversi ruoli
	1.1.2 Eventuali documenti in formato cartaceo vengono conservati negli archivi dei centri regionali. Dopo 10 anni devono essere trasferiti nell'archivio ECAP	Illimitata	➤ S, RS, DC: illimitato ➤ I: solo per i loro corsi correnti	Stanze o armadietti chiusi con accesso riservato alle persone autorizzate
1.2 Diario del corso⁷	1.2.1 Viene salvato in formato elettronico sui server ECAP ⁸	10 anni	➤ S, RS, DC: limitato al proprio centro regionale	Login individuale protetto da password
	1.2.2 Eventuali documenti in formato cartaceo vengono conservati negli archivi dei centri regionali. Dopo 10 anni devono essere trasferiti nell'archivio ECAP	Illimitata	➤ S, RS, DC: illimitato ➤ I: solo per i loro corsi correnti	Stanze o armadietti chiusi con accesso riservato alle persone autorizzate
1.3 Progetti	1.3.1 Vengono salvati su server ECAP	Illimitata	➤ RS, DC, DN: illimitato	Login individuale protetto da password
2. Dati personali				

⁶ Le informazioni sulla durata della conservazione dei dati sono un'indicazione generale valida in assenza di istruzioni specifiche da parte dei committenti o delle autorità di sovvenzione.

⁷ I diari dei corsi non contengono dati personali.

⁸ Tutti i server di ECAP e dei suoi partner si trovano in Svizzera.

2.1 Dati amministrativi del corso ➤ Dati personali ➤ Percentuale di impiego ➤ Durata del contratto ➤ Piano di lavoro ➤ Qualifiche	2.1.1 Le informazioni vengono salvate esclusivamente nelle banche dati tocco e Abacus	Illimitata	➤ DN, Amm: illimitato ➤ S, RS, DC: limitato al proprio centro regionale e ai propri settori di competenza	Login individuale protetto da password con diversi ruoli
	2.1.2 Eventuali documenti in formato cartaceo vengono conservati negli archivi dei centri regionali. Dopo 10 anni, tutte le informazioni vengono distrutte	10 anni	➤ S, RS, DC: limitato al proprio centro regionale e ai propri settori di competenza	Stanze o armadietti chiusi con accesso riservato alle persone autorizzate
2.2 Dati personali rilevanti per salario e assicurazioni: ➤ Coordinate bancarie ➤ Tutte le informazioni necessarie al pagamento del salario ➤ Tutte le informazioni richieste dalle assicurazioni sociali	2.2.1 Le informazioni sono salvate esclusivamente nella banca dati di Abacus e sul server di amministrazione	Illimitata	➤ DN, Amm	Login individuale protetto da password con diversi ruoli
	2.2.2 I documenti in formato cartaceo vengono conservati nell'archivio dell'Amm.	10 anni dopo la fine del rapporto lavorativo	➤ DN, Amm	Stanze chiuse con accesso riservato alle persone autorizzate
2.3 Dossier personale ➤ Documenti di candidatura ➤ Contratti di lavoro ➤ Colloqui con i/le dipendenti, ammonimenti, ecc. ➤ Certificati ➤ Colloqui con i/le dipendenti	2.3.1 I documenti elettronici sono archiviati nella cartella di lavoro della direzione regionale e sul server dell'amministrazione	Cartella di lavoro della DC: fino alla fine del rapporto lavorativo Server dell'amministrazione: 10 anni dopo la fine del rapporto lavorativo	➤ DC: limitato al proprio centro regionale ➤ DN, Amm: illimitato	Login individuale protetto da password
	2.3.2 I documenti in formato cartaceo vengono conservati in armadi chiusi nell'ufficio della Direzione regionale e negli archivi dell'amministrazione	Ufficio di/delle DC: fino alla fine del rapporto lavorativo Archivio dell'amministrazione: 10 anni dopo la fine del rapporto lavorativo	➤ DC: limitato al proprio centro regionale ➤ DN, Amm: illimitato	Stanze o armadietti chiusi con accesso riservato alle persone autorizzate
3. Dati dei/delle partecipanti				

3.1 Dati amministrativi dei corsi: ➤ Dati sulla persona ➤ Indirizzo (corrispondenza e fattura) ➤ Telefono e e-mail ➤ Nazionalità ➤ Lingue ➤ Ev. permesso di soggiorno ➤ Test in ingresso, progressi nell'apprendimento e attestati di frequenza ➤ Persone di contatto ➤ Ev. corrispondenza con gli enti mandatori ➤ Ev. informazioni di marketing ➤ Ev. documentazione per la riduzione dei costi ➤ Etc. Vengono salvati solo i dati necessari per ➤ La realizzazione e gestione del corso ➤ Il rilascio e l'eventuale ristampa di certificati e attestati di frequenza ➤ Il reporting e i rendiconti per enti committenti e/o finanziatori ➤ La semplificazione di altre iscrizioni future. È severamente vietato raccogliere e salvare informazioni sull'orientamento religioso e/o politico.	3.1.1 Le informazioni vengono archiviate elettronicamente esclusivamente nel database di Tocco	Illimitata	➤ DN, Amm: illimitato ➤ S, RS, DC: limitato al proprio centro regionale e ai propri settori di competenza	Login individuale protetto da password con diversi ruoli
	3.1.2 I documenti in formato cartaceo sono conservati negli archivi dei centri regionali. Dopo 10 anni, tutte le informazioni vengono distrutte	10 anni	➤ S, RS, DC: limitato al proprio centro regionale e ai propri settori di competenza	Stanze o armadietti chiusi con accesso riservato alle persone autorizzate
	3.1.3 Tutti gli ulteriori documenti, necessari per la stesura del rapporto o per la rendicontazione, vengono salvati sui server dei centri regionali fino al termine della procedura contabile	Fino alla fine della rendicontazione. Alla fine della procedura di rendicontazione i dati vengono archiviati, senza possibilità di accesso, e conservati per 5 anni	➤ S, RS, DC: durante la fase di reporting e rendicontazione, limitatamente al proprio centro regionale e alle proprie aree di competenza ➤ In seguito all'archiviazione, i dati possono essere resi accessibili solamente dagli IT-Supporter	Login individuale protetto da password con diversi ruoli

3.2 Dati personali attinenti il corso Curricula e tutte le altre informazioni personali, trattate durante lo svolgimento del corso (per es. Corsi di ricollocamento lavorativo, ecc.). I dati personali vengono salvati fondamentalmente solo in formato elettronico. L'eventuale documentazione cartacea viene consegnata direttamente ai partecipanti o distrutta alla fine del corso. Durante il corso la produzione cartacea viene conservata sotto chiave negli armadietti degli insegnanti.	3.2.1 Variante 1 → Bassa o media sensibilità dei dati e nessun lavoro intenso dei partecipanti al PC. I dati vengono archiviati nell'area di lavoro riservata al corso sul cloud ECAP e/o sulla piattaforma ECAP	Fino alla fine del corso. Alla fine dei corsi, i dati vengono cancellati o archiviati senza possibilità di accesso ⁹	➤ I: per la durata del corso ➤ RS durante la fase di reporting e rendicontazione ➤ In seguito all'archiviazione, i dati possono essere resi accessibili solamente dagli IT-Supporter	Login individuale protetto da password
	3.2.2 Variante 2 → Media o alta sensibilità dei dati e lavoro intenso dei partecipanti al PC. I dati vengono archiviati nello spazio di lavoro riservato ai singoli partecipanti sul cloud ECAP e/o sulla piattaforma ECAP	Fino alla fine del corso. Alla fine dei corsi, i dati vengono cancellati o archiviati senza possibilità di accesso	➤ I: per la durata del corso ➤ In seguito all'archiviazione, i dati possono essere resi accessibili solamente dagli IT-Supporter	Login individuale protetto da password e profilo individuale
	3.2.3 Variante 3 → Non c'è un server. I partecipanti lavorano con una chiavetta USB personale	Fino alla fine del corso	➤ I	Tutte le informazioni salvate su un PC nelle aule ECAP vengono automaticamente cancellate quando il dispositivo viene spento. Alla fine di ogni giorno di corso, il docente deve assicurarsi che i partecipanti salvino i loro file sulle proprie chiavette USB.

⁹ Secondo le indicazioni del committente.

4. Dati di contatto				
4.1 Informazioni non sensibili sui contatti , vale a dire su persone esterne e istituzioni con cui collaboriamo: ➤ Dati sulla persona ➤ Informazioni sulla comunicazione ➤ Fatturazione ➤ Etc.	4.1.1 Le informazioni restano salvate nella banca dati Tocco	Illimitata	➤ DN, Amm: illimitato ➤ S, RS, RL: limitato al proprio centro regionale e ai propri settori di competenza	Login individuale protetto da password con diversi ruoli
5. Contabilità				
5.1 Contabilità finanziaria e dei salari	5.1.1 Le informazioni sono salvate esclusivamente nella banca dati di Abacus sul server dell'amministrazione centrale	Illimitata	➤ DN, Amm	Login individuale protetto da password
5.2 Contabilità dei crediti	5.2.1 Le informazioni sono salvate esclusivamente nella banca dati di Abacus sul server dell'amministrazione centrale	Illimitata	➤ DN, Amm: illimitato ➤ Responsabile per il visum: limitato al proprio centro regionale	Login individuale protetto da password
6. Corrispondenza				
6.1 E-Mail	6.1.1 Le e-mail con dati personali dei partecipanti possono essere inviate, ricevute e archiviate solo con gli indirizzi e-mail ECAP dei dipendenti su server Microsoft Exchange. Le e-mail contenenti dati personali e sensibili sono gestite secondo le istruzioni del committente o dell'ente assegnatario ¹⁰	Illimitata. Le email private devono essere cancellate alla fine del rapporto lavorativo. Le email di lavoro vengono archiviate. Le e-mail contenenti dati personali e sensibili dei partecipanti (vedi 3.2)	➤ Ogni dipendente ha accesso solo agli indirizzi e-mail che gli sono stati assegnati. ➤ Dopo l'archiviazione, i dati possono essere resi accessibili solo dai Supporter IT	Login individuale protetto da password

¹⁰ Per es. con IncaMail

		sono archiviate per il periodo concordato con il committente.		
6.2 Corrispondenza	6.2.1 La corrispondenza cartacea è conservata in armadi chiusi e negli archivi dei centri regionali	10 anni Dopo 10 anni viene trasferita nell'archivio ECAP	➤ DN, Amm: illimitato ➤ S, RS, DC: limitato al proprio centro regionale	Stanze o armadietti chiusi
7. Documenti non personali				
7.1 Documenti di lavoro corrente ➤ Documenti di lavoro interni ➤ Rapporti ➤ Bozze ➤ Documenti delle riunioni ➤ Protocolli ➤ ecc.	7.1.1 Le versioni elettroniche condivise dei documenti di lavoro correnti sono archiviate sui server ECAP (o in Microsoft Teams) con la struttura appropriata	Illimitata	➤ Tutti i collaboratori e le collaboratrici hanno accesso solo alla documentazione attinente alla loro funzione	Login individuale protetto da password con diversi ruoli
	7.1.2 Eventuali versioni cartacee dei documenti condivisi vengono conservate nei magazzini dei centri regionali	10 anni Dopo dieci anni devono essere trasferite nell'archivio della Fondazione	➤ DN, Amm: illimitato ➤ S, RS, DC: limitato al proprio centro regionale	Stanze o armadietti chiusi con accesso riservato alle persone autorizzate
	7.1.3 I documenti personali di lavoro in formato elettronico vengono salvati nei profili individuali del/la collaboratore/trice sul server dei centri regionali (o in Microsoft Teams)	Durata del rapporto di lavoro Alla fine del rapporto di lavoro i documenti vengono archiviati	➤ Ciascun collaboratore ha accesso solo ai propri dati	Login individuale protetto da password

La Direzione

Guglielmo Bozzolini, Giuliana Tedesco-Manca

Zurigo, in luglio 2023