

Regolamento sul trattamento dei dati in qualità di responsabile

Versione settembre 2024

Il presente regolamento descrive gli obblighi delle parti in relazione alla protezione dei dati. CYP esegue determinati mandati per i propri clienti, nell'ambito dei quali tratta dati personali ai sensi della legge svizzera sulla protezione dei dati e/o del regolamento generale europeo sulla protezione dei dati (insieme denominati «disposizioni in materia di protezione dei dati»). Il presente regolamento si applica a tutte le attività correlate al contratto stipulato nell'ambito del quale avviene il trattamento di dati personali («dati») del cliente.

1. Ruoli e responsabilità delle parti

Ai sensi delle disposizioni in materia di protezione dei dati, il committente è il titolare del trattamento dei dati, mentre CYP è il responsabile del trattamento. Sia il committente che CYP rispondono della piena ottemperanza a tutte le disposizioni in materia di protezione dei dati ad essi applicabili.

Il committente garantisce e assicura di aver informato in maniera esaustiva, comprensibile e con forma e linguaggio accessibili le persone i cui dati personali sono oggetto di trasmissione a CYP (o i cui dati personali giungono in possesso di CYP per altre vie) riguardo al trattamento ad opera di CYP ai sensi del presente regolamento. Garantisce e assicura altresì che, laddove necessario, tali persone hanno dato il proprio consenso a tale trattamento o che sussiste un altro motivo giustificativo in merito.

Qualora le disposizioni in materia di protezione dei dati prevedano un ulteriore obbligo di informare da parte del committente, quest'ultimo si impegna a fornire alle persone interessate le informazioni oggetto di tale obbligo.

Il committente garantisce e assicura inoltre che il trattamento dei dati da parte di CYP ai sensi del presente regolamento è in linea con le disposizioni in materia di protezione dei dati applicabili e in particolare si limita alle operazioni di trattamento che lo stesso committente sarebbe autorizzato a svolgere e non si oppone a obblighi di tutela del segreto legali o contrattuali.

2. Oggetto e durata

Oggetto, durata, tipo e scopo del trattamento si desumono fondamentalmente dal contratto principale.

La durata del presente regolamento si inferisce dalla durata del contratto principale fra CYP e il cliente. Fanno eccezione le disposizioni del presente regolamento implicanti obblighi che si protraggono oltre tale scadenza.

CYP tratta i dati personali fintanto che ciò è necessario per il perseguimento degli scopi stabiliti dal presente regolamento o per l'adempimento di obblighi contrattuali e di legge, o anche più a lungo qualora i dati siano soggetti a un obbligo legale di conservazione o siano necessari a fini probatori.

Non appena i dati personali trattati ai sensi del presente regolamento non saranno più necessari, CYP provvederà a cancellarli o a renderli anonimi. Sono fatti salvi i dati salvati nel contesto dei consueti backup operativi effettuati da CYP.

La base legale per il trattamento dei dati personali, ove richiesta dalla legge, è il consenso delle persone interessate o l'interesse legittimo del committente ad affidare a un responsabile il trattamento dei dati per il perseguimento degli scopi sopra descritti. La responsabilità di comprovare il suddetto consenso o interesse legittimo al trattamento dei dati da parte di CYP incombe al committente. Se una persona interessata revoca il consenso o se l'interesse legittimo viene meno, il committente ne dà tempestiva comunicazione a CYP.

3. Categorie di dati personali trattati

CYP tratta le seguenti categorie di dati personali:

- dati di base (ad es. nome, indirizzo, data di nascita)
- dati di comunicazione (ad es. numero di telefono, indirizzo e-mail)
- dati relativi a giudizi, valutazioni e formazioni

Persone interessate:

- partecipanti ai corsi
- persone di contatto dei partecipanti ai corsi
- responsabili amministrativi di aziende
- collaboratori

persone che mostrano interesse per i servizi offerti da CYP

4. Istruzioni del committente

Il trattamento dei dati descritto nel presente regolamento va inteso come istruzione generale fornita dal committente a CYP affinché tratti i dati personali. Le istruzioni sono stabilite dal contratto.

Eventuali istruzioni specifiche, esulanti da quanto definito dal contratto, fornite a CYP in merito al trattamento di dati personali verranno attuate se saranno ritenute proporzionali e comporteranno un impegno ragionevolmente esigibile da CYP.

5. Sub-responsabili del trattamento e luogo del trattamento

CYP ha facoltà di trasmettere i dati personali a terzi che operino in qualità di sub-responsabili del trattamento. Tali soggetti sono indicati sul sito web di CYP, al seguente link: <https://cyp.ch/it/protezione-dei-dati> e si considerano approvati dal committente contestualmente alla stipula del contratto.

Il committente accetta inoltre a livello generale che CYP, a propria discrezione, coinvolga ulteriori sub-responsabili del trattamento o sostituisca sub-responsabili con cui ha collaborato. CYP è comunque tenuta a comunicare preventivamente al committente l'eventuale coinvolgimento di ulteriori sub-responsabili o la sostituzione di tali figure. Il committente ha facoltà di opporsi a detti provvedimenti. Qualora non manifesti la propria opposizione entro 10 giorni dalla relativa comunicazione, il coinvolgimento/la sostituzione si considerano approvati. In caso di opposizione del committente, CYP può rinunciare al coinvolgimento/alla sostituzione o proporre un'alternativa; qualora ciò sia impossibile o inesigibile, il servizio corrispondente verrà sospeso.

Il trattamento dei dati su istruzione del committente viene effettuato in Svizzera, all'interno dell'UE, all'interno del SEE o in un Paese giudicato dalla Commissione europea e dal Consiglio federale come in grado di garantire un livello di protezione adeguato e che offre una tutela dei dati personali conforme a quanto previsto dalla legge svizzera sulla protezione dei dati. Qualsiasi trasferimento del trattamento dei dati in questione in un Paese non compreso nella suddetta area può avvenire solo previa approvazione del committente e in conformità alle norme di legge applicabili (in particolare nel rispetto delle condizioni sancite dal capo V del GDPR e dalla legge svizzera sulla protezione dei dati). In tal caso, il responsabile del trattamento si impegna, in particolare prima della trasmissione o della comunicazione di dati, a stipulare opportuni contratti supplementari e adotta, se necessario, i provvedimenti legali, tecnici o organizzativi del caso.

I sub-responsabili del trattamento vengono obbligati per contratto da CYP a proteggere adeguatamente tutti i dati di cui vengono in possesso contestualmente all'incarico ricevuto e a utilizzarli esclusivamente per gli scopi connessi a detto incarico.

6. Sicurezza dei dati

CYP si impegna ad adottare tutti i provvedimenti tecnici e organizzativi necessari per proteggere adeguatamente (in particolare da manipolazione, divulgazione, smarrimento, cancellazione e distruzione) i dati trattati ai sensi del presente regolamento. A tal fine emana istruzioni, forma i responsabili e implementa adeguati dispositivi di sicurezza nonché soluzioni di sicurezza IT e per la rete.

CYP limita l'accesso ai dati personali alle persone che ne hanno bisogno per adempiere ai propri compiti e si assicura che tutti i collaboratori, mandatarî o fornitori di servizi coinvolti nel trattamento dei dati ne rispettino la riservatezza. Prima di iniziare la propria attività, tali soggetti devono garantire che ottempereranno al suddetto obbligo di tutela del segreto.

7. Violazione della sicurezza dei dati

CYP si impegna a informare il committente con la massima tempestività non appena dovesse riscontrare una violazione della sicurezza dei dati ai sensi delle disposizioni in materia di protezione dei dati.

CYP supporta il committente, per quanto possibile e ragionevolmente esigibile, nell'adozione di provvedimenti volti a porre rimedio alle violazioni della sicurezza dei dati riscontrate presso l'organizzazione, a condizione che il committente le riconosca un adeguato indennizzo.

A tali scopi, CYP inoltra al committente eventuali informazioni rilevanti, se disponibili. Quest'ultimo, da parte sua, rimane responsabile di tutte le notifiche necessarie ad autorità di controllo della protezione dei dati e alle persone interessate. CYP, dal canto proprio, provvede alla notifica alle autorità di controllo della protezione dei dati qualora sussista un obbligo in tal senso.

8. Richieste di persone interessate

Le persone i cui dati sono oggetto di trattamento ai sensi del presente regolamento possono far valere i propri diritti individuali nei confronti di entrambe le parti. Qualora una persona, nell'esercitare un diritto individuale, si rivolga a CYP benché quest'ultima non sia la parte che sta provvedendo al trattamento, CYP inoltra tale istanza al committente, indipendentemente dall'obbligo di risposta. Il committente fornisce una risposta ed evade l'istanza. Dietro richiesta del committente, CYP mette a sua disposizione le informazioni necessarie a tal fine, se disponibili. Il committente si accerta che le persone esercitino diritti individuali effettivamente spettanti ad esse e richiede i dati necessari per identificarle senza ombra di dubbio. CYP non si assume alcuna responsabilità per eventuali risposte inesatte o non pervenute in tempo utile.

9. Rapporti con le autorità di controllo della protezione dei dati

Qualora un'autorità di controllo si rivolga a CYP in merito a dati personali trattati ai sensi del presente regolamento, CYP inoltra la relativa istanza o disposizione al committente, indipendentemente dall'obbligo di risposta. Il committente avvia una corrispondenza con l'autorità richiedente o disponente e risponde alle sue domande o dà seguito alla sua disposizione, di comune accordo con CYP. Dietro richiesta del committente, CYP mette a sua disposizione le informazioni necessarie a tal fine, se disponibili. Cfr. anche il punto 7.

10. Responsabilità e risarcimento

Il committente e CYP sono responsabili nei confronti delle persone interessate ai sensi delle disposizioni di cui all'art. 82 GDPR e alle disposizioni corrispondenti del diritto svizzero.

11. Comunicazioni

Tutte le comunicazioni tra le parti nel quadro del presente regolamento avvengono in forma scritta (anche tramite e-mail).

Per CYP: CYP Association, Giessereistrasse 18, 8005 Zurigo / datenschutz@cyp.ch

Per il committente: in sede di stipula del contratto viene designata una persona o un'istanza di riferimento per le questioni inerenti alla protezione dei dati.

12. Diritto applicabile e foro competente

Il presente regolamento è soggetto al diritto materiale svizzero.

Per eventuali controversie derivanti dal presente regolamento o ad esso relative sono competenti esclusivamente i tribunali ordinari di Zurigo, Svizzera.

13. Disposizioni finali

Ciascuna parte è responsabile del rispetto del presente regolamento ad opera dei propri collaboratori, mandatari, agenti e terzi da essa reclutati.

Qualsiasi modifica e integrazione al presente regolamento è valida solo se è redatta in forma scritta e precisa esplicitamente la propria natura di modifica o integrazione alle presenti condizioni.

Panoramica delle misure tecniche e organizzative

Controllo degli accessi ai sistemi

È l'insieme dei provvedimenti volti a impedire che persone non autorizzate accedano ai sistemi di elaborazione dei dati.

Provvedimenti

- Gli account utente e i computer sono protetti da espedienti tecnici adeguati e al passo con i tempi.
- L'accesso da smartphone privati richiede l'impiego di un PIN sicuro e di un sistema operativo aggiornato.
- Utilizzo obbligatorio di un programma di gestione delle password.
- Ingresso agli uffici attraverso porte dotate di dispositivi di sicurezza e allestimento di protocolli per la gestione delle chiavi.

Controllo degli accessi ai dati

È l'insieme dei provvedimenti volti a garantire che solo utenti autorizzati possano accedere a determinati dati.

Provvedimenti

- Rigoroso piano in materia di autorizzazioni e verifica periodica, anche nell'ambito di audit.
- Processo di autorizzazione per il rilascio degli accessi.
- Accessi come amministratore fortemente limitati a una cerchia ben definita di persone.

Controllo delle procedure di trasmissione

È una forma di controllo volta a garantire che i dati, in fase di trasmissione elettronica, non vengano letti, modificati o cancellati in modo illecito.

Provvedimenti

- Crittografia per i laptop tramite Bitlocker.
- Trasmissione crittografata dei dati (TLS/SSL).
- WLAN protetta.

Controllo dell'aderenza al mandato

È l'insieme di provvedimenti volti a garantire che i dati personali vengano trattati esclusivamente in conformità alle istruzioni del committente.

Provvedimenti

- Accordo sul trattamento dei dati (DPA) con i fornitori di servizi, se possibile.
- Verifica periodica dei responsabili del trattamento.

Controllo della disponibilità

È una misura tecnica che consente di ripristinare i dati dopo una perdita, un danneggiamento o un guasto.

Provvedimenti

- Backup di dati e interventi di manutenzione.
- Conservazione dei backup in luoghi diversi.
- Protezione dalle minacce.
- Aggiornamento e formazione periodici del personale (almeno 3 volte l'anno).