

Contratto per il trattamento dei dati per le aziende (CTD)

1 Oggetto e campo di applicazione del CTD

Le disposizioni del presente CTD integrano le Condizioni generali per l'utilizzo della piattaforma «SIAC» da parte delle aziende (**contratto principale**) e disciplinano ogni trattamento di dati personali effettuato dal prestatore nel suo ruolo di responsabile del trattamento dei dati per l'azienda quale titolare del trattamento. L'oggetto e la durata del trattamento, il tipo e la finalità del trattamento, il tipo di dati personali, le categorie di persone interessate e i diritti e gli obblighi delle parti risultano dalle Condizioni Generali di cui sopra, dal presente Allegato 1 e dagli Allegati 2 e 3.

2 Trattamento dei dati personali da parte del prestatore

Il prestatore s'impegna nei confronti dell'azienda a:

- a) trattare i dati personali, salvo diverso accordo, esclusivamente per le finalità dell'azienda e di volta in volta al mero scopo di adempiere il contratto principale secondo le istruzioni documentate dell'azienda;
- b) *non comunicare o trasmettere dati personali all'estero, tranne:*
 - *salvo accordo più restrittivo nel contratto principale, a un destinatario in un Paese con un adeguato livello di protezione dei dati;*
 - *salvo accordo più restrittivo, a un destinatario che non si trova in un Paese con un adeguato livello di protezione dei dati, purché siano stati soddisfatti i requisiti richiesti per una comunicazione risp. trasmissione dei dati personali lecita ai sensi della LPD; oppure*
 - *quando ciò sia stato concordato con il committente nel contratto principale o in altro modo;*
- c) prevedere e mantenere misure tecniche od organizzative adeguate per garantire la riservatezza, l'integrità e la disponibilità dei dati personali, segnatamente le misure elencate nell'Allegato 3; il prestatore può adattare tali misure ove necessario, purché nel complesso venga sostanzialmente mantenuto il livello di protezione; in tali casi, egli modifica l'Allegato 3 (misure tecniche e organizzative) e lo comunica al committente in modo adeguato;
- d) affidare il trattamento dei dati personali solo a dipendenti e altro personale ausiliario che abbiano un obbligo legale o contrattuale alla riservatezza, ferma restando la responsabilità del prestatore per il comportamento dei suoi dipendenti o di altro personale ausiliario e per il proprio comportamento;
- e) delegare il trattamento dei dati personali a un terzo (fatta eccezione per i dipendenti e altro personale ausiliario che soddisfano i requisiti di cui al paragrafo d)) solo previa autorizzazione scritta dell'azienda e unicamente a un subincaricato tenuto a rispettare disposizioni in materia di riservatezza e protezione dei dati che siano almeno altrettanto rigorose quanto le disposizioni delle CG e del presente CTD, ferma restando la responsabilità del prestatore per il comportamento dei suoi subincaricati e per il proprio comportamento; il consenso è ritenuto dato, in generale, per tutti i subincaricati indicati nello specifico elenco di cui all'Allegato 4; il consenso, inoltre, è ritenuto dato per i subincaricati comunicati per iscritto dal prestatore all'azienda con almeno 30 giorni di anticipo, fermo restando tuttavia che qualora l'azienda si

- opponga al subincaricato entro 30 giorni dal ricevimento della comunicazione, al prestatore è fatto divieto di delegare il trattamento dei dati a tale subincaricato; in tal caso il prestatore ha tuttavia facoltà di porre fine all'utilizzo accordato all'azienda con un preavviso di tre mesi;
- f) comunicare tempestivamente all'azienda (i) ogni violazione vera o presunta della protezione dei dati unitamente a tutte le informazioni ai sensi dell'articolo 33 capoverso 3 GDPR, ove applicabile, o di altre normative applicabili in materia di protezione dei dati a disposizione del prestatore, (ii) comunicare tempestivamente ogni alterazione o insufficienza effettiva o imminente del prestatore nell'esecuzione di una delle disposizioni del presente CTD e (iii) comunicare ogni domanda di accesso a dati personali e ogni accesso effettivo a dati personali da parte di autorità, salvo il caso in cui la legge vieti tale comunicazione per motivi d'interesse pubblico;
- g) su richiesta dell'azienda, assistere quest'ultima nel rispetto delle disposizioni applicabili in materia di protezione dei dati nel modo auspicato (assistere quindi, ma non solo, l'azienda nell'adempimento dei suoi obblighi, (i) rispondere alle persone interessate che esercitano i loro diritti ai sensi delle normative applicabili in materia di protezione dei dati (incluso il Capo III del GDPR, ove applicabile) e (ii) soddisfare i requisiti di cui agli articoli 32-36 del GDPR, ove applicabile, e le relative disposizioni di altre normative applicabili in materia di protezione dei dati, nel rispetto della natura del trattamento e delle informazioni a disposizione del prestatore). L'azienda rimborsa al prestatore i costi e le spese ragionevoli, sostenuti dal prestatore nell'assistenza allo stesso ai sensi del presente paragrafo;
- h) informare senza indugio l'azienda se un'istruzione impartita dall'azienda al prestatore in merito al trattamento dei dati personali potrebbe probabilmente violare le disposizioni applicabili della legge sulla protezione dei dati o altre disposizioni applicabili;
- i) fornire all'azienda tutte le informazioni necessarie per comprovare il rispetto del presente articolo 2 da parte del prestatore nonché consentire l'esecuzione di ispezioni e l'assistenza durante il loro svolgimento, incluse le ispezioni eseguite dall'azienda o da un revisore incaricato dalla stessa, nel rispetto dei consueti accordi di riservatezza. Su richiesta dell'azienda il prestatore deve inoltre mettere a disposizione della stessa ogni relazione di audit predisposta dal revisore del prestatore che confermi il rispetto del presente articolo 2 da parte del prestatore e
- j) fatti salvi gli obblighi di conservazione legale applicabili, al termine del trattamento dei dati su incarico oppure su richiesta dell'azienda, restituire i dati personali alla parte contraente o cancellarli, senza conservare fotocopie, e confermare la cancellazione all'azienda.

3 Obblighi dell'azienda

L'azienda s'impegna nei confronti del prestatore a:

- a) garantire che il trattamento dei dati personali e le istruzioni fornite dall'azienda al prestatore siano conformi alle CG e alle disposizioni applicabili in materia di protezione dei dati;
- b) trasmettere o richiedere ogni comunicazione, registrazione, autorizzazione ufficiale e consenso delle persone interessate necessari al corretto trattamento dei dati personali da parte del prestatore;
- c) rispondere a ogni domanda o pretesa delle persone interessate conformemente a quanto previsto dalle disposizioni in vigore, ad eccezione del caso in cui tale compito sia stato delegato al prestatore.

4 Ulteriori disposizioni

- a) Salvo diverso accordo nelle CG o tra le parti, ogni parte si fa carico dei propri costi per l'attuazione del presente accordo aggiuntivo.
- b) In caso di azione intentata da terzi per una sua violazione del presente CTD o di ogni altra disposizione in materia di protezione dei dati, ciascuna parte contraente tiene l'altra esente e indenne da ogni risarcimento o responsabilità. La constatazione che precede include in particolare tutti i danni, i costi, le pretese o le spese derivanti da simili violazioni.
- c) Con l'accettazione del presente CTD, le sue disposizioni sono considerate valide per tutti gli accordi relativi all'emissione di «Carte SIAC» esistenti e futuri, che l'azienda conclude con il prestatore. In caso di contraddizione tra una disposizione del presente CTD e una disposizione di un simile accordo, prevale la disposizione del presente CTD, nel caso e nella misura in cui sia interessato il trattamento dei dati personali da parte del prestatore nel quadro del contratto principale.
- d) Le disposizioni del presente CTD trovano applicazione anche dopo la fine del trattamento dei dati su incarico del titolare e restano in vigore fino a quando il prestatore è in possesso dei dati personali interessati dal presente CTD. In tal caso, il CTD è retto dal diritto svizzero e il foro competente è la sede del prestatore.
- e) Salvo diversa indicazione nel presente CTD, le disposizioni delle CG restano invariate.

Condizioni generali per l'utilizzo della piattaforma «SIAC» da parte delle aziende

Allegato 2: trattamento dei dati su incarico del titolare

Nel quadro delle CG, CTD incluso, e con riserva dell'autorizzazione della commissione paritetica competente (che viene richiesta dal prestatore), il prestatore viene incaricato dall'azienda di emettere le «Carte SIAC» e di consegnarle all'azienda.

A tal fine, l'azienda trasmette al prestatore i seguenti dati personali per ogni dipendente per il quale deve essere emessa una «Carta SIAC»:

- nome e cognome
- data di nascita
- foto
- impiego
- funzione
- assoggettamento del dipendente a un CCL (soprattutto nelle aziende miste)
- grado di occupazione
- entrata in servizio (e se nota data di uscita dall'azienda)
- numero di telefono del dipendente (facoltativo)
- numero AVS
- copia di un documento d'identità ufficiale
- contatto in caso di emergenza (facoltativo)

Su incarico dell'azienda, il prestatore salva questi dati nella sua banca dati per la durata della validità delle «Carte SIAC». A tal fine l'azienda conferisce inoltre al prestatore il mandato di mettere a disposizione della commissione paritetica competente o dell'organo di controllo da questa incaricato i seguenti dati nel quadro della verifica online delle «Carte SIAC» tramite l'applicazione di controllo SIAC:

- nome e cognome
- data di nascita
- ragione sociale dell'azienda
- numero del documento
- documento valido (sì/no)
- avvertenza
- stato del documento
- data di scadenza del documento
- foto/foto tessera
- inizio del rapporto di lavoro
- fine del rapporto di lavoro
- nome e cognome del contatto in caso di emergenza
- numero di cellulare per il contatto in caso di emergenza
- assoggettamento al CCL del dipendente *
- funzione conformemente al CCL *
- grado di occupazione * *) eventualmente per ogni assoggettamento a un CCL

L'azienda dispone di un proprio accesso online per aggiornare i dati dei dipendenti da essa registrati e aggiungere o cancellare dipendenti.

Condizioni generali per l'utilizzo della piattaforma «SIAC» da parte delle aziende

Allegato 3: misure tecniche e organizzative

Di seguito vengono descritte le misure tecniche e organizzative che il prestatore adotta ai fini del trattamento dei dati personali e dell'adempimento dei suoi obblighi nel quadro delle CG.

Requisito: impedire a persone non autorizzate di accedere al sistema di elaborazione dei dati in cui vengono trattati o utilizzati i dati personali:

L'adozione di misure adeguate consente di garantire un controllo fisico degli accessi. I locali vengono chiusi adottando le consuete misure. I sistemi del prestatore vengono protetti da appositi controlli fisici degli accessi. Per i sistemi ospitati e gestiti da fornitori di servizi esterni, il prestatore ha posto in essere apposite misure che vengono attuate e mantenute dal fornitore di servizi interessato. Tali misure includono il controllo degli accessi con relativa documentazione, le misure per il monitoraggio e l'identificazione degli ospiti nell'edificio e la videosorveglianza di tutte le entrate e le uscite.

Requisito: impedire che i sistemi di elaborazione dei dati possano essere letti, copiati, modificati o rimossi senza autorizzazione:

Il prestatore garantisce il controllo elettronico degli accessi adottando misure adeguate. In particolare, l'accesso ai sistemi di elaborazione dei dati è protetto da password e viene accordato solo a persone autorizzate, tenute alla riservatezza e al rispetto della normativa in materia di protezione dei dati. Il prestatore ha implementato tecnologie di crittografia appropriate e utilizza adeguati rilevamenti antimalware e antivirus per impedire che software dannosi possano accedere in modo indesiderato ai dati personali. Il prestatore si avvale di un sistema di assegnazione delle autorizzazioni strutturato in modo intelligente e garantisce che le autorizzazioni per l'accesso dei dati vengano assegnate solo a persone che ne hanno bisogno e sono autorizzate ad accedervi. Il prestatore garantisce che le persone autorizzate all'utilizzo dei sistemi di elaborazione dei dati siano unicamente in grado di accedere ai dati previsti dal rispettivo permesso di accesso e che i dati personali non possano essere letti, copiati, modificati o rimossi senza autorizzazione durante l'elaborazione o l'utilizzo o dopo il salvataggio.

Requisito: impedire che i dati vengano letti, copiati, modificati o cancellati da parti non autorizzate durante la loro trasmissione o durante il trasporto dei supporti dei dati e garantire che sia possibile verificare e stabilire a quali organismi è previsto il trasferimento di dati mediante infrastrutture di trasmissione dei dati:

Il prestatore garantisce il controllo della trasmissione adottando misure adeguate, in particolare tramite una connessione criptata per l'accesso ai dati e la trasmissione dei dati tramite reti pubbliche. La trasmissione dei dati tramite internet è prevista unicamente laddove sia assolutamente necessaria per lo svolgimento dei compiti del prestatore. I dati vengono salvati su supporti dati portatili solo ove sia strettamente necessario ai fini dello svolgimento dei compiti del prestatore. In tal caso si procede a un'apposita cifratura. È esclusa una trasmissione dei dati a terzi non conosciuti. Il prestatore adotta misure appropriate per garantire la rimozione dei dati personali dai suoi sistemi dopo la risoluzione del relativo accordo in vigore.

Requisito: garantire che sia possibile verificare e stabilire se e da chi siano stati immessi, modificati o rimossi dati personali in sistemi di elaborazione:

Il prestatore garantisce il controllo degli inserimenti implementando misure adeguate. In particolare documenta chi può inserire o modificare i dati e quando. All'occorrenza è possibile ripristinare in ogni momento la versione precedente. Le modifiche dei dati vengono verbalizzate, segnatamente la consultazione di certificazioni di conformità al CCL nonché l'ordinazione e la consultazione di Carte SIAC¹. Il prestatore registra le violazioni della sicurezza descrivendo l'infrazione commessa, il periodo interessato, le conseguenze della violazione, il nominativo della persona che redige il rapporto e il nominativo della persona a cui è stata segnalata la violazione nonché la procedura per il ripristino dei dati.

Requisito: garantire che i dati personali elaborati da un subincaricato possano essere trattati solo conformemente alle istruzioni delle commissioni paritetiche:

Il prestatore garantisce il controllo dei subincaricati adottando misure adeguate, in particolare concludendo contratti scritti con il subincaricato in linea con le normative in materia di protezione dei dati e verificando il rispetto di tali contratti da parte dei subincaricati.

Requisito: garantire che i dati personali siano protetti dalla distruzione o dalla perdita accidentale:

Il prestatore garantisce il controllo della disponibilità adottando misure adeguate. In particolare ha implementato e attuato un sistema di backup e ripristino. I backup vengono effettuati regolarmente (almeno una volta al giorno) e il prestatore è in grado di ripristinare i dati di questi backup. Il prestatore adotta procedure adeguate per garantire che i dati personali non più necessari vengano cancellati in sicurezza e che i dati personali sui supporti dati non più necessari non possano più essere consultati o ripristinati. Il prestatore garantisce che tutte le funzioni rilevanti in termini di sicurezza siano monitorate e disponibili e introduce misure adeguate per garantire l'individuazione immediata di ogni guasto rilevante.

Prerequisito: garantire che i dati raccolti per finalità diverse possano essere elaborati separatamente:

Il prestatore garantisce questo trattamento separato adottando misure adeguate. In particolare questi record di dati possono essere identificati e separati grazie alle funzioni di selezione del sistema utilizzato.

Requisito: garantire che l'efficacia delle misure tecniche e organizzative a tutela della sicurezza del trattamento dei dati personali venga verificata, valutata e analizzata a cadenza regolare:

Il prestatore s'impegna a verificare, valutare e analizzare a cadenza regolare l'efficacia delle misure tecniche e organizzative, a documentare i risultati di queste verifiche, valutazioni e analisi e a rimuovere in modo adeguato le carenze constatate in occasione delle suddette verifiche, valutazioni e analisi.

Requisito: garantire misure organizzative adeguate a tutela dei dati personali:

Il prestatore garantisce l'attuazione di misure organizzative adeguate a tutela dei dati personali. Il prestatore elegge, istruisce e monitora con cura e in modo adeguato i dipendenti e altre persone coinvolte nel trattamento di dati personali. Il prestatore ha implementato direttive adeguate in

¹ Osservazione: per ragioni tecniche, la tracciabilità delle consultazioni di Carte SIAC effettuate tramite l'applicazione di controllo SIAC non è realizzabile nella versione 1.0.

materia di riservatezza e protezione dei dati e verifica il rispetto di tali direttive e dà loro attuazione. I dipendenti e altre persone coinvolte nel trattamento di dati personali seguono formazioni a cadenza regolare in materia di protezione dei dati e protezione della sfera privata. Il prestatore documenta in modo adeguato le misure organizzative adottate.

Condizioni generali per l'utilizzo della piattaforma «SIAC» da parte delle aziende

Allegato 4: elenco dei subincaricati

Prestatore	Indirizzo	Scopo / Funzione
Elca Informatik AG	Flurstrasse 62, 8048 Zurigo	Hosting

Zurigo,

Associazione paritetica Sistema d'informazione alleanza costruzione (SIAC)

Dichiarazione giuridicamente vincolante

(cognome, nome, posizione nell'azienda, numero di telefono e indirizzo e-mail)

dichiara a nome dell'azienda

(azienda, indirizzo, numero IDI)

in primo luogo

di aver letto e compreso le condizioni generali di cui sopra, incluso il CTD con gli allegati 2 e 3, nonché le tariffe SIAC e il Regolamento concernente la Carta SIAC ([link](#)) e di essere autorizzato ad accettarne il carattere vincolante per l'azienda summenzionata cliccando sulla presente casella

e in secondo luogo

di essere autorizzato a designare (cognome, nome, posizione nell'azienda, lingua, numero di telefono e indirizzo e-mail) come super-user per l'azienda summenzionata conformemente all'articolo 4.1 delle CG di cui sopra e pertanto a disporre l'invio dei dati di login al super-user del SIAC nonché la comunicazione dei dati di login e dell'identità del super-user alle seguenti persone con diritto di firma conformemente al registro di commercio (in caso di firma collettiva indicare due persone):

Cognome, nome, funzione, indirizzo e-mail