

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

1 Associazione paritetica Sistema d'informazione alleanza costruzione (SIAC)

L'associazione paritetica Sistema d'informazione alleanza costruzione (SIAC), con sede in Waldeggstrasse 37, 3097 Berna-Liebefeld, di seguito denominata **prestatore**, si adopera per mettere a disposizione delle parti sociali dati nazionali per l'esecuzione dei CCL. Essa opera in modo centralizzato e tramite una banca dati elettronica.

A tal fine il prestatore gestisce una piattaforma elettronica basata su una banca dati per la trasmissione di informazioni. Il prestatore declina tuttavia ogni responsabilità per le informazioni trasmesse dalle commissioni paritetiche o dalle aziende e risponde unicamente del funzionamento tecnico del Sistema d'informazione alleanza costruzione (banca dati SIAC).

2 Certificazione di conformità al CCL

In nome e per conto delle commissioni paritetiche, il prestatore emette certificazioni di conformità al CCL sulla base delle informazioni da esse trasmesse. Le certificazioni vengono generate automaticamente dalla banca dati SIAC. Informazioni dettagliate figurano nel Regolamento SIAC, consultabile sul sito www.isab-siac.ch.

L'azienda è autorizzata a richiedere gratuitamente certificazioni digitali di conformità al CCL relative a sé stessa.

3 La «Carta SIAC»

Su incarico di varie commissioni paritetiche, il prestatore emette documenti d'identificazione standardizzati («Carte SIAC») per i dipendenti di aziende assoggettate a un determinato contratto collettivo di lavoro (CCL) e per le quali la commissione paritetica (CP) competente per l'esecuzione del CCL ha rilasciato l'autorizzazione in base ai suoi criteri.

L'azienda può richiedere che sia rilasciata una simile autorizzazione. Nel caso in cui la commissione paritetica la conceda, ha facoltà di far emettere dal prestatore i documenti d'identificazione («Carte SIAC») per i dipendenti da essa designati. A tal fine l'azienda accetta le presenti CG e inserisce nella banca dati SIAC i dati personali dei suoi dipendenti, necessari ai fini dell'emissione delle «Carte SIAC» (ai sensi della Legge federale sulla protezione dei dati LPD).

4 Conferimento del mandato all'associazione SIAC da parte dell'azienda

Le presenti CG e l'addendum sulla protezione dei dati (Allegato 1) disciplinano il trattamento dei dati personali inseriti dall'azienda effettuato dal prestatore su incarico dell'azienda e ne assicura la conformità alle disposizioni applicabili in materia di protezione dei dati. Benché il trattamento dei dati non sottostia al Regolamento generale sulla protezione dei dati (GDPR) per tutte le aziende, ne deve comunque soddisfare i requisiti.

L'azienda conosce e accetta il fatto che il prestatore agisca come responsabile del trattamento non solo per l'azienda, ma anche per le commissioni paritetiche.

5 Utilizzo della piattaforma SIAC da parte dell'azienda

5.1 Gestione degli utenti

Per l'azienda viene attivata un'autorizzazione come super-user per accedere al sistema della banca dati SIAC. L'azienda designa il suo super-user, fornendo i dati necessari indicati alla fine del presente documento. Il super-user può attivare ulteriori utenti per l'azienda e cancellarli e inoltre è responsabile dell'istruzione degli utenti da esso designati. L'azienda ha facoltà di modificare il super-user trasmettendo un'apposita comunicazione scritta all'associazione SIAC.

Il super-user e gli utenti possono consultare tutti i dati disponibili nella banca dati SIAC, che concernono l'azienda (o la parte aziendale) e il relativo CCL.

La banca dati SIAC prevede unicamente la possibilità di creare utenti personali. I dipendenti che ottengono un'autorizzazione utente sono tenuti alla riservatezza e al rispetto delle normative applicabili in materia di protezione dei dati.

L'azienda è tenuta a garantire un'apposita istruzione degli utenti che registra e su richiesta del prestatore esibisce la prova dell'impegno assunto in tal senso dagli utenti.

L'azienda è inoltre tenuta a disattivare le autorizzazioni utente non più necessarie.

5.2 Registrazione dei dati dei dipendenti

L'azienda risponde della registrazione corretta e completa dei dati dei suoi dipendenti.

L'azienda e gli utenti da essa designati rispondono delle conseguenze civili e penali della registrazione di dati errati dei dipendenti.

6 Aspetti commerciali

Fanno stato le «tariffe SIAC» in vigore, consultabili anche sul sito www.isab-siac.ch.

La fatturazione viene effettuata su base mensile con pagamento in 30 giorni. Se dopo il primo sollecito la fattura non viene saldata entro 30 giorni, il prestatore ha facoltà di bloccare all'azienda l'accesso alla piattaforma SIAC.

7 Gestione contrattuale

7.1 Adeguamento della piattaforma SIAC

Il prestatore ha facoltà di recepire le modifiche legislative, i nuovi sviluppi tecnologici o le nuove circostanze adeguando la piattaforma SIAC.

Essa notifica quanto prima gli adeguamenti per iscritto all'azienda, affinché quest'ultima possa modificare la sua infrastruttura nonché i suoi processi e le sue procedure.

7.2 Interlocutori

La persona che approva formalmente le presenti CG è considerata l'interlocutore amministrativo dell'azienda. Per le questioni informatiche l'interlocutore è il super-user designato nella dichiarazione giuridicamente vincolante.

L'interlocutore del prestatore è l'ufficio amministrativo.

7.3 Adeguamento delle CG e degli allegati

Il prestatore ha facoltà di modificare in ogni momento le presenti CG e i loro allegati. Le modifiche vengono notificate al cliente in tempo utile.

8 Diritti di proprietà intellettuale

Il prestatore mantiene interamente i diritti di proprietà intellettuale che gli spettano e in particolare i diritti di autore, di marchio e societari nonché i diritti relativi al suo know how.

Il prestatore solleva l'azienda da ogni responsabilità in caso di violazione dei diritti d'autore svizzeri e di altri diritti di proprietà intellettuale di terzi, a condizione che e nella misura in cui tale violazione sia stata provocata dall'utilizzo della piattaforma SIAC conformemente a quanto previsto a livello contrattuale.

9 Durata e fine del contratto

9.1 Entrata in vigore

Le presenti CG entrano in vigore con la firma delle due parti.

9.2 Fine del contratto

L'azienda e il prestatore hanno facoltà di disdire l'utilizzo della banca dati per la fine di un mese civile osservando un termine di preavviso di un mese. Le prestazioni percepite vengono fatturate dal prestatore alla data della disdetta e devono essere pagate entro un termine di 30 giorni.

L'azienda garantisce la migrazione dei dati dei dipendenti da essa registrati entro la fine del contratto.

La disdetta dell'utilizzo della banca dati o il venir meno di un assoggettamento a un CCL dichiarato di obbligatorietà generale non comporta la soppressione dei dati registrati dalla commissione paritetica dalla piattaforma SIAC.

10 Ulteriori disposizioni

10.1 Esclusione della responsabilità / limitazione della responsabilità

Nessuna parte è responsabile nei confronti dell'altra per

1. guasti sorti nell'ambito dei gestori della rete;
2. guasti dei server presso i provider di internet;
3. indisponibilità del sistema informatico o dei contenuti del prestatore, qualora il guasto non sia intenzionale o dovuto a negligenza grave di una parte contraente;

4. lieve negligenza di una parte.

Per il resto il prestatore risponde unicamente nella misura di quanto previsto dalle presenti CG. È interamente esclusa ogni ulteriore responsabilità. In particolare è interamente esclusa la responsabilità degli organi nell'ambito della negligenza lieve.

È interamente esclusa la responsabilità dei dipendenti del prestatore e del personale ausiliario esterno.

10.2 Diritto applicabile / foro competente

Il rapporto contrattuale tra il prestatore e l'azienda e le presenti CG sono retti dal diritto svizzero. Il foro competente è Berna.

In caso di incertezza, vale la versione tedesca.

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

Allegato 1: addendum sulla protezione dei dati (APD)

1 Campo di applicazione

Ogni trattamento di dati personali effettuato dal prestatore nel suo ruolo di responsabile del trattamento dei dati per l'azienda quale titolare del trattamento è disciplinato dal presente ADP. 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) elaborare i dati personali esclusivamente per le finalità dell'azienda;
- b) non esportare dati personali (neanche nel quadro di un trattamento di dati personali consentito nel quadro delle CG) senza previa autorizzazione scritta dell'azienda o a un destinatario in un Paese SEE;
- c) prevedere e mantenere misure tecniche od organizzative adeguate, segnatamente le misure elencate nell'Allegato 3, al fine di impedire un trattamento dei dati non autorizzato, la perdita o l'alterazione di dati personali;
- 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 APD, ferma restando la responsabilità del prestatore per il comportamento dei suoi subincaricati e per il proprio comportamento; il consenso 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 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 APD 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 e (ii) soddisfare i requisiti di cui agli articoli 32-36 del GDPR 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 APD 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 APD, 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 APD e una disposizione di un simile accordo, prevale la disposizione del presente APD, nel caso e nella misura in cui sia interessato il trattamento dei dati personali da parte del prestatore nel quadro delle CG.
- d) Le disposizioni del presente APD 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 APD. In tal caso l'APD è retto dal diritto svizzero e il foro competente è la sede del prestatore.
- e) Salvo diversa indicazione nel presente APD, 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, APD 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 (facoltativo)
- 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.

Nell'erogazione di questo servizio e nell'esecuzione dei trattamenti di dati per la commissione paritetica il prestatore è inoltre tenuto ad attenersi alle seguenti disposizioni:

- **Regolamento sulla protezione dei dati e Regolamento SIAC pubblicati su www.isab-siac.ch**

Ulteriori prescrizioni risultano dalle CG.

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.

Berna,

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 l'addendum sulla protezione dei dati con gli allegati 2 e 3, nonché le tariffe SIAC, il Regolamento sulla protezione dei dati 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