Regolamento sulla protezione dei dati

Art. 1 Finalità

L'associazione paritetica «Sistema d'informazione alleanza costruzione» (SIAC) gestisce una banca dati.

Le commissioni paritetiche, gli organi di controllo e le aziende gestiscono dei dati sul Sistema d'informazione alleanza costruzione. Incaricano l'associazione SIAC di eseguire determinati processi quali l'emissione di certificazioni di conformità al CCL o di documenti per i dipendenti di aziende che sottostanno al CCL (Carta SIAC) e la loro consultazione online tramite un'applicazione di controllo SIAC (app SIAC).

Le disposizioni esecutive relative al presente regolamento sono contenute nei principi applicabili al trattamento dei dati SIAC, che costituiscono l'Allegato 1 al presente regolamento.

Art. 2 Responsabilità del trattamento dei dati

L'associazione SIAC effettua ogni trattamento di dati di persone fisiche o giuridiche nella sua veste di responsabile del trattamento dei dati. La responsabilità in ordine al contenuto dei dati spetta alle commissioni paritetiche, agli organi di controllo e alle aziende.

Art. 3 Accordo di utilizzo e CG

L'associazione SIAC conclude un accordo di utilizzo con le commissioni paritetiche e gli organi di controllo che trasmettono i dati al sistema. Le aziende che registrano i dati nella piattaforma SIAC e ordinano certificazioni di conformità al CCL o Carte SIAC sottoscrivono le Condizioni generali (CG).

Art. 4 Emissione di autorizzazioni per gli utenti

Quando una commissione paritetica, un organo di controllo, un ente aggiudicatore o un'azienda firma l'accordo di utilizzo o le CG, può accedere al Sistema d'informazione alleanza costruzione. Questo accesso consente di creare e gestire autorizzazioni per gli utenti.

Un utente può essere creato solo previa firma dell'accordo di utilizzo o delle CG.

Non sono considerati terzi gli organi SIAC e l'ufficio amministrativo SIAC con il loro personale nonché i fornitori di servizi informatici per lo sviluppo e la manutenzione della banca dati SIAC. Queste autorizzazioni interne all'associazione SIAC vengono accordate solo per il tempo e nella misura in cui risultino necessarie per lo svolgimento dei compiti della persona interessata.

Art. 5 Gestione degli utenti

L'associazione SIAC prevede unicamente la possibilità di creare utenti personali. Gli utenti che ottengono un'autorizzazione utente sono tenuti alla riservatezza e al rispetto delle normative applicabili in materia di protezione dei dati e di tutte le altre normative pertinenti.

Le commissioni paritetiche, gli organi di controllo, gli enti aggiudicatori e le aziende che gestiscono autorizzazioni sul Sistema d'informazione alleanza costruzione, sono tenuti a impartire un'apposita istruzione degli utenti che registrano. Sono inoltre tenuti a disattivare un'autorizzazione utente non più necessaria.

Su richiesta dell'associazione SIAC, sono tenuti a rendere conto degli utenti registrati e dimostrare di aver impartito le istruzioni adeguate.

L'ufficio amministrativo SIAC disciplina l'utilizzo delle autorizzazioni utente interne all'associazione.

Art. 6 Registrazione

Ogni modifica di dati nel Sistema d'informazione alleanza costruzione viene documentata. Tale obbligo include segnatamente anche la consultazione di una certificazione di conformità al CCL, l'ordinazione di Carte SIAC e la loro consultazione.

L'associazione SIAC monitora attivamente il sistema e 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.

L'associazione SIAC mette a disposizione delle commissioni paritetiche, degli organi di controllo e delle aziende le valutazioni relative alle modifiche dei dati nella loro sfera di responsabilità.

Su richiesta, l'associazione SIAC mette inoltre a disposizione valutazioni relative agli utenti.

Art. 7 Verifica dei mezzi tecnici utilizzati e della sicurezza dei dati

Avvalendosi di una società IT adeguata, l'associazione SIAC verifica a scadenza periodica, ma almeno una volta all'anno, se i requisiti tecnici sono ancora sufficienti a garantire un'adeguata protezione dei dati e in particolare a

- minimizzare gli errori tecnici e le perdite accidentali o la distruzione dell'intera raccolta di dati;
- impedire manomissioni della raccolta e accessi non autorizzati;
- verificare che i sistemi utilizzati corrispondano allo stato dell'arte.

Viene stilato un verbale dell'audit e delle eventuali raccomandazioni.

Art. 8 Richieste d'informazioni

Le commissioni paritetiche e gli organi di controllo che hanno firmato un accordo di utilizzo conferiscono all'associazione SIAC l'incarico di elaborare le richieste d'informazioni a loro nome conformemente alla legge sulla protezione dei dati. I dettagli sono disciplinati nei relativi contratti.

Chiunque richieda informazioni sui dati salvati che lo riguardano ai sensi della legge sulla protezione dei dati deve dichiarare se richiede tali informazioni

- in veste di persona fisica
- in veste di rappresentante autorizzato di una persona giuridica.

I richiedenti devono identificarsi esibendo appositi documenti e una procura debitamente firmata della persona giuridica, qualora la legittimazione ad agire per conto di questa non emerga già in modo univoco dal registro di commercio.

Quando la persona è stata identificata, l'associazione SIAC fornisce le informazioni e ne dà comunicazione alle commissioni paritetiche competenti e agli organi di controllo.

Quando la persona è stata identificata e la richiesta d'informazioni si riferisce a dati dei dipendenti

gestiti da aziende, l'associazione SIAC indirizza la persona richiedente alla o alle aziende competenti.

Art. 9 Richieste di rettifica

Quando perviene una richiesta di rettifica o di cancellazione di una registrazione, l'associazione SIAC appone tempestivamente un'annotazione nella banca dati e inoltra la richiesta alle commissioni paritetiche competenti, agli organi di controllo e alle aziende, che prendono in carico la procedura.

Art. 10 Entrata in vigore e modifiche

Il presente regolamento e l'allegato «Principi applicabili al trattamento dei dati» sono stati approvati dall'assemblea degli associati dell'associazione «Sistema d'informazione alleanza costruzione» in data 27.2.2019 e sono entrati in vigore con effetto immediato.

In caso di incertezza, vale la versione tedesca.

Allegato al regolamento sulla protezione dei dati SIAC: Principi applicabili al trattamento dei dati SIAC

L'associazione SIAC contrae i seguenti obblighi nei confronti dei partner contrattuali che siglano con essa un accordo di utilizzo:

1 Protezione dei dati

a) Elabora i dati personali solo per perseguire le finalità dei partner contrattuali e unicamente per eseguire l'accordo di utilizzo o le CG, conformemente alle istruzioni documentate del partner contrattuale. A tal fine l'associazione SIAC concorda con il partner contrattuale che il servizio previsto dall'accordo di utilizzo nonché la configurazione e il controllo dello stesso assicurati dal partner contrattuale siano conformi alle istruzioni definitive e vincolanti fornite dal partner contrattuale. Qualora siano necessarie ulteriori istruzioni e queste ultime non possano essere attuate dal prestatore nell'ambito delle sue risorse e delle risorse messegli a disposizione, il partner contrattuale deve modificare di conseguenza le istruzioni o rescindere l'accordo di utilizzo;

b) non esporta dati personali (neanche nel quadro di un trattamento dei dati personali ammesso dal rispettivo accordo in essere) in assenza di un'apposita base contrattuale;

c) prevede e mantiene misure tecniche od organizzative adeguate al fine di impedire un trattamento dei dati non autorizzato, la perdita o l'alterazione di dati personali e segnatamente le misure elencate al numero 2;

d) affida 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 dell'associazione SIAC per il comportamento dei suoi dipendenti o di altro personale ausiliario e per il proprio comportamento;

e) delega 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 del partner contrattuale e unicamente a un subincaricato tenuto a rispettare le disposizioni in materia di riservatezza e protezione dei dati che siano almeno altrettanto rigorose quanto le disposizioni dell'accordo di utilizzo, del regolamento sulla protezione dei dati e dei presenti principi applicabili al trattamento dei dati, ferma restando la responsabilità dell'associazione SIAC per il comportamento dei suoi subincaricati e per il proprio comportamento; il consenso è ritenuto dato per i subincaricati comunicati per iscritto dal prestatore al partner contrattuale con almeno 30 giorni di anticipo, fermo restando tuttavia che qualora il partner contraente si opponga al subincaricato entro 30 giorni dal ricevimento della comunicazione, all'associazione SIAC è fatto divieto di delegare il trattamento dei dati a tale subincaricato; in tal caso l'associazione SIAC ha tuttavia facoltà di disdire l'accordo di utilizzo con un preavviso di tre mesi;

f) comunica tempestivamente al partner contrattuale (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 dell'associazione SIAC, (ii) comunica tempestivamente ogni alterazione o insufficienza effettiva o imminente dell'associazione SIAC nell'esecuzione di una delle disposizioni dell'accordo di utilizzo, del regolamento sulla protezione dei dati o dei presenti principi applicabili al trattamento dei dati e

(iii) comunica 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 del partner contrattuale, assiste quest'ultimo nel rispetto delle disposizioni applicabili in materia di protezione dei dati nel modo auspicato (assiste quindi, ma non solo, il partner contrattuale nell'adempimento dei suoi obblighi, (i) risponde 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) soddisfa 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 dell'associazione SIAC). Il partner contrattuale rimborsa all'associazione SIAC i costi e le spese ragionevoli, sostenuti dall'associazione nell'assistenza allo stesso ai sensi del presente paragrafo;

h) informa tempestivamente il partner contrattuale qualora un'istruzione fornita dallo stesso all'associazione SIAC sul trattamento dei dati personali sia suscettibile di violare normative applicabili in materia di protezione dei dati o altre normative applicabili;

i) fornisce al partner contrattuale tutte le informazioni necessarie per comprovare il rispetto dell'articolo 3 del presente regolamento da parte dell'associazione SIAC nonché consentire l'esecuzione di ispezioni e l'assistenza durante il loro svolgimento, incluse le ispezioni eseguite dal partner contrattuale o da un revisore incaricato dallo stesso, nel rispetto dei consueti accordi di riservatezza. L'associazione SIAC deve inoltre mettere a disposizione del partner contrattuale ogni relazione di audit predisposta dal revisore dell'associazione SIAC e avente ad oggetto il rispetto dell'articolo 3 da parte dell'associazione SIAC; e

j) fatti salvi gli obblighi di conservazione legale applicabili, al termine dell'accordo di utilizzo o su richiesta del partner contrattuale restituisce i dati personali alla parte contraente o li cancella, senza conservare fotocopie, e conferma la cancellazione al partner contrattuale.

2 Principi applicabili al trattamento dei dati del prestatore nei confronti delle aziende

Il prestatore garantisce un'informazione delle aziende registrate nella piattaforma del SIAC conforme alla normativa in materia di protezione dei dati. Il prestatore garantisce che le certificazioni di conformità al CCL delle aziende che non intendono mettere a disposizione dei committenti e degli enti aggiudicatori le informazioni che le riguardano siano contrassegnate come bloccate.

3 Misure tecniche e organizzative

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, l'associazione SIAC 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:

L'associazione SIAC 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. L'associazione SIAC 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. L'associazione SIAC gestisce un elenco dei supporti dati su cui vengono trattati dati personali. L'associazione SIAC 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. L'associazione SIAC 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:

L'associazione SIAC 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. L'associazione SIAC 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:

L'associazione SIAC garantisce il controllo degli inserimenti dei dati 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 SIAC[1]. L'associazione SIAC 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 elaborati da un subincaricato (ai sensi dell'art. 1e) possano essere trattati solo conformemente alle istruzioni delle commissioni paritetiche:

L'associazione SIAC 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

[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.

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:

L'associazione SIAC 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 l'associazione SIAC è in grado di ripristinare i dati di questi backup. L'associazione SIAC 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[2]. L'associazione SIAC 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:

L'associazione SIAC 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:

L'associazione SIAC 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

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

[2] Osservazione: non è realizzabile la richiesta di cancellare anche i dati personali eventualmente ancora presenti sui supporti dati di backup.