Brescia Infrastrutture

POLITICA SULLA PROTEZIONE DEI DATI PERSONALI

(Documento approvato dal Consiglio di Amministrazione in data 11/05/2021)

REV.	DATA	REDATTO	AUTORIZZATO	DESCRIZIONE VARIAZIONI APPORTATE
00	11/12/2020	RSGQ	Presidente del CdA	Prima emissione.
01	11/05/2021	RSGQ	Presidente del CdA	Seconda emissione.

1. CAMPO D'APPLICAZIONE, SCOPO E DESTINATARI

Brescia Infrastrutture S.r.l. si impegna a rispettare le leggi e i regolamenti applicabili relativi alla protezione dei dati personali in conformità al Regolamento (UE) 2016/679 e alla normativa vigente in tema di privacy, sicurezza delle informazioni e videosorveglianza. Questa Politica stabilisce i principi di base con cui Brescia Infrastrutture S.r.l. tratta i dati personali di fornitori, consulenti, dipendenti e altre persone, indicando le responsabilità delle proprie Aree e Unità Organizzative aziendali e dipendenti durante il trattamento.

I destinatari di questo documento sono tutti i dipendenti, permanenti o temporanei, e tutti i collaboratori che lavorano per conto dell'Azienda.

2. DOCUMENTI DI RIFERIMENTO

- Il Regolamento (UE) 2016/679 (di seguito GDPR).
- Decreto legislativo n. 196/2003 (Codice Privacy) e ss.mm.ii.
- Provvedimenti del Garante in materia di videosorveglianza.
- Mappatura delle attività di trattamento e analisi del rischio.
- Valutazione d'impatto sulla protezione dei dati (DPIA).

3. OGGETTO E FINALITÀ

Il GDPR stabilisce le norme per la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché le norme per la libera circolazione di tali dati.

I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

I dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

Tenendo conto delle tecnologie e di altre misure di sicurezza disponibili, dei costi di attuazione e la probabilità e gravità dei rischi per i dati personali, l'Azienda ha messo in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato per i dati personali, inclusa la protezione dalla distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati.

Obiettivo di Brescia Infrastrutture S.r.l. è adottare e migliorare costantemente i propri processi organizzativi ed operativi per raccogliere il minor numero di dati personali possibile. Se i dati personali sono raccolti da terzi, il Responsabile del trattamento deve garantire che i dati personali siano raccolti legalmente.

Le finalità, i metodi, il limite di registrazione e il periodo di conservazione dei dati personali devono essere coerenti con le informazioni contenute nell'Informativa sulla Privacy. L'azienda deve mantenere l'esattezza, l'integrità, la riservatezza e la rilevanza dei dati personali in base allo scopo del trattamento. È necessario

utilizzare adeguati meccanismi di sicurezza volti a proteggere i dati personali per impedire che vengano rubati, utilizzati in modo improprio o abusati e prevenire le violazioni dei dati personali.
Ogni volta che la Società utilizza un fornitore per il trattamento dei dati personali per suo conto, è necessario ottenere garanzie che questo fornisca misure di sicurezza per salvaguardare i dati personali adeguate ai rischi associati. L'Azienda si impegna a richiedere contrattualmente al fornitore di fornire un adeguato livello di protezione dei dati (Nomina Responsabile Esterno Trattamento). I fornitori devono trattare i dati personali solo per adempiere ai propri obblighi contrattuali nei confronti dell'Azienda o dietro istruzioni dell'Azienda e non per altri scopi.

4. DIRITTI DEGLI INTERESSATI

L'Azienda deve fornire agli interessati un ragionevole meccanismo di accesso per consentire loro di accedere ai propri dati personali e consentire loro di accedere, rettificare, cancellare i propri dati personali, se del caso o se richiesto dalla legge.
Gli interessati hanno il diritto di ricevere, su richiesta, una copia dei dati che sono stati forniti e di trasmettere tali dati a un altro Titolare, gratuitamente. Brescia Infrastrutture S.r.l. garantisce che tali richieste vengano elaborate entro un mese, non siano eccessive e non incidano sui diritti relativi ai dati personali di altre persone.
Su richiesta, gli interessati hanno il diritto di ottenere dall'Azienda la cancellazione dei propri dati personali se sussiste uno dei seguenti motivi:

- I dati personali non sono più necessari rispetto alle finalità per le quali erano stati raccolti o altrimenti trattati.
- L'interessato revoca il consenso su cui si basa il trattamento e non sussiste altro fondamento giuridico per il trattamento.
- L'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento.
- I dati personali sono stati trattati illecitamente.
- I dati personali devono essere cancellati per adempiere un obbligo legale.

5. LINEE GUIDA SUL CORRETTO TRATTAMENTO

I dati personali devono essere trattati solo se esplicitamente autorizzati dal Titolare del trattamento. Il Titolare stabilisce se eseguire la Valutazione d'Impatto sulla protezione dei dati per ciascuna attività di trattamento.

6. REQUISITI PER IL TRATTAMENTO DEI DATI PERSONALI DEI FORNITORI

Qualsiasi trattamento dei dati personali dei dipendenti da parte delle Aree/U.O. all'interno dell'Azienda deve avvenire per uno scopo legittimo e deve soddisfare i seguenti requisiti.

INFORMATIVA AI FORNITORI

Al momento della raccolta o prima della raccolta di dati personali per qualsiasi tipo di attività di trattamento, il Titolare informa adeguatamente gli interessati in merito a:

- l'identità e i dati di contatto del Titolare del trattamento;
- se nominato, l'identità e i dati di contatto del Responsabile della Protezione dei dati (DPO);
- modalità e finalità del trattamento dei dati;
- presupposti giuridici al trattamento dei dati;
- categorie di destinatari;
- i potenziali trasferimenti dei dati (eventuale);
- il periodo di conservazione;
- i diritti dell'interessato riguardo ai suoi dati personali;
- se i dati saranno condivisi con terzi e le misure di sicurezza stabilite dall'Azienda per proteggere i dati personali;
- le conseguenze del mancato consenso al trattamento.

Queste informazioni sono fornite tramite l'Informativa sulla Privacy (Informativa per i Fornitori). L'Azienda, inoltre, in osservanza al principio di Accountability (responsabilizzazione) dovrà ottenere dall'interessato la conferma che lo stesso ha letto e compreso il contenuto dell'informativa.

INCARICATI AL TRATTAMENTO

L'U.O. Appalti e Contratti, unitamente al DEC del contratto, al RUP e all'U.O. Direzione Lavori sono i soggetti interni incaricati al trattamento dei dati personali dei fornitori.

7. REQUISITI PER IL TRATTAMENTO DEI DATI PERSONALI DEI DIPENDENTI

Qualsiasi trattamento dei dati personali dei dipendenti da parte delle Aree/U.O. all'interno dell'Azienda deve avvenire per uno scopo legittimo e deve soddisfare i seguenti requisiti.

INFORMATIVA AI DIPENDENTI

Ai fini della trasparenza del trattamento dei dati personali dei dipendenti, quando un'Area/U.O. all'interno dell'Azienda raccoglie i dati personali di un dipendente, il

dipendente deve essere informato dei tipi di dati raccolti, delle finalità e dei tipi di trattamento, dei diritti del dipendente e delle misure di sicurezza adottate per proteggere i dati personali. Queste informazioni sono fornite da apposita Informativa al trattamento dei dati personali (Informativa Raccolta Dati presso interessato e Informativa Videosorveglianza).

SCELTA E CONSENSO DEI DIPENDENTI

In linea di principio, l'Azienda può trattare i dati personali dei dipendenti per finalità legittime come datore di lavoro e generalmente può farlo senza ottenere il consenso del dipendente, per migliorare l'efficienza delle operazioni interne. Le attività di sicurezza e di gestione delle risorse umane come colloqui, assunzioni, cessazione del rapporto di lavoro, presenza, compensi e benefici, servizi dei dipendenti, salute e sicurezza sul lavoro possono comportare il trattamento di dati personali sensibili.

RACCOLTA

Le Aree/U.O. aziendali e le persone fisiche devono raccogliere i dati personali dei dipendenti per finalità legittime e devono rispettare il principio della minimizzazione dei dati.

USO, CONSERVAZIONE E SMALTIMENTO

Le Aree/U.O. aziendali e le persone fisiche devono utilizzare, conservare e disporre dei dati personali dei dipendenti in modo coerente con la comunicazione al dipendente. Devono inoltre garantire la sua esattezza, integrità e rilevanza. L'Azienda ha messo in atto misure di sicurezza adeguate a proteggere i dati personali dei dipendenti da distruzione accidentale o illecita, perdita, modifica, accesso non autorizzato o divulgazione, in accordo alla politica di sicurezza delle informazioni e altri documenti che descrivono la sicurezza dei dati. Le Aree/U.O. aziendali e le persone fisiche non devono distruggere o modificare illecitamente i dati personali dei dipendenti. Non devono accedere, vendere o fornire illecitamente o senza autorizzazione, dati personali dei dipendenti a terzi.

DIVULGAZIONE A TERZI

Quando le Aree/U.O. aziendali e gli individui devono comunicare i dati personali dei dipendenti a un fornitore o a terzi, devono cercare di garantire che gli stessi forniscano misure di sicurezza per salvaguardare i dati personali dei dipendenti che siano adeguate ai rischi associati. Dovrebbero inoltre richiedere al terzo di fornire lo stesso livello di protezione dei dati che forniscono all'Azienda per contratto o altro accordo (Nomina Responsabile Trattamento). Inoltre, quando le Aree/U.O.

aziendali e gli individui rivelano i dati personali dei dipendenti in risposta a una richiesta da parte delle forze dell'ordine o di un'autorità giudiziaria, devono prima informare il Responsabile della protezione dei dati (DPO) che è autorizzato dall'Azienda a gestire la richiesta.

ACCESSO DEI DIPENDENTI

Le Aree/U.O. aziendali devono fornire mezzi ragionevoli ai dipendenti per accedere ai dati personali detenuti su di essi e consentire alle risorse di aggiornare, correggere, cancellare o trasmettere i propri dati personali se necessario o richiesto dalla legge. Quando si risponde a una richiesta di accesso di un dipendente, i dipartimenti aziendali possono non fornire alcun dato personale fino a quando non abbiano verificato l'identità del dipendente. L'azienda deve assicurarsi di conoscere l'identità della persona che effettua la richiesta prima di poter inviare i dati personali alla persona stessa.

INCARICATI AL TRATTAMENTO

L'Area Legale, Societaria e Personale è il soggetto interno incaricato al trattamento dei dati personali dei dipendenti.

8. REQUISITI PER IL TRATTAMENTO DEI DATI PERSONALI DEI TERZI TRAMITE VIDEOSORVEGLIANZA

Qualsiasi trattamento dei dati personali dei dipendenti da parte delle Aree/U.O. all'interno dell'Azienda deve avvenire per uno scopo legittimo e deve soddisfare i seguenti requisiti.

INFORMATIVA AI TERZI

Al momento della raccolta o prima della raccolta di dati personali per qualsiasi tipo di attività di trattamento, il Titolare informa adeguatamente gli interessati in merito a:

- l'identità e i dati di contatto del Titolare del trattamento;
- se nominato, l'identità e i dati di contatto del Responsabile della Protezione dei dati (DPO);
- modalità e finalità del trattamento dei dati;
- presupposti giuridici al trattamento dei dati;
- categorie di destinatari;
- i potenziali trasferimenti dei dati (eventuale);
- il periodo di conservazione;
- i diritti dell'interessato riguardo ai suoi dati personali;

- se i dati saranno condivisi con terzi e le misure di sicurezza stabilite dall'Azienda per proteggere i dati personali;
- le conseguenze del mancato consenso al trattamento.

Queste informazioni sono fornite tramite l'Informativa sulla Privacy (Informativa Videosorveglianza per i Terzi/Visitatori). L'Azienda, inoltre, in osservanza al principio di Accountability (responsabilizzazione) dovrà ottenere dall'interessato la conferma che lo stesso ha letto e compreso il contenuto dell'informativa.

INCARICATI AL TRATTAMENTO

L'U.O. Facility e la Direzione, per la parte di videosorveglianza e l'U.O. Normativa interna e Auditing, per quanto concerne la parte dei sinistri, sono i soggetti interni incaricati al trattamento dei dati personali di terzi.

9. ORGANIZZAZIONE AZIENDALE

Il GDPR introduce nuovi obblighi organizzativi. La responsabilità di garantire un adeguato trattamento dei dati personali spetta a chiunque lavori per o con l'Azienda e abbia accesso ai dati personali trattati dall'Azienda; a tal fine l'Azienda ha implementato un proprio organigramma Privacy.

Le principali aree di responsabilità sono identificabili nei seguenti ruoli organizzativi:

- il Titolare del trattamento dei dati prende decisioni e approva le strategie generali della Società in materia di protezione dei dati personali. Tale ruolo è ricoperto dal legale rappresentante *pro tempore*.
- il Responsabile della Protezione dei Dati (DPO) è responsabile della gestione del programma di protezione dei dati personali ed è responsabile dello sviluppo e della promozione delle politiche di protezione dei dati personali.
- l'Amministratore di sistema garantisce che tutti i sistemi, i servizi e le attrezzature utilizzati per la registrazione dei dati soddisfino standard di sicurezza accettabili. Inoltre, conduce controlli e scansioni regolari per garantire che l'hardware e il software di sicurezza funzionino correttamente.
- le Persone autorizzate, dipendenti formalmente autorizzati a compiere operazioni di trattamento dal titolare.

10. OBBLIGHI GENERALI

Sono di seguito descritti.

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Il Titolare del trattamento deve tenere un registro delle attività di trattamento contenente le seguenti informazioni:

- dati di contatto del Titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- finalità del trattamento;
- categorie di interessati;
- categorie di dati personali trattati;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

RISPOSTA AGLI INCIDENTI DI VIOLAZIONE DEI DATI PERSONALI

Quando l'Azienda viene a conoscenza di una presunta o effettiva violazione dei dati personali, il Titolare coadiuvato dal DPO deve eseguire un'indagine interna e adottare misure correttive appropriate in modo tempestivo, in base alla Procedura di risposta e comunicazione della violazione dei dati definita dal Garante.

AUDIT E RESPONSABILIZZAZIONE

Il Titolare coadiuvato dal DPO verifica le modalità con cui le Aree/U.O. aziendali implementano questa politica.

BRESCIA INFRASTRUTTURE S.r.l.

Il Presidente del Consiglio di Amministrazione

f.to Ing. Marcello Peli