POLITICA SULLA PROTEZIONE DEI DATI PERSONALI

1. CAMPO D'APPLICAZIONE

La Presente Politica stabilisce le regole di base per la tutela dei Dati Personali

L'Azienda Civis S.p.A. si impegna a rispettare le leggi ed i regolamenti applicabili relativi alla protezione dei dati personali ed ha previsto misure tecniche ed organizzative per la protezione. Questa Politica si applica ai dati personali dei clienti, fornitori, partner commerciali, dipendenti e altre persone ed indica le responsabilità durante il trattamento.

I destinatari di questo documento sono tutti i dipendenti ed i collaboratori che lavorano per conto dell'Azienda.

2. DOCUMENTI DI RIFERIMENTO

- Il Regolamento (UE) 2016/679 del 27 Aprile 2016 (di seguito GDPR)
- Modulistica Privacy
- Registro del trattamento dei dati
- Organigramma Privacy
- Procedura di comunicazione di una violazione di dati
- Procedura gestione dei diritti dell'interessato
- Procedura DPIA (Data Protection Impact Assessment)
- Documento Sistema di gestione integrato della Qualità

3. OGGETTO E DEFINIZIONI

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.

- Dato Personale (Art.4): qualsiasi informazione (es. nome) concernente una persona fisica identificata o identificabile (definito «Interessato») direttamente o indirettamente;
- Categorie particolari di dati personali: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

- Titolare del trattamento dei dati (Titolare): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
- Responsabile del trattamento dei dati: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare.
- Responsabile della protezione dei dati (Data Protection Officer DPO): la persona fisica, la società, l'ente pubblico o privato, l'associazione o l'organismo cui il titolare affida, anche all'esterno della sua struttura organizzativa, specifici e definiti compiti di gestione e controllo del trattamento dei dati.
- Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come ad esempio la raccolta, la registrazione, la conservazione, la cancellazione.
- Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.
- Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
- Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile. membro;
- Autorità di Controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR dell'UE; per l'Italia è il Garante per la protezione dei dati personali (GARANTE)

4. PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

I principi applicabili al trattamento e alla protezione dei dati definiscono le responsabilità delle organizzazioni nella gestione dei dati personali e sono regolamentati in modo puntuale dalle procedure di riferimento. I dati personali sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- 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;
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

5. ORGANIZZAZIONE E LINEE GUIDA SUL CORRETTO TRATTAMENTO

Il Management della società è tenuto ad assicurare la protezione dei Dati Personali nell'ambito delle loro responsabilità. Qualsiasi trattamento dei dati personali dei dipendenti da parte di dipartimenti e individui all'interno dell'Azienda deve avvenire per uno scopo legittimo.

La responsabilità di garantire un adeguato trattamento dei dati personali spetta, in ogni caso, a chiunque lavori per o con l'Azienda e abbia accesso ai dati personali trattati dall'Azienda.

Di seguito le linee guida adottate:

- Organizzazione aziendale: Il GDPR introduce nuovi obblighi organizzativi e a tal fine l'Azienda ha implementato un proprio organigramma Privacy con ruoli e responsabilità definite, nominando responsabili interni al trattamento ed un Responsabile della protezione dei dati (DPO)
- Comunicazione agli interessati: al momento della raccolta, o prima della raccolta di dati personali per qualsiasi tipo di attività di trattamento, il Titolare o i Responsabili interni sono tenuti a informare adeguatamente gli interessati tramite un'Informativa sulla Privacy
- Ottenimento consenso: ogni volta che il trattamento dei dati personali si basa sul consenso dell'interessato, o su altri motivi legittimi, verranno fornite agli interessati le opzioni per dare il consenso, informando che il consenso puo' essere revocato in qualsisia momento
- Registro del trattamento: Il Titolare ed i Responsabili interni del trattamento sono responsabili della creazione e della manutenzione del registro delle attività di trattamento
- Gestione degli 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.

- 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.
- Divulgazione a terzi: l'azienda si impegna a richiedere contrattualmente al fornitore o partner commerciale di fornire un adeguato livello di protezione dei dati (Nomina Responsabile Esterno Trattamento). I fornitori o i partner commerciali devono trattare i dati personali solo per adempiere ai propri obblighi contrattuali e non per altri scopi.
- Diritto di accesso: l'azienda è responsabile di fornire agli interessati un ragionevole meccanismo di accesso per consentire loro di accedere ai propri dati personali e deve consentire loro di aggiornare, rettificare, cancellare o trasmettere i propri dati personali, se del caso o richiesto dalla legge. Il meccanismo di accesso è ulteriormente dettagliato nella Procedura di gestione dei diritti dell'interessato.
- Audit e Responsabilizzazione: gli Internal Audit periodici hanno lo scopo di verificare in che modo i reparti aziendali implementino questa politica. Qualsiasi dipendente che violi questa Politica sarà soggetto ad azioni disciplinari e potrebbe anche essere soggetto a responsabilità civili o penali qualora la sua condotta violasse leggi o regolamenti.

Specifichiamo infine che, dal punto di vista tecnologico, sono state messe in atto le misure necessarie al fine di proteggere l'accesso ai dati personali e che anche tali misure sono oggetto di Audit periodici. A titolo di esempio: sistemi di autenticazione informatica, credenziali di autenticazione, firewalling e software antivirus, backup e ripristino dei dati.

La struttura Sistemi Informativi è responsabile di garantire che i servizi e le attrezzature utilizzate soddisfino adeguati standard di sicurezza

6. CONTATTI

Il Responsabile della Protezione dei Dati (DPO) puo' essere contattato all' indirizzo mail rpd.privacy@civisspa.com

La Direzione aziendale