Dichiarazione di Conformità al RGPD

Contesto di riferimento

Il ***Regolamento Generale Europeo per la Protezione dei Dati Personali EU 2016/679*** (in sigla, '**RGPD**' o '**GDPR**'), è entrato in vigore il 25 maggio 2016 ed è divenuto pienamente applicabile a partire dal 25 maggio 2018. Il ***Decreto Legislativo 101/2018*** del 10 agosto 2018 ha successivamente armonizzato il quadro legislativo nazionale in modo da renderlo compatibile con i dettami del Regolamento Europeo.

Il nostro impegno

C.E.R.D.O. S.r.l. si impegna a garantire la protezione e la sicurezza dei dati personali da essa trattati, e a perseguire un approccio alla protezione dei dati concreto e coerente. **C.E.R.D.O.** gestisce da sempre la protezione dei dati personali seguendo pratiche rigorose e consolidate, conformi agli obblighi normativi vigenti e rispettose dei principi della privacy. Nondimeno, **C.E.R.D.O.** riconosce la necessità di aggiornare e potenziare, laddove necessario, le proprie pratiche di protezione dei dati per rispondere a tutti gli obblighi posti dal *Regolamento Europeo 2016/679* e dal *D.lgs. 101/2018*.

C.E.R.D.O. è focalizzata sulla salvaguardia dei dati personali sotto sua custodia, e sullo sviluppo di un sistema interno di protezione che sia costantemente efficace e adeguato, tale da dimostrare la piena comprensione e il pieno supporto al nuovo Regolamento. Il modo in cui **C.E.R.D.O.** si è preparata e gli obiettivi che si è posta per assicurare la sua conformità al RGPD sono riassunti nella presente dichiarazione, ed includono lo sviluppo e l'attuazione di ruoli, politiche, procedure, controlli e altre misure tecniche e organizzative – nuove o rinnovate – volte a consentire un livello di conformità al Regolamento che sia il più possibile ampio e continuativo.

Come ci siamo preparati per il RGPD

C.E.R.D.O., in aggiunta agli esistenti livelli di sicurezza e protezione dei dati già applicati alle diverse funzioni aziendali, ha attuato o rafforzato le seguenti misure tecniche e organizzative, con lo scopo di essere pienamente conforme con il RGPD.

Le misure tecniche e organizzative intraprese comprendono:

- ***Audit delle Informazioni*** – Esecuzione periodica di un audit delle informazioni gestite da tutte le funzioni aziendali, al fine di identificare e classificare quali dati personali siano detenuti, la loro origine, il come e il perché vengano trattati, e a quali terze parti siano sati o possano eventualmente essere trasmessi.

- ***Politiche e Procedure*** – Introduzione di apposite politiche e di speciali procedure di protezione dei dati personali, volte a far fronte ai requisiti e alle pratiche imposte dal RGPD e ad ogni altra norma cogente pertinente. Tali politiche e procedure vertono su:
  - ***Protezione dei Dati*** – le nostre Politiche e le nostre procedure sulla protezione dei dati sono state revisionate per rispondere ai requisiti del RGPD. Misure di responsabilizzazione e di *governance* sono state poste in essere per assicurare che gli obblighi e le responsabilità in materia di protezione dei dati personali siano ben comprese, disseminate e poste in evidenza, con una particolare attenzione verso i principi della Privacy by Design e per il rispetto dei Diritti degli Interessati.
  - ***Conservazione e Cancellazione dei Dati*** – le nostre Politiche e le nostre tempistiche sulla cancellazione dei dati sono state opportunamente aggiornate per assicurare il rispetto dei principi di *'minimizzazione dei dati'* and *'limitazione della conservazione'*, e per garantire che i dati personali siano registrati, archiviati e distrutti in maniera legalmente conforme ed eticamente corretta. Abbiamo inoltre posto in atto procedure specifiche per la cancellazione dei dati, così da rispettare gli obblighi dettati dal 'diritto alla cancellazione' (o 'diritto all'oblio').
  - ***Violazione dei dati*** (***Data Breaches***) – Le nostre procedure di gestione e prevenzione delle violazioni dei dati assicurano la presenza di salvaguardie tecnologiche e di altre misure tecnico/organizzative atte ad identificare, esaminare, investigare e denunciare qualsiasi violazione dei dati personali, nel più breve tempo possibile. Tali procedure sono state trasmesse a tutto il personale aziendale pertinente, al fine di creare conoscenza e consapevolezza sui comportamenti da adottare in caso di notizie di violazione.
  - ***Trasferimenti internazionali e Comunicazioni a terze parti*** – nei casi in cui **C.E.R.D.O.** debba conservare o trasferire dati personali al di fuori dell'Unione Europea, lo fa adottando solide procedure e misure di salvaguardia atte a garantire l'integrità e la confidenzialità dei dati. Le nostre procedure includono una revisione periodica dei Paesi destinatari di una '*decisione di adeguatezza*' da parte della Commissione Europea, e di quelle Organizzazioni dotate di '*norme vincolanti di impresa'* approvate dalle rispettive Autorità di Protezione dei Dati. In ogni caso, eseguiamo sempre rigorosi controlli di *due diligence* sui destinatari di un trasferimento di dati personali, così da verificare che questi abbiano posto in essere adeguate salvaguardi per proteggere i dati personali.
  - ***Richieste di Accesso da parte degli Interessati*** – abbiamo rivisto le nostre procedure per la gestione delle richieste di accesso degli Interessati ai dati trattati, così da poter rispettare la finestra temporale di 30 giorni e fornire le informazioni richieste senza addebitare alcun costo. Le nostre nuove procedure definiscono aspetti fondamentali come la verifica dell'identità del richiedente, i passaggi corretti per gestire una richiesta di accesso, quali eccezioni possano sussistere in questo ambito, ecc. Tali procedure assicurano altresì che le comunicazioni verso i soggetti Interessati siano sempre conformi, complete e adeguate.

- ***Basi giuridiche per il trattamento*** – abbiamo riesaminato tutte le nostre attività di trattamento dati per identificare e classificare le basi giuridiche sottese a ogni specifico trattamento, per assicurare che ciascuna base giuridica sia corretta e idonea al trattamento cui si riferisce. Tale base giuridica è inoltre riportata nel nostro Registro dei Trattamenti.
- ***Informative sulla Privacy*** – abbiamo rivisto le nostre Informative sulla Privacy per renderle conformi al RGPD, assicurando che tutti i soggetti Interessati siano correttamente informati sul perché stiamo trattando i loro dati, sul come vengono trattati, su quali siano i loro diritti, verso quali terze parti siano eventualmente trasmessi i loro dati, e quali misure di salvaguardia siano state poste in essere per proteggere i loro dati e i loro diritti.
- ***Ottenimento del consenso al trattamento*** – abbiamo rivisto i meccanismi di acquisizione dei dati e del relativo consenso al loro trattamento, assicurandoci che i soggetti Interessati possano comprendere la natura dei dati forniti, il come e il perché questi saranno impiegati, e le possibilità offerte loro per ritirare tale consenso qualora lo desiderino, così da poter esprimere un consenso esplicito, libero e realmente informato.
- ***Marketing Diretto*** – abbiamo riformulato i testi e i processi impiegati per il marketing diretto, inclusi i meccanismi di '*opt-out*' per renderli ancora più chiari e immediati, così da rendere ancora più semplice per l'utente la disiscrizione dalle nostre mailing list.
- ***Data Protection Impact Assessments (DPIA)*** – nei casi in cui i trattamenti effettuati possano essere considerati ad elevato rischio per i diritti e le libertà dei soggetti Interessati, come nei casi di trattamenti su larga scala che includano forme di monitoraggio dei comportamenti, oppure coinvolgano categorie speciali di dati (dati sanitari, dai biometrici, dati sensibili, ecc.), prima di dare avvio al trattamento dati vero e proprio effettuiamo un esteso ed attento esame dei possibili impatti sulla protezione dei dati e sui diritti degli Interessati, così da poter adottare tutte le salvaguardie necessarie per poter procedere al trattamento in conformità col RGPD.
- ***Rapporti con i Responsabili esterni del trattamento (Data Processor)*** – nei casi in cui **C.E.R.D.O.** fa ricorso a terze parti per l'elaborazione di dati personali per proprio conto (ad es., per le buste paga, per la selezione del personale, per specifiche esigenze di hosting, ecc.), il rapporto con la terza parte viene tassativamente normato attraverso un documento vincolante in cui vengono richiamati gli obblighi e specificate le istruzioni cui deve essere soggetto il Responsabile esterno del trattamento. In via preliminare, inoltre, viene eseguita un'opportuna '*due-diligence*' per assicurare che la terza parte rispetti tutti gli obblighi e gli standard dettati dal RGPD, e soprattutto che sia in possesso di tutti i requisiti etici e di professionalità necessari a per poter ricevere i dati che ci sono stati affidati in custodia.
- ***Categorie speciali di dati*** – nei casi in cui raccogliamo e trattiamo dati appartenenti ad una delle categorie speciali di dati, lo facciamo in piena conformità con i requisiti dettati dall'art. 9 del RGPD, applicando le necessarie misure tecniche e organizzative per assicurare la più elevata protezione di tali dati. Dati appartenenti alle categorie speciali (dati sensibili, dati giudiziari, dati sanitari, dati biometrici, dati genetici) sono elaborati solo se oggettivamente richiesto, per la misura strettamente necessaria, e qualora sussista una base giuridica che giustifichi lo specifico trattamento.

Diritti dei soggetti Interessati

In aggiunta alle Politiche e alle procedure sopra menzionate, ci assicuriamo che ciascun Interessato possa esercitare i propri diritti fornendogli le necessarie informazioni attraverso il canale più rilevante a seconda dei casi (sito web, comunicazioni e-mail, modulistica cartacea), così che l'Interessato possa richiedere ed essere al corrente, al minimo:

- Di quali dati personali deteniamo circa la sua persona;
- Degli scopi di ogni singolo trattamento che possa riguardarlo;
- Delle categorie di dati personali utilizzate nei trattamenti;
- Dei destinatari cui i dati personali sono stati o potrebbero essere trasmessi;
- Per quanto tempo contiamo di conservare i suoi dati personali;
- Se i dati personali sono stati raccolti tramite fonti terze, quali siano queste fonti;
- Del suo diritto a richiedere la correzione dei suoi dati, laddove questi fossero errati o incompleti;
- Del suo diritto a richiedere la cancellazione dei propri dati personali (laddove possibile) o di limitarne il trattamento in accordo alle previsioni del Regolamento, nonché del suo diritto ad opporsi a qualsiasi forma di marketing diretto e di essere informato circa eventuali forme di decisioni automatizzate operate su di lui, impiegando i suoi dati personali.
- Del suo diritto a depositare un ricorso, o a ricercare un provvedimento giudiziario, e di chi contattare in tali eventualità.

Sicurezza delle Informazioni e altre misure tecniche ed organizzative

C.E.R.D.O. pone la massima priorità nei confronti della privacy degli Interessati e della sicurezza delle informazioni gestite; per questo assume qualsiasi precauzione e qualsiasi misura ragionevole per proteggere i dati personali trattati. Abbiamo posto in essere Politiche e procedure molto solide per proteggere i dati personali da accessi non autorizzati, da alterazioni dolose, dalla divulgazione o dalla distruzione accidentale. Tali obiettivi sono conseguiti anche attraverso l'adozione di molteplici misure di sicurezza, fra le quali:

- Cifratura dei dati in transito (*data in-transit*) e dei dati 'a riposo' (*data at-rest*);
- Pseudoanonimizzazione, laddove possibile e preferibile alla cifratura;
- Utilizzo di tecnologie di prevenzione attiva delle violazioni perpetrate da agenti di minaccia esterni (NIPS/HIPS, DLPS, antimalware, anti-rootkit, ecc.);
- Utilizzo di tecnologie di prevenzione attiva delle violazioni perpetrate da agenti di minaccia interni (autenticazione multifattore, meccanismi di accesso RBAC, accessi a scadenza, ecc.);
- Politiche e procedure di assegnazione, verifica periodica, e revoca degli accessi ai dati sulla scorta dei principi della necessità del fare (*need to do*) e del conoscere (*need to know*);
- Processi di gestione (rilevamento e contenimento) degli Incidenti di sicurezza;
- Programmi di formazione e consapevolezza, rivolti a dipendenti e collaboratori;

- Politiche sanzionatorie nei casi di condotte nocive per la protezione dei dati personali.

Per qualsiasi domanda circa la conformità di **C.E.R.D.O.** rispetto agli obblighi del RGPD, si prega di contattare l'ufficio legale all'indirizzo di posta elettronica legale@cerdo.it.