SYSTERM SPA

Data Protection Policy

G.D.P.R 679/2016

Contesto e overview

- Policy preparata da : JONDINI FEDERICA
- Approvata dal management il : MAGGIO 2018
- Policy in vigore dal : 26 MAGGIO 2018
- Revisione numero : 01
- Revisione del : 26 MAGGIO 2018

Introduzione

SYSTERM SPA raccoglie ed utilizza determinate informazioni personali per obblighi legali e per fini lavorativi.
Queste informazioni possono includere anagrafiche clienti, fornitori, impiegati, contatti di business più altri che abbiano una relazione o entrino in contatto con l'azienda.

Suddetta policy dichiara come i dati personali sopra citati siano raccolti, gestititi e conservati al fine di adeguarsi alle politiche di data protection dell'azienda, e come quest'ultime siano conformi alla normativa vigente.

Perché questa policy esiste

La politica di protezione dei dati assicura che l'azienda:

- sia conforme alla legge in materia di protezione dei dati e segua le best practice come linee guida consolidate
- protegga i diritti delle persone coinvolte, dei clienti e dei partners
- sia chiara ed esplicita circa le modalità utilizzate per archiviare e processare le informazioni personali
- protegga sè stessa da un possibile danno, perdita o corruzione dei dati personali (Data Breach).

Data Protection

Il G.D.P.R. 679/2016 descrive come un' organizzazione debba proteggere i dati personali raccolti per fine lavorativi, e come debba garantire la trasparenza della loro gestione nei confronti degli utenti stessi.

Per "dati personali" si intende qualunque informazione relativa ad un individuo, collegata alla sua vita sia privata, che professionale o pubblica. Può riguardare diverse aree : nomi, foto, indirizzi email, dettagli bancari, interventi su siti web di social network, informazioni mediche o indirizzi IP di computer.

Le regole dettate dalla normativa della Comunità Europea si applicano indipendentemente dal fatto che i dati personali vengano archiviati elettronicamente, su archivi fisici o su altra tipologia di materiale.

Per essere conformi alla normative, le informazioni personali devono essere raccolte ed utilizzate con discrezione, archiviate in modo sicuro e non rese disponibili illegalmente.

I principi cardine su cui si fonda il G.D.P.R. 679/2013 indicano che i dati personali devono essere:

1. processati correttamente nel rispetto della legge
2. ottenuti solo per scopi specifici e legali
3. adeguati, utili ed essenziali allo scopo per il quale vengono raccolti
4. accurati e mantenuti costantemente aggiornati
5. archiviati per un periodo di tempo, non superiore a quanto strettamente necessario per i fini civili e fiscali
6. processati nel rispetto dei diritti dei soggetti
7. protetti con misure di sicurezza adeguate.

Tuttavia è consentito traferire i dati personali al di fuori della Comunità Europea se, e solo se, lo Stato destinatario garantisce i medesimi diritti dello Stato di provenienza dell'utente.

Ambito della Policy : Persone, rischi e responsabilità

Suddetta policy viene applicata :

- presso La Sede centrale di SYSTERM SPA
- alle persone in organico presso SYSTERM SPA
- ai terzi, ai fornitori ed alle persone che lavorano per SYSTERM SPA

La policy si applica a tutti i dati che l'azienda archivia relativamente a persone fisiche, anche nel caso in cui l'informazione stessa ricada al di fuori dell'ambito del G.D.P.R 679/2016 (es. anagrafica società).

Suddette informazioni possono includere :

- Nome, Cognome delle persone
- Indirizzo Postale
- Indirizzo Email
- Numero di telefono
- … più ogni altra informazione che consenta l'identificazione di una specifica persona.

Data Protection e Rischi

La Policy aiuta a proteggere SYSTERM SPA da alcuni rischi legati alla sicurezza delle informazioni, quali:

- **Il rischio di violazione della riservatezza.** Ad esempio, la fuoriuscita di informazioni inappropriate.
- **Il rischio di mancata scelta.** Gli utenti hanno il diritto di prestare il consenso al trattamento dei loro dati.
- **Il rischio di danno d'immagine.** Nel caso di accesso non autorizzato ai dati personali l'immagine dell'azienda potrebbe essere compromessa e subire un danno economico.

Responsabilità

Chiunque lavori presso SYSTERM SPA ha la responsabilità di assicurarsi che i dati personali siano raccolti, archiviati e gestiti in modo appropriato, in armonia con i principi in materia di protezione dei dati personali sanciti dalla Unione Europea.

Le seguenti persone o cariche sono coinvolte nel garantire il rispetto della normativa all'interno di SYSTERM SPA:

- L'AMMINISTRATORE DELEGATO che è il Titolare del Trattamento nonché Responsabile del Trattamento che si assicura che SYSTERM SPA rispetti gli obblighi previsti dalla legge.

- La dipendente incaricata, JONDINI FEDERICA deve:

    - assicurarsi che tutti i sistemi, servizi ed equipaggiamenti utilizzati per archiviare i dati rispettino gli standard di sicurezza adottati;
    - eseguire controlli periodici per verificare lo stato di sicurezza dei processi e che il sistema funzioni correttamente;
    - valutare la sicurezza di qualsiasi servizio erogato da terze parti che [nome azienda] possa considerare per archiviare e processare i dati personali.

La figura del "Data Protection Officier" presso [nome azienda] non è applicata in quanto non sussistono le motivazioni indicate nell'articolo 37 par 1 del GDPR – Regolamento Generale sulla Protezione dei Dati (UE/2016/679).

Guida Generale per lo staff

- Le uniche persone che possono accedere ai dati coperti da questa policy sono coloro che ne hanno necessità al fine di adempiere alle proprie mansioni operative.

- I dati personali non devono essere condivisi in modo informale. Quando si accede a dati personali i dipendenti dovrebbero richiedere il permesso al proprio superiore.

- **SYSTERM SPA** si impegna ad istruire i dipendenti al fine di aiutarli a comprendere le responsabilità derivanti dalla gestione dei dati.

- Gli impiegati dovrebbero mantenere i dati in modo sicuro, prendendo le dovute precauzioni e seguendo le linee guida sotto descritte:

    - in particolare dovrebbero **Utilizzare Password Complesse,** imponendone l'obbligo ove tecnicamente possibile;
    - i dati personali non dovrebbero essere resi accessibili a persone non autorizzate, sia interne che esterne all'azienda;
    - i dati personali dovrebbero essere rivisiti ed aggiornati, nel caso fossero ritenuti non più conformi con la situazione realmente esistente. Nel caso di dati non più richiesti o necessari, questi ultimi dovrebbero essere eliminati o archiviati nel rispetto della legge.

- Gli impiegati dovrebbero richiedere aiuto al proprio superiore nel caso di incertezze o dubbi circa le modalità di protezione dei dati.

Archiviazione Dati

Le regole seguenti descrivono come e dove i dati sono archiviati.

Eventuali chiarimenti possono essere richiesti dalla responsabile o al proprio responsabile in organigramma.

I dati cartacei sono archiviati in un luogo sicuro inaccessibile a persone non autorizzate.

I dati cartacei di produzione sono conservati presso la sede SYSTERM SPA in apposita stanza con accesso ristretto.

I dati cartacei per conservazione storica sono custoditi presso la sede SYSTERM SPA sempre in apposita stanza ad accesso limitato.

Le seguenti linee guida si applicano ai dati elettronici che eventualmente possono essere stampati per fini lavorativi ed ai sistemi che li coinvolgono:

- quando il documento non è richiesto o non più necessario, ma è essenziale la sua conservazione, quest'ultimo viene archiviato in armadio/stanza chiusa a chiave. La chiave viene poi rilasciata solo a persone autorizzate.

- I dipendenti sono stati istruiti a non lasciare documenti o stampe incustoditi (es. lasciare eventuali fogli stampati, senza recuperarli, su dispositivi di stampa situati in ambienti comuni)

- I documenti non più necessari sono distrutti in modo sicuro, tramite l'adozione di trita documenti.

- I dati in formato elettronico si trovano in apposite location e sono protetti da cancellazione o distruzione tramite politiche di backup.

- I dati, sia informato cartaceo che elettronico, sono protetti da appositi permessi che consentono l'accesso solo a personale autorizzato.

- Le password utilizzate ove richiesto sono di tipo "forte", cioè rispettano i criteri per aumentare la loro complessità in modo da renderle di difficile individuazione.

- I dati sono depositati su **server e drive dedicati**, e nel caso se ne faccia uso sono uploadati solo su servizi cloud abilitati.

- I server sono localizzati in apposite aree protette da accessi non autorizzati.

- Sono attive delle procedure di backup periodiche per garantire la salvaguardia del dato e gestire situazioni di disaster recovery.

- Se I dati sono salvati su media rimovibilli , questi sono archiviati in un luogo sicuro.

- I dati temporanei necessari al lavoro e salvati localmente su laptop e/o notebook, permangono per il minor tempo possibile.

- I notebook e/o dispostivi mobili che possono contenere dati personali per fini lavorativi sono sottoposti a meccanismi di cifratura.

- Su tutte le postazioni lavorative è attivo un antivirus gestito centralmente, volto ad evitare che un codice malevolo possa corrompere I dati personali.

- Vengono applicati periodicamente aggiornamenti ai sistemi interni volti a risolvere problematiche di sicurezza, o attivare nuove feature se queste valutate positivamente dall'It Manager.

- L'azienda è dotata di firewall perimetrale atto a proteggere e regolamentare le comunicazioni in uscita ed in entrata.

- L'azienda è dotata di un opportuno sistema antispam volto ad impedire la propagazione di mail o malware che possono compromettere le funzioni aziendali.

- L'azienda è dotata di un sistema per il controllo della navigazione dell'utenza atta a proteggere la postazione dell'utente dalle infezione veicolate attraverso siti web che includano codice malevole o appartengano a categorie ad alto rischio.

- I dispositivi mobili rilasciati ad uso aziendale sono gestite centralmente in modo da proteggerli da eventuali manomissioni fraudolenti o furto.

Utilizzo dai dati

I dati personali non hanno valore per SYSTERM SPA a meno che non ricadano nell'ambito del servizio. Tuttavia quando i dati personali sono acceduti ed utilizzati, sussiste sempre una componente di rischio e di possibile furto:

- quando si utilizzano i dati personali, gli impiegati dovrebbero assicurarsi che il computer sia lockato quando la postazione non è presieduta (screensaver o lock della postazione);
- i dati personali non dovrebbero essere condivisi informalmente ma solo attraverso mezzi sicuri (posta cifrata, supporti rimovibili cifrati, protocolli di trasporto cifrati, archivi cifrati).
- i dati personali devono essere cifrati prima di essere condivisi con enti esterni autorizzati ed esistono apposite procedure per lo scambio di informazioni:
    - file zippati con password e password comunicate su canali differente
    - ambienti di condivisione cifrati
- i dati personali non dovrebbero essere trasferiti al di fuori della Comunità Europea
- Gli impiegati non dovrebbero salvare copie di dati personali nel proprio computer, ma accedere esclusivamente a dati gestiti centralmente per garantire la consistenza delle procedure di backup e l'aggiornamento delle informazioni.

Accuratezza del Dato

La legge impone che SYSTERM SPA garantisca l'uso di modalità idonee per mantenere i dati personali accurati e aggiornati.

E' responsabilità di tutti gli impiegati, che per fini lavorativi utilizzano dati personali, che quest'ultimi siano accurati e aggiornati il più possibile.

Al fine di garantire quanto sopra descritto, vengono dettate alcune linee guida:

- I dati sono mantenuti nel minor numero di posti possibili e lo Staff non dovrebbe creare copie, se non strettamente necessarie.
- Lo staff cercherà di sfruttare ogni opportunità di mantenere i dati aggiornati, come ad esempio apprendendo di una variazione di indirizzo anche nel corso una conversazione telefonica.

- SYSTERM SPA permette di modificare i propri dati precedentemente comunicati attraverso varie informative disponibili ad esempio mediante il sito web, appese in bacheca centrale, o depositate presso la reception.

- I dati personali dovrebbero essere aggiornati non appena si venga a conoscenza di una qualche imprecisione.

Diritto di Accesso "Subject Access Requests"

Tutti gli individui che sono soggetti alla gestione dei dati personali presso SYSTERM SPA sono informati su come:

- chiedere quali informazioni l'azienda possiede ed il perché [finalità espressa delle informative];

- accedere alle proprie informazioni e mantenerle aggiornate;

- l'azienda rispetta gli obblighi per la protezione dei dati

se un individuo contatta l'azienda richiedendo queste informazioni, allora il processo è chiamato "subject access request"

Le "Subject access requests" sono emesse da individui via e-mail , indirizzando la richiesta a federica@systerm.it nel caso l'utente non sappia come presentare una richiesta formale può chiede indicazione a: JONDINI FEDERICA che fornirà il modello standard di richiesta.

I dati verranno comunicati entro 14 giorni.

L'incaricato della gestione del dato verificherà sempre l'identità della persona richiedente prima di rilasciare qualsiasi informazione.

Accesso ai dati per ragioni diverse

In alcune circostanze il G.D.P.R 679/2016 permette l'accesso ai dati personali per vincolo di legge e senza l'esplicito permesso dell'utente.

Di conseguenza sotto queste circostanze, SYSTERM SPA concederà l'accesso ai dati richiesti agli enti preposti.

In ogni caso l'incaricato della gestione del dato si assicurerà che l'accesso richiesto sia legittimato, ricercando assistenza da parte del Titolare del Trattamento o attraverso l'ufficio legale dell'azienda.

Fornire informazioni all'utenza

SYSTERM SPA vuole assicurarsi che gli individui siano avvertiti che i loro dati verranno processati e che comprendano come:

- i loro dati vengano utilizzati
- possano esercitare i propri diritti.

A tal fine, l'azienda è in possesso di una informativa sulla privacy, in diversi punti di contatto con l'utenza, che indica come i dati personali dell'utente verranno utilizzati all'interno dell'azienda stessa.

Suddetta informativa è accessibile su richiesta, attraverso il sito web dell'azienda o all'atto di assunzione.