Politica sulla protezione dei dati e delle informazioni (A.5 Security Policy)

INDICE:

1. Scopo – Applicazione

Le politiche qui descritte forniscono le regole per la protezione dei dati personali trattati dall'organizzazione aziendale con il proprio sistema informativo, servono a mantenere e dimostrare la nostra integrità nei rapporti con le parti interessate allo scopo di garantire:

- la confidenzialità dei dati personali e la protezione contro accessi non autorizzati;
- l'integrità dei dati personali da modifiche non autorizzate;
- la disponibilità dei dati personali quando necessari agli utenti autorizzati;
- la piena conformità ai requisiti normativi e legislativi;
- la formazione sulla protezione dei dati personali a tutto il personale interessato;
- i dati personali non sono rivelati a persone od entità non autorizzate a causa di azioni deliberate od accidentali.

RACI S.r.l. intende promuovere questa politica all'interno della propria organizzazione, ovvero in tutte le attività dove sono trattati i dati personali sia in qualità di Titolare sia in qualità di Responsabile per conto di altro Titolare del trattamento:

- si applica al Sistema di Gestione Privacy, ovvero al sistema informativo aziendale che include le infrastrutture, i sistemi informatici e le risorse per l'elaborazione delle informazioni, i processi aziendali con i dati trattati, il personale interno, fornitori, clienti, tutte le parti interessate dal campo di applicazione;
- viene inclusa nella regolamentazione degli accordi con qualsiasi soggetto esterno che tratta dati personali in qualità di Responsabile del trattamento per conto della nostra organizzazione.

2. Aggiornamento e distribuzione

Queste politiche sono soggette a revisione periodica, nell'ambito delle attività di verifica e di aggiornamento del sistema di trattamento dei dati personali e delle relative misure di sicurezza.
Ogni revisione del documento deve essere resa disponibile al personale addetto al trattamento dei dati personali, ovvero a tutte le parti interessate.

3. Riferimenti e definizioni

- Regolamento (Ue) 2016/679 Del Parlamento Europeo E Del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" (regolamento generale sulla protezione dei dati) di seguito abbreviato "Regolamento" o "GDPR";
- D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" con successive modifiche ed integrazioni;
- D.Lgs. 101/2018 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679.";

I termini citati nel documento si riferiscono alle definizioni incluse nel GDPR.

4. Responsabilità

- il Titolare del trattamento dei dati personali ha la responsabilità di approvare, rivedere, pubblicare, promuovere, divulgare questa politica;
- la Direzione aziendale con tutto il personale interessato e le terze parti coinvolte facilita l'attuazione di questa politica attraverso la progettazione e la realizzazione di un sistema gestito per la protezione dei dati personali, composto da politiche e procedure, misure di sicurezza organizzative e tecnologiche, istruzione e formazione;

- il Responsabile della Protezione dei Dati Personali ha la responsabilità di valutare e promuovere questa politica per il rispetto dei requisiti della normativa sulla protezione dei dati personali;
- tutto il personale addetto o incaricato al trattamento dei dati personali è responsabile dell'osservanza e dell'applicazione di questa politica con il sostegno della Direzione;
- tutto il personale, i collaboratori, i clienti, i fornitori, i partner e le terze parti coinvolte hanno la responsabilità di riportare qualunque incidente o minaccia o sospetto di evento negativo per la protezione dei dati personali, ovvero qualunque debolezza o falla identificata nel sistema informativo che possa rappresentare un rischio per i dati;
- qualsiasi atto, deliberato o involontario, di mettere a repentaglio la protezione e la sicurezza dei dati personali trattati dall'organizzazione, sarà soggetto alle appropriate azioni disciplinari e/o legali nei confronti dei responsabili.

5. Politica generale del Sistema di Gestione Privacy

Il Sistema di Gestione Privacy implementato definisce le misure organizzative, tecnologiche e procedurali volte a garantire il rispetto dei requisiti di protezione per i dati personali trattati ed il raggiungimento degli obiettivi individuati.
L'Azienda intende formalizzare il proprio impegno verso questa Politica tenendo conto dell'attività svolta, della dimensione, della natura e del livello dei rischi.
Ci impegniamo a perseguire il miglioramento della protezione e della sicurezza dei dati personali, attraverso i seguenti princìpi:

- Adeguata classificazione e valutazione periodica dei dati personali trattati dall'organizzazione, per identificare in modo continuo e sistematico le minacce incombenti valutandone le esposizioni ai rischi, anche con idonee azioni preventive, allo scopo di adottare le necessarie misure di sicurezza per la protezione da minacce e vulnerabilità;
- Definizione di ruoli e responsabilità del personale addetto al trattamento dei dati personali;
- Svolgimento periodico di controlli e riesami sul sistema di trattamento, a partire dalle attività più critiche, per aggiornare i programmi di sicurezza pianificati per il raggiungimento degli obiettivi;
- Formazione del personale con adeguate istruzioni per le attività di trattamento, aumento della consapevolezza attraverso la diffusione della cultura orientata alla sicurezza delle informazioni ed alla protezione dei dati personali;
- Fornitura e utilizzo di strumenti e mezzi tecnologicamente adeguati, in linea con il progresso e mantenuti in perfetto stato di efficienza;
- Diffusione della cultura della sicurezza e della privacy, attraverso la sensibilizzazione del personale addetto e delle terze parti coinvolte, in merito ai loro ruoli e responsabilità in quest'ambito;
- Definizione di procedure, con azioni e responsabilità, per gestire e contrastare eventuali incidenti con violazioni ai dati personali che dovessero verificarsi, collaborando le Autorità preposte e le terze parti coinvolte per tutelare i soggetti interessati.

Al fine di garantirne la protezione, è necessario che sia disposto un processo formale per l'identificazione, la classificazione e la gestione dei dati personali trattati e di tutti gli asset di supporto che gestiscono tali dati, così da assicurare le misure di sicurezza e protezione le più adeguate al rischio.
I dati personali devono essere classificati in conformità alla normativa vigente e secondo il relativo livello di criticità, che deve essere stabilita nel modo più oggettivo possibile e con l'utilizzo di adeguate metodologie di valutazione del rischio per la definizione delle conseguenti misure di sicurezza.

Le modalità di gestione ed i sistemi di protezione dei dati personali devono essere coerenti con il livello di criticità identificato, per tale motivo deve essere resa disponibile una procedura specifica sulle modalità di gestione dei dati personali.
A seguito del processo di classificazione devono essere condotte attività di analisi e valutazione dei rischi, con l'obiettivo di conoscere le minacce e le vulnerabilità specifiche ai dati personali nei processi aziendali, per acquisire la consapevolezza sul livello di esposizione al rischio del sistema di trattamento e definire le azioni necessarie per gestire i rischi al livello residuo accettabile, attraverso le misure di sicurezza più idonee e coerenti rispetto ai propri obiettivi di privacy.

6. Obiettivi

Con queste politiche si intendono formalizzare i seguenti obiettivi:

- determinare e valorizzare i dati personali trattati nei processi aziendali, individuare le vulnerabilità e le minacce che possono esporli al rischio;
- garantire un adeguato livello di protezione dei dati personali trattati nei processi aziendali, attraverso l'identificazione, la valutazione ed il trattamento dei rischi ai quali sono soggetti allo scopo di proteggerli per garantirne la riservatezza, l'integrità, la disponibilità;
- proteggere il patrimonio dei dati personali trattati dall'organizzazione;
- garantire il rispetto della normativa vigente, ovvero di leggi e regolamenti applicabili alla protezione dei dati personali;
- rispondere adeguatamente alle richieste e condizioni contrattuali dei clienti relative alla protezione dei dati personali;
- garantire il rispetto delle direttive aziendali e contrattuali in regolamenti, procedure ed istruzioni operative, accordi tra le parti;
- sensibilizzare il proprio personale in merito alla protezione di dati personali.

6.1 Politica di sicurezza per il personale

Al fine di garantire la Privacy adeguata, tutto il personale che tratta dati personali deve avere le necessarie competenze e capacità per il ruolo e deve essere consapevole delle responsabilità nel sistema di gestione privacy.
Per tale motivo risulta di fondamentale importanza definire i requisiti di protezione dei dati personali e le attività cui occorre prestare attenzione nell'ambito della gestione del personale:

- nelle fasi di selezione ed ingresso del personale devono essere valutati anche i livelli di conoscenza degli obiettivi e delle problematiche di protezione dei dati personali, in funzione delle attività che dovranno essere svolte;
- durante la permanenza nell'organizzazione il personale deve ricevere un'adeguata e continuativa formazione inerente alla protezione dei dati personali;
- devono essere indicati i princìpi e le regole da seguire in caso di chiusura del rapporto di lavoro o in caso di cambio della mansione da parte del dipendente o collaboratore in linea con la normativa vigente e con le politiche aziendali di sicurezza; tali principi e regole devono riguardare anche gli asset con dati personali che devono essere restituiti in caso di cessazione del rapporto di lavoro;
- tutto il personale deve garantire il rispetto dei requisiti di privacy attraverso la sottoscrizione di una clausola di riservatezza all'atto dell'assunzione o del conferimento dell'incarico.

6.2 Politica di sicurezza per sistemi ed infrastrutture fisiche

Al fine di garantire adeguati livelli di protezione ai dati personali trattati occorre che vengano definite e mantenute opportune soluzioni di sicurezza anche con riferimento agli ambienti all'interno dei quali le stesse vengono trattate e verso le apparecchiature per mezzo delle quali i dati sono trattati.

In accordo a questa politica si dovranno implementare le adeguate misure di sicurezza nei seguenti ambiti di intervento:

- sicurezza perimetrale;
- accessi fisici;
- sicurezza di uffici, stanze ed attrezzature;
- delimitazione delle aree sicure.

Per quanto attiene le apparecchiature, la gestione della privacy deve interessare tutti gli strumenti di trattamento utilizzati, con particolare attenzione allo smaltimento dei supporti di memoria con dati personali in caso di dismissione dello strumento che li contiene.
Al fine di prevenire l'accesso a personale non autorizzato, si devono fornire le adeguate procedure o istruzioni che definiscono:

- l'accesso ai locali in base alla criticità dei dati personali in essi trattati;
- l'accesso per il personale esterno e per i visitatori, con il registro per l'accesso (riferito alla server farm esterna);
- per i soli scopi di sicurezza sul luogo di lavoro, le modalità di tracciamento delle presenze nell'edificio.

6.3 Politica di Data Retention per la conservazione dei dati personali

È necessario stabilire ed applicare i criteri adeguati alla conservazione dei dati personali, al fine di garantire il principio di "minimizzazione dei dati" e l'obbligo di esattezza previsto dal GDPR, che richiede di garantire che non si conservino dati personali che non siano più necessari per le attività di trattamento, ovvero che siano irrilevanti, eccessivi, inesatti o non aggiornati.
Il Titolare del trattamento deve garantire che i dati personali e i documenti con dati personali siano conservati e distrutti in conformità alla normativa e secondo i principi di questa politica di Data Retention; l'organizzazione è tenuta ad implementare misure e procedure idonee all'identificazione di ogni periodo di conservazione, per determinare se i dati personali devono essere cancellati o distrutti.
Si devono effettuare revisioni periodiche dei dati personali archiviati, al fine di determinare se e quali dati vanno conservati o distrutti in conformità a questa politica nel rispetto dei requisiti normativi o legali applicabili.

6.4 Politica di sicurezza nei rapporti con fornitori e responsabili del trattamento

È necessario garantire la sicurezza delle risorse informative fornite ed accedute dai soggetti terzi che agiscono nel ruolo di Responsabile del trattamento per conto dell'organizzazione, ai fini del rispetto della normativa vigente durante l'esecuzione degli specifici obblighi contrattuali e nei limiti dell'autorizzazione assegnata.
Devono essere definite contrattualmente con gli outsourcer le procedure di sicurezza da applicare nonché le normative cogenti, i controlli da attuare per assicurare un adeguato livello di protezione dei dati personali trattati, i livelli di servizio da garantire ai fini della continuità operativa e le responsabilità, anche giuridiche, derivanti in caso di inosservanza.

6.5 Politica per la protezione dei dati personali nel cloud

L'Azienda definisce la propria politica di cloud computing nel ruolo di "cliente dei servizi cloud erogati da terzi".
Pertanto, in funzione delle nostre politiche di Privacy e basandoci sul ruolo di cliente di servizi cloud, il processo di gestione dei rischi ai dati personali trattati nel cloud deve tenere in considerazione i seguenti elementi:

- i dati personali archiviati nell'ambiente di cloud computing possono essere soggetti all'accesso e alla gestione da parte del fornitore del servizio cloud;

- gli asset, ad esempio i software applicativi, vengono mantenuti nell'ambiente cloud;
- chi sono gli utenti del servizio cloud e qual è contesto in cui essi utilizzano il servizio cloud;
- chi sono gli amministratori che hanno accesso privilegiato al servizio cloud di cui si è cliente;
- quali sono le posizioni geografiche del cloud provider e i paesi dove il può memorizzare (anche temporaneamente) i dati del cliente del servizio cloud.

6.6 Politica di sicurezza per la gestione degli accessi logici

Per un corretto accesso ai sistemi informatici al fine di garantire un adeguato livello di Privacy, è necessario che vengano rispettati determinati requisiti da parte di chiunque abbia in carico la gestione degli accessi logici o vi partecipi.
La gestione sicura degli accessi logici si concentra sui requisiti di Privacy che devono essere applicati durante l'intero ciclo di vita delle utenze: creazione; modifica; sospensione; ripristino; revisione; disabilitazione o cessazione.
L'accesso alle risorse informatiche deve sempre essere garantito attraverso un processo di autenticazione che verifichi le credenziali di accesso fornite dall'utente: tale requisito ha valenza anche qualora l'accesso avvenga da parte di un outsourcer e/o di un cliente.
I profili di autorizzazione devono essere individuati e configurati in via preliminare, così da limitare l'accesso ai soli dati necessari per effettuare le attività di trattamento assegnate. Le eccezioni devono essere giustificate, documentate e approvate dal proprio responsabile di riferimento.
L'autorizzazione all'accesso deve essere verificata periodicamente (almeno una volta l'anno) e sospesa qualora non esista più la necessità di accedere a tali dati personali e/o risorse informative o non siano più soddisfatti da parte dell'utente i requisiti di sicurezza necessari.
Si devono adottare opportune procedure che consentano, per le sole necessità di operatività e di sicurezza dell'Azienda, di intervenire e di accedere ai dati anche nei casi di assenza prolungata o impedimento delle persone normalmente incaricate al trattamento.
La gestione dei profili degli utenti e l'accesso ai loro dati, da parte del personale di amministrazione dei sistemi informatici, devono essere fatti nel rispetto della normativa vigente per la protezione dei dati personali.

6.7 Politica di sicurezza per dispositivi mobili

Si devono adottare le procedure adeguate a garantire la protezione delle informazioni registrate sui dispositivi mobili quali notebook, smartphone, tablet oppure trattate attraverso questi dispositivi, allo scopo di garantirne la disponibilità ma soprattutto preservarne la riservatezza, ad esempio ma non solo in caso di errori, guasti, furto, perdita o smarrimento.
Le regole e le procedure devono garantire la protezione fisica dei dispositivi, le limitazioni all'installazione di software non autorizzato, le limitazioni per le connessioni alle reti non autorizzate, i controlli di accesso, la protezione da malware, dove necessario l'utilizzo di tecniche di crittografia per limitare l'accesso ai dati personali memorizzati nei dispositivi mobili.

6.8 Politica di sicurezza per dispositivi personali

Si deve evitare l'utilizzo per attività di lavoro degli strumenti personali privati dei lavoratori addetti al trattamento; nel caso questo si renda necessario, è necessaria l'applicazione dei principi di "Privacy By Design e By Default" con lo scopo di limitare il più possibile i dati personali dei processi aziendali che vengono trattati attraverso il dispositivo personale e le operazioni di trattamento sui dati; inoltre, si deve evitare l'accesso alle informazioni private del lavoratore memorizzate sul proprio strumento.

6.9 Politica di sicurezza per procedure di backup e restore

Devono essere progettate, configurate e pianificate le adeguate procedure di backup per il salvataggio dati, allo scopo di preservare l'integrità e garantire la disponibilità dei dati personali trattati, ad esempio ma non solo in caso di errori, guasti, difetti dei sistemi, manomissioni, atti vandalici, contaminazione da virus, perdita o distruzione anche involontaria.
Il tempo di conservazione dei dati personali sottoposti a backup deve essere coerente con quanto individuato dall'analisi dei rischi, nonché con le previsioni discendenti dalla normativa applicabile, tenuto conto anche della tipologia di dati archiviati e delle modalità usate per il backup.
Devono essere predisposte specifiche procedure per il backup che tengano conto delle modalità di ripristino, si devono prevedere dei regolari test di verifica periodica per il ripristino dei backup.
Il backup si deve applicare ad apparati che gestiscono servizi, laddove applicabile e ritenuto opportuno o necessario a seguito di analisi dei rischi, per sistemi operativi; applicazioni e configurazioni; archivi strutturati, databases, documenti digitali. Per quanto riguarda le singole postazioni di lavoro, gli utenti sono tenuti a non salvare file in locale.

6.10 Politica di gestione delle violazioni ai dati personali

Al fine di preservare i dati personali trattati e garantire il rispetto dei requisiti legali o contrattuali, l'Azienda deve essere in grado di prevenire i potenziali eventi anomali/incidenti che possono tradursi in violazioni dei dati personali trattati e farvi fronte nel momento in cui si manifestano, assicurando le adeguate misure di contenimento e di contrasto.
Per tale scopo è importante definire i requisiti cui attenersi e descrivere le attività cui dare luogo per prevenire potenziali eventi anomali/incidenti e per garantire la loro analisi e risoluzione nel momento in cui dovessero concretizzarsi. Tali attività possono essere suddivise tra:

- attività preventive e proattive: prevenzione ed individuazione di potenziali eventi anomali/incidenti con violazioni ai dati personali;
- attività reattive: attuazione di attività al verificarsi di un evento anomalo/incidente;
- attività investigative: analisi degli eventi registrati per l'identificazione delle responsabilità, per la valutazione dell'impatto e delle conseguenze sugli interessati e per il miglioramento delle attività preventive e reattive;
- attività formative e divulgative: istruzione e sensibilizzazione del personale sui casi standard in cui può prefigurarsi una violazione ai dati personali e sulle modalità più comuni di gestione di tali eventi.

Al personale dell'organizzazione che è incaricato al trattamento dei dati personali e alle figure responsabili in materia di protezione dei dati personali si devono fornire le adeguate istruzioni da seguire in caso di violazione dei dati personali, al fine di minimizzarne gli impatti e le conseguenze per gli interessati e per l'organizzazione del Titolare o del Responsabile.

6.11 Politica di monitoraggio e tracciamento

Scopo delle attività di monitoraggio è quello di rilevare situazioni critiche, accessi non autorizzati e di ottenere indicazioni sull'utilizzo dei sistemi informatici usati per il trattamento dei dati personali, nel rispetto delle regole stabilite o previste dalla normativa applicabile.
Il monitoraggio deve garantire adeguati livelli di confidenzialità e integrità per i dati raccolti e non alterare i livelli di disponibilità dei sistemi controllati; deve essere integrato con un sistema strutturato di parametri ed allarmi per la rilevazione, segnalazione e gestione degli eventi e degli allarmi.
L'attività di tracciamento deve riguardare la registrazione delle informazioni che permettono di identificare e descrivere in modo dettagliato l'evento oggetto del monitoraggio, non deve raccogliere dati ed informazioni eccessivi e non pertinenti all'oggetto del monitoraggio.
Il risultato delle attività di tracciamento deve contenere un set di informazioni coerente con le finalità dell'analisi e si dovrà tener conto di specifici requisiti durante le fasi di conservazione e di archiviazione,

le registrazioni devono essere adeguatamente protette da cancellazioni volontarie o involontarie, per il periodo di tempo prestabilito, nel rispetto delle leggi e delle normative vigenti alle quali sono soggette le attività di tracciamento, soprattutto perché vengono tracciati dati personali e le operazioni di trattamento su tali dati.

6.12 Dismissione dispositivi informatici

La semplice cancellazione dei file o la formattazione dell'hard disk non sempre realizzano una vera cancellazione delle informazioni registrate, che rimangono spesso fisicamente presenti e tecnicamente recuperabili.
Per prevenire l'acquisizione indebita di dati è necessario operare in diversi modi e tempi a seconda delle circostanze:

- immediatamente prima della cessione o dismissione dell'apparato elettronico, con strumenti software di cancellazione sicura (a condizione che l'apparato sia funzionante);
- al momento della cessione o dismissione, con la demagnetizzazione (degaussing), che azzera tutte le aree di memoria elettronica e rende l'apparato inutilizzabile, o con la distruzione fisica del dispositivo di memorizzazione.

Nel caso della cancellazione sicura esistono vari software gratuiti OpenSource che permettono di ottenere il risultato.

Nel caso in cui il dispositivo elettronico da sottoporre a smaltimento non sia più funzionante, e non siano pertanto applicabili le misure software, allo scopo di garantire l'impossibilità di recupero dei dati da parte di terzi estranei occorre procedere con modalità hardware, basate sull'uso di dispositivi di demagnetizzazione (degausser), o con la distruzione fisica.
I degausser permettono l'azzeramento delle aree magnetiche delle superfici dei dischi o di altre memorie a stato solido, agendo anche sui circuiti elettronici che fanno parte del dispositivo e causandone l'inutilizzabilità successiva.
In determinati casi è necessario ricorrere alla distruzione fisica dei dispositivi di memoria. Tale procedura è l'unica praticabile con i supporti ottici a sola lettura (CD-ROM, DVD-R), che possono essere distrutti o polverizzati con appositi macchine analoghe ai "tritacarta" in uso negli uffici. Gli hard-disk possono essere resi inutilizzabili aprendone l'involucro protettivo e danneggiando meccanicamente le superifici magnetiche (piatti) con l'azione deformante di uno strumento o con appositi punzonatori (trapano)

6.13 Riesame delle politiche di Privacy

Le politiche qui descritte devono essere soggette a revisione periodica, con frequenza almeno annuale oppure a seguito di cambiamenti significativi nel Sistema di Gestione Privacy attuato.
Nel riesame si deve verificare la corrispondenza dei processi di trattamento dei dati personali rispetto alle politiche qui descritte e la conformità a leggi, norme e regolamenti vigenti e cogenti, oltre al rispetto di eventuali vincoli contrattuali esistenti. Si deve verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione Privacy, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie ai processi di trattamento al variare delle condizioni del contesto e degli obiettivi aziendali, con lo scopo di garantire ogni adeguamento necessario al suo corretto funzionamento.