Green Media Lab

SISTEMA DI GESTIONE DELLA PRIVACY - MODELLO ORGANIZZATIVO DI PROTEZIONE DEI DATI

(REGOLAMENTO UE 2016/679 D. Lgs.196/2003 smi -
protezione delle persone fisiche con riguardo al trattamento dei dati personali)

Release 1.1.5 del 2021

INDICE

SISTEMA DI GESTIONE DELLA PRIVACY - MODELLO ORGANIZZATIVO DI PROTEZIONE DEI DATI

1. OGGETTO E SCOPO

Il Titolare del trattamento è chiamato a mettere in atto misure tecniche e organizzative adeguate non solo a garantire che il trattamento sia effettuato in conformità alle disposizioni del Regolamento, ma altresì a consentire allo stesso Titolare di dimostrare tale conformità.
Il Sistema di Gestione della Privacy è il modello di gestione, organizzazione e controllo che governa il trattamento in sicurezza dei dati personali ed il rispetto dei principi e delle regole delle normative di riferimento. Per sistema di gestione privacy si intendono la struttura organizzativa, le responsabilità, i documenti, le procedure, i registri, le misure di sicurezza e le risorse messe in atto dall'organizzazione per pianificare, implementare, mantenere e migliorare un sistema di gestione e controllo.

Attraverso l'adozione del Sistema di Gestione, che prevede gli elementi relativi alla organizzazione della sicurezza dei dati e strategie, linee guida generali e disposizioni operative interne volte a disciplinare il trattamento dei dati personali effettuato dall'ente, l'Azienda intende quindi:

- stabilire politiche e processi atti a conseguire obiettivi di protezione e sicurezza dei dati nel rispetto della normativa in materia, per la salvaguardia dei diritti degli interessati;
- garantire l'osservanza dei principi e delle disposizioni del Regolamento UE e della normativa nazionale di adeguamento attraverso la progressiva implementazione di un sistema strutturato ed organico di procedure e di attività di controllo (ex ante ed ex post) volto a prevenire e/o presidiare eventuali rischi privacy;
- governare in tal modo ogni aspetto dei processi legati al trattamento di dati personali in conformità alla disciplina applicabile;
- creare al proprio interno una cultura della prevenzione del rischio privacy e del controllo dei dati personali trattati nell'ambito del raggiungimento degli obiettivi aziendali, anche attraverso l'implementazione di un sistema di monitoraggio costante dell'attività aziendale che sia in grado di prevenire la commissione di illeciti in materia di privacy e/o di scongiurare la eventuale reiterazione di condotte inosservanti della normativa di settore;
- affermare e diffondere una cultura improntata alla legalità, con espressa riprovazione di qualsivoglia comportamento contrario al GDPR, alla normativa nazionale in materia di protezione dei dati personali e al presente Sistema di Gestione della Privacy;
- introdurre un processo di miglioramento continuo per assicurare la *compliance* alla disciplina di settore.

A tal fine, il presente documento, redatto secondo criteri di sostenibilità da parte dei soggetti chiamati ad applicarlo, enuclea i principi comportamentali e indica le misure necessarie per assicurare che i processi aziendali che implichino un trattamento di dati personali siano gestiti in modo tale da intercettare e tempestivamente governare eventuali situazioni di rischio per la *privacy* degli interessati e, in ogni caso, garantire il puntuale e costante rispetto della disciplina europea e nazionale di riferimento.

Allo scopo, nel presente documento vengono riportate, tra le altre, informazioni riguardo a:

- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati
- l'analisi dei rischi cui sono soggetti i dati
- le principali misure utili a garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia e accessibilità, il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento.

Il documento è parte integrante della politica di privacy e di sicurezza delle informazioni di Green Media Lab Srl SB, insieme alle procedure, istruzioni, lettere di incarico e a tutti gli altri documenti aziendali che recano indicazioni in materia di trattamento dei dati personali. Per l'applicazione generale della normativa in materia di protezione dei dati personali l'Azienda può altresì dotarsi di ulteriori disposizioni interne, anche a carattere procedurale o regolamentare, alle quali si rimanda per quanto non esplicitato in questo documento.

Con l'adozione di questo documento s'intende, tra le altre cose, richiamare tutte le risorse operanti all'interno dell'Azienda al rispetto della normativa sulla sicurezza dei dati personali.
Periodicamente, il documento verrà aggiornato in relazione alla evoluzione della disciplina ovvero di modifiche gestionali e/o organizzative che impattino su di esso.

2. RIFERIMENTI NORMATIVI

Per la stesura del presente documento si tiene conto di:

- 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, che abroga la direttiva 95/46/CE (GDPR - Regolamento Generale sulla Protezione dei Dati);
- Codice Privacy: Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" come modificato dal Decreto Legislativo 10 agosto 2018, n. 101;
- Direttive e Linee guida del Parlamento Europeo in materia
- Autorizzazioni generali, provvedimenti, regole deontologiche specifiche e indicazioni diverse del Garante della Privacy vigenti nel tempo, cui si fa espresso richiamo.

Vengono fatti salvi gli ulteriori aggiornamenti e disposizioni normative, regolamentari e determinazioni delle Autorità preposte eventualmente sopravvenute, da intendersi qui parimenti citati.
Le attività di protezione della privacy e di tutela dei dati personali vengono poste in essere nei più generali ambiti della normativa applicabili all'Azienda.

3. DEFINIZIONI

Secondo le previsioni di cui al Regolamento Europeo 2016/679, come recepite in sede nazionale (anche con provvedimenti diversi del Garante della Privacy), si intende:

a) per *dato personale:* qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; sono, quindi, dati personali le informazioni che identificano o rendono identificabile – direttamente o indirettamente – una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc.

   Rilevano, particolarmente:
   - Dati che permettono l'identificazione diretta, quali: dati anagrafici, immagini etc.
   - Dati che permettono l'identificazione indiretta, quali: codice fiscale, indirizzo IP, numero di targa etc.

- Dati rientranti in particolari categorie (dati sensibili), che rivelano l'origine razziale o etnica, le convinzioni religiose o filosofiche, le opinioni politiche, l'appartenenza sindacale, gli orientamenti sessuali etc., nonché:
  dati genetici: il dato personale relativo alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
  dati biometrici: il dato personale ottenuto da un trattamento tecnico specifico e relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
  dati relativi alla salute: il dato personale attinente alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- Dati relativi a condanne penali e reati (dati giudiziari), che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale, o la qualità di imputato o indagato, o l'assoggettamento a correlate misure di sicurezza;
- Dati riferiti alle comunicazioni elettroniche (mail, internet, telefono) o che consentono la geolocalizzazione fornendo informazioni su luoghi frequentati e sugli spostamenti.

b) per *trattamento del dato:* qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione,

c) per *Titolare del trattamento dei dati:* persona fisica o giuridica, autorità pubblica, ente pubblico o privato etc. che adotta le decisioni sugli scopi e sulle modalità del trattamento

d) per *Responsabile del trattamento dei dati:* persona fisica o giuridica alla quale il titolare chieda di eseguire per suo conto specifici e definiti compiti di gestione e controllo del trattamento dei dati. È possibile anche che il medesimo, secondo determinate condizioni, designi un sub-titolare

e) per *Incaricato del trattamento dei dati:* soggetto individuato per la gestione operativa delle attività di trattamento

f) per *Amministratore di sistema:* soggetto individuato dal Titolare del Trattamento per la gestione e la manutenzione di un impianto di elaborazione o di sue componenti, o figura equiparabile dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi

g) per *Responsabile della Protezione dei Dati:* un soggetto in possesso di adeguata professionalità che svolge le attività di competenza specifica previste dal DGPR

h) per *Interessato:* la persona fisica alla quale si riferiscono i dati personali

4. PRINCIPI E LICEITA' DEL TRATTAMENTO

Principi generali del trattamento di dati personali

Ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati all'articolo 5 del Regolamento (UE) 2016/679:

- liceità, correttezza e trasparenza del trattamento nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: ossia, i dati devono essere adeguati, pertinenti, non eccedenti, indispensabili e limitati a quanto necessario rispetto alle finalità del trattamento perseguite nei singoli casi;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Liceità del trattamento di dati personali

Ogni trattamento deve trovare fondamento in un'idonea base giuridica. I fondamenti di liceità del trattamento di dati personali sono:

- consenso,
- adempimento obblighi contrattuali,
- interessi vitali della persona interessata o di terzi,
- obblighi di legge cui è soggetto il titolare,
- interesse pubblico o esercizio di pubblici poteri,
- interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Il trattamento di **"categorie particolari di dati personali"** (dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, ved. art.3, lett. a, terzo punto), è vietato a meno che il Titolare dei Trattamenti dell'Azienda possa dimostrare di soddisfare almeno una delle seguenti condizioni:

- l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
- il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- il trattamento è necessario per uno dei seguenti scopi:
  - per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del Trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
  - per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
  - per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
  - per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri;
  - per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali;

- per motivi di interesse pubblico nel settore della sanità pubblica (se tali dati sono trattati sotto la responsabilità di un professionista soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza);
- per il perseguimento di fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

I dati trattati sono essenziali per lo svolgimento delle attività istituzionali, quando le finalità di interesse pubblico non possono essere adempiute mediante il trattamento di dati anonimi o di dati personali di natura diversa.

Questi dati non possono essere diffusi.

(Per alcune di tali finalità sono previste limitazioni o prescrizioni ulteriori, anche nel diritto nazionale).

Consenso

Quando il trattamento si fonda sul consenso dell'interessato, il Titolare deve sempre essere in grado di dimostrare che l'interessato ha prestato il proprio consenso, che è valido se:

- all'interessato è stata resa l'informazione sul trattamento dei dati personali;
- è stato espresso dall'interessato liberamente, in modo inequivocabile e, se il trattamento persegue più finalità, specificamente con riguardo a ciascuna di esse.

La richiesta di consenso deve essere chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato per esempio all'interno di modulistica.
Quando il trattamento riguarda le "categorie particolari di dati personali" il consenso deve essere "esplicito"; lo stesso vale per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione).
Non è comunque ammesso il consenso tacito o presunto (per esempio, presentando caselle già spuntate su un modulo).

Il consenso deve essere sempre revocabile.

Interesse vitale di un terzo

Si può invocare tale base giuridica per il trattamento di dati personali solo se nessuna delle altre condizioni di liceità può trovare applicazione.

Interesse legittimo prevalente di un titolare o di un terzo

Il ricorso a questa base giuridica per il trattamento di dati personali presuppone che il titolare stesso effettui un bilanciamento fra il legittimo interesse suo o del terzo e i diritti e libertà dell'interessato.
L'interesse legittimo del titolare o del terzo deve risultare prevalente sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità.
L'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.
Il legittimo interesse non può essere invocato isolatamente quale base giuridica per il trattamento delle "categorie particolari di dati personali".

Motivi di interesse pubblico rilevante sulla base del diritto italiano (D.lgs. 196/2003 smi)

È rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle materie

individuate all'art. 2-sexies del d.lgs., tra le quali per l'Azienda rilevano o potrebbero rilevare in particolare:

- accesso a documenti amministrativi
- esercizio del mandato degli organi rappresentativi, ivi compresa la sospensione o lo scioglimento, nonché l'accertamento di cause di ineleggibilità, incompatibilità o di
- decadenza, ovvero di rimozione o sospensione da cariche pubbliche
- concessione, liquidazione, modifica, e revoca di benefici, agevolazioni, elargizioni, altri emolumenti e abilitazioni
- accertamento di requisiti di onorabilità e di professionalità per le nomine ad uffici e cariche direttive di persone giuridiche ed imprese
- concessione di patrocini
- adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali
- rapporti con gli enti del terzo settore
- attività di tutela in sede amministrativa o giudiziaria
- rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose
- attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti ed incapaci
- attività amministrative e certificatorie
- compiti di igiene e sicurezza sui luoghi di lavoro
- salvaguardia della vita e dell'incolumità fisica
- istruzione e formazione in ambito professionale
- ricerca scientifica
- instaurazione, gestione, estinzione di qualsiasi rapporto di lavoro, materia sindacale, collocamento, previdenza e assistenza, pari opportunità, obblighi retributivi fiscali o contabili, igiene e sicurezza del lavoro o della popolazione

Trattamento di dati relativi a condanne penali e reati

Al ricorrere di una delle fattispecie seguenti (trattamento in base a consenso dell'interessato, per l'esecuzione di un contratto o di misure precontrattuali su richiesta dell'interessato, in base a obbligo di legge, per la salvaguardia di interessi vitali dell'interessato, per lo svolgimento di un compito di interesse pubblico, per il perseguimento di un legittimo interesse del titolare), è consentito se autorizzato da leggi o regolamenti riguardanti in particolare, per l'Azienda:

- adempimento di obblighi e esercizio di diritti in materia di diritto del lavoro o nell'ambito di rapporti di lavoro
- accertamento e verifica di requisiti di idoneità morale, onorabilità, requisiti soggettivi, presupposti interdittivi
- accertamento di responsabilità per sinistri e eventi attinenti alla vita umana
- accertamento, esercizio, difesa di un diritto in sede giudiziaria
- esercizio del diritto di accesso a dati e documenti amministrativi
- esecuzione di investigazioni, ricerche, raccolta di informazioni
- adempimenti di obblighi in materia di antimafia e altre gravi forme di pericolosità sociale, anche per la produzione di documentazione per partecipare a gare d'appalto

5. CONTESTO AZIENDALE

Green Media Lab Srl SB è un'azienda privata che opera nei campi della comunicazione e consulenza di impresa È dotata di autonomia organizzativa, gestionale, contabile ed opera sul mercato in regime di libera concorrenza.
La mission istituzionale dell'Azienda è fornire servizi di PR, Ufficio Stampa, SMM, consulenza aziendale ambientale e non presso le sue strutture operative.
L'Azienda attiva altresì iniziative di marketing pubblico al fine precipuo di far conoscere i propri servizi e promuovere attività ed eventi connessi agli stessi, gestisce e sviluppa un sistema di relazioni per fidelizzare il rapporto con l'utenza e con i soggetti che abitualmente

interagiscono con l'Azienda, innova ed ottimizza i servizi avvalendosi di strumenti di customer satisfaction, nonché ricorrendo a campagne di crowdfunding con il coinvolgimento di target mirati di riferimento.
L'Azienda si avvale complessivamente di circa 35 tra dipendenti, collaboratori tirocinanti etc.
Per l'assetto organizzativo, l'attribuzione degli incarichi ed il relativo funzionigramma si rimanda alle sezioni di riferimento del sito web aziendale.

6. RESPONSABILITA' CONNESSE AL TRATTAMENTO DEI DATI

"Titolare del trattamento dei dati" è Green Media Lab Srl SB legalmente rappresentata dall'Amministratore Unico.
"Responsabile della protezione dei dati" è un manager di ruolo dell'Azienda in possesso dei requisiti di legge, individuato pro-tempore nella persona di Daniele Denegri, mail privacy@greenmedialab.com.

Si occupa principalmente di:
- sorvegliare l'osservanza del regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
- collaborare con il titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);
- informare e sensibilizzare il titolare o i responsabili del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
- cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;
- supportare il titolare o il responsabile in ogni attività connessa al trattamento
- di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento.

"Responsabili del trattamento dei dati" possono essere:

- soggetti interni:
  i dipendenti delle strutture organizzative aziendali presso cui i dati sono conservati e trattati, in base alle competenze attribuite alla struttura organizzativa medesima cui è collegato il trattamento dei dati pertinenti allo svolgimento delle funzioni istituzionali, nonché a quelle derivanti dall'incarico ricoperto.

- soggetti esterni o terzi all'Azienda (qualora gestori di banche dati originate dal rapporto contrattuale instaurato con l'Azienda) possono essere, tra gli altri:
  - fornitori diversi e altri soggetti, nell'ambito di servizi o prestazioni da questi ultimi eseguiti in favore dell'Azienda

  Si occupano principalmente di:
  - trattare dati personali per conto del titolare del trattamento e su istruzione di questi, mettendo in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato;
  - garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
  - mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alle vigenti normative.

Inoltre, in particolare nel caso di responsabile esterno, su scelta del titolare del trattamento, cancellare o restituirgli tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento.

Rapporti con i Responsabili esterni del Trattamento

La nomina a Responsabile esterno del Trattamento va adeguatamente contrattualizzata, come da apposite indicazioni aziendali vigenti, a cura del Dipartimento competente alla redazione degli accordi con il soggetto terzo. Ai fini dell'efficacia delle stesse, le istruzioni devono essere personalizzate, almeno per tipologia di fornitore/soggetto da incaricare e di attività svolta. La corretta applicazione delle istruzioni e dei requisiti di sicurezza richiesti alle terze parti che si configurano come Responsabili Esterni del Trattamento vanno verificate da parte del dipartimento competente per materia o, nel caso di forniture o servizi esternalizzati da parte del dipendente responsabile dell'esecuzione del contratto.

"Incaricati del trattamento dei dati", sono le persone autorizzate a compiere le operazioni del trattamento operando sotto la diretta autorità del Responsabile del Trattamento ed attenendosi alle istruzioni impartite dallo stesso; ciascun dipendente formalmente assegnato ad una struttura organizzativa o documentatamente preposto allo svolgimento di un'attività che prevede il trattamento dei dati riveste automaticamente la qualifica di *"incaricato del trattamento"* per i dati di competenza - senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni. I rispettivi Responsabili del Trattamento curano la definizione dei compiti degli stessi in base alla organizzazione interna di settore, e forniscono le istruzioni del caso, anche in materia di gestione in sicurezza delle banche dati e degli archivi correnti di riferimento di pertinenza.
In mancanza della documentata preposizione delle persone fisiche alle unità organizzative, il Responsabile interno del trattamento dei dati di assegnazione provvede a formalizzare gli incarichi in tal senso per gli Uffici diretti.

Gli incaricati del trattamento si occupano, tra le altre cose, di:

- trattare i dati secondo le modalità in uso in Azienda;
- trattare i dati in modo lecito e secondo correttezza;
- effettuare le sole mansioni di trattamento necessarie allo svolgimento della propria mansione;
- attenersi alle istruzioni impartite;
- applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali;
- prevenire e/o evitare la comunicazione o diffusione illecita dei dati;
- astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati;
- informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati.

"Amministratore di Sistema", individuato per l'Azienda preposto al Servizio Sistemi Informativi.
Per le attribuzioni del medesimo, si veda oltre, al punto 7-A.

Banche dati ed archivi

L'Azienda implementa le seguenti principali banche dati ed archivi, informatizzati o meno, in taluni casi di carattere trasversale e su cui intervengono e alla cui gestione concorrono - ciascuna per la parte necessaria per lo svolgimento delle attività di rispettiva competenza - diverse strutture operative. Ne sono responsabili, ciascuno per la parte di competenza in relazione ai trattamenti effettuati, i manager ed il personale assegnati alle singole strutture.

- banca dati fornitori/appaltatori/tecnici professionisti
- banca dati clienti
- banca dati personale dipendente
- banca dati personale ad incarico professionale/consulenti/collaboratori; amministratori e incarichi diversi
- banca dati personale appartenente ad altre organizzazioni, ma operante presso l'Azienda
- banca dati partecipanti a corsi o attività formative/docenti
- banca dati elenchi e indirizzari autorità e personalità
- banca dati tirocinanti

I dati afferenti alle sopra citate banche dati ed archivi possono essere conosciuti ed utilizzati anche da strutture aziendali a qualsiasi titolo coinvolte in attività per i quali gli stessi si rendano necessari, nel rispetto dei principi di pertinenza e non eccedenza rispetto alle incombenze di assegnazione.

Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre:

i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative;
ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti;
iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale.
iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso.
v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del lavoro.

7. PRINCIPI DI ANALISI DEL RISCHIO E MISURE DI SICUREZZA

Viene posto in essere un preliminare e periodico processo di *risk assessment* finalizzato alla valutazione del "*rischio privacy*" – ovverossia dell'eventuale impatto negativo sulle libertà e i diritti degli interessati - connesso alle attività di trattamento di dati personali effettuate, condotto mediante analisi dei dati personali trattati e degli strumenti organizzativi, di gestione e di controllo volti a verificare la rispondenza dei principi comportamentali, delle procedure e/o delle prassi organizzative in essere ai principi, regole e finalità dettati dal Regolamento UE e, ove necessario, ad integrare le misure di sicurezza organizzative e tecniche per assicurarne l'adeguatezza, tenuto conto del contesto di riferimento.
Il rischio viene calcolato mediante i parametri di probabilità, impatto e vulnerabilità e l'analisi è centrata su

- rischi derivanti da contenuto intrinseco del trattamento
- rischi derivanti da possibili violazioni di sicurezza in relazione ai possibili controlli applicabili, ricavando, così, un indice di rischio "normalizzato" rispetto al contesto aziendale.

A livello aziendale vengono individuati i seguenti macrofattori di rischio relativi ai dati trattati:

- rischio di danneggiamento, modifica, distruzione o perdita, correlati ad eventi relativi al contesto in cui si opera o relativi agli strumenti

- rischio di accesso non autorizzato, di trattamento non autorizzato, di rivelazione, di modifica, di trattamento non conforme alla finalità della raccolta o illecito, correlato a comportamenti degli operatori

Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati.

In particolare, vengono adottate tra le altre le seguenti principali misure:
- organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative
- fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti
- logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione

A) - TRATTAMENTO EFFETTUATO CON STRUMENTI ELETTRONICI

Le attività condotte in Azienda prevedono l'utilizzo di strumenti elettronici quali elaboratori o personal computer, anche portatili, connessi alla rete aziendale. Grazie alla suddetta interconnessione da ogni postazione di lavoro sono usufruibili (in base ad una opportuna profilazione degli utenti interni) le informazioni presenti sulle banche dati attraverso i software gestionali dedicati alle varie attività.

I server aziendali in cui sono memorizzate le principali basi dati, sono collocati nella sala server principale. Ulteriori server periferici, adibiti principalmente per disaster recovery, sono collocati in località diversa dalla sede aziendale. Su di essi sono predisposti delle quote disco condivise per consentire attività collaborative.

Il sistema è presidiato a livello centralizzato da un Amministratore di Sistema che – anche avvalendosi dei dipendenti facenti capo al Servizio Sistemi Informativi aziendale – ha il compito di sovrintendere alle risorse del sistema informatico in termini di hardware, sistemi operativi, sistemi per la gestione di basi di dati, applicazioni informatiche (cioè software di base e applicativo) e reti e di consentirne l'utilizzazione, come pure di a garantire, in relazione alle conoscenze informatiche acquisite in base al progresso tecnologico, lo sviluppo delle misure di sicurezza necessarie al fine di:
a) ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati memorizzati su supporti magnetici e ottici gestiti, nonché delle banche dati e dei locali ove esse sono collocate;
b) evitare l'accesso non autorizzato alle banche dati, alla rete e, in generale, ai servizi informatici dell'Azienda;
c) prevenire trattamenti di dati non conformi alla legge od ai regolamenti;
d) evitare la cessione o la distribuzione dei dati in caso di cessazione del trattamento.

Anche a tal fine l'Azienda – in un'ottica informativa e formativa - può mettere a disposizione degli utenti interni, attraverso piattaforme condivise, indicazioni, documenti, procedure operative di carattere generale e/o riguardo a specifici argomenti in materia.

Rischio	Misura	Possibili ulteriori misure
danneggiamento, distruzione o perdita del dato	effettuazione di copie di sicurezza, salvataggio settimanale dei dati, backup centralizzato periodico, aggiornamento dei programmi di protezione per elaboratore ed effettuazione di backup full dei database dei gestionali	sistematizzare l'emanazione di indicazioni atte a responsabilizzare gli utenti interni sui rischi connessi all'utilizzo degli strumenti elettronici (ad esempio, rischi derivanti dalla tenuta ed archiviazione di dati sui rispettivi hard disk) e sui comportamenti, accorgimenti e misure da adottare per limitare/abolire danni correlati
accesso non autorizzato (ai locali, al sistema ed ai dati)	- i server aziendali sono collocati in locali chiusi - le copie di sicurezza vengono custoditi in luogo non accessibile a persone diverse dalle autorizzate - assegnazione di credenziali di accesso alla rete differenziate per servizio/gestionale e di password personalizzate - utilizzo di salvaschermo protetti da password in caso di inattività - tutti i PC fissi e mobili e gli elaboratori sono coperti da sistemi di rilevamento e di prevenzione delle intrusioni e anti-hackers, firewall di sistema, antivirus, antispyware la cui efficacia è periodicamente verificata ed aggiornata - attivazione di switch e access point di rete in cui sono state configurate VLAN	- sistema di tracciabilità degli eventuali accessi di personale non autorizzato - utilizzo di codici identificativi personali che non consentano l'accesso contemporaneo alla stessa applicazione da diverse stazioni di lavoro - definizione di istruzioni per l'uso, la custodia e la distruzione dei supporti rimovibili o del contenuto degli stessi, al fine di evitare accessi non autorizzati e trattamenti impropri - apposizione di clausole di sicurezza ai contratti di manutenzione software – ove non già esistenti - impostazione del controllo degli accessi sugli apparati di rete - totale sostituzione di apparati privi di management
trattamento non autorizzato	- ogni incaricato del trattamento è munito di credenziali di autenticazione e/o parola chiave; è operativa la procedura che ne consente l'autonoma sostituzione periodica da parte del singolo operatore - di norma il codice identificativo personale fornito ad ogni operatore non viene assegnato a persone diverse; - i supporti rimovibili e le copie di sicurezza vengono custoditi in luogo non accessibile a persona diversa dall'incaricato del trattamento - i dati non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative - implementazione di regole centralizzate finalizzate ad aumentare la robustezza delle password	- disattivazione dei codici personali nel caso in cui vi sia perdita della qualità che permette l'accesso all'operatore o di mancato utilizzo superiore ai sei mesi
trattamento non conforme alla finalità della raccolta o illecito	- è previsto da parte dei soggetti responsabili del trattamento l'aggiornamento periodico delle banche dati aziendali di rispettiva competenza, in particolare per quanto riguarda i dati sensibili e giudiziari, secondo i principi di pertinenza, non eccedenza, indispensabilità rispetto alle finalità perseguite nei singoli casi - a tal fine, dati non più occorrenti vengono di norma cancellati o distrutti (anche facendone richiesta all'Amministratore di Sistema, ove il soggetto responsabile non fosse in possesso delle necessarie abilitazioni); qualora fossero conservati, non sono comunque utilizzabili.	- adozione di tecniche di cifratura o codici identificativi o di altre soluzioni che rendano temporaneamente inintelligibili i dati anche a chi è autorizzato ad accedervi, e permettano di identificare gli interessati solo in caso di necessità - trasferimento cifrato dei dati sensibili e giudiziari in formato elettronico (già attivo per VPN) - conservazione separata dei dati idonei a rivelare lo stato di salute e la vita sessuale rispetto ad altri dati personali oggetto di trattamento

Il Titolare del trattamento dei dati, per il tramite il responsabile del Servizio Sistemi Informativi aziendale e con il supporto dell'Amministratore di Sistema provvede a testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative di cui sopra, anche mediante l'adozione di apposite procedure, nonché a controllarne a campione il rispetto da parte degli utenti interni.

B) - TRATTAMENTO EFFETTUATO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Tale trattamento prevede che i dati siano conservati in archivi cartacei o su supporti di tipo magnetico e/o ottico.

Rischio	Misura
accesso non autorizzato	- la conservazione dei documenti contenenti dati personali e/o sensibili avviene in archivi ad accesso selezionato e controllato; i locali in cui sono conservati tali documenti devono essere chiusi al termine dell'orario di lavoro - i documenti contenenti dati sensibili, se affidati all'incaricato del trattamento, devono da questo essere conservati in modo tale da non garantire a terzi la consultabilità degli stessi fino alla restituzione all'archivio d'ufficio - l'accesso agli archivi non è consentito dopo l'orario di chiusura degli stessi, coincidente con l'orario di chiusura degli uffici o con l'effettivo termine delle attività lavorative. Peraltro, qualora si renda necessario consentire l'accesso agli archivi dopo l'orario di chiusura degli stessi, occorre prevedere procedure di controllo e di identificazione e registrazione dei soggetti ammessi, fatte salve preventive autorizzazioni - i documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro - fare attendere soggetti estranei in luoghi in cui non siano presenti informazioni riservate o dati personali; se per ragioni di lavoro gli stessi possono accedere agli uffici, avere cura di riporre eventuali documenti e se necessario di attivare il salvaschermo dei p.c. - evitare l'esportazione di dati personali e/o l'installazione degli stessi su attrezzature diverse da quelle messe a disposizione dall'Azienda (ad es. computer di casa)
trattamento non autorizzato	- gli incaricati al trattamento sono autorizzati al trattamento dei soli dati la cui conoscenza sia strettamente necessaria per lo svolgimento dell'incarico affidato o per l'espletamento delle competenze attribuite alla struttura organizzativa di riferimento - divieto di richiedere, raccogliere e/o conservare in fascicolo dati personali non pertinenti con le competenze e le attività svolte o eccedenti le necessità istruttorie delle attività assegnate - i dati non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative - il trasporto di dati personali all'esterno dei locali ove si svolge il trattamento, ma comunque all'interno dell'Azienda avviene in modo da garantirne la riservatezza
trattamento non conforme alla finalità della raccolta o illecito	- i dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo - è previsto da parte dei soggetti responsabili del trattamento l'aggiornamento periodico delle banche dati aziendali di rispettiva competenza, in particolare per quanto riguarda i dati sensibili e giudiziari, secondo i principi di pertinenza, non eccedenza, indispensabilità rispetto alle finalità perseguite nei singoli casi - a tal fine, i documenti riportanti dati non più occorrenti - se non protocollati e/o allegati in fascicolo - vengono di norma distrutti (con modalità che ne garantiscano la non intelligibilità) e qualora fossero conservati, non sono comunque utilizzabili. - i supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di un eventuale riutilizzo; se ciò non è possibile devono essere distrutti

8. DOCUMENTI DI PRIVACY COMPLIANCE

Oltre al presente Modello Organizzativo – Sistema di Gestione, l'Azienda adotta ed implementa, in via non esaustiva, i documenti sotto indicati:

- Registro dei Trattamenti del titolare (RAT)
  tale documento indica le singole ATTIVITA' DI TRATTAMENTO, specificando per ciascuna:

  - Responsabilità sul trattamento dei dati
  - Base giuridica del trattamento
  - Principali fonti normative e legislative
  - Finalità del trattamento
  - Categorie di interessati
  - Tipologia dei dati trattati
  - Modalità di trattamento dei dati
  - Tipologia delle operazioni eseguite
  - Descrizione del trattamento e del flusso informativo
  - Termini di cancellazione
  - Descrizione generale delle misure di sicurezza tecniche e organizzative
  - Categorie di destinatari per la comunicazione

- Registro dei Trattamenti dei Responsabili interni
  Tali documenti evidenziano, per ciascun responsabile:
  - le attività di trattamento effettuate
    e, per ogni attività:
    - finalità dei singoli trattamenti
    - categorie dei trattamenti svolti
    - descrizione generale delle misure di sicurezza adottate

I Registri dei Trattamenti vengono di norma revisionati almeno annualmente, e comunque in occasione di rilevanti variazioni dei trattamenti dei dati personali, e/o di variazioni dell'organizzazione interna, e/o delle norme vigenti in tema di protezione dei dati personali.

- Nomine dei Responsabili del trattamento
- Nomine degli incaricati del trattamento dei dati
- Eventuale valutazioni di impatto
- Registro delle violazioni (affidato per competenza alla struttura organizzativa deputata alla progettazione, attivazione e manutenzione del sistema di protezione dei dati, da implementare al bisogno)
- Informative sul trattamento, redatte secondo le indicazioni normative in materia.

Quanto sopra è integrato da documentazione di supporto relativa a specifiche attività di trattamento (es relazioni tecniche, valutazioni preliminari, autorizzazioni ecc.).

9. INFORMAZIONE/FORMAZIONE DEGLI INCARICATI AL TRATTAMENTO

Gli incaricati al trattamento dei dati sono destinatari di istruzioni in ordine al trattamento dei dati, alle sue finalità, al controllo ed alla custodia degli atti e dei documenti contenenti dati personali, alla gestione in sicurezza delle banche dati e degli archivi di riferimento.

Vengono, inoltre, in particolare formati sui rischi relativi ai dati e sulle correlate misure di sicurezza, sugli accorgimenti operativi da adottare per la protezione degli stessi, sulle responsabilità derivanti dal processo di trattamento dei dati.
Tale formazione è prevista al momento dell'ingresso in servizio nell'unità operativa di riferimento dell'operatore destinato ad operazioni di trattamento dei dati, e – se del caso - in occasione di cambiamento di mansioni o di introduzione di nuovi strumenti o procedure rilevanti rispetto al trattamento dei dati personali. L'informazione e la formazione del caso sono effettuate e rendicontate direttamente dal Responsabile del Trattamento della struttura organizzativa di assegnazione del dipendente, sulla base in particolare delle procedure operative, delle regole di buona condotta e delle indicazioni vigenti anche come riportate nel presente Sistema di gestione-modello di organizzazione.
Una formazione di carattere più generale riguardo alle norme in materia di tutela dei dati secondo le vigenti previsioni di carattere nazionale e sovranazionale può essere prevista all'interno dei Piani di Formazione aziendale.

10.DIRITTO ALLA PROTEZIONE DEI DATI

Diritti dell'interessato
Ai sensi delle vigenti norme gli interessati possono esercitare, rispetto ai dati, i seguenti principali diritti:

- Diritto di accesso: l'interessato ha il diritto di ottenere dal titolare del trattamento conferma riguardo l'esistenza di trattamenti dei dati personali che lo riguardano, e in caso affermativo, di accedere ai dati personali e alle relative informazioni di trattamento (finalità, categorie di dati trattati, destinatari dei dati, periodo di conservazione, origine dei dati trattati, estremi identificativi di chi tratta i dati, esistenza di processi decisionali automatizzati/profilazione), anche per esercitare gli ulteriori diritti connessi. L'esercizio di tali diritti non deve recare danno ai diritti ed alle libertà altrui, o causare pregiudizi effettivi e concreti allo svolgimento di indagini difensive o all'esercizio di un diritto in sede giudiziaria.
- Diritto di rettifica: l'interessato ha il diritto di ottenere dal titolare del trattamento, senza ingiustificato ritardo, la rettifica dei dati personali inesatti che lo riguardano, tenendo conto delle finalità del trattamento. L'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.
- Diritto di cancellazione/diritto all'oblio: in particolare, gli interessati possano richiedere la cancellazione senza ingiustificato ritardo dei dati personali che li riguardano per i seguenti motivi:
    - perché i dati non sono più necessari per la finalità per i quali erano stati raccolti;
    - perché l'interessato ha revocato il consenso al trattamento dei dati;
    - perché l'interessato si oppone al trattamento;
    - perché i dati sono trattati illecitamente.

Il diritto all'oblio si configura come diritto alla cancellazione in forma rafforzata, essendo previsto l'obbligo da parte del titolare che abbia pubblicato dati personali per i quali venga esercitato il diritto, di informare altri titolari che trattino i medesimi. L'interessato ha diritto di chiedere la cancellazione dei propri dati anche dopo revoca del consenso al trattamento.

Diritto di limitazione del trattamento: in particolare, gli interessati possano richiedere la limitazione del trattamento dei dati personali che li riguardano per i seguenti motivi:

- contestazione da parte dell'interessato dell'esattezza dei dati personali (limitazione per il periodo necessario al titolare del trattamento per verificare l'esattezza dei dati personali);

- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- sebbene il titolare non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- opposizione da parte dell'interessato al trattamento (limitazione in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato).

Se il trattamento è limitato, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

- Diritto alla portabilità dei dati: l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti, quando il trattamento si basa sul consenso dell'interessato o sia necessario per l'esecuzione di un contratto a cui è soggetto l'interessato o per prendere provvedimenti su richiesta dell'interessato prima di stipulare un contratto. L'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento ad un altro, laddove risulti essere tecnicamente possibile. Il diritto alla portabilità dei dati non pregiudica il diritto di cancellazione. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di autorità pubbliche attribuite al titolare del trattamento.
- Diritto di opposizione al trattamento: L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o ai fini statistici, l'interessato ha il diritto di opporsi al trattamento, fatta eccezione se il trattamento è necessario per l'esecuzione di un compito di pubblico interesse.

Il titolare del trattamento comunica le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18 del Regolamento (UE) 2016/679, a ciascuno dei destinatari cui siano stati trasmessi i dati personali in questione tenendo conto della tecnologia disponibile e dei costi attuazione, e salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora lo stesso lo richieda.

Limitazioni e deroghe all'esercizio dei diritti

L'articolo 23 del GDPR consente agli Stati membri di limitare i diritti degli interessati, per diversi motivi, tra cui la sicurezza nazionale e pubblica, per motivi di interesse generale e così via. Tali restrizioni devono rispettare l'essenza dei diritti e delle libertà fondamentali e devono essere a misura necessaria e proporzionata in una società democratica.
Tali limitazioni devono essere previste dalle disposizioni nazionali, quali le limitazioni e deroghe stabilire dal "Codice in materia di protezione dei dati personali", come segue:

art. 2-undecies: i diritti non possono essere esercitati con richiesta al titolare del trattamento, o con reclamo al Garante, qualora dall'esercizio dei medesimi possa derivare un pregiudizio effettivo e concreto:

a. agli interessi tutelati in materia di riciclaggio;
b. agli interessi tutelati in materia di sostegno alle vittime di richieste estorsive;
c. all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
d. alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
e. allo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;
f. alla riservatezza dell'identità del dipendente che segnala l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio
f-bis. agli interessi tutelati in materia tributaria e allo svolgimento delle attività di prevenzione e contrasto all'evasione fiscale.

Tali diritti possono essere esercitati conformemente alle rispettive discipline di settore.

art. 2-duodecies: i diritti e gli obblighi relativi ai trattamenti di dati personali effettuati per ragioni di giustizia nell'ambito di procedimenti avanti le autorità competenti sono disciplinati nei limiti e con le modalità previste dalle disposizioni che regolano tali procedimenti. Le ragioni di giustizia non ricorrono per l'ordinaria attività amministrativo gestionale di personale, mezzi o strutture quando non è pregiudicata la segretezza di atti direttamente connessi alla trattazione giudiziaria di procedimenti.

art. 3-terdecies: i diritti riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.
L'esercizio di uno o più dei diritti non è consentito nei casi previsti dalla legge, o quando l'interessato lo abbia espressamente vietato con dichiarazione scritta, non equivoca, specifica, libera e informata, al titolare del trattamento.
In ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte di terzi dei diritti patrimoniali che derivano dalla morte dell'interessato, nonché del diritto di difesa in giudizio dei propri interessi.

Inoltro delle richieste

L'interessato ad esercitare i diritti di cui sopra può inviare la propria richiesta:
i. scrivendo all'indirizzo di posta elettronica privacy@greenmedialab.com,
ii. scrivendo a Green Media Lab Srl SB – Affari Generali e Trasparenza - all'indirizzo di via Tertulliano 68/70 20137 Milano, tramite posta.

Ai fini della evasione della richiesta occorre specificare i motivi della doglianza e le azioni ritenute necessarie (modifica, cancellazione, etc.) e corredare la stessa con fotocopia del documento di identità del richiedente in corso di validità. Qualora la richiesta provenga da un soggetto terzo rispetto all'interessato, va altresì prodotta delega scritta da parte dell'interessato.
Nell'ipotesi in cui la richiesta fosse ricevuta da altri soggetti aziendali, sarà cura degli stessi comunicare all'interessato il corretto percorso, oppure inoltrare la richiesta in questione alla predetta Affari Generali e Trasparenza, senza per il momento dare altro o diverso seguito all'istanza, anche se afferente a trattamenti di competenza diretta.

Gestione delle richieste

A seguito della ricezione di richiesta da parte dell'interessato, l'ufficio Affari Generali e Trasparenza la prende in carico e procede all'istruttoria relativa alla medesima, provvedendo in primo luogo alla verifica dell'identità del richiedente, della validità dell'istanza e dell'effettiva sussistenza del diritto dell'interessato, anche sulla base dei seguenti parametri:

- esistenza ed effettivo trattamento dei dati che riguardano l'interessato;
- contenuto dei dati che riguardano l'interessato (dati personali comuni, sensibili);
- valutazione dell'ampiezza della richiesta in relazione al diritto esercitato (proporzionalità).

Nei casi in cui la documentazione pervenuta non dovesse risultare adeguata, si richiedono all'interessato gli opportuni chiarimenti e/o l'integrazione della stessa con le informazioni mancanti. In caso di rifiuto da parte del richiedente, o di mancato inoltro di risposta in termini congrui e prefissati, si procede a rigettare la richiesta.
Le richieste da parte dell'interessato devono essere evase per iscritto (anche in caso di diniego) senza ingiustificato ritardo, e comunque entro il termine generale di 30 gg. Dal ricevimento da parte dell'ufficio Affari Generali e Trasparenza. Detto termine si considera sospeso in caso di richiesta di chiarimenti, e riprende a decorrere dalla data in cui l'ufficio viene a conoscenza dei medesimi. Qualora dovessero verificarsi situazioni di particolare complessità, è possibile estendere fino ad un massimo di tre mesi le scadenze per l'evasione della richiesta dandone motivata notizia all'interessato.

Rilascio copie e richiesta contributi

Il titolare del trattamento su richiesta da parte dell'interessato deve fornire una copia dei dati personali oggetto di trattamento. Nel caso di richieste manifestamente infondate o eccessive, o ripetitive, o in cui l'interessato richieda più copie, si prevede un contributo spese ragionevole basato sui costi amministrativi, calcolato anche prendendo a riferimento eventuali tariffari adottati dall'Azienda per fattispecie analoghe.

11. DATA BREACH - VIOLAZIONE DELLA SICUREZZA DEI DATI

Nozione e cause

Per "violazione della sicurezza dei dati personali" si intende ogni evento che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzati ai dati personali trasmessi, conservati o comunque trattati, e può assumere il carattere di:

- Violazione della riservatezza, in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- Violazione della disponibilità, in caso di perdita di accesso o distruzione di dati personali, anche a causa di eventi avversi;
- Violazione dell'integrità, in caso di alterazione non autorizzata o accidentale dei dati personali.

Le cause più comuni che portano ad un data breach si possono categorizzare in:

- Violazione involontaria ed accidentale: ad es. smarrimento di un supporto cartaceo, come un documento, o elettronico come un'unità flash USB, un palmare, un portatile;
- Furto: ad es, dei detti supporti cartacei e/o elettronici;
- Comportamento illecito da parte di dipendenti: ad es. violazione causata da un soggetto interno all'organizzazione, accedendo in maniera autorizzata alle informazioni, ma
- trattandole poi illegittimamente;
- Accesso non autorizzato/Alterazione dei dati: ad es. conduzione di un attacco avente come fine l'accesso senza autorizzazioni ai sistemi informatici, l'acquisizione dei dati personali e/o l'alterazione/divulgazione degli stessi;
- Impossibilità di accedere ai dati: per cause accidentali o per attacchi esterni (virus, malware…)

Segnalazione e gestione dell'evento dannoso

1) Chiunque venga a conoscenza di una effettiva o sospetta violazione della sicurezza dei dati personali, segnala immediatamente l'incidente al Responsabile del Trattamento interessato
2) Il Responsabile del Trattamento:
   - prende in carico la segnalazione - informandone contestualmente il Titolare del Trattamento e il Responsabile della Protezione dei Dati - e conduce una valutazione iniziale dell'incidente per stabilire se si sia verificata una effettiva violazione della sicurezza dei dati personali, quando necessario avvalendosi dell'Amministratore di Sistema e/o di altri soggetti aziendali utili alla migliore definizione della problematica
   - in caso di accertata avvenuta violazione, - si occupa di acquisire, preservare, e documentare le evidenze e le analizza al fine di stabilire quantomeno:
     a) Quali dati personali sono coinvolti nella violazione
     b) La causa della violazione
     c) Come si è verificata la violazione
     d) L'entità della violazione (il numero di persone interessate)
     e) Le persone coinvolte nella violazione della sicurezza
     f) I dettagli delle informazioni, sistemi informatici, apparecchiature o dispositivi coinvolti nella violazione della sicurezza e qualsiasi informazione persa o compromessa a seguito dell'incidente.

L'analisi è finalizzata anche all'individuazione di adeguate misure per arginare o eliminare l'intrusione e alla valutazione della necessità di attivare le procedure di comunicazione e di notifica

- effettua la valutazione dei rischi correlati alla violazione, analizzando le conseguenze potenziali della violazione della sicurezza ed i possibili impatti sotto il profilo del rischio per i diritti e le libertà delle persone fisiche, e le probabilità di accadimento
- evidenzia le azioni intraprese per risolvere la violazione, determina quali possibili ulteriori azioni correttive dovrebbero essere intraprese, sulla base del rapporto dell'incidente, per mitigare i rischi relativi alla violazione ed evitare che essa si ripresenti
- a seguito delle analisi, informa il Titolare del Trattamento e il Responsabile della Protezione dei Dati, trasmettendo tutti i dati e le informazioni opportuni. Il Titolare e l'RPD vanno informati anche nel caso in cui l'istruttoria non evidenzi una violazione dei dati.

Notifica al Garante

Vanno notificate unicamente le violazioni che possono avere effetti avversi significativi causando danni fisici, materiali o immateriali agli interessati e comportando un rischio per i diritti e le libertà delle persone fisiche (ad esempio: la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità, il rischio di frode, la perdita di riservatezza di dati protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione, qualsiasi significativo svantaggio economico o sociale,….).
Il Titolare del Trattamento, valutata la necessità di attivare le procedure di comunicazione e di notifica anche con riferimento a quanto sopra sula base della situazione rappresentata dal Responsabile del Trattamento coinvolto, in caso affermativo notifica la violazione al Garante per la Protezione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. In caso di ritardo nella notifica, oltre il termine delle 72 ore, devono esserne giustificati i motivi.
La notifica deve essere effettuata inoltrando al Garante il Modello in allegato al "Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali" (disponibile sul sito del Garante), compilato in ogni sua parte.
La notifica deve essere inviata al Garante tramite posta elettronica certificata all'indirizzo protocollo@pec.gpdp.it oppure tramite posta elettronica ordinaria all'indirizzo

protocollo@gpdp.it e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa.
In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.

L'oggetto del messaggio deve contenere obbligatoriamente la dicitura "NOTIFICA VIOLAZIONE DATI PERSONALI" e opzionalmente la denominazione del titolare del trattamento.

Comunicazioni

Il Titolare del Trattamento nel caso in cui la violazione comporti un rischio elevato per i diritti e le libertà delle persone fisiche, come sopra, comunica obbligatoriamente la violazione a tutti gli interessati utilizzando i canali più idonei, a meno che siano già state poste in essere misure tali da ridurne l'impatto.

Contenimento e ripristino

Una volta accertato che si è verificata una violazione dei dati, l'Azienda deve intraprendere azioni immediate e appropriate per limitare la violazione.
Allo scopo, il Titolare del trattamento:

a. Valuta le eventuali azioni da intraprendere, proposte dal Responsabile del Trattamento a seguito delle analisi al fine di contenere l'incidente, mitigare i rischi, eradicare le eventuali minacce, e ripristinare la normale operatività
b. Qualora il Responsabile non abbia già provveduto in tal senso, comunica agli attori coinvolti le misure da adottare al fine di contenere la violazione e coordina le attività
c. Emana le raccomandazioni per azioni future e miglioramenti nella protezione dei dati come rilevanti per l'incidente

12. MONITORAGGIO E MIGLIORAMENTO DEL SISTEMA

L'efficacia e l'efficienza del Sistema di Gestione della Privacy sono soggette a verifica periodica (indicativamente annuale, e/o secondo necessità) in modo di assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e di favorire l'attivazione di un processo di aggiornamento continuo. La revisione deve verificare lo stato delle azioni preventive e correttive e l'aderenza alla politica privacy delle procedure in atto così come di quelle previste e non ancora applicate. Deve inoltre tenere conto di tutti i cambiamenti che possono influenzare l'approccio alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali, nonché dei risultati di precedenti riesami.

L'attività di controllo del sistema viene condotta principalmente prendendo in esame, quando presenti:

- I risultati della valutazione dei rischi
- I risultati delle valutazioni d'impatto
- Le registrazioni riferite alla violazione di dati personali
- Le segnalazioni di non conformità
- I reclami degli interessati e le azioni di esercizio dei diritti
- I nuovi pareri, linee-guida ed emanazioni del Garante
- I pareri e le opinioni delle parti interessate all'applicazione del sistema.

Il risultato dell'intero processo di revisione periodica include tutte le decisioni prese e le azioni adottate in merito al miglioramento del Sistema di Gestione della Privacy e se del caso può dare luogo ad un piano di miglioramento, che raccoglie le azioni da intraprendere, la relativa tempistica, l'impiego di risorse, i costi, le responsabilità e le altre valutazioni opportune allo scopo di risolvere eventuali criticità rilevate in fase di monitoraggio, affinché ne siano eliminate le cause e non se ne ripresentino le condizioni.