POLITICA PER LA PROTEZIONE DEI DATI PERSONALI

Data Protection Policy adottata in recepimento del Regolamento (UE) 2016/679, al fine di garantire e tutelare i diritti e le libertà fondamentali delle persone fisiche

TITOLO	Data Protection Policy
DATA DI APPLICAZIONE	10/06/2026
Autore	Data Protection Officer
Verificata da	Area HR Technacy
Approvato da	Amministratore delegato Technacy

STORIA DELLE REVISIONI

Versione	Data	Autore revisione	Natura delle modifiche
1.0	21 maggio 2021	DPO – Studio Paci & C.	Prima emissione
2.0	Giugno 2026	DPO – Avv. Elisa Rosso	Integrazione con procedura di Data Protection di alto livello; estensione di ruoli, responsabilità, definizioni e disposizioni di dettaglio; armonizzazione complessiva del documento.

INDICE

1. INTRODUZIONE

Technacy S.r.l. (di seguito anche “Technacy”, “la Società” o “l’Organizzazione”) pone la massima attenzione alla protezione dei dati personali trattati nell’ambito delle proprie attività. Questo impegno si estende a dipendenti, clienti, potenziali clienti, fornitori, partner commerciali e a qualsiasi altro soggetto che entri in contatto con la Società.

La presente Politica per la protezione dei dati personali (di seguito anche “Policy”) intende fornire un quadro di riferimento comune, coerente e armonizzato per la protezione dei dati personali, adottando standard omogenei di sicurezza e conformità al Regolamento (UE) 2016/679 (“GDPR”), nonché ai principi, alle linee guida e alle best practice in materia di protezione dei dati personali applicabili ai contesti operativi della Società.

In particolare, il presente documento definisce i requisiti, gli obblighi e i comportamenti che devono essere adottati dal Titolare del trattamento, nonché dai ruoli privacy interni – come il Data Protection Officer (DPO), i Responsabili (privacy) interni del trattamento, gli Autorizzati/Incaricati e gli Amministratori di sistema – per assicurare un trattamento lecito, corretto e sicuro dei dati personali ed evitare la comunicazione e/o diffusione non autorizzata degli stessi.

La Policy si applica sia ai trattamenti svolti dalla Società in qualità di “Titolare del trattamento”, sia a quelli svolti in qualità di “Responsabile del trattamento” per conto della propria clientela, e mira a garantire a tutti i soggetti interessati una adeguata protezione attraverso l’adozione di un Sistema di gestione dei dati personali, nel rispetto dei diritti e delle libertà fondamentali delle persone.

2. SCOPO E CAMPO DI APPLICAZIONE

Scopo del presente documento è descrivere la politica dell’Organizzazione, le modalità e le procedure generali per il trattamento, nonché per la sicurezza e la riservatezza dei dati e delle informazioni.

Il presente documento si applica a tutti i trattamenti di dati personali effettuati da Technacy S.r.l., sia direttamente sia per il tramite di fornitori esterni di servizi, nonché alle attività gestite per conto di terzi. La Policy si applica a tutto il personale interno e si condivide con le terze parti che collaborano alla gestione delle informazioni, nonché a tutti i processi e a tutte le risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa dei servizi.

Rientrano nel campo di applicazione:

- tutti i trattamenti svolti in qualità di **Titolare** o di **Responsabile del trattamento**;
- le attività di trattamento effettuate nel contesto di servizi erogati a clienti pubblici e privati;
- i trattamenti operati su supporti digitali, cartacei o misti.

Sono esclusi dal perimetro della presente Policy:

- i trattamenti di dati riferiti a persone giuridiche (ad esempio società con personalità giuridica), compresi il nome, la forma giuridica e i dati di contatto aziendali;
- i trattamenti di dati anonimizzati in modo irreversibile, tali da non consentire (nemmeno indirettamente) l’identificazione di un soggetto interessato.

2.1. Attività della Società

La Policy viene applicata per le attività principali ed accessorie del Titolare del trattamento, descritte nel Registro delle attività del trattamento. L'Azienda si occupa di sviluppo di software, applicazioni ed integrazioni, in particolare nell'ambito dei servizi accessori alle telecomunicazioni.

Le operazioni di gestione, sviluppo software e test sono eseguite, ove tecnicamente possibile, in un ambiente dedicato e separato dal sistema IT utilizzato per il trattamento dei dati personali; nelle attività di test sono di norma utilizzati dati fittizi e non dati reali. Nei casi in cui ciò non sia possibile, sono previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.

3. RIFERIMENTI NORMATIVI E PROCEDURE INTERNE

La presente Policy si fonda sui seguenti riferimenti normativi e documenti interni.

3.1. Riferimenti normativi

- 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 (di seguito anche "GDPR");
- D.Lgs. n. 196 del 30 giugno 2003 – Codice in materia di protezione dei dati personali, e successive modifiche;
- D.Lgs. n. 101 del 10 agosto 2018 – Disposizioni per l'adeguamento della normativa nazionale al GDPR;
- Provvedimento del Garante del 27 novembre 2008 – "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";
- Provvedimenti e Linee guida del Garante in materia di marketing diretto e contrasto allo spam, videosorveglianza, trattamento dei dati dei lavoratori e utilizzo di posta elettronica e internet;
- Linee guida del Gruppo di lavoro ex art. 29 e del Comitato Europeo per la Protezione dei Dati (EDPB) in materia di consenso, portabilità dei dati, DPO, autorità di controllo capofila, DPIA, decisioni automatizzate e profilazione, notifica di data breach;
- L. n. 48 del 18 marzo 2008 – Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica (Budapest, 23 novembre 2001).

3.2. Procedure e documenti interni

La presente Policy è integrata e attuata dai seguenti documenti interni, ai quali si rimanda integralmente per il dettaglio operativo:

- Procedura aziendale di gestione dei diritti degli interessati;
- Procedura (policy) aziendale di Data Retention;
- Procedura aziendale di Data Breach;
- Procedura per la conduzione delle DPIA;
- Contratti / clausole di nomina a Responsabile del trattamento ex art. 28 GDPR;

- Regolamento informatico.

4. TERMINI E DEFINIZIONI

Dato personale comune: qualunque informazione relativa a persona fisica, identificata o identificabile ("interessato"). Il dato personale può riferirsi solo a una persona fisica e comprende anche ditte individuali e liberi professionisti, mentre non comprende i dati delle persone giuridiche. L'indirizzo e-mail aziendale legato a uno specifico individuo (es. nome.cognome@technacy.it) è un dato personale, mentre l'indirizzo e-mail generico (es. info@technacy.it) non è considerato un dato personale. In caso di dubbio sulla qualificazione di una informazione quale dato personale, ciascun dipendente deve chiedere al proprio Responsabile (privacy) interno.

Categorie particolari di dati: dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, 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. Comprendono in particolare i dati relativi alla salute, i dati genetici e i dati biometrici. In caso di trattamento di tali categorie, il GDPR prevede obblighi maggiori e specifici.

Dati giudiziari: dati personali idonei a rivelare provvedimenti definitivi dell'autorità giudiziaria, l'anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o indagato ai sensi degli artt. 60 e 61 c.p.p.

Dati rischiosi: dati il cui trattamento presenta rischi specifici per i diritti e le libertà fondamentali e per la dignità dell'interessato; vi rientrano in particolare i dati di geolocalizzazione e i dati di videosorveglianza.

Interessato: la persona fisica cui si riferiscono i dati personali (es. dipendenti, fornitori, clienti, utenti, visitatori dei siti web, altri soggetti).

Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso al trattamento dei dati personali che lo riguardano. Il consenso deve essere ottenuto unicamente sulla base dei modelli precedentemente approvati dal Responsabile (privacy) interno; in caso di dubbi è necessario consultare il Responsabile competente o il DPO.

Profilazione: qualsiasi trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica (rendimento professionale, situazione economica, salute, preferenze, interessi, affidabilità, comportamento, ubicazione o spostamenti). È considerata attività "a rischio" ai sensi del GDPR.

Pseudonimizzazione: il trattamento dei dati personali svolto in modo tale che essi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive conservate separatamente e soggette a misure tecniche e organizzative adeguate.

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

Responsabile (privacy) interno del trattamento: soggetto formalmente designato che ha il controllo e la responsabilità dei trattamenti svolti nell'area/struttura di competenza, assicurando il rispetto della normativa e garantendo un appropriato accesso ai dati personali e ai sistemi informatici.

Data Protection Officer (DPO): il soggetto nominato dalla Società ai sensi degli artt. 37 e ss. del GDPR, coinvolto in tutte le questioni attinenti al trattamento dei dati personali rispetto ai quali la Società opera come Titolare o Responsabile.

Autorizzati/Incaricati del trattamento: persone fisiche (dipendenti e/o altri terzi) autorizzate a compiere operazioni di trattamento di dati personali di cui la Società sia Titolare.

Amministratore di sistema: figura professionale dedicata alla gestione o alla manutenzione delle infrastrutture di elaborazione o delle loro componenti con cui vengono effettuati trattamenti di dati personali (sistemi di gestione delle basi di dati, software di base complessi, sistemi di posta elettronica e telefonia, reti e sistemi di sicurezza), nella misura in cui consentano di intervenire sui dati personali.

Responsabile del trattamento (esterno): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (es. società di gestione paghe, fornitori di infrastrutture IT).

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato.

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, quali raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, limitazione, cancellazione o distruzione.

Violazione dei dati personali (Data Breach): la violazione di sicurezza che comporta 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.

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal titolare, dal responsabile e dagli incaricati, in qualunque forma.

Autorità di Controllo: per l'Italia, il Garante per la protezione dei dati personali. In generale, l'Autorità nazionale preposta alla verifica del rispetto delle normative in materia di protezione dei dati personali.

Misure di sicurezza adeguate: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali adeguate a proteggere i dati in relazione al livello di rischio associato ai trattamenti.

Registro delle attività di trattamento: documento predisposto dalla Società che mappa i trattamenti di dati personali effettuati per mezzo di strumenti cartacei ed elettronici.

Normativa Privacy: il Codice Privacy, il GDPR e qualsiasi altra normativa sulla protezione dei dati personali applicabile, già in vigore o che entrerà in vigore, ivi compresi i provvedimenti, le linee guida e le opinioni del Garante, dell'EDPB e di ogni altra autorità competente.

5. COMPETENZE E RESPONSABILITÀ

5.1. Titolare del trattamento

Il Titolare ha la responsabilità di:

- nominare e revocare il Responsabile (privacy) interno per il corretto coordinamento dei trattamenti aziendali;
- sottoscrivere gli atti non delegabili;
- vigilare sull'osservanza della normativa privacy e degli adempimenti connessi, delegando a tal fine i Responsabili interni del trattamento;
- dare attuazione agli obblighi in materia di protezione dei dati personali previsti dal GDPR e dal D.Lgs. n. 196/2003 e ss.mm.ii.;
- presidiare le operazioni di trattamento effettuate all'interno della Società al fine di garantirne la conformità alle disposizioni di legge.

5.2. Data Protection Officer (DPO)

La Società ha nominato quale Responsabile della Protezione dei Dati l'**Avv. Elisa Rosso**, contattabile all'indirizzo e-mail dpo@technacy.it.

La nomina del DPO, ai sensi dell'art. 37 del GDPR, è obbligatoria in specifiche ipotesi (trattamento da parte di autorità o organismo pubblico; attività principali che richiedono monitoraggio regolare e sistematico degli interessati su larga scala; trattamento su larga scala di categorie particolari di dati o di dati relativi a condanne penali e reati). In assenza di obbligo specifico, il Regolamento consente la designazione del DPO su base volontaria; in tal caso si applicano le medesime disposizioni degli artt. 37–39 GDPR. Si richiamano le Linee Guida sulla figura del DPO (WP243), confermate dall'EDPB.

Il DPO ha il compito di:

- informare e fornire consulenza al Titolare e ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre disposizioni in materia di protezione dei dati;
- sorvegliare sull'osservanza del GDPR e delle politiche del Titolare in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale;
- predisporre, con la collaborazione dei Responsabili (privacy) interni, le modifiche e i correttivi alla presente Policy e alle altre procedure, per preservarne la coerenza;
- monitorare le attività formative e informative verso le persone autorizzate al trattamento;
- collaborare nella predisposizione e verifica di informative, formule di consenso e nomine a responsabile del trattamento;
- verificare periodicamente la corretta tenuta del registro dei trattamenti, del registro dei data breach e dell'elenco dei responsabili del trattamento;
- collaborare nel rispondere tempestivamente alle richieste di esercizio dei diritti degli interessati;
- fornire la propria raccomandazione nell'ambito delle DPIA di cui all'art. 35 GDPR e sorvegliarne lo svolgimento;

- cooperare con l'Autorità di Controllo e fungere da punto di contatto, anche ai fini della consultazione preventiva ex art. 36 GDPR.

Presso l'ufficio del DPO sono archiviate tutte le comunicazioni all'Autorità di Controllo competente.

5.3. Responsabile (privacy) interno del trattamento

I Responsabili (privacy) interni operano attenendosi alle direttive impartite dal Titolare e hanno il controllo e la responsabilità dei trattamenti svolti nell'area/struttura di competenza. In particolare, hanno la responsabilità di:

- assicurare il rispetto della normativa vigente nella funzione/area di competenza, con particolare riguardo alla sussistenza di una corretta base giuridica per ogni trattamento;
- vigilare sull'attuazione delle misure di sicurezza tecniche e organizzative richieste dalla normativa;
- presidiare l'aggiornamento/censimento delle operazioni di trattamento e l'aggiornamento del Registro dei Trattamenti, segnalando eventuali trasferimenti di dati fuori dallo Spazio Economico Europeo (SEE);
- presidiare, ove necessario, i processi di valutazione d'impatto e di rischio dei trattamenti di competenza;
- garantire la partecipazione degli Incaricati ai piani/corsi di formazione;
- identificare gli eventuali Responsabili (esterni) del trattamento e vigilare sul corretto adempimento dei loro compiti, anche tramite verifiche periodiche e ispezioni;
- informare il Titolare su eventuali violazioni di dati personali e sulle non conformità rilevate;
- coadiuvare l'aggiornamento di informative e consensi, anche nelle relazioni con i fornitori esterni;
- supportare l'attività di riscontro alle istanze degli interessati ex artt. 15–22 GDPR;
- tenere aggiornato il registro dei data breach;
- predisporre, con l'ausilio delle funzioni competenti, le DPIA di cui al successivo paragrafo dedicato;
- collaborare con le funzioni aziendali per garantire l'osservanza dei principi di privacy by design e by default;
- sottoporre al DPO le problematiche più rilevanti in materia di trattamento dei dati personali.

5.4. Autorizzati/Incaricati del trattamento

Sono tutti i dipendenti e collaboratori che, agendo sotto l'autorità del Responsabile (privacy) interno della propria area, trattano dati personali. Hanno la responsabilità di:

- svolgere le attività di trattamento secondo le istruzioni ricevute;
- non modificare i trattamenti esistenti o introdurne di nuovi senza l'esplicita autorizzazione del proprio Responsabile;
- rispettare le norme di sicurezza per la protezione dei dati;
- informare tempestivamente il Responsabile (privacy) interno in caso di violazione dei dati personali di cui vengano a conoscenza o che sospettino;
- partecipare ai corsi di formazione predisposti dalla Società.

All'atto dell'assunzione o della sottoscrizione del contratto di collaborazione, ogni dipendente o collaboratore riceve e accetta espressamente, oltre all'informativa sul trattamento dei propri dati personali, anche la presente Policy. È responsabilità di ogni utente svolgere con regolarità la formazione in tema di privacy resa disponibile dalla Società; la violazione di tale obbligo può dare luogo a provvedimenti disciplinari.

5.5. Amministratori di sistema

Hanno il compito di manutenere e gestire le infrastrutture di elaborazione o le loro componenti tramite cui vengono effettuati trattamenti di dati personali. Per le modalità di nomina e verifica del loro operato si rimanda alla *specifica sezione dedicata "Nomine" di Confluence al seguente indirizzo https://technacy.atlassian.net/wiki/spaces/ADS/overview .*

5.6 Operatori di sistema

Hanno il compito di gestire e supervisionare il corretto funzionamento dei sistemi e degli applicativi loro affidati, operando sotto le istruzioni della Società. Per le modalità di nomina e verifica del loro operato si rimanda alla *specifica sezione dedicata "Nomine" di Confluence al seguente indirizzo https://technacy.atlassian.net/wiki/spaces/ADS/overview .*

5.7. Ruoli organizzativi e formazione

I ruoli definiti all'interno dell'Organizzazione sono: amministrazione, assistenza clienti, commerciale e marketing, direzione, sistemisti, sviluppatori, amministratori di sistema, operatori di sistema.

Ai sensi dell'art. 29 del GDPR e dell'art. 2-quaterdecies del D.Lgs. 196/2003, tutti i soggetti autorizzati al trattamento devono essere debitamente istruiti e formati sui compiti, sulle responsabilità e sulle operazioni di trattamento, nonché impegnati alla riservatezza. La formazione ha le seguenti caratteristiche:

- **Specifica** – corrispondente alla tipologia di mansione/ruolo svolto;
- **Appropriata** – in relazione alla tipologia dei trattamenti realizzati;
- **Permanente** – con programmazione temporale e aggiornamento periodico, in particolare per i nuovi assunti;
- **Documentata** – il suo svolgimento e i successivi aggiornamenti devono risultare da registri, attestati o altre forme che ne diano evidenza;
- **Efficace** – deve essere verificata periodicamente la comprensione e il recepimento delle procedure adottate.

6. DISPOSIZIONI GENERALI PER IL TRATTAMENTO DEI DATI PERSONALI

6.1. Trattamento del dato personale

I dati personali possono essere trattati unicamente per le finalità indicate nell'Informativa Privacy consegnata all'interessato al primo contatto utile e nel rispetto di quanto previsto nelle singole nomine a incaricato/autorizzato. In generale, i dati devono essere trattati:

- in modo lecito, corretto e trasparente;
- raccolti e registrati per finalità determinate, esplicite e legittime, e utilizzati in modo compatibile con tali finalità;

- adeguati, pertinenti e non eccedenti rispetto alle finalità per cui sono raccolti o trattati;
- esatti e, se necessario, aggiornati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario alle finalità;
- trattati in maniera da garantire un'adeguata sicurezza, mediante misure tecniche e organizzative adeguate.

I dati personali non possono essere comunicati a terzi salvo che l'interessato abbia rilasciato espresso consenso ovvero sussista altra base giuridica (ad esempio terzi il cui intervento è necessario per la gestione del contratto, quali consulenti o gestori delle buste paga che trattano i dati in qualità di Responsabili). Per il trasferimento all'estero si rimanda alla sezione dedicata.

6.2. Classificazione dei dati personali

I dati personali sono classificati ai sensi del GDPR nelle seguenti categorie:

1) dati personali comuni;
2) categorie particolari di dati personali (art. 9 GDPR);
3) dati relativi a condanne penali e reati o a connesse misure di sicurezza (art. 10 GDPR), il cui trattamento avviene soltanto sotto il controllo dell'autorità pubblica o se autorizzato dal diritto dell'Unione o degli Stati membri;
4) dati rischiosi (di profilazione, geolocalizzazione, videosorveglianza e comportamentali);
5) dati di autenticazione (codici, password o PIN atti a consentire l'accesso fisico o logico a sistemi, applicazioni o locali).

6.3. Principi e regole del trattamento

Ai sensi degli artt. 5 e 24 del GDPR, nel trattamento dei dati personali devono essere rispettati i seguenti principi: liceità, correttezza e trasparenza; limitazione delle finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza. Tali principi e garanzie sono applicati e verificati anche a cascata nei confronti degli eventuali subfornitori (sub-responsabili).

Liceità, trasparenza e correttezza

Un trattamento è lecito solo se ricorre almeno una delle seguenti basi giuridiche: consenso dell'interessato; esecuzione di un contratto o di misure precontrattuali; adempimento di un obbligo legale; salvaguardia di interessi vitali; esecuzione di un compito di interesse pubblico; legittimo interesse del titolare o di terzi, a condizione che non prevalgano i diritti e le libertà dell'interessato. Il consenso è quindi solo una delle basi giuridiche e non l'unica. Per finalità diverse da quelle del contratto cui l'informativa si riferisce (es. marketing) è necessario un consenso espresso e separato, documentato e tracciato.

Limitazione delle finalità

I dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. L'introduzione di una nuova finalità richiede la condivisione tempestiva con gli interessati della documentazione aggiornata (informativa ed eventuale consenso).

Minimizzazione dei dati

I dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità. Quando non sia possibile utilizzare dati anonimi o aggregati, l'impiego di dati personali deve essere il più limitato possibile.

Esattezza

I dati devono essere esatti e, se necessario, aggiornati; devono essere previste procedure per la cancellazione o la rettifica tempestiva dei dati inesatti.

Limitazione della conservazione

I dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità.

Integrità e riservatezza

I dati personali devono essere trattati in modo da garantirne integrità e riservatezza, impedendo l'accesso o l'utilizzo non autorizzato.

6.4. Informativa Privacy

L'interessato deve ricevere un'adeguata Informativa Privacy. Quando i dati sono raccolti direttamente presso l'interessato, l'informativa è resa ai sensi dell'art. 13 del GDPR al momento della raccolta. Quando i dati sono ottenuti tramite terzi, l'informativa è resa ai sensi dell'art. 14: entro un termine ragionevole e comunque non oltre un mese; al più tardi al primo contatto utile, in caso di comunicazione con l'interessato; non oltre la prima comunicazione, in caso di comunicazione ad altro destinatario.

L'aggiornamento delle informative è a carico del Responsabile (privacy) interno competente, che si consulta con il DPO. Non è possibile apportare modifiche alle informative adottate senza la previa approvazione scritta del Responsabile (privacy) interno e/o del DPO.

6.4.1. Informativa diretta (art. 13 GDPR)

In caso di raccolta presso l'interessato, l'informativa contiene, tra l'altro: identità e dati di contatto del titolare; dati di contatto del DPO; finalità e base giuridica del trattamento; eventuali legittimi interessi; eventuali destinatari; eventuale intenzione di trasferire i dati verso paesi terzi e relative garanzie; periodo di conservazione; diritti dell'interessato; diritto di revoca del consenso; diritto di reclamo all'Autorità di Controllo; natura obbligatoria o facoltativa del conferimento; esistenza di un processo decisionale automatizzato.

6.4.2. Informativa successiva (art. 14 GDPR)

Qualora i dati non siano raccolti presso l'interessato, l'informativa, resa entro un termine ragionevole non superiore al mese, contiene, in aggiunta a quanto previsto dall'art. 13, le categorie di dati raccolte e l'indicazione delle fonti. Non è dovuta qualora l'interessato disponga già dell'informazione, la registrazione sia prevista per legge, o informare l'interessato si riveli impossibile o richieda uno sforzo sproporzionato.

6.4.3. Informativa ulteriore (nuove finalità)

Quando vengono introdotte nuove finalità, è fornita all'interessato un'apposita informativa ulteriore, prima dell'inizio del trattamento per la nuova finalità. Contestualmente i Responsabili (privacy) interni provvedono all'aggiornamento del registro dei trattamenti.

6.5. Trattamento dei dati personali della Società

I trattamenti riguardano principalmente dati relativi a dipendenti, clienti, fornitori, interessati dagli impianti di videosorveglianza e visitatori dei siti web.

6.5.1. Dipendenti

I dati personali dei lavoratori, sia nella fase precedente all'instaurazione del rapporto sia durante lo svolgimento dello stesso, sono raccolti presso ogni lavoratore e, solo ove necessario, presso terzi, per finalità connesse al reclutamento, alla costituzione e alla gestione del rapporto di lavoro. La Società tratta tali dati, anche senza consenso, quando ciò sia necessario per adempiere obblighi di contratto, di legge o di contrattazione collettiva, nonché per la difesa di un diritto in sede giudiziaria e per la salvaguardia della salute del lavoratore. Negli altri casi è acquisito il consenso espresso.

6.5.2. Accesso ai dati in assenza dell'Incaricato (utenze di emergenza)

In caso di necessità di accedere a dati e/o strumenti elettronici in dotazione a un dipendente assente (es. cessazione del rapporto, malattia, decesso), il responsabile gerarchico diretto, verificata l'assenza di alternative, richiede per iscritto al Responsabile (privacy) interno l'accesso ai dati. Il Responsabile (privacy) interno, verificata la richiesta, fornisce indicazioni e ne dà comunicazione al Responsabile Sistemi Informativi. Al termine delle operazioni il richiedente ne dà comunicazione scritta e, ove possibile, ne informa l'incaricato assente.

6.5.3. Clienti

I clienti sono resi edotti, tramite specifiche informative, del trattamento dei propri dati personali, sia per finalità commerciali sia per finalità contrattuali.

6.5.4. Fornitori nominati Responsabili ex art. 28 GDPR

Per i fornitori nominati Responsabili del trattamento, la Società utilizza i dati esclusivamente per le finalità contrattuali.

6.5.5. Visitatori dei siti web

I visitatori dei siti web sono resi edotti, tramite apposita informativa ed eventuale cookie policy consultabili sui siti istituzionali, circa i dati registrati in sede di connessione, navigazione, registrazione e/o compilazione di moduli.

6.5.6. Videosorveglianza

Qualora sia installata, tramite specifiche informative, rese sia in forma estesa sia attraverso apposita cartellonistica posta prima del raggio di azione delle telecamere, gli interessati vengono resi edotti delle modalità di trattamento in caso di installazione di impianti di videosorveglianza.

7. DIRITTI DELL'INTERESSATO

La Società mette a disposizione degli interessati un indirizzo postale e un indirizzo e-mail attraverso i quali esercitare i diritti previsti dal Capo III del GDPR (artt. 15–22): accesso, rettifica, cancellazione, limitazione, portabilità, opposizione e diritto di non essere sottoposto a processi decisionali automatizzati, compresa la profilazione.

L'Organizzazione ha adottato una specifica *Procedura per la Gestione dei Diritti degli Interessati*, cui si rimanda per il dettaglio operativo. In sintesi, la procedura disciplina:

- la ricezione delle richieste (via e-mail, modulo web, posta ordinaria);

- la verifica dell'identità del richiedente prima di dare seguito alla richiesta;
- i termini di risposta: 1 mese dal ricevimento, prorogabile di ulteriori 2 mesi (fino a un massimo complessivo di 3 mesi) in caso di particolare complessità o elevato numero di richieste, con obbligo di comunicare la proroga all'interessato entro il primo mese; il riscontro è dovuto anche in caso di diniego;
- la registrazione di ogni richiesta e del relativo esito in apposito registro interno;
- le modalità di coinvolgimento del DPO nei casi di incertezza giuridica o di potenziale conflitto tra i diritti dell'interessato e gli obblighi di legge.

Se un dipendente riceve una richiesta di esercizio dei diritti, ne deve dare immediata comunicazione al proprio Responsabile (privacy) interno.

8. MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE (ART. 32 GDPR)

L'Organizzazione adotta misure tecniche e organizzative adeguate al rischio, ai sensi dell'art. 32 del GDPR, tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

In funzione della valutazione del rischio, la Società adotta o si impegna ad adottare, a titolo esemplificativo e non esaustivo, le seguenti misure:

- cifratura dei dati personali in transito e a riposo, ove tecnicamente applicabile;
- pseudonimizzazione dei dati nei contesti di sviluppo e test;
- controllo degli accessi basato su ruoli (RBAC) e autenticazione a più fattori (MFA) per i sistemi critici;
- procedure di backup regolari con verifica periodica del ripristino;
- piani di Business Continuity e Disaster Recovery testati periodicamente;
- attività periodiche di vulnerability assessment e penetration testing;
- monitoraggio e logging degli accessi ai sistemi di trattamento.

L'adeguatezza delle misure è riesaminata almeno annualmente e in occasione di modifiche significative ai sistemi o ai processi di trattamento. Le misure sono potenziate nei trattamenti che coinvolgono categorie particolari di dati, in conformità al principio di proporzionalità.

9. CONTRATTI: NOMINA DI FORNITORI TERZI A RESPONSABILI DEL TRATTAMENTO (ART. 28 GDPR)

Ogni qualvolta un fornitore o, in generale, un soggetto esterno abbia accesso a dati personali trattati dalla Società, è necessario procedere alla sua nomina quale Responsabile del trattamento ai sensi dell'art. 28 GDPR, previa verifica dell'idoneità del soggetto a trattare dati personali in conformità alla Normativa Privacy applicabile, tramite gli eventuali controlli richiesti dal Responsabile (privacy) interno di concerto con il DPO.

Ove dai controlli risulti che il fornitore non è in grado di prestare garanzie sufficienti dal punto di vista tecnico e/o organizzativo, non sarà possibile sottoscrivere il contratto. In caso positivo, il responsabile della funzione aziendale competente ottiene l'approvazione del Responsabile (privacy) interno alla sottoscrizione della lettera di nomina ex art. 28 GDPR. Conclusa la verifica e

sottoscritta la nomina, il Responsabile (privacy) interno aggiorna l'elenco dei responsabili del trattamento e notifica l'avvenuta nomina al DPO; copia della nomina è conservata a cura della Società.

Tali principi e garanzie sono verificati per ogni fornitore il cui servizio prevede il trattamento di dati personali, anche attraverso audit periodici e il monitoraggio sistematico dello stato di implementazione delle garanzie. Le garanzie sono applicate e verificate a cascata anche nei confronti degli eventuali sub-responsabili.

Si specifica che, qualora sia Technacy a trattare dati personali per conto di un Cliente, è la stessa Società a dover ricevere la nomina a Responsabile del trattamento ex art. 28 GDPR.

10. PRIVACY BY DESIGN E PRIVACY BY DEFAULT (ART. 25 GDPR)

Il Responsabile (privacy) interno monitora il corretto trattamento dei dati personali, la loro esattezza, affidabilità e aggiornamento, sia in fase di acquisizione sia durante il trattamento. Ogni nuova tipologia di trattamento è segnalata al Responsabile (privacy) interno, che valuta il coinvolgimento del DPO e l'eventuale aggiornamento del registro.

Qualora si intenda compiere una nuova attività, sviluppare o aggiornare un prodotto o servizio che comporti il trattamento di dati personali, devono essere rispettati i seguenti principi:

6) Principio di privacy by design: ogni progetto o prodotto deve essere sviluppato tenendo in considerazione le problematiche di protezione dei dati personali sin dalla progettazione, determinando le misure tecniche e organizzative adeguate sulla base della valutazione del rischio;
7) Principio di privacy by default: ogni progetto o prodotto deve garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (qualità dei dati, portata del trattamento, periodo di conservazione e accessibilità), evitando che i dati siano resi accessibili a un numero indefinito di persone senza l'intervento della persona fisica.

A tal fine l'utente si coordina con il proprio Responsabile (privacy) interno, il quale si coordina con il DPO per valutare se eseguire una DPIA e se coinvolgere altre strutture nell'analisi dei rischi e nella definizione del piano d'azione. Al termine del progetto il Responsabile (privacy) interno effettua, anche con il DPO, una valutazione generale di conformità del nuovo prodotto o servizio ai principi del GDPR. Non è possibile realizzare nuovi prodotti, servizi, tool o funzionalità che comportino il trattamento di dati personali senza seguire le presenti indicazioni.

11. TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (ART. 9 GDPR)

L'Organizzazione, nella propria veste di Titolare del trattamento, può trovarsi a trattare categorie particolari di dati: in tal caso, provvede preventivamente a identificare un'idonea base giuridica tra quelle previste dall'art. 9, par. 2 del GDPR (tra cui il consenso esplicito dell'interessato; gli obblighi in materia di diritto del lavoro e sicurezza sociale; le finalità di medicina del lavoro o di assistenza sanitaria; i motivi di interesse pubblico nel settore della sanità pubblica).

Talvolta, in qualità di Responsabile del trattamento per conto di clienti, potrebbe anche trovarsi – seppur sporadicamente – a trattare categorie particolari di dati personali ai sensi dell'art. 9 del GDPR (es. dati sanitari, biometrici, relativi all'origine etnica) in funzione della natura dei servizi erogati. In tali casi:

- il Registro delle Attività di Trattamento riporta esplicitamente la tipologia di dati particolari trattati per ciascun cliente/trattamento;
- i contratti ex art. 28 GDPR con i clienti titolari del trattamento specificano le istruzioni applicabili e le misure di sicurezza rafforzate richieste;
- le misure tecniche e organizzative adottate per tali trattamenti sono potenziate rispetto allo standard, in conformità al principio di proporzionalità;
- viene valutata sistematicamente la necessità di effettuare una DPIA prima dell'avvio o della modifica di trattamenti che coinvolgono categorie particolari di dati.

12. GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH) (ARTT. 33–34 GDPR)

Gli articoli 33 e 34 del GDPR delineano i requisiti del processo di gestione degli incidenti privacy. Tale incidente si configura come una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati, ovvero la loro indisponibilità.

Una violazione, se non affrontata in modo adeguato e tempestivo, può provocare danni fisici, materiali o immateriali alle persone fisiche (perdita di controllo dei dati, discriminazione, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, ecc.).

Il GDPR impone in capo al Titolare l'obbligo di comunicare all'Autorità di Controllo l'avvenuta violazione entro 72 ore (o comunque senza ingiustificato ritardo). Qualora la violazione faccia presumere un elevato rischio per i diritti e le libertà degli interessati, anche questi ultimi devono essere informati senza ritardo. A tal fine l'Organizzazione è dotata di un registro degli incidenti (registro dei data breach).

Chiunque rilevi un caso, anche solo sospetto, di violazione dei dati personali lo segnala nel più breve tempo possibile al proprio Responsabile (privacy) interno e segue quanto descritto nell'apposita *Procedura di Data Breach*, cui si rimanda integralmente.

13. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) (ART. 35 GDPR)

Ai sensi dell'art. 35 del GDPR, il Titolare è tenuto a effettuare una Valutazione d'impatto sulla protezione dei dati (DPIA) quando un tipo di trattamento presenta un rischio elevato per i diritti e le libertà delle persone fisiche. L'obbligo di DPIA sussiste, in particolare, in presenza di almeno due dei fattori di rischio elevato individuati dall'EDPB (Linee Guida WP248 rev. 01):

- valutazione o scoring sistematico, inclusa la profilazione;
- decisioni automatizzate che producono effetti giuridici o incidono significativamente sull'interessato;
- monitoraggio sistematico, anche di aree pubblicamente accessibili;
- trattamento su larga scala di categorie particolari di dati (art. 9) o di dati relativi a condanne penali e reati (art. 10);
- trattamento di dati su larga scala;
- corrispondenza o combinazione di dataset;

- dati relativi a soggetti vulnerabili (in particolare minori);
- uso innovativo o applicazione di nuove tecnologie;
- trattamenti che impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Si rimanda altresì all'elenco dei trattamenti che richiedono la DPIA pubblicato dal Garante ai sensi dell'art. 35, par. 4 del GDPR. L'Organizzazione ha adottato una *Procedura per la conduzione delle DPIA*, cui si rimanda. La DPIA è effettuata preventivamente rispetto all'avvio del trattamento e, ove necessario, con la consultazione del DPO; i risultati sono documentati e conservati agli atti.

Qualora il DPO valuti che il trattamento presenta un rischio elevato in assenza di misure di attenuazione, si procede alla consultazione preventiva dell'Autorità di Controllo ai sensi dell'art. 36 del GDPR.

14. REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO (ART. 30 GDPR)

L'Organizzazione predispone e mantiene aggiornato il Registro delle Attività di Trattamento, sia in qualità di Titolare sia in qualità di Responsabile del trattamento. Sebbene l'art. 30, par. 5 del GDPR preveda un'esenzione formale per le organizzazioni con meno di 250 dipendenti, tale esenzione è nella pratica inapplicabile a Technacy S.r.l., in quanto l'Azienda:

- effettua trattamenti non occasionali nell'ambito dei servizi erogati continuativamente alla propria clientela;
- tratta dati per conto di terzi in qualità di responsabile del trattamento, con trattamenti che possono includere dati di categorie particolari ai sensi dell'art. 9 GDPR;
- opera nel settore delle telecomunicazioni e dello sviluppo software, con trattamenti che per natura e scala rendono il registro obbligatorio.

Il Registro contiene, tra l'altro: nome e dati di contatto del Titolare (ed eventuali contitolare, rappresentante e Responsabile interno); finalità del trattamento; descrizione delle categorie di interessati e di dati personali; categorie di destinatari; eventuali trasferimenti verso paesi terzi e relative garanzie; termini di cancellazione delle diverse categorie di dati; descrizione generale delle misure di sicurezza adottate.

Il Registro è conservato sotto la responsabilità del Responsabile (privacy) interno, che ne cura l'aggiornamento per la propria area. Ogni cambiamento è comunicato al DPO. Il Registro costituisce uno strumento di accountability permanente ed è messo a disposizione dell'Autorità di Controllo su richiesta.

15. TEMPI DI CONSERVAZIONE (ARTT. 5 E 17 GDPR)

I dati personali sono trattati per il tempo strettamente necessario a dare esecuzione alla finalità indicata nell'Informativa Privacy. I termini di conservazione specifici per ciascuna categoria di trattamento, nonché le modalità di cancellazione o anonimizzazione al termine del periodo di retention, sono definiti nella *Procedura di Data Retention*, cui si rimanda integralmente.

La procedura stabilisce altresì i responsabili interni dell'esecuzione delle attività di cancellazione e le modalità di verifica e documentazione delle stesse. È obbligo di tutti gli utenti non utilizzare i dati dopo la scadenza del relativo termine di conservazione e segnalare al proprio Responsabile (privacy) interno l'eventuale scadenza non seguita da cancellazione/anonimizzazione.

16. TRASFERIMENTI DI DATI VERSO PAESI TERZI (ARTT. 44–49 GDPR)

Il Titolare, nell'ambito delle proprie attività, tende a non trasferire dati personali in Paesi extra-UE. Qualora se ne presenti la necessità, sono previamente informati gli interessati e sono adottate adeguate misure di garanzia, che a seconda delle casistiche potranno essere:

- verifica dell'esistenza di una decisione di adeguatezza della Commissione europea per il Paese destinatario (art. 45 GDPR); tra queste si segnala il Data Privacy Framework UE–USA, adottato con Decisione di esecuzione (UE) 2023/1795 del 10 luglio 2023, con verifica della certificazione del destinatario presso il registro ufficiale DPF prima del trasferimento;
- sottoscrizione di clausole contrattuali standard adottate dalla Commissione europea (art. 46, par. 2, lett. c, GDPR);
- adozione di misure supplementari ove necessario, in conformità alla Raccomandazione 01/2020 dell'EDPB e ai successivi aggiornamenti;
- in deroga alle garanzie di cui sopra, per specifici trattamenti (art. 49 GDPR), verifica dell'esistenza di un contratto o di misure precontrattuali a favore dell'interessato, ovvero acquisizione del consenso esplicito al trasferimento.

L'Organizzazione verifica periodicamente l'adeguatezza delle garanzie adottate, anche alla luce delle evoluzioni normative e giurisprudenziali, aggiornando le misure in caso di mutamento del quadro di riferimento.

17. MONITORAGGIO E CONTROLLO

Per ragioni organizzative e produttive e per la tutela del patrimonio aziendale, la Società può avere la necessità di controllare l'utilizzo dei propri sistemi ICT. Tale attività non costituisce monitoraggio del dipendente ed è condotta in conformità alla legge italiana in materia di diritti dei lavoratori e protezione dei dati personali. Come meglio indicato nel *Regolamento informatico*, cui si rimanda integralmente, le ragioni del controllo includono: identificare e prevenire accessi o comunicazioni non autorizzati; assicurare conformità a leggi e regolamenti; prevenire e identificare attività criminali; controllare virus e codice malevolo; assicurare la continuità del business; investigare, in caso di sospetto, usi inappropriati o violazioni; rispondere a reclami; svolgere investigazioni disciplinari o legali.

Il monitoraggio è effettuato nei limiti di quanto permesso o richiesto dalla legge e in quanto necessario e giustificabile. Le informazioni identificate (comprese quelle personali) possono essere utilizzate e conservate per la durata di ogni procedimento e divulgate a terzi quando necessario. L'utilizzo dei sistemi IT non conforme alla presente Policy può dar luogo all'applicazione di sanzioni disciplinari.

18. GESTIONE DELLE RELAZIONI CON LE AUTORITÀ DI CONTROLLO

Il DPO è l'unico punto di contatto per i rapporti con le Autorità di controllo della privacy e coordina il relativo processo di comunicazione. Le singole funzioni della Società collaborano, se necessario, in relazione alle comunicazioni con l'Autorità di controllo italiana ed eventualmente con le autorità di altri Paesi. I rapporti con le Autorità comprendono in particolare: la consultazione preventiva nel caso in cui un trattamento comporti un rischio residuo elevato; la notifica di violazioni dei dati; la rappresentanza della Società in caso di audit condotti dalle Autorità.

19. CONDIZIONI GENERALI PER INFLIGGERE SANZIONI

L'effettiva operatività della presente Policy è garantita da un adeguato Sistema Disciplinare che può sanzionare il mancato rispetto e la violazione delle norme ivi contenute, a prescindere dall'eventuale instaurazione di un giudizio penale.

L'art. 83 del GDPR detta i criteri per infliggere sanzioni amministrative pecuniarie, tenendo conto, tra l'altro, di: natura, gravità e durata della violazione; carattere doloso o colposo; misure adottate per attenuare il danno; grado di responsabilità; eventuali precedenti violazioni; grado di cooperazione con l'Autorità; categorie di dati interessate; modalità con cui l'Autorità è venuta a conoscenza della violazione; adesione a codici di condotta o meccanismi di certificazione.

Le violazioni degli obblighi del Titolare e del Responsabile (artt. 8, 11, 25–39, 42 e 43 GDPR) sono soggette a sanzioni fino a 10.000.000 € o, per le imprese, fino al 2% del fatturato mondiale annuo, se superiore. Le violazioni dei principi di base del trattamento, dei diritti degli interessati e delle regole sui trasferimenti (artt. 5, 6, 7, 9, 12–22 e 44–49 GDPR) sono soggette a sanzioni fino a 20.000.000 € o, per le imprese, fino al 4% del fatturato mondiale annuo, se superiore.

20. RESPONSABILITÀ PER L'ADOZIONE DELLA POLITICA

L'Organizzazione, sia in qualità di Titolare sia di Responsabile del trattamento, è responsabile della politica per la protezione dei dati, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando le azioni da intraprendere a fronte di eventi quali:

- evoluzioni significative del business;
- nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni;
- utilizzo di nuove tecnologie.

21. RIESAME E AGGIORNAMENTO DELLA POLITICA

Periodicamente, almeno una volta all'anno, è svolto un riesame per la verifica dell'efficienza, dell'efficacia e dell'adeguatezza delle misure tecniche e organizzative applicate. Le istruzioni fornite agli addetti designati ai trattamenti costituiscono politica aziendale per il trattamento dei dati e sono revisionate e/o aggiornate almeno una volta all'anno.

In aggiunta al riesame ordinario, è prevista una revisione straordinaria della presente Policy al verificarsi di uno o più dei seguenti eventi: significative modifiche normative o regolamentari; adozione di nuove tecnologie di trattamento; esito critico di una DPIA; violazione dei dati personali di particolare gravità; audit interno o ispezione dell'Autorità di controllo. L'esito del riesame e le eventuali modifiche apportate sono documentati nella Storia delle Revisioni in apertura del presente documento.

22. MODALITÀ DI DIFFUSIONE DELLA POLICY

Technacy S.r.l. provvede alla pubblicazione e diffusione della presente Policy al proprio personale e ai collaboratori, anche tramite gli strumenti informativi interni (es. intranet aziendale),

assicurandone la conoscenza da parte di tutti i soggetti autorizzati al trattamento e la condivisione, ove pertinente, con le terze parti coinvolte.

TECHNACY S.R.L.
Sede legale ed operativa: Via Molveno, 5 – 48015 Cervia (RA)
P. IVA: 02399920392 | E-mail: info@technacy.it | Sito: www.technacy.it

Per approvazione – Titolare del trattamento

Technacy S.r.l Unipersonale
Via Molveno, 5 48015 Cervia (RA)
Tel 0544971446 Fax 0544913182
P.IVA Cod. Fisc. Reg. Imp. 02399920392

_____
(Data, Timbro e Firma)

Cervia, 24 Giugno 2026