STUDIO TOZZI & C.
SOCIETÀ TRA PROFESSIONISTI

PRIVACY POLICY

La presente policy richiama le procedure interne sulla protezione dei dati personali. Approvata in data 01-03-2023

Storico documento

Revisione	Data	Autore	Note
1.0web	23/04/2018	DPER	Stesura documentazione
1.1web	10/09/2019	DPER	Aggiornamento denominazione societaria e logo intestazione
1.2web	27/04/2022	DPER	Aggiornamento grafica copertina, aggiornamento paragrafo 9.1
1.3web	01/03/2023	DPER	Aggiornamento logo intestazione

Allegati documento

File	Titolo	Note

Approvato da (DPER) in data 01/03/2023

Autorizzato da (DGE) in data 01/03/2023

Studio Tozzi

INDICE

1. **Scopo e definizioni del documento** 2
2. **Principi, ambito di applicazione e destinatari della policy** 3
3. **Oggetto e modalità di applicazione** 4
4. **Organigramma e sistema di nomine e responsabilità** 4
   - **4.1 Titolare del Trattamento** 4
   - **4.2 Responsabile del Trattamento** 5
   - **4.3 Referenti privacy** 6
   - **4.4 Autorizzati al Trattamento** 7
   - **4.5 Referente esecutivo per la protezione dei dati personali (DPER)** 7
   - **4.6 Amministratore di sistema (AdS)** 8
5. **Impegno alla riservatezza** 9
6. **Trattamento dei dati personali (definizione e mappatura dei trattamenti)** 9
   - **6.1 Dati dei dipendenti dei collaboratori e dei componenti degli Organi Aziendali** 10
   - **6.2 Dati dei clienti** 10
   - **6.3 Dati dei terzi** 11
7. **Misure di sicurezza e relativi controlli** 11
   - **7.1 La gestione della sicurezza: ruoli e responsabilità** 11
   - **7.2 Misure per garantire l'integrità a protezione dell'accesso ai dati** 11
   - **7.3 Clean Desk Policy** 11
   - **7.4 Misure per garantire la disponibilità dei dati** 12
     - 7.4.1 Processo di assunzione dei dipendenti 12
     - 7.4.2 User ID Management 13
     - 7.4.3 Processo di dimissione del dipendente 13
     - 7.4.4. Dismissione dei dispositivi utilizzati dagli utenti dello Studio. 13
   - **7.5 Livelli di sicurezza** 13
8. **Informazione e formazione dei destinatari** 14
9. **Disposizioni interne per il corretto utilizzo degli strumenti informatici e telematici** 14
   - **9.1 Utilizzo del personal computer e internet** 15
   - **9.2 Gestione delle credenziali di accesso** 16

Studio Tozzi

1. Scopo e definizioni del documento

Lo scopo del presente documento è definire il modello Privacy, ovvero individuare le disposizioni operative interne volte a disciplinare il trattamento dei dati personali effettuato dalla Società, ai sensidel D.Lgs. n. 169 del 2003 e del Regolamento UE n. 679 del 2016, nonché ulteriori provvedimenti inmateria di fonte normativa secondaria, in vigore al momento dell'approvazione della seguente policy. In essa sono quindi disciplinati i ruoli e le responsabilità nonché gli adempimenti da seguire in materia di protezione dei Dati Personali ai sensi del "Codice Privacy" e del "GDPR", anche con riferimento alle decisioni e ai provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali.

Ai fini della presente Policy si applicano le seguenti definizioni, coerenti con quanto previsto dalla normativa di settore:

- Regolamento: 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 (c.d GDPR - Regolamento Generale sulla Protezione dei Dati);
- Normativa: D.Lgs. n. 169 del 2003 e Regolamento UE n. 679 del 2016, nonché ulteriori provvedimenti in materia di fonte normativa secondaria in vigore al momento dell'approvazione della seguente policy.
- Codice Privacy: Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";
- Società: Studio Tozzi & C. S.a.s. S.t.p.
- Affiliate: società controllate o collegate da Studio Tozzi & C. S.a.s. S.t.p. stabilite nel territorio dello Stato italiano o in un luogo comunque soggetto alla sovranità dello Stato italiano;
- 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;
- 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 osociale;
- Dati genetici: i dati personali relativi 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: i dati personali ottenuti da un trattamento tecnico specifico relativi 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: i dati personali attinenti 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;
- Interessato: la persona fisica cui si riferiscono i dati personali;
- Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Studio Tozzi

- Referente esecutivo per la protezione dei dati personali (DPER - Data Protection Executive Referent): la persona fisica preposta alla sorveglianza sull'applicazione e il rispetto delle disposizioni in materia di trattamento di dati impartite dal Titolare del trattamento o dal DPO qualora nominato;
- Referente: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;
- Autorizzato: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;
- Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- Paesi terzi: paesi non appartenenti all'UE o allo spazio Economico Europeo;
- Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- Trattamento transfrontaliero: a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.

2. Principi, ambito di applicazione e destinatari della policy

Il presente documento si applica a tutti i trattamenti dei dati effettuati dagli uffici di Studio Tozzi & C. S.a.s. S.t.p., automatizzati o svolti manualmente, in cui la predetta agisce in qualità di Titolare.

La presente Policy è di applicazione immediata per Studio Tozzi & C. S.a.s. S.t.p..

La Società si impegna a garantire e dimostrare che il trattamento dei dati avviene in maniera conforme a quanto previsto dalla normativa e secondo i seguenti principi di liceità di trattamento:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati; a tal proposito sono state adottate misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Le presenti indicazioni sono valide anche, per tutti quei trattamenti di cui Studio Tozzi & C. S.a.s. S.t.p. è nominata Responsabile esterno da altri Titolari, salvo la presenza di misure più restrittive in materia di protezione dei dati personali.

La stessa garanzia di protezione e di adozione di adeguate misure di sicurezza è richiesta altresì aquei soggetti terzi ai quali la società ha affidato l'incarico della gestione di alcuni trattamenti. A tal fine la policy in oggetto sarà resa disponibile presso i responsabili del trattamento qualora nominati.

Tale policy si applica a tutti i Soci, ai dipendenti di Studio Tozzi & C. S.a.s. S.t.p. e ai collaboratori esterni, che collaborano in modo continuo con quest'ultima.

3. Oggetto e modalità di applicazione

Oggetto della presente Policy è il trattamento dei Dati Personali effettuatoda Studio Tozzi & C. S.a.s. S.t.p..

Sono esclusi dall'ambito di applicazione:

- i Trattamenti dei Dati Personali effettuati da persone fisiche per fini esclusivamente personali e nei casi in cui i dati non sono destinati ad una comunicazione sistematica o alla diffusione (anche se utilizzati ai fini di esigenze di lavoro: ad esempio, banca dati su PC accessibile ed utilizzata solo ed esclusivamente dall'utente - persona fisica per un'elaborazione personale - rubrica telefonica).

4. Organigramma e sistema di nomine e responsabilità

Al fine di garantire la tutela dei diritti delle persone fisiche relativamente al trattamento dei dati personali, la Società ha implementato un sistema di figure e ripartizione delle responsabilità di seguito delineate, parametrate alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento, nonché ai rischi per i diritti e le libertà delle persone fisiche analizzati, come riportato nell'organigramma privacy allegato sotto la lettera "**A**" alla presente Privacy Policy.

4.1 *Titolare del Trattamento*

Conformemente a quanto previsto dalla normativa, è Titolare del trattamento la società Studio Tozzi & C. S.a.s. S.t.p. e quest'ultima si impegna a:

- adeguare il proprio assetto organizzativo per il governo della privacy;
- adottare le modalità operative connesse con la gestione degli adempimenti ed il trattamento dei dati ai fini privacy;
- assumere le decisioni in ordine alle finalità, alle modalità del trattamento dei dati e agli strumenti utilizzati, ivi compreso il profilo della sicurezza, sia per i trattamenti svolti all'interno che all'esterno della propria struttura;
- individuare e designare i Responsabili del trattamento dei dati, impartendo loro le relative istruzioni;
- vigilare sulla puntuale osservanza delle disposizioni e istruzioni impartite, anche nei confronti dei Responsabili del trattamento (sia interni che esterni).

Studio Tozzi

Essa, inoltre, si impegna a garantire l'esercizio dei diritti degli interessati e a tal scopo, haimplementato apposite procedure al fine di informare gli interessati dell'esistenza dei seguenti diritti:

- diritto di ottenere la conferma dell'esistenza o meno di dati personali che la riguardano e di averne accesso; c.d. diritto all'accesso. In particolare l'interessato ha diritto di conoscere l'origine dei dati personali; le finalità e modalità del trattamento; la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; gli estremi identificativi del titolare, dei responsabili e del rappresentante designato; l'elenco dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati;
- diritto di ottenere l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; c.d. diritto alla rettifica;
- diritto di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c.d. diritto alla cancellazione;
- diritto di limitare od opporsi, per motivi legittimi, al trattamento, rivolgendosi al personale espressamente incaricato; c.d. diritto di opposizione.

Al fine di esercitare i diritti sopra descritti, la Società si impegna a rispondere senza ritardo alle richieste presentate da parte dell'interessato ai Responsabili o agli Incaricati nominati, in forma oraleo attraverso ulteriori idonei strumenti.

4.2 *Responsabile del Trattamento*

Il responsabile del trattamento dei dati è la persona nominata dal Titolare al fine di garantire l'attuazione delle misure di sicurezza previste in materia di trattamento dei dati.

La persona preposta allo svolgimento della funzione viene individuata in quanto dotata di adeguategaranzie e tra le sue funzioni sono comprese:

- osservare le procedure in materia di protezione dei dati personali adottate dal Titolare;
- organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni di legge e predisporre tutti i documenti nonché le misure tecniche organizzative richiesti dal Codice e dal Regolamento;
- adottare e verificare il rispetto delle misure di sicurezza indicate dal Codice e dal Regolamento e la conformità dei sistemi e delle misure di sicurezza;
- redigere e aggiornare il registro delle attività di trattamento, qualora venga adottato;
- informare il Titolare del trattamento di tutte le misure adottate e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato;
- individuare gli incaricati che svolgono le funzioni di amministratore di sistema, conservando i relativi estremi identificativi, definendo gli ambiti di operatività ai medesimi consentiti e verificando il relativo operato per controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti il trattamento dei dati personali;
- individuare gli autorizzati al trattamento dei dati ai sensi dell'art. 30 del Codice, conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione;
- controllare le operazioni di trattamento svolte dagli incaricati e la conformità all'ambito di

trattamento consentito;

- redigere e aggiornare la lista dei nominativi degli autorizzati e verificarne l'ambito del trattamento consentito ai medesimi;
- proporre al Titolare del trattamento dei dati la nomina di soggetti esterni quali Responsabile del trattamento dei dati in relazione all'affidamento agli stessi di determinate attività;
- attuare gli obblighi di informazione ed acquisizione del consenso, quando richiesto, nei confronti degli interessati;
- garantire all'interessato che ne faccia richiesta l'effettivo esercizio dei diritti previsti dalla normativa di settore;
- distruggere i dati personali alla fine dei trattamenti degli stessi nei casi previsti dal Regolamento, secondo le procedure atte a garantire la sicurezza degli stessi e provvedere alle formalità di legge e agli adempimenti necessari anche mediante comunicazione al Garante, se dovuta;
- comunicare immediatamente al titolare non oltre le 24 ore successive al loro ricevimento, ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità Giudiziaria;
- osservare le procedure in materia di protezione dei dati personali adottate dal Titolare;
- informare l'interessato dell'eventuale trasferimento dei dati all'estero.

Il responsabile può essere anche esterno e in tal caso sarà tenuto a garantire l'applicazione delle misure individuate dal Titolare.

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare allo stato non ha nominato alcun Responsabile esterno, ma esclusivamente Responsabili interni.

4.3 *Referenti privacy*

Il Titolare ha provveduto ad individuare, presso le Unità Organizzative in cui vengono svolti i trattamenti, i Referenti privacy.

I compiti del Referente privacy sono di seguito sintetizzati:

- individuare e promuoverne l'autorizzazione per area di competenza delle persone da autorizzare al trattamento dei dati;
- segnalare al DPER eventuali casi di data breach, segnalati da parte delle sue risorse oautonomamente individuati;
- segnalare al DPER eventuali richieste ricevute da parte dell'interessato sull'esercizio deirelativi diritti, nonché attenersi alla procedura interna sull'esercizio dei diritti;
- cooperare in caso di attività di controllo in ambito privacy da parte di strutture interne o esterne, fornendo eventuale documentazione richiesta e garantendo l'accesso ai locali;
- informare il DPER dell'esistenza di un nuovo progetto che impatta sulla protezione dei dati, inapplicazione del principio di privacy by design e by default;
- informare il DPER dell'esistenza di un nuovo trattamento per cui risulta necessario aggiornareil registro o modificarlo, in applicazione del principio di privacy by design e by default;
- informare il DPER della presenza di una nuova risorsa che tratta dati personali al fine divalutare necessità di formazione in ambito privacy;
- controllare che le persone autorizzate al trattamento rispettino le indicazioni impartite dalla

Società;

- segnalare casi di mancato rispetto delle disposizioni in tema di protezione dei dati al DPER.

4.4. *Autorizzati al Trattamento*

Il Titolare ha provveduto ad individuare, presso le Unità Organizzative in cui vengono svolti i trattamenti, le persone autorizzate al trattamento dei dati, così come indicato dall'art. 30 del Codice Privacy e come indicato dal Garante Privacy[1].

L'Autorizzato effettua tutte le operazioni di Trattamento dei Dati Personali attinenti all'attivitàlavorativa di competenza dell'area di appartenenza ed opera sotto l'autorità del Titolare o del Responsabile del Trattamento, attenendosi alle istruzioni dallo stesso impartite nonché alle specifiche procedure che regolamentano le modalità di utilizzo delle banche dati cui lo stesso abbiaaccesso.

In particolare, i compiti ad esso attribuiti sono così sintetizzati:

- segnalare al DPER eventuali richieste ricevute da parte dell'interessato sull'esercizio dei relativi diritti, nonché attenersi alla procedura interna sull'esercizio dei diritti;
- avvisare il Referente Privacy nel caso in cui nello svolgimento di un'attività dovesse riscontrare il trattamento di nuovi dati e finalità per cui risultasse necessario aggiornare il registro dei trattamenti, in applicazione del principio di privacy by design e by default;
- informare immediatamente il DPER qualora le istruzioni le risultino non conformi alla normativa sulla protezione dai dati;
- segnalare al DPER eventuali accessi non autorizzati;
- rilasciare all'interessato l'informativa e acquisire il consenso laddove necessario, secondo le istruzioni impartite dal Titolare.

4.5 *Referente esecutivo per la protezione dei dati personali (DPER)*

Alla luce dell'analisi dei rischi aziendali in materia di trattamento dei dati personali, il Titolare ha ritenuto opportuno procedere all'individuazione del Referente esecutivo per la protezione dei dati personali(DPER). A tal riguardo si precisa che non vengono effettuate attività di trattamento a monitoraggio regolare e sistematicodi dati personali, né tantomeno tali attività costituiscono il *core* business di Studio Tozzi & C. S.a.s. S.t.p..

I compiti affidati al Referente esecutivo per la protezione dei dati personali (DPER) sono i seguenti:

- sorvegliare l'osservanza della normativa in materia di privacy nonché delle politiche del Titolare del trattamento, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti;
- vigilare sull'effettivo funzionamento delle prescrizioni adottate dalla Società in materia di Privacy;
- informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla normativa in materia privacy;
- promuovere la cultura della protezione dei dati all'interno della società e contribuire a dare attuazione a elementi essenziali del Regolamento (es. principi fondamentali del trattamento, diritti degli interessati, privacy by design e by default, registro delle attività di trattamento, sicurezza dei trattamenti e data breach);
- conservare e aggiornare l'elenco dei Referenti privacy e autorizzati al trattamento dei dati;
- fungere da punto di contatto tra i referenti privacy/autorizzati al trattamento e il Titolare del

[1] Cfr. Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali.

Studio Tozzi

trattamento;
- fungere da punto di contatto per l'interessato relativamente a tutte le questioni inerenti il trattamento dei loro dati personali e all'esercizio dei diritti;
- tenere e aggiornare il Registro dei trattamenti;
- supportare il Titolare del trattamento nella Valutazione rischi Privacy, fornendo eventuale parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
- cooperare con l'autorità di controllo;
- informare tempestivamente il Titolare del trattamento in caso di data breach;
- garantire riservatezza in merito all'adempimento dei propri compiti, in conformità con il diritto previsto dall'UE o dagli Stati Membri.

4.6 *Amministratore di Sistema (AdS)*

La figura professionale che, in ambito informatico, mantiene, configura e gestisce (i) un sistema di elaborazione dati o sue componenti, ivi inclusi sistemi software complessi quali i sistemi EnterpriseResource Planning (system administrator), ovvero (ii) una base dati (database administrator), ovvero
(iii) reti e apparati di telecomunicazione di sicurezza (network administrator) è nominata Amministratore di Sistema.
L'attribuzione delle funzioni di Amministratore di sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di Trattamento, ivi compreso il profilorelativo alla sicurezza.

La nomina ad amministratore di sistema deve essere individuale, formalizzata, con l'indicazione degli ambiti di applicazione di operatività consentiti in base al profilo di autorizzazione assegnato.
In generale, l'Amministratore di sistema ha le seguenti responsabilità:

- sovraintendere alle risorse dei sistemi computerizzati al fine di consentirne una corretta ed efficiente utilizzazione;
- in accordo con il DPER, fornire guida e supporto ai Referenti e agli Incaricati in merito al trattamento dei dati personali;
- amministrare e gestire la sicurezza informatica operando anche come gestore e custode delle password;
- nell'ambito delle responsabilità assegnate, effettuare controlli e verifiche tecniche, anche nei riguardi dei Responsabili e degli Incaricati in merito a quanto previsto dal presentedocumento;
- individuare l'eventuale soggetto/i esterno/i quale manutentore del sistema stesso. L'amministratore che provvede alla individuazione dei soggetti incaricati alla manutenzione deve preventivamente informare il Titolare del Trattamento e deve essere formalizzata per iscritto l'attribuzione dell'incarico eventualmente specificando i limiti dell'intervento e le manutenzioni richieste. Per manutenzione s'intende non soltanto l'intervento tecnico diretto ad eliminare eventuali avarie hardware, ma anche gli interventi volti alla ricostruzione di archivi che dovessero in qualche modo risultare danneggiati o corrotti oltre all'intervento tecnico diretto ad eliminare eventuali avarie al software di sistema e all'applicativo utilizzato;
- per poter svolgere funzioni, allo stesso vengono concesse dal Titolare le "Autorità di sistema", che consistono nell'assegnazione di attributi, privilegi, o accessi che consentono la gestione delle "risorse critiche del sistema operativo", ovvero degli oggetti informatici necessari al funzionamento dei sistemi e del servizio di elaborazione dati.

5. Impegno alla riservatezza

La Società, in qualità di Titolare del trattamento dei dati, si impegna a garantire la riservatezza, conformemente alle procedure interne e la confidenzialità delle informazioni e dei dati degli interessati acquisiti nel corso della propria attività.

A tal scopo, i dati e le informazioni raccolte durante lo svolgimento dell'incarico sono trattati per:

- finalità strettamente connesse alla gestione dell'incarico oggetto della presente proposta;
- finalità connesse agli obblighi previsti da leggi, regolamenti e normativa comunitaria nonché da disposizioni impartite da autorità a ciò legittimate dalla legge;
- finalità connesse alla disciplina in tema di antiriciclaggio.

In relazione alle indicate finalità il trattamento dei dati avverrà in modo da garantire la sicurezza e lariservatezza e potrà essere effettuato attraverso strumenti manuali, informatici e telematici atti a memorizzare, gestire e trasmettere i dati stessi nel rispetto delle misure di sicurezza previste dal Codice. Tutti gli Amministratori e dipendenti di Studio Tozzi & C. S.a.s. S.t.p. sono tenuti al segreto previsto dall'art. 2407 del codice civile.

Tutti i dati e le informazioni acquisite, in aggiunta alle comunicazioni previste nei confronti di soggettie organi che hanno responsabilità di direzione, supervisione e controllo potranno essere comunicatiesclusivamente a:

- autorità di Vigilanza, italiane o estere, nei casi e con le limitazioni previste dalla legge;
- autorità Amministrativa, giudiziaria e fiscale, nei casi e con le limitazioni previsti dalla legge;
- providers di servizi e/o consulenti tecnico-informatici, anche in Paesi terzi non comunitari, unicamente per esigenze tecniche connesse all'utilizzo da parte del Titolare di sistemi e/o applicazioni strumentali nell'esecuzione degli obblighi contrattuali assunti nell'ambito dell'incarico in oggetto e dei correlati obblighi di legge, fermo restando che il ricorso a tali soggetti avverrà previo impegno da parte loro a rispettare tutte le prescrizioni in materia di sicurezza dei dati previste dal Codice e dal Regolamento.

La Società si impegna a garantire gli standard indicati nelle disposizioni in oggetto nei confronti deiterzi con la medesima diligenza e livello di protezione utilizzati per la sicurezza e la riservatezza deipropri dati.

6. Trattamento dei dati personali (definizione e mappatura dei trattamenti)

Secondo quanto previsto dal Regolamento, il Titolare ed eventualmente, il Responsabile, qualora nominato, sono tenuti alla redazione e all'aggiornamento del registro dei trattamenti, da sottoporre all'Autorità di controllo, laddove richiesto.

Il predetto registro deve contenere:

a) il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del contitolare del trattamento, del Rappresentante esterno del trattamento se nominato, ed eventualmente (non obbligatoriamente) del Referente esecutivo per la protezione dei dati personali;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche.

Nello svolgimento delle proprie attività, Studio Tozzi & C. S.a.s. S.t.p. può svolgere trattamenti di dati che riguardano il personale dipendente, nonché candidati, i clienti o terzi fornitori/collaborati.

Alla luce dell'attività di mappatura dei trattamenti svolta, risultano essere presenti i dati di seguitoindicati.

6.1 *Dati dei dipendenti dei collaboratori e dei componenti degli Organi Aziendali*

Studio Tozzi & C. S.a.s. S.t.p. al fine di adempiere ai propri obblighi di gestione del personale, raccoglie i dati dei componenti degli organi aziendali e dei propri dipendenti, informandoli dei propri diritti.
In particolare, il trattamento dei dati delle suddette categorie è previsto per finalità amministrativo-contabili, quali ad esempio:

- gestione delle buste paga, gestione delle trasferte, promozioni e premi;
- pianificazione degli avanzamenti di carriera;
- gestione dei piani di formazione;
- gestione dei dati anagrafici per finalità di legge (ad es. in adempimento del D. lgs. 81/08 in tema di sicurezza sul lavoro).

Con riferimento al trattamento dei dati dei candidati, Studio Tozzi & C. S.a.s. S.t.p. si impegna a verificare l'acquisizione del consenso al trattamento dei dati e a fornire adeguata informativa.

6.2 *Dati dei clienti*

Studio Tozzi & C. S.a.s. S.t.p. per mezzo dei propri Referenti o Autorizzati, può raccogliere i dati personali dei clienti direttamente presso la clientela ovvero presso terzi, al fine di perfezionare accordi contrattuali, per poter effettuare le necessarie valutazioni, le quali hanno ad oggetto prevalentementela valutazione del rischio di credito.
I dati personali dei clienti potranno essere trattati nell'ambito della normale attività di Studio Tozzi & C. S.a.s. S.t.p. per le seguenti finalità:

- prestare i servizi richiesti e gestire i rapporti con la clientela (es. acquisizione di informazioni preliminari alla conclusione di un contratto, esecuzione di operazioni sulla base degli obblighi derivanti dal contratto concluso con la clientela, ecc);
- adempiere ad obblighi previsti da un regolamento o dalla normativa comunitaria (es. centrale rischi, normativa in materia di antiriciclaggio ecc.), nonché per osservare disposizioni impartite dalle pubbliche Autorità ed organi di vigilanza e controllo a ciò legittimati dalla legge. In tal caso il conferimento dei dati personali è necessario e obbligatorio e per il trattamento di tali dati non è richiesto il consenso;
- svolgimento di indagini di mercato/customer satisfaction e marketing, tra cui rientrano indagini di mercato e rilevazione del grado di soddisfazione della clientela e promozione e vendita di prodotti e servizi di Studio Tozzi & C. S.a.s. S.t.p. o di società terze con le quali possono essere stati conclusi accordi commerciali.

Al fine del trattamento dei dati personali per le finalità di marketing, trasferimento a terzi, nonché alloscopo di trattare i dati sensibili, il Titolare garantisce di presentare un autonomo consenso, rispetto all'uso degli ulteriori dati.

6.3 *Dati dei terzi*

Durante lo svolgimento dell'attività, Studio Tozzi & C. S.a.s. S.t.p. può venire a conoscenza di dati che riguardano terzi, ovvero fornitori, collaboratori ecc.
In tali casi Studio Tozzi & C. S.a.s. S.t.p. si impegna a sottoscrivere apposita clausola o accordo al fine di garantire la corretta applicazione delle presenti indicazioni anche nei rapporti con i terzi.

7. Misure di sicurezza e relativi controlli

7.1 *La gestione della sicurezza: ruoli e responsabilità*

La responsabilità dell'attività di impostazione e coordinamento dei sistemi che garantiscono la sicurezza e la tutela di tutti i dati oggetto di trattamento aziendale sia da un punto di vista logico chefisico, la loro gestione diretta o tramite fornitori, sono in carico all'Amministratore di Sistema.

L'amministrazione della sicurezza logica segue i seguenti criteri generali:

- in base alle figure professionali presenti in azienda, vengono definiti i profili standard daassegnare agli utenti con le autorizzazioni necessarie all'espletamento delle rispettive mansioni definite per ruoli e competenze;
- la validità delle richieste di accesso alla rete è verificata automaticamente dal sistema stesso prima di consentire l'accesso ai dati, tramite un sistema di autenticazione costituito da User-ID e password.

Studio Tozzi & C. S.a.s. S.t.p., in qualità di Titolare del trattamento dei dati, è tenuta a proteggere i dati personali trattati in modo sicuro.
I dati in formato elettronico possono essere archiviati su: Cartelle in Cloud, cartelle su Server noncifrato, cartelle all'interno di PC non cifrato, protetti con password policy elevata.

7.2 *Misure per garantire l'integrità a protezione dell'accesso ai dati*

Sono le misure di sicurezza volte a minimizzare i rischi che le informazioni siano rivelate o modificatesenza autorizzazione, ovvero perse o alterate accidentalmente o intenzionalmente.
Il sistema in atto prevede un sistema di autenticazione, basato su codice identificativo e passwordindividuale segreta, per assicurare che la persona che accede al sistema, nelle sue diverse articolazioni, sia identificata con certezza, nonché un sistema di autorizzazione, che prevede che aciascuna persona che accede al sistema sia assegnato un profilo di accesso che definisce i dati ai quali l'utente è autorizzato ad accedere e, ove applicabile, le operazioni che per ciascun dato o gruppo di dati è autorizzato ad eseguire (consultazione, inserimento, modifica, cancellazione).

7.3 *Clean Desk Policy*

La politica di "scrivania pulita" è una delle migliori strategie da attuare quando si cerca di ridurre il rischio di violazioni della sicurezza della postazione di lavoro.
Lo scopo di questa politica è di stabilire i requisiti minimi per adeguarsi non solo ai controlli della ISO27001, ma anche per prevenire eventi di data breach e responsabilizzare i dipendenti aziendali. Di seguito sono elencati

i comportamenti da applicare:

- i dipendenti sono tenuti a garantire che tutte le informazioni sensibili o confidenziali in formato elettronico o cartaceo siano messe al sicuro nella propria postazione di lavoro, in particolare alla fine della giornata lavorativa e in caso di assenza prolungata;
- i computer devono essere bloccati quando le postazioni di lavoro non sono occupate;
- tutti i computer devono essere spenti alla fine della giornata lavorativa;
- qualsiasi informazione e/o dato particolare/sensibile deve essere rimosso dalla scrivania e chiuso a chiave in un cassetto quando la postazione di lavoro non è occupata e alla fine della giornata lavorativa;
- le cartelle contenenti informazioni riservate e/o dati particolari/ sensibili devono essere tenute chiuse e bloccate quando non utilizzate;
- le chiavi utilizzate per accedere alle informazioni riservate e/o ai dati particolari/sensibili non devono essere lasciate su una scrivania non presidiata;
- i laptotp devono essere bloccati con un cavo di bloccaggio o conservati in un cassetto se non utilizzati;
- le password non possono essere lasciate su note adesive attaccate sopra o sotto un computer, né possono essere lasciate per iscritto su una postazione accessibile;
- le stampe contenenti informazioni riservate e/o dati particolari/sensibili devono essere immediatamente rimosse dalle stampanti;
- al momento dello smaltimento, i documenti riservati o contenenti dati particolari/sensibili devono essere triturati;
- le lavagne contenenti informazioni riservate e/o dati particolari/sensibili devono essere cancellate;
- i dispositivi portatili come laptop, smartphone o tablet non devono mai essere lasciati sbloccati e incustoditi;
- tutti i dispositivi di archiviazione di massa come CDROM, DVD o chiavi USB contenenti informazioni riservate e/o dati particolari/sensibili devono essere conservati in cassetti chiusi a chiave.

Il dipendente che viola queste norme di comportamento può essere soggetto ad azioni disciplinari, fino al licenziamento.

7.4 *Misure per garantire la disponibilità dei dati*

Sono le attività volte a ridurre i rischi di indisponibilità (parziale o totale) nell'accesso al sistema informatico di Studio Tozzi & C. S.a.s. S.t.p..

7.4.1 *Processo di assunzione dei dipendenti*

Nel contesto di assunzione di una nuova risorsa in Studio Tozzi & C. S.a.s. S.t.p., la direzione è tenuta ad avvisare con congruo anticipo l'AdS, prima della data di ingresso della risorsa, per la creazione dell'utenza, e per la preparazione della postazione PC.

7.4.2 *User ID Management*

Tutte le utenze hanno un unico ID ed un unico dominio. L'utenza è personale e non è concesso cheessa sia

Studio Tozzi

condivisa con uno o più soggetti.
Studio Tozzi & C. S.a.s. S.t.p. può modificare i diritti di accesso ai servizi e ai sistemi in qualsiasi momento eper qualsiasi ragione.
Tutti i dipendenti di Studio Tozzi & C. S.a.s. S.t.p. non sono amministratori di macchina dei dispositivi rilasciati in dotazione.

7.4.3 *Processo di dimissione del dipendente*

Nel caso di dimissioni di una risorsa da Studio Tozzi & C. S.a.s. S.t.p., la direzione è tenuta ad avvisare l'AdS con congruo anticipo, prima della data di cessazione del rapporto di lavoro, per la disabilitazione dell'utenza e per la riconsegna della postazione PC. Alla cessazione del rapporto, l'AdS disabilita immediatamente tutti i diritti di accesso del dipendente alla rete ed ai sistemi IT aziendali.

7.4.4 *Dismissione dei dispositivi utilizzati dagli utenti di Studio Tozzi & C. S.a.s. S.t.p.*

Tutti i dispositivi di Studio Tozzi & C. S.a.s. S.t.p., rilasciati in dotazione ai dipendenti, vengono formattati a seguito delle dimissioni degli stessi al fine di rimuovere tutti i dati personali contenuti al loro interno.

Tutti i dipendenti di Studio Tozzi & C. S.a.s. S.t.p. sono, quindi, tenuti ad assicurarsi che venga correttamente eseguito il passaggio di consegne tra i colleghi del team affinché venga assicurata la continuità dei servizi erogati e la conservazione delle carte di lavoro relative ai clienti.

7.5 *Livelli di sicurezza*

L'amministrazione della sicurezza logica segue i seguenti criteri generali:

- applicazione del principio "need to know" e del minimo privilegio, secondo cui la definizione dei profili standard da assegnare agli utenti con le autorizzazioni necessarie all'espletamento delle rispettive mansioni (definite per ruoli e competenze) avviene alla luce delle effettive esigenze operative. A tal scopo viene limitato l'accesso logico a reti, sistemi e basi dati;
- la validità delle richieste di accesso alla rete è verificata automaticamente dal sistema stesso prima di consentire l'accesso ai dati, tramite un sistema di autenticazione costituito da User-ID e password;
- sono adottate delle indicazioni per la gestione delle password che indicano la lunghezza, la complessità, la durata, la conservazione sicura richiesta, in conformità a quanto richiesto dagli standard in materia di Privacy, nel caso di trattamenti dei dati effettuati con strumenti elettronici;
- sono adottate tecniche e metodologie per la verifica nel continuo dell'utilizzo dei sistemi applicativi e per il controllo del traffico di rete generato, al fine di garantire pronto intervento in caso di attività anomale;
- sono previsti presidi rafforzati per l'accesso da remoto, in particolare nei confronti di utenti appartenenti a soggetti terzi;
- è prevista la verifica periodica delle misure di sicurezza, anche attraverso l'effettuazione di *test*, al fine di prevenire ipotesi di Data Breach;
- sono organizzate sessioni di formazione dei dipendenti, nonché regolamenti e/o altre forme di documentazione interna, al fine di rendere gli stessi edotti dei rischi in materia di privacy.

Studio Tozzi

8. Informazione e formazione dei destinatari

L'obiettivo di garantire un corretto trattamento dei dati, conforme ai requisiti previsti dalla normativa[2], viene raggiunto dalla Società anche e soprattutto grazie alla particolare attenzione riposta nei confronti della formazione del proprio personale.

A tal proposito, fin dal momento di ingresso di una nuova risorsa, Studio Tozzi & C. S.a.s. S.t.p. presenta a quest'ultima la Policy Privacy, nonché comunica eventuali aggiornamenti a tuttii dipendenti. Tale policy viene comunque archiviata all'interno della rete aziendale accessibile atutti gli utenti di Studio Tozzi & C. S.a.s. S.t.p..

La formazione degli incaricati e, ove necessario, dei responsabili del trattamento riguarda inparticolare:

- aspetti della disciplina di protezione dei dati personali, in ambito generale ed ambito specifico
- i rischi che minacciano i dati;
- le conseguenze derivate dalla violazione di dati personali (Data Breach);
- le procedure da seguire in caso di Data Breach;
- le misure disponibili per evitare eventi di Data Breach;
- aspetti della disciplina di protezione dei dati personali, in ambito generale ed ambito specifico (particolari provvedimenti in ambito sanitario, telco, bancario, ecc.);
- training per aggiornare il personale sulle misure adeguate di sicurezza e protezione dei dati personali adottate dal Titolare del trattamento;

La formazione deve essere:

- adeguata al proprio sistema di trattamenti dei dati;
- capace di trasmettere agli incaricati e responsabili del trattamento misure adeguate di sicurezza e protezione dei dati personali adottate dal Titolare;
- documentabile, in quanto la formazione dell'avvenuto training è parte integrante della policy privacy di Studio Tozzi & C. S.a.s. S.t.p., e può essere richiesta in qualsiasi momento da enti specifici.

9. Disposizioni interne per il corretto utilizzo degli strumenti informatici etelematici

La Società si è dotata di procedure specifiche per l'uso dei sistemi informatici nonché l'accesso ad internet. Tali procedure, che vengono diffuse tra i dipendenti della Società, hanno lo scopo di ridurre i rischi di natura patrimoniale, di danneggiamento di immagine della Società nonché di incorrere in responsabilità penali conseguentialla violazione di specifiche disposizioni di legge.
Le regole che disciplinano l'utilizzo delle risorse informatiche e telematiche si ispirano al principio della diligenza e correttezza, principi che normalmente si adottano nell'ambito dei rapporti di lavoro.Per quanto non espressamente indicato, si rimanda alla normativa specifica in materia, adottata

dalla Società.
Il mancato rispetto delle indicazioni in materia di uso delle risorse aziendali conferite ai dipendenti espone gli stessi a provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, nonché a tutte le azioni civili e penali consentite.

[2] Art. 29 del Regolamento – "Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento" Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Studio Tozzi

9.1 *Utilizzo del personal computer e internet*

Il Personal Computer affidato all'utente è uno strumento di lavoro, pertanto ogni utilizzo non inerenteall'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. È quindi assolutamente proibita la navigazione in Internet permotivi personali e diversi da quelli strettamente legati all'attività lavorativa.
Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.
L'accesso alla rete ed ai sistemi IT aziendali avviene solo attraverso specifiche credenziali di autenticazione, che devono essere custodite da parte dell'utente.
L'AdS nonché i tecnici incaricati dell'assistenza IT hanno la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazionetecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.
Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dall'AdS per conto della Società né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.
L'inosservanza della presente disposizione espone la stessa Società a gravi responsabilità civili; sievidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che imponela presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protettodal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di unaresponsabilità amministrativa a carico della società, come disposto dall'art. 25-nonies del D.lgs. 8 giugno 2001, n. 231, con applicazione di sanzioni pecuniarie ed interdittive.
Salvo preventiva espressa autorizzazione dell'AdS, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem ecc.).
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'AdS nel caso in cui siano rilevati virus.
Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo, salvo disposizioni e/o richieste specifiche da parte dell'AdS.
In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.
Qualora, l'utente sia dotato di un PC portatile, egli è responsabile di custodirlo con diligenza sia se l'utilizzo avviene fuori sede sia durante l'utilizzo nel luogo di lavoro.

I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.
Tutti i supporti magnetici rimovibili (CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati conparticolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
I supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dagli utenti in armadi chiusi. E' vietato l'utilizzo di supporti rimovibili personali.
Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware,ecc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, ecc.), comunque estranei a qualsiasi finalità di controllodell'attività lavorativa, è facoltà della Direzione Aziendale, tramite l'AdS o tecnici addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del trafficotelefonico.

9.2 *Gestione delle credenziali di accesso*

Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dall'AdS, previo preavviso da parte della Direzione Aziendale sull'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dall'AdS, associato ad una Password riservata che dovrà venir custodita dall'autorizzato con la massima diligenza e non divulgata.
La Password, formata da lettere (maiuscole o minuscole), numeri e/o caratteri speciali, anche in combinazione fra loro, dovrà in ogni caso soddisfare i requisiti delle singole applicazioni, nonché gli standard minimi di sicurezza.
È necessario procedere alla modifica della parola chiave a cura dell'utente autorizzato del trattamento al primo utilizzo e/o, comunque, quando richiesto dall'applicazione.
Qualora la parola chiave dovesse venir sostituita, per decorso del termine ove previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con l'AdS.
Il soggetto preposto alla custodia delle credenziali di autenticazione è l'AdS.

Studio Tozzi