



POLITICA IN MATERIA DI TRATTAMENTO E PROTEZIONE DEI DATI PERSONALI

INDICE

1.	OBIETTIVO.....	3
2.	NORMATIVA DI RIFERIMENTO	3
3.	DEFINIZIONI	3
4.	CAMPO DI APPLICAZIONE	5
5.	ORGANIZZAZIONE PER LA PROTEZIONE E IL TRATTAMENTO DEI DATI	6
6.	POLITICA PER LA PROTEZIONE DEI DATI PERSONALI	9
7.	DIRITTI DEGLI INTERESSATI	14
8.	CONTROLLO E CONFORMITÀ	16
9.	DATI DI CONTATTO	16

1. OBIETTIVO

Il documento della Politica in materia di trattamento e protezione dei dati personali (di seguito "*Policy*") viene redatto dal Titolare del Trattamento per rappresentare l'applicazione delle regole e dei principi in ossequio a quanto stabilito dalla Normativa di riferimento (vedi Punto 2), per:

- proteggere e salvaguardare i dati personali e confidenziali;
- disciplinare il trattamento dei dati personali e confidenziali;
- stabilire i principi di buona gestione per i dati personali e confidenziali;
- garantire che tutti i trattamenti avvengano nel rispetto dei diritti, delle libertà fondamentali nonché della dignità delle persone fisiche;
- assicurare la riservatezza delle informazioni riferite alla gestione del personale e dei collaboratori;
- assicurare la riservatezza delle informazioni riferite agli interessati;

2. NORMATIVA DI RIFERIMENTO

- Regolamento UE n. 679/2016 Regolamento Generale sulla Protezione dei dati (di seguito anche "GDPR" o "Regolamento");
- Decreto Legislativo n. 196/2003 "Codice in materia di protezione dei dati personali" (di seguito "Codice Privacy"), dagli allegati al Codice così come modificati dalla Legge 25 ottobre 2017, n. 163 Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017;
- D.Lgs 101/ 2018 di adeguamento della normativa nazionale
- Provvedimenti, Linee Guida e Pareri emessi dall'Autorità Garante per la protezione dei dati personali (di seguito "Garante Privacy"), dal Comitato Europeo per la Protezione dei Dati e dal Garante Europeo della Protezione dei Dati (GEPD);

3. DEFINIZIONI

Ai fini di una agevole comprensione il documento della *Policy*, si riportano alcune delle definizioni contenute nell'art. 4 del Regolamento:

- "**dato personale**" anche definito come "**Informazioni Personali Identificabili (PII)**": 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 ad un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- "**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;
- "**limitazione di trattamento**": il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- "**profilazione**": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento

professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

- **“pseudonimizzazione”**: il trattamento dei dati personali in modo tale che gli stessi non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, purché le medesime siano conservate separatamente e soggette a misure tecniche e organizzative tali da assicurare che i dati non siano attribuiti ad una persona fisica identificata o identificabile;
- **“archivio”**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- **“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 ed i mezzi del trattamento dei dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri
- **“responsabile del trattamento”**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare;
- **“destinatario”**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi (non sono considerati destinatari quelle autorità pubbliche che possono ricevere comunicazioni nell'ambito di una specifica indagine conformemente al diritto dell'Unione Europea);
- **“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 che operano sotto l'autorità diretta del titolare o del responsabile;
- **“consenso dell'interessato”**: qualsiasi manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- **“violazione dei dati personali”**: la 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 trasmessi, conservati o comunque trattati.
- **“autorità di controllo”**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51 GDPR;
- **“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.

4. CAMPO DI APPLICAZIONE

La presente *Policy* si applica al trattamento di tutti i dati personali di persone fisiche (tra cui, a titolo esemplificativo e non esaustivo, quelli afferenti a dati dei dipendenti, dei clienti, dei fornitori e dei soggetti terzi che operano in qualità di persona fisica) nonché a qualsiasi informazione di carattere personale o con le caratteristiche di dato personale ricevute da Partners Tecnici e Commerciali. ***Particolare riguardo viene riservato al trattamento delle informazioni personali identificabili (PII)***. Il documento si applica ai dati personali trattati dal Titolare del Trattamento anche quando agisce in qualità di Responsabile del Trattamento e ha lo scopo di garantire che il trattamento analogico, automatizzato o cartaceo di dati personali, effettuato anche tramite soggetti autorizzati ai sensi degli articoli 28 e 29 del GDPR, avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché, della dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale, secondo le disposizioni vigenti in materia di protezione dei dati. Il Titolare del Trattamento adotta tutte le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato, così da assicurare il rispetto dei principi di liceità, correttezza e trasparenza nel trattamento dei dati personali e assicura l'adozione di adeguate e preventive misure di sicurezza, idonee ad evitare situazioni di rischio e di non conformità o di alterazione dei dati.

5. ORGANIZZAZIONE PER LA PROTEZIONE E IL TRATTAMENTO DEI DATI

All'interno dell'organico del Titolare del Trattamento sono individuati i ruoli e i compiti dei soggetti autorizzati a trattare i dati personali, attività consentita esclusivamente ai soggetti autorizzati, Responsabili del trattamento, eventuali Sub-Responsabili del trattamento e Amministratori di Sistema. Il trattamento effettuato da soggetti non preventivamente autorizzati è illecito.

Titolare del trattamento dei dati personali

È considerato Titolare del trattamento ai sensi della presente *Policy* l'ente giuridico nel suo complesso, stante la sua autonomia decisionale in merito alle finalità e ai mezzi del trattamento dei dati personali degli Interessati. Il Titolare del Trattamento è la persona giuridica in persona del Legale Rappresentante. Il Titolare del Trattamento adotta tutte le misure tecniche e organizzative atte a garantire che il trattamento dei dati personali sia effettuato conformemente alla normativa vigente. Il Titolare del Trattamento nei casi previsti dalla legge, provvede a:

- assolvere ogni obbligo di comunicazione, interpello o notificazione all'Autorità Garante per la Privacy;
- cooperare, su richiesta, con l'Autorità Garante per la Privacy nell'esecuzione dei suoi compiti ai sensi dell'art. 31 GDPR;
- richiedere a tale Autorità ogni necessaria autorizzazione al trattamento dei dati personali, ove necessaria;
- adottare, per quanto di competenza, le misure necessarie a garantire la protezione dei dati personali, anche per quanto riguarda il processo di digitalizzazione;
- adottare una procedura di valutazione d'impatto privacy (Data Privacy Impact Assessment) per le attività di trattamento dati al fine di attivare e mantenere aggiornato il Registro delle attività di trattamento effettuate - in formato cartaceo o elettronico - svolte sotto la propria responsabilità, conformemente a quanto prescritto dall'art. 30 n. 1 del GDPR;
- assicurare l'informazione e la formazione del personale sul tema della tutela della protezione dei dati personali;
- nominare i Designati, Incaricati autorizzati, Responsabili Interni del trattamento dati personali impartendo loro le necessarie istruzioni per la corretta gestione e protezione dei dati personali.

Il Titolare del trattamento è tenuto a effettuare, nei confronti di tutti coloro che svolgono per suo conto attività di trattamento, le verifiche e i controlli atti a garantire il rispetto degli obblighi previsti dalle disposizioni vigenti in materia.

Incaricati/Soggetti autorizzati al trattamento

Ai sensi dell'art. 29 GDPR, il Responsabile di ogni specifico trattamento individua - con apposite nomine e quali persone autorizzate al trattamento medesimo - tutti i dipendenti, collaboratori e consulenti, che intervengono, in relazione all'esercizio delle rispettive mansioni e competenze, nell'esecuzione dei trattamenti.

Le persone "autorizzate al trattamento" dei dati personali agiscono, dunque, sotto l'autorità del Responsabile o del Titolare del trattamento. Pertanto, al fine della corretta gestione dei dati in trattamento, l'Incaricato Autorizzato dovrà:

- trattare i dati in modo lecito e secondo correttezza e secondo le prescrizioni nel Regolamento UE 679/16 e nella normativa nazionale;
- verificare che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati

raccolti o successivamente trattati, secondo le indicazioni ricevute dal Responsabile del trattamento dei dati; attenersi alle procedure operative e alle istruzioni di lavoro impartite dal Responsabile del Trattamento dei dati del Settore.

- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza esplicita autorizzazione del Titolare e del Responsabile del trattamento;
- mantenere la massima riservatezza sui dati oggetto di trattamento;
- osservare ai sensi dell'art. 32 del Regolamento UE 679/16 che il trattamento dei dati avvenga mediante l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio;
- informare tempestivamente il Responsabile del Trattamento dei dati del Settore di appartenenza in caso di incidenti o problematiche relative alla sicurezza dei dati trattati.

Responsabile esterno del trattamento

Per Responsabili esterni si intendono tutti i soggetti “non dipendenti” del Titolare del Trattamento, che effettuano trattamenti sulle banche dati dello stesso, per suo conto e nel suo interesse.

I trattamenti effettuati da parte del Responsabile esterno del trattamento sono disciplinati, ai sensi dell'art. 28 GDPR, da un contratto o altro atto giuridico che individui la durata, la natura, la finalità del trattamento, il tipo di dati personali e le categorie degli interessati, le responsabilità affidate al Responsabile, gli obblighi e i diritti del Titolare. In particolare, il Responsabile, sebbene non in via esaustiva, avrà questi compiti e attribuzioni:

- garantire che il trattamento dei dati personali di cui è Titolare del Trattamento la Società e di cui venga a conoscenza con l'attività svolta avvenga in conformità a quanto previsto dalla vigente normativa e dalle presenti istruzioni;
- aggiornare periodicamente l'elenco dei trattamenti dei dati personali; tenere il Registro delle attività di trattamento dei dati, come previsto da art. 30 del GDPR, in formato elettronico, di tutte le categorie di attività relative al trattamento svolte per conto della Società;
- mettere in atto, ai sensi dell'art. 32 del GDPR, tutte le misure tecniche e organizzative necessarie a garantire un livello di sicurezza adeguato al rischio, tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento effettuato in esecuzione del Contratto;
- provvedere affinché vengano rigorosamente adottate tutte le misure idonee a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati trattati con l'attività di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità per le quali i dati sono stati raccolti;
- verificare periodicamente lo stato di applicazione del Regolamento Europeo 2016/679, nonché la corretta applicazione, il buon funzionamento dei sistemi e, ai sensi dell'art.32 del GDPR, delle adeguate misure tecniche e organizzative adottate per la tutela dei dati personali e la conformità alle indicazioni dell'Autorità Garante e del Titolare del Trattamento;
- tenere i dati personali, trattati in esecuzione del Contratto, separati rispetto a quelli eventualmente trattati per conto di altre terze parti applicando una segregazione fisica e logica, ove possibile;
- garantire la stretta osservanza dell'incarico ricevuto, escludendo qualsiasi trattamento o utilizzo dei dati personali di titolarità della Società non coerente con gli specifici trattamenti svolti in adempimento del Contratto e le relative suddette finalità;
- garantire la portabilità dei dati personali trattati in esecuzione del Contratto, ai sensi dell'art. 20 del GDPR, assicurando che gli stessi possano essere trasmessi;
in un formato strutturato, di uso comune e leggibile da qualsiasi dispositivo automatico;

- assistere il Titolare del Trattamento per quanto concerne gli obblighi di notifica e ogni altra comunicazione verso il Garante, ove dovute;
- tenendo conto della natura del trattamento, assistere il Titolare del Trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del Trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del Regolamento Europeo 2016/679;
- mettere a disposizione del Titolare del Trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa vigente in particolare l'adozione delle adeguate misure organizzative e di sicurezza ai sensi art. 32 del GDPR;
- comunicare al Titolare del Trattamento qualsiasi variazione della situazione oggettiva o delle sue proprie caratteristiche soggettive, tali da compromettere il corretto espletamento dei compiti descritti nella presente;
- provvedere alla nomina del/i proprio/i amministratore/i di sistema, in adempimento a quanto previsto dal provvedimento del Garante della Privacy del 27/11/2008, pubblicato in G.U. n. 300 del 24/12/2008, ove ne ricorrano i presupposti, curando, altresì, l'applicazione di tutte le ulteriori prescrizioni contenute nel suddetto provvedimento;
- Informare il Titolare del Trattamento senza ingiustificato ritardo e comunque non oltre le 72 ore dal momento in cui ne è venuto a conoscenza (art. 33 del GDPR), eventuali violazioni dei dati personali (data breach) adottando, di concerto con lo stesso, nuove adeguate misure di sicurezza atte a circoscrivere gli effetti negativi dell'evento e a ripristinare la situazione precedente;
- Predisporre e aggiornare un registro che dettagli, in caso di eventuali data breach, la natura delle violazioni, gli interessati coinvolti, le possibili conseguenze e le nuove misure di sicurezza implementate;
- supportare il Titolare del Trattamento durante la stesura della valutazione dell'impatto (ove prevista) dei trattamenti stabiliti sulla protezione dei dati personali, nei casi in cui un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- supportare il Titolare del Trattamento durante le fasi di consultazione con l'autorità di controllo, qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento possa presentare un rischio elevato in assenza di misure adottate dal Titolare del Trattamento per attenuare il rischio;
- ottemperare tempestivamente alle eventuali richieste inoltrate dal Titolare del Trattamento al fine di rendere conforme il trattamento dei dati posto in essere in esecuzione del Contratto, agli eventuali provvedimenti emessi dal Garante Privacy in materia di trattamento di dati personali;
- avvertire prontamente il Titolare del Trattamento in merito alle eventuali richieste degli interessati che dovessero pervenire, inviando copia delle istanze ricevute all'indirizzo e-mail indicato al termine del presente documento collaborare al fine di garantire il pieno esercizio da parte degli interessati di tutti i diritti previsti dall'articolo 7 del Codice;
- avvisare immediatamente, e comunque entro tre (3) giorni lavorativi, il Titolare del Trattamento di qualsiasi richiesta o comunicazione da parte dell'Autorità Garante o di quella Giudiziaria o di Pubblica Sicurezza eventualmente ricevuta, inviando copia delle istanze all'indirizzo e-mail indicato al termine del presente documento per concordare congiuntamente il riscontro.

6. POLITICA PER LA PROTEZIONE DEI DATI PERSONALI

Raccolta e trattamento delle informazioni

Il Titolare del Trattamento adotta le misure e le precauzioni per verificare che le informazioni contenenti dati personali siano pertinenti, accurate, complete e attuali come è necessario per gli scopi per i quali devono essere utilizzate.

I trattamenti di dati personali effettuati si conformano al principio di minimizzazione dei dati ai sensi dell'art. 5, co. 1, lett. c), del Regolamento in base al quale la raccolta e il successivo trattamento di dati personali avvengono in maniera da ridurre al minimo indispensabile l'utilizzo di dati personali identificativi degli Interessati.

Il trattamento deve essere attuato in modo da assicurare il rispetto dei diritti e della dignità dell'interessato.

Qualora alcune operazioni di trattamento, ovvero processi o fasi di processo, non necessitino la visualizzazione in chiaro di dati personali e identificativi degli Interessati, le medesime operazioni di trattamento devono essere effettuate mediante dati resi anonimi o, quantomeno, codificati.

I dati che, anche a seguito di verifica, risultino eccedenti o non pertinenti o non necessari, non possono essere utilizzati salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene.

I soggetti autorizzati delegati al trattamento sono tenuti a verificare periodicamente l'esattezza e l'aggiornamento dei dati personali, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'Interessato fornisce di propria iniziativa.

Registro dei trattamenti

Il Titolare del Trattamento individua, come elementi fondamentali delle politiche di protezione dei dati personali, l'analisi dei trattamenti e la distribuzione dei compiti e delle responsabilità attribuite a coloro che sono incaricati di trattare dati personali. Il Titolare del Trattamento tiene un Registro delle attività di trattamento dei dati personali di riferimento, costantemente aggiornato, che evidenzia i diversi livelli di responsabilità attribuiti nell'ambito del trattamento. In particolare, ha predisposto e mantiene aggiornato:

- un Registro delle "attività di trattamento" svolte in quanto Titolare del trattamento
- un Registro delle "categorie delle attività di trattamento" svolte in quanto Responsabile esterno del trattamento, formalmente incaricato dai Clienti Titolari del trattamento.

I Registri sono tenuti dal Titolare del Trattamento.

Informativa

Il Titolare del Trattamento si adopera affinché tutte le operazioni di trattamento avvengano conformemente a quanto richiesto dall'art. 13 del Regolamento.

L'Informativa deve essere sempre resa agli interessati all'atto della raccolta dei dati, anche quando non è necessario richiedere il loro consenso al trattamento.

Per il rispetto di quanto indicato nell'Informativa devono essere adottati i seguenti principi:

- non è consentito effettuare trattamenti di dati personali senza aver fornito preventivamente l'Informativa;
- non è consentito effettuare trattamenti di dati personali per finalità diverse da quelle indicate nell'Informativa già resa agli interessati; ulteriori finalità possono essere integrate nell'Informativa previa condivisione con i Responsabili del trattamento;
- non è consentita la comunicazione dei dati alle categorie dei soggetti terzi diverse da quelle indicate nell'Informativa. Eventuali ulteriori categorie di soggetti ritenute necessarie ai fini

del trattamento dei dati possono essere inserite nell'Informativa previa condivisione con i Responsabili del trattamento.

Il Titolare del Trattamento si impegna affinché sia previsto un aggiornamento periodico e/o una review delle varie informative sia cartacee (i.e. informativa dipendenti, informativi clienti, informativi fornitori, etc.) sia elettroniche (i.e. informative siti web).

Scelta e consenso

Il Titolare del Trattamento s'impegna a rispettare l'obbligo di raccolta del consenso come stabilito dagli artt. 6 e 7 del Regolamento. Il consenso è validamente prestato quando:

- è preceduto da un'Informativa corretta e completa;
- è espresso liberamente;
- è riferito univocamente a un determinato trattamento;
- è documentato per iscritto in relazione al tipo di dati raccolti (ad es. uso di dati sensibili).

Ai sensi dell'art. 6, comma 1, lett. b) – f), del Regolamento, il consenso non è dovuto quando:

- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

Trasferimento di dati personali

Il Titolare del Trattamento s'impegna ad adottare le misure necessarie per garantire che i trasferimenti di dati personali siano conformi con la normativa applicabile anche nel caso in cui questo dovesse avvenire da parte di soggetti terzi che agiscono in qualità di sub-appaltatori.

Il trasferimento di Dati personali all'esterno dell'Unione Europea può avvenire, in presenza di almeno una delle seguenti condizioni (Artt. 44, 45 e 46 GDPR):

- una decisione di adeguatezza della Commissione Europea;
- clausole tipo di protezione ("Model Contract Clauses") dei dati adottate dalla Commissione Europea;
- clausole contrattuali tra il Titolare del trattamento e il Titolare/Responsabile destinatario dei Dati personali nel paese terzo approvate dall'autorità di controllo;
- adozione di un codice di condotta o meccanismo di certificazione e contestuale impegno del Titolare/Responsabile destinatario dei Dati personali di applicare le garanzie adeguate.

Il trasferimento di Dati personali verso un paese terzo o un'organizzazione internazionale sarà inoltre possibile nel caso in cui:

- l'interessato abbia prestato esplicitamente il consenso dopo essere stato informato dei possibili rischi;
- il trasferimento sia necessario per l'esecuzione di un contratto concluso tra l'interessato e il titolare ovvero di misure precontrattuali adottate su istanza dell'interessato;
- il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare e un terzo a favore dell'interessato;
- il trasferimento sia necessario per importanti motivi di interesse pubblico.

Integrità dei dati

Il Titolare del Trattamento, ai sensi dell'art. 5 del Regolamento, effettua i trattamenti di dati personali adeguando il loro operato ai seguenti criteri generali:

- ciascun trattamento deve avvenire in modo lecito, trasparente e secondo correttezza;
- i dati trattati devono essere raccolti e registrati per scopi determinati, espliciti e legittimi, e utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;
- i dati trattati devono essere esatti e, se necessario, aggiornati;
- i dati trattati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- i dati trattati devono essere 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;
- i dati devono essere 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 («disponibilità, integrità e riservatezza»).

Sicurezza dei dati

Il Titolare del Trattamento s'impegna ad adottare, nei limiti del possibile, le misure di sicurezza necessarie e adeguate affinché i dati e le informazioni personali siano protetti da perdita, uso improprio, accesso non autorizzato, divulgazione, alterazione o distruzione oltre che le ragionevoli verifiche affinché tali misure risultino costantemente aggiornate.

In base a quanto disposto dagli articoli 24 e 32 del Regolamento, il Titolare del Trattamento ha adottato un programma di sicurezza che prevede l'adozione di misure in linea con i seguenti principi:

- garantire che siano trattati i dati personali per impostazione predefinita necessari per ogni specifica finalità del trattamento (Security e Privacy by Default - art. 25 GDPR);
- attuare in modo efficace i principi di protezione dei dati e integrare nel trattamento fin dalla progettazione le necessarie garanzie al fine di tutelare i diritti degli interessati (Security e Privacy by Design - art. 25 GDPR);
- assicurare, in caso di violazione dei dati personali, la comunicazione verso gli interessati e il Garante Privacy nei modi e nei tempi del Regolamento;
- effettuare per quei trattamenti che presentano rischi elevati per i diritti e la libertà degli interessati la valutazione d'impatto nei modi e nei tempi previsti dal Regolamento;
- garantire adeguata formazione specialistica sulle tematiche di sicurezza IT;
- adottare misure tecniche, organizzative e di sicurezza adeguate, nonché adeguati meccanismi di controllo della costante conformità di tali misure nel tempo e ne dispone il costante aggiornamento (Accountability - Art. 5 GDPR);
- documentare le attività svolte per garantire che i trattamenti siano effettuati in conformità alla normativa applicabile e tiene tale documentazione a disposizione per eventuali accessi del Garante (Accountability - Art. 5 GDPR).

Sistemi di autenticazione informatica

Il Titolare del Trattamento adotta credenziali di autenticazione che consistono in un codice per l'identificazione dell'utente (UserID) associato a una parola chiave riservata conosciuta solamente dal medesimo (password). A ogni utente sono assegnate e associate individualmente una o più credenziali per l'autenticazione.

Segretezza e custodia delle credenziali di autenticazione

Il Titolare del Trattamento invita gli utenti a conservare con la massima riservatezza le proprie credenziali di autenticazione e a non condividerle con altri utenti. Tutti gli utenti sono responsabili del corretto e lecito utilizzo delle di credenziali di autenticazione assegnate.

Password

Il Titolare del Trattamento utilizza password composte almeno da un numero di caratteri non inferiore da quello richiesto, volta per volta, per legge e con caratteristiche tali da rendere difficoltoso l'eventuale tentativo di individuazione.

Disattivazione delle credenziali di autenticazione

Il Titolare del Trattamento assicura che le credenziali di autenticazione sono disattivate in caso di mancato utilizzo per un periodo temporale di almeno 6 mesi. La disattivazione delle credenziali avviene anche nel caso in cui il possessore non abbia più necessità di utilizzarle a causa del cambiamento delle proprie mansioni lavorative ovvero dell'interruzione del rapporto di lavoro.

Firewalling e software antivirus

Tutti i dispositivi sono dotati di software antivirus aggiornato allo scopo di limitare il rischio di intrusione di virus e di programmi dannosi.

Aggiornamento dei programmi per elaboratore

Il Titolare del Trattamento provvede periodicamente all'installazione degli aggiornamenti per risolvere le problematiche emerse nel rispetto delle indicazioni e delle politiche in uso.

Backup e ripristino dei dati

Il Titolare del Trattamento attua azioni in grado di garantire la disponibilità delle informazioni in linea con le prescrizioni di legge, nonché verifiche periodiche dell'effettiva leggibilità e integrità delle informazioni salvate.

Strumenti elettronici per la protezione da accessi abusivi

La rete informatica utilizzata, sia internamente che per il collegamento al Data Center ove risiedono gli strumenti elettronici di trattamento dei dati, sia del Titolare del Trattamento stesso che dei propri clienti, è protetta da specifici strumenti quali firewall, sistemi di Intrusion prevention e detection, in grado di ridurre il rischio di accessi abusivi.

Supporti removibili

Il Titolare del Trattamento adotta specifici protocolli per la custodia, cancellazione e distruzione sicura sia dei supporti removibili utilizzati per il salvataggio o il trasferimento di dati personali sia degli elaboratori, fissi e portatili, dismessi o non più utilizzati.

Analisi dei rischi

L'adeguatezza delle misure di sicurezza adottate e riportate al paragrafo precedente è stata valutata mediante una specifica procedura di analisi dei rischi, la quale prevede di fare una valutazione del livello di rischio al quale ogni trattamento incluso nel Registro dei trattamenti, è soggetto, sulla base delle possibili minacce e dei relativi impatti.

Conservazione dei dati

Il Titolare del Trattamento adotta le misure per conservare le informazioni personali solo per il tempo necessario a soddisfare gli scopi per cui sono stati raccolti e comunque in maniera non eccedente rispetto a quanto richiesto da obblighi di legge. I dati personali pertanto possono essere oggetto di conservazione, sia analogica che digitale, solo per il tempo previsto dalla normativa vigente e successivamente sottoposti a scarto d'archivio e distruzione.

I tempi di conservazione saranno regolati da idonee procedure operative e comunicati agli Interessati da apposite informative e secondo le indicazioni contenute in Provvedimenti del Garante ovvero indicate dalla normativa in vigore.

Violazione dati personali

Il Titolare del Trattamento, qualora ritenga che sia avvenuta una violazione di dati personali e che sia probabile che da tale violazione possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione:

- al Garante Privacy, nel caso in cui sia Titolare del trattamento
- al Titolare del trattamento, nel caso in cui sia stato nominato Responsabile del trattamento.

La notifica avviene senza ingiustificato ritardo, entro i tempi previsti dal Regolamento e secondo una specifica procedura operativa interna.

Per violazione dei dati personali si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dalla società.

I principali rischi per i diritti e le libertà degli interessati conseguenti a una violazione, in conformità al considerando 75 del GDPR, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale.
- decifrazione non autorizzata della pseudonimizzazione (quando prevista);
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (dati doganali).

7. DIRITTI DEGLI INTERESSATI

I diritti attribuiti dal GDPR agli interessati si dividono in due categorie: (1) i diritti che necessitano di una richiesta espressa dell'interessato; (2) i diritti ai quali la normativa collega un obbligo del titolare in modo autonomo dalla ricezione di una previa richiesta dell'interessato.

I diritti subordinati a una richiesta espressa dell'interessato (Artt. 15- 21 GDPR)

Il processo per la gestione dei diritti esercitati dagli Interessati mediante espressa richiesta è riconducibile alle seguenti fasi principali:

- ricezione della richiesta;
- gestione della richiesta;
- riscontro all'interessato e archiviazione.

Le modalità di gestione del predetto processo sono disciplinate nell'apposita Procedura tempo per tempo aggiornata e pubblicata nel Documentale.

I principali diritti che il GDPR garantisce all'interessato e che lo stesso può esercitare mediante richiesta sono i seguenti:

- **Diritto di Accesso:** l'Interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di Dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai Dati personali che comprendono i Dati personali conferiti dall'Interessato, i Dati personali osservabili generati in esecuzione del contratto, i termini del trattamento compreso il periodo di conservazione previsto.
- **Diritto di Rettifica:** l'Interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei Dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'Interessato ha il diritto di ottenere l'integrazione dei Dati personali incompleti, anche fornendo una dichiarazione integrativa.
- **Diritto di Cancellazione:** l'Interessato ha il diritto di ottenere dal titolare del trattamento, se sussistono i motivi indicati dal GDPR, la cancellazione dei Dati personali che lo riguardano senza ingiustificato ritardo e il Titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i Dati personali, salvo che ne sia impedito dall'obbligo di espletamento di tutti gli adempimenti di legge.
- **Diritto di limitazione di trattamento:** l'Interessato ha il diritto di ottenere dal Titolare del trattamento la limitazione del trattamento quando si verificano le ipotesi previste dall'art. 18 del GDPR;
- **Diritto di Opposizione / Revoca:** l'Interessato ha il diritto di opporsi o revocare il consenso in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei Dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del GDPR, compresa la profilazione. Il Titolare del trattamento si astiene dal trattare ulteriormente i Dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento,

l'esercizio o la difesa di un diritto in sede giudiziaria.

- **Diritto alla Portabilità:** L'Interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i Dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali Dati a un altro titolare del trattamento senza impedimenti da parte del Titolare del trattamento cui li ha forniti qualora il trattamento è effettuato con mezzi automatizzati.

Infine, nel caso di esercizio dei diritti di rettifica, cancellazione e/o limitazione del trattamento da parte dell'Interessato, il Titolare provvede anche a effettuare la comunicazione ai destinatari interessati prevista dall'articolo 19 del GDPR.

I diritti non subordinati a una richiesta dell'interessato

Pur in assenza di richiesta da parte dell'Interessato, il Titolare garantisce che allo stesso sia fornita idonea informativa al momento della raccolta dei suoi Dati personali presso lo stesso o, se i Dati non sono raccolti direttamente presso l'Interessato, entro i seguenti termini:

- entro un termine ragionevole dall'ottenimento dei Dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i Dati personali sono trattati;
- nel caso in cui i Dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato;
- nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei Dati personali.

Esercizio dei diritti dell'Interessato e tempi di riscontro

L'Interessato ha la facoltà di esercitare i propri diritti secondo le modalità e nei limiti previsti dal GDPR. Il Titolare del Trattamento si impegna a fornire all'Interessato le informazioni relative all'azione intrapresa riguardo a una richiesta senza ingiustificato ritardo dal ricevimento della richiesta stessa. Apposite procedure sono in essere per la gestione delle richieste. Se la richiesta dell'Interessato sarà presentata mediante mezzi elettronici, le informazioni saranno fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'Interessato.

Tali diritti possono essere esercitati dall'Interessato attraverso l'invio di una mail all'indirizzo indicato al termine del presente documento oppure tramite comunicazione scritta, specificando l'oggetto della richiesta, all'attenzione dell'Amministrazione, domiciliato presso la sede.

Una volta ricevuta la richiesta, **Il Titolare del trattamento dati** non può rifiutarsi di soddisfare la richiesta dell'Interessato, salvo che dimostri di non essere in grado di identificare l'interessato.

8. CONTROLLO E CONFORMITÀ

Il Titolare del Trattamento ha stabilito procedure per controllare il rispetto dei principi previsti dal Regolamento. È responsabilità di tutto il personale conoscere, comprendere e rispettare questa Politica e i suoi contenuti. La mancata osservanza potrebbe comportare rischi significativi per il Titolare del Trattamento e può subordinare ciascun individuo ad azioni disciplinari, fino al licenziamento o all'interruzione del rapporto professionale.

9. DATI DI CONTATTO

Domande o dubbi sull'interpretazione o sulle modalità di applicazione della presente *Policy* possono essere rivolti scrivendo al seguente indirizzo e-mail: elena.reja@elatos.net