# MODELLO ORGANIZZATIVO
# PRIVACY

## AI SENSI DEL REGOLAMENTO n. 679/2016/UE (GDPR)

Sommario

Technogenetics S.p.A. P.IVA 09279340153, con sede legale in Milano, Via Privata Cesare Battisti n. 1 CAP 20122

# Introduzione

### Ambito di applicazione e scopo

Con l'adozione di questo documento si intende richiamare tutte le risorse operanti all'interno dell'azienda al rispetto della normativa sulla sicurezza dei dati personali, con espressa attenzione all'impiego delle risorse informatiche.
Periodicamente, il MOP (Modello Organizzativo Privacy) viene aggiornato in relazione alla evoluzione della disciplina ovvero di modifiche gestionali e/o organizzative che impattino su di esso.
Questo documento è vincolante per il personale dell'azienda, sia dipendente sia collaboratore.
Si precisa che la commissione di illeciti rientranti nella nozione di cybercrime può comportare, oltre alla responsabilità penale personale, anche la responsabilità della Technogenetics Spa che pertanto, di ciò consapevole, attuerà, in conformità alle proprie politiche ed alle norme e prassi applicabili nel settore (Regolamento UE 2016/679 - GDPR e prescrizioni del Garante per il trattamento dei dati personali, e D.lgs. 231/2001) tutte le precauzioni reputate opportune per evitare la commissione di reati informatici o ridurne le conseguenze.
La presente Policy si applica alla Technogenetics Spa nelle attività di trattamento di dati personali nel corso dello svolgimento della propria attività di business (Biotecnologie e Diagnostica).
Lo scopo del presente documento è quello di disciplinare le attività di trattamento di dati personali all'interno della Società I Girasoli S.r.l., al fine di garantire la piena conformità alle disposizioni dettate dal Regolamento Europeo n. 2016/679 (GDPR).

### Responsabilità

Tutti i soggetti coinvolti nel trattamento di dati personali devono contribuire alla protezione dei dati personali dando applicazione alla presente Policy ed ai "*Privacy Principles*" di seguito indicati.
La presente Policy potrà venire implementata e integrata, ove necessario, a seguito di indicazioni da parte della Technogenetics Spa e/o dei propri consulenti.

# PRIVACY PRINCIPLES

**Trattamento e finalità**

Technogenetics Spa tratta i dati personali in modo lecito, corretto e trasparente, per il raggiungimento delle finalità di business che siano determinate, esplicite e legittime ed adotta misure ragionevoli per garantire che i dati personali siano esatti e, se necessario, aggiornati.

**Terze parti**

Le Terze Parti (fornitori, business partner, consulenti) che svolgono attività di supporto di qualsiasi tipo per l'offerta di beni e servizi nei confronti della Technogenetics Spa, in relazione alle quali effettuano operazioni di trattamento di dati personali per conto della stessa, sono designate Responsabili del trattamento e sono contrattualmente vincolate al rispetto delle misure per la sicurezza e la riservatezza dei dati, nonché ad astenersi da qualunque utilizzo o divulgazione che non sia autorizzata dalla Technogenetics Spa

La Technogenetics Spa attribuisce particolare importanza alla protezione della riservatezza dei dati personali, sollecitando il contributo di tutti i collaboratori nel raggiungimento di tale obiettivo.

**Comunicazione dei dati personali**

I dati personali conferiti possono essere comunicati a soggetti terzi per adempiere ad obblighi di legge, in esecuzione di ordini provenienti da pubbliche autorità ovvero per fare valere o difendere un diritto in sede giudiziaria, nonché per necessità di business e per fini amministrativi interni, compreso il trattamento dati personali di clienti, fornitori e dipendenti.

I dati personali possono essere comunicati a soggetti terzi, in qualità di autonomi Titolari del trattamento o di Responsabili del trattamento, con il consenso degli Interessati, se richiesto per legge, e comunque previa adeguata informativa volta a specificare le finalità del trattamento. I dati personali non sono diffusi.

In particolare, i dati personali comunicati dai clienti vengono trattati dalla Technogenetics Spa per il corretto espletamento degli adempimenti contrattuali e/o di legge.

Inoltre, i dati personali acquisiti dai clienti vengono trattati dalla Technogenetics Spa per adempiere all'obbligo previsto dal "Testo unico delle leggi di pubblica sicurezza" (articolo 109 R.D. 18.6.1931 n. 773) che impone di comunicare alla Questura, per fini di pubblica sicurezza, le generalità dei soggiornanti secondo le modalità stabilite dal Ministero dell'Interno. I dati acquisiti per tale finalità saranno conservati presso la sede operativa, Via della Filanda 24-26, 26900, Lodi, ovvero mediante un sistema in cloud.

Peraltro, i Dati dei clienti verranno raccolti anche per legittimo interesse del titolare.

Il conferimento dei Dati per le finalità sopra evidenziate è necessario (i) per l'assunzione dei dipendenti, per partecipare alle gare, per comprare e vendere prodotti da fornitori e/o clienti e (ii) per adempiere ai fini di pubblica sicurezza. A tal proposito, sussiste un obbligo di fornire tali Dati per il conseguimento della finalità di cui sopra; il loro mancato, parziale o inesatto conferimento potrebbe avere come conseguenza l'impossibilità dell'erogazione dei servizi.

**Conservazione**
I dati personali sono conservati solo per il tempo necessario a raggiungere le finalità per le quali sono stati raccolti o in conformità ai termini previsti per legge o necessari per far valere un diritto in sede giudiziaria. I dati personali sono conservati in conformità alle normative vigenti.

**Rapporti di lavoro**
Con riferimento ai dati trattati nello svolgimento dei rapporti di lavoro, la Technogenetics Spa utilizza i dati personali solo per il raggiungimento delle finalità connesse (quali, ad esempio, esecuzione del rapporto di lavoro; payroll, benefits, adempimenti fiscali, assistenziali e previdenziali, igiene e sicurezza sul lavoro; attività formative e di sviluppo della carriera, valutazione delle performance; utilizzo di dati personali, incluse immagini fotografiche e video, per scopi istituzionali).

**Attività commerciali e di marketing**
Nel rispetto dei principi di liceità, correttezza e trasparenza, e con il previo consenso degli Interessati se richiesto per legge, la Technogenetics Spa può trattare dati personali per il raggiungimento di finalità commerciali e di marketing (quali, ad es., invio di materiale pubblicitario e altre iniziative promozionali e di marketing; attività di vendita diretta, ed elaborazioni statistiche).

**Sicurezza**
Technogenetics Spa adotta tecnologie sicure e ragionevoli precauzioni per proteggere i dati personali contro l'indebita divulgazione, alterazione o uso improprio. Le protezioni attivate si propongono, in particolare, di ridurre al minimo i rischi di distruzione e di perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
Technogenetics Spa adotta attività periodiche di analisi dei rischi per verificare l'aderenza agli standard di sicurezza definiti ed eventualmente adottare nuove misure di sicurezza a seguito di cambiamenti organizzativi ed innovazioni tecnologiche o cambiamenti nella tipologia dei dati raccolti. Le misure di sicurezza sono costantemente controllate e periodicamente verificate.

**Assesment**
Technogenetics Spa effettua una periodica autovalutazione al fine di verificare che la presente Policy venga effettivamente applicata e che tutte le persone all'interno della società si conformino ai presenti Principles.

**Compliance**
Nella definizione dei Privacy Principles, la Technogenetics Spa si conforma al Regolamento europeo n. 679/2016 e, in generale, alle leggi ed ai regolamenti applicabili che tutelano la riservatezza dei dati personali.

**Contatto**
Per qualsiasi domanda e/o dubbio riguardante l'applicazione della presente Policy, si invita a contattare il seguente indirizzo mail privacy@technogenetics.it

## 1. Obiettivi

Il Regolamento europeo n. 679/2019 (GDPR) ha introdotto il principio di accountability o di "rendicontazione" ("responsabilizzazione", nella versione italiana del Regolamento), in virtù del quale il Titolare del trattamento è chiamato a porre in essere misure tecniche ed organizzative adeguate non solo a garantire che il trattamento sia effettuato in conformità alle disposizioni del Regolamento, ma altresì a consentire allo stesso Titolare di dimostrare tale conformità (cfr. art. 24, par. 1, del GDPR). Per tale ragione, la Technogenetics Spa si è dotata di un Sistema di Gestione della Data Protection che viene quindi richiamato nel presente MOP, che si fonda su un preliminare processo di risk assessment finalizzato alla valutazione del "rischio privacy", ovverosia l'eventuale impatto negativo sulle libertà e i diritti degli interessati - connesso alle attività di trattamento di dati personali effettuate.
Essa ha pertanto intrapreso un progetto di analisi dei dati personali trattati e dei propri strumenti organizzativi, di gestione e di controllo volto a verificare la rispondenza dei principi comportamentali, delle procedure e/o delle prassi organizzative in essere ai principi, regole e finalità dettati dal Regolamento UE e, ove necessario, ad integrare le misure di sicurezza organizzative e tecniche per assicurarne l'adeguatezza, tenuto conto del contesto di riferimento.
Attraverso l'adozione del Sistema di Gestione della Data Protection, la Technogenetics Spa intende quindi:

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

A tal fine, il presente Modello organizzativo privacy enuclea i principi comportamentali ed indica le misure necessarie per assicurare che i processi aziendali che implichino un trattamento di dati personali siano gestiti in modo tale da intercettare e tempestivamente governare eventuali situazioni di rischio per la privacy degli interessati e, in ogni caso, garantire il puntuale e costante rispetto della disciplina europea e nazionale di riferimento.

**Principali definizioni ai sensi del regolamento UE n. 679/2016 (GDPR)**

**Titolare del Trattamento:** All'art. 4, par. 1, n. 7), il GDPR definisce «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; 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:** Il GDPR – all'art. 4, par. 1, n. 8) - definisce il «responsabile del trattamento» come «la persona fisica, giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

**Addetti al Trattamento:** le persone fisiche autorizzate a compiere operazioni di trattamento da titolare o dal responsabile.

**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.

**Interessato:** la persona fisica a cui si riferiscono i dati personali (tutti noi siamo interessati).

**Destinatario:** la persona fisica o giuridica, l'autorità pubblica; il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

**Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

**Dato sensibile:** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale.

**Dato giudiziario:** i dati personali idonei a rivelare informazioni in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti; o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

**Dati genetici:** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia, sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

**Dati biometrici:** 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.

**Trattamento Dati:** 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.
**Autorità di controllo:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.
**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 i dati personali non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
**Stabilimento principale:** per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione Europea, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione Europea e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione Europea o, se il responsabile del trattamento non ha una sua amministrazione centrale nell'Unione Europea, lo stabilimento del responsabile del trattamento nell'Unione Europea in cui sono condotte le principali attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto ad obblighi specifici ai sensi del regolamento.
**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.

**Principi generali adottati dall'organizzazione**
Technogenetics Spa è tenuta a garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

**Obblighi di sicurezza**
Technogenetics Spa è tenuta a garantire che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base allo stato dell'arte e all'avanzamento tecnologico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al

minimo, mediante l'adozione di idonee misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

**Misure di Sicurezza Idonee**

Technogenetics Spa è tenuta ad adottare un complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza per assicurare un livello idoneo di protezione dei dati personali sia nel caso di trattamenti con strumenti elettronici sia per trattamenti senza l'ausilio di strumenti elettronici.

## 2. Dati Generali

Di seguito si riporta uno schema grafico relativo alle principali figure e ruoli aziendali in tema di privacy.

**Titolare del trattamento**

Technogenetics Spa, nello svolgimento delle attività che comportano il trattamento di dati personali, agisce quale Titolare del trattamento.

Nello specifico, l'elenco del trattamento di dati personali effettuato da Technogenetics Spa in qualità di Titolare del trattamento è elencato nel Registro del trattamento che essa ha provveduto a redigere e tiene in conformità a quanto previsto dall'art. 30 del GDPR.

Technogenetics Spa - quale Titolare del trattamento - opera osservando quanto stabilito nel presente Modello e, in ogni caso, nel rispetto delle previsioni del GDPR e della normativa nazionale di adeguamento al duplice fine di garantire la protezione dei dati personali oggetto di trattamento e di essere in grado di dimostrare che quest'ultimo sia effettuato conformemente alla disciplina di settore.

**Responsabili del trattamento per conto della società**

Il GDPR – all'art. 4, par. 1, n. 8) - definisce il «responsabile del trattamento» come «la persona fisica, giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

In base al successivo art. 28 del GDPR, qualora un trattamento sia effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino sufficienti garanzie per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.

L'art. 28 del GDPR statuisce inoltre che «i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento».

L'art. 28 del GDPR statuisce inoltre che «i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia

disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento».
Il contratto o atto giuridico in questione dovrà prevedere in particolare – in relazione al responsabile del trattamento – quanto stabilito dall'art. 28, par. 3, del GDPR.
Responsabili del trattamento dei dati sono i soggetti con responsabilità individuale sulle rispettive banche dati. Le responsabilità sono indicate per iscritto nelle relative lettere di nomina.

**Incaricati del trattamento**
Il GDPR menziona le persone autorizzate al trattamento dei dati personali nell'art. 4, par. 1, n. 10 (vale a dire nella definizione di «terzo», identificato con 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) e, soprattutto, nell'art. 29, che, rubricato "Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento", prevede che «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».
In base a quanto previsto da ultimo dal D.Lgs. 10 agosto 2018, n. 101, il vigente D.Lgs. n. 196 del 2003, all'art. 2-quaterdecies, rubricato "Attribuzioni di funzioni e compiti", stabilisce che «1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. 2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta».
La persona autorizzata è, in sintesi, colui che effettua materialmente le operazioni di trattamento sui dati personali.
É fondamentale tenere presente che, in assenza di nomina/autorizzazione, qualsiasi operazione svolta dai dipendenti o collaboratori del Titolare o del Responsabile sui dati personali di cui trattasi sarà qualificabile come trattamento effettuato da terzi. La normativa non prevede requisiti quantitativi, per cui anche la semplice consultazione di un dato personale potrà integrare gli estremi di un trattamento, con conseguente necessità di una autorizzazione allo stesso affinché possa considerarsi lecito.
Technogenetics Spa – in compliance con la normativa in materia di tutela dei dati personali – formalizza la "nomina" dei propri dipendenti a persone autorizzate al trattamento dei dati personali ai sensi e per gli effetti degli artt. 4 e 29 del GDPR, fornendo all'uopo le opportune istruzioni ed assicurandone l'adeguata formazione in materia.
In conformità al principio di minimizzazione dei dati, l'autorizzazione è comunque limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento. Le autorizzazioni all'accesso sono rilasciate e revocate dal titolare e/o dal Responsabile che periodicamente, e comunque almeno una volta l'anno, provvedono alle opportune verifiche in ordine al perdurare delle condizioni alla base dell'autorizzazione.
Gli incaricati del trattamento sono designati dal titolare del trattamento con atto di nomina scritto, controfirmato. Le responsabilità sono indicate per iscritto nella lettera di nomina o in altri documenti.

Gli Incaricati del trattamento hanno ricevuto idonee ed analitiche istruzioni, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti. Agli incaricati sono state assegnate credenziali di autenticazione ed individuati i profili di autorizzazione in funzione dei dati che possono trattare, delle operazioni da essi eseguibili e dei trattamenti loro consentiti.
Copia delle nomine è conservata a cura titolare del trattamento in luogo sicuro all'interno dell'Ufficio Risorse Umane.
La nomina degli Incaricati è a tempo indeterminato e decade per revoca, per loro dimissioni o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.
In ogni caso, l'ambito di trattamento consentito agli incaricati del trattamento ed il relativo profilo di autorizzazione sono verificati dal titolare del trattamento e/o dall'amministratore di sistema con cadenza almeno annuale.
Per un dettaglio della distribuzione dei compiti si rimanda al Registro del trattamento dei dati da cui è possibile rilevare le operazioni di trattamento consentite a ciascuno, i tipi di dati a cui è consentito l'accesso e l'ufficio di riferimento.
La Società si è altresì dotata del "Regolamento per l'utilizzo delle risorse informatiche e di comunicazione", che è stato adeguato ai sensi della normativa privacy ed in seguito all'entrata in vigore del GDPR, viene consegnato ai dipendenti incaricati del trattamento contestualmente all'assunzione in forma cartacea.

**Amministratore di sistema**
L'Amministratore di Sistema è una figura soggettiva che non viene contemplata dal GDPR. Parimenti, essa non era menzionata nel previgente Codice in materia di protezione dei dati personali, ma solamente nell'Allegato B al Codice medesimo, peraltro abrogato a seguito dell'entrata in vigore del recente D.Lgs. n. 101 del 2018.
In data 27 novembre 2008, tuttavia, l'Autorità Garante ha emanato uno specifico provvedimento, aggiornato nel 2009, intitolato "Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema". Esso continua ad applicarsi, in quanto compatibile con il GDPR e con le disposizioni del novellato Codice Privacy.
Ai sensi e per gli effetti del citato provvedimento, rientrano nella definizione di "amministratore di sistema" non solo «[…] le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti», ma «[…] anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi».
L'Amministratore di Sistema è pertanto la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi - quali i sistemi ERP (Enterprise Resource Planning) - utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.
Non rientrano invece nella definizione soprariportata quei soggetti che solo occasionalmente intervengono (per esempio per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi software.
Alla data di redazione del presente documento gli Amministratori di Sistema sono individuati come nell'allegato A al presente MOP.

**Finalità del trattamento**

Le finalità del trattamento dei dati effettuati da Technogenetics Spa in proprio o per suo conto risultano censite nel dettaglio nell'apposito Registro trattamento dei dati e nei verbali/report di risk assessment periodicamente redatti dalla Funzione di Internal Audit, da intendersi qui richiamati.

Al fine di perseguire le finalità connesse con l'attività di business svolta, la predetta società tratta dati personali - sia comuni sia sensibili per talune categorie di interessati - di fornitori, clienti e dipendenti.

Ciò premesso, i trattamenti effettuati, sia con strumenti elettronici sia manualmente, attengono in generale alle seguenti finalità di carattere gestionale:

- trattamento giuridico ed economico del personale, sua selezione e organizzazione delle attività, adempimenti previdenziali ed assistenziali, adempimenti connessi con l'iscrizione a sindacati da parte dei dipendenti;
- adempimenti di obblighi fiscali e contabili, nonché adempimenti in osservanza di altre norme, regolamenti o normativa comunitaria;
- gestione della clientela e dei fornitori (contratti, ordini, pagamenti e incassi, spedizioni e ricezione merci, verifica solvibilità e affidabilità finanziaria). Inoltre, i dati personali acquisiti dai clienti vengono trattati dalla Technogenetics Spa per adempiere all'obbligo previsto dal "Testo unico delle leggi di pubblica sicurezza" (articolo 109 R.D. 18.6.1931 n. 773) che impone di comunicare alla Questura, per fini di pubblica sicurezza, le generalità dei soggiornanti secondo le modalità stabilite dal Ministero dell'Interno. I dati acquisiti per tale finalità saranno conservati presso l'Ufficio Risorse Umane, ovvero mediante un sistema in cloud;
- tutela del legittimo interesse del titolare del trattamento.

Le finalità specifiche di trattamento dei dati da parte di Technogenetics Spa sono dettagliate nell'apposita informativa ex art. 13 Reg.to EU n. 679/16 che la Società mette a disposizione sul proprio sito internet. Clienti e fornitori devono prendere visione dell'informativa e dare comunicazione di accettazione nella modulistica che ricevono al primo contatto con Technogenetics Spa.

I dipendenti firmano l'informativa privacy che viene fornita insieme al contratto.

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, gli amministratori di sistema hanno valutato la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati.

In ogni caso i dati vengono salvati in parte attraverso un sistema di cloud (per ciò che riguarda i dati ottenuti e caricati sul software gestionale) ed in altra parte mediante NAS.

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita di dati a causa di virus informatici, gli amministratori di sistema hanno stabilito gli strumenti di prevenzione e le norme di utilizzo dei sistemi da adottare.

La soluzione adottata garantisce un aggiornamento costante rapido della base dati che consente l'identificazione di virus e malware.

Viene inoltre effettuato un regolare aggiornamento di tutte le soluzioni software adottate, in particolar modo per tutti gli aggiornamenti legati alla sicurezza.

I criteri sono stati definiti anche in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

Nel caso in cui su uno o più sistemi si dovesse verificare perdita di informazioni o danni a causa di contagio da virus informatici si provvede a:

- Isolare il sistema;
- Verificare se ci sono altri sistemi infettati con lo stesso virus informatico;
- Bonificare il sistema infetto;
- Valutare la necessità di ripristinare i dati dal back up più recente;
- Dell'incidente viene tenuta traccia in un apposito registro.

È fatto divieto a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni;
- Effettuare copie fotostatiche o di qualsiasi altra natura, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento;
- Sottrarre, cancellare, distruggere stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento;
- Consegnare a persone non autorizzate dal Responsabile del trattamento dei dati stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

Il Titolare del trattamento e gli Amministratori di sistema, come indicati nell'allegato A, sono gli unici soggetti autorizzati ad accedere ai locali in cui sono presenti sistemi o apparecchiature di gestione e memorizzazione dei dati trattati, ovvero ai locali del Reparto Information Technology (IT),

In particolare, la sala server (ubicata al primo piano) è sistematicamente chiusa e accessibile solo tramite l'utilizzo di un badge in possesso agli amministratori di sistema. Il locale rispetta le prescrizioni della normativa antincendio vigente.

Gli amministratori di sistema, preposti all'area dei sistemi informativi, verificano, con cadenza settimanale, tramite appositi tool di monitoraggio, la funzionalità dei sistemi con cui vengono trattati i dati. La verifica ha lo scopo di controllare l'affidabilità dei sistemi, per quanto riguarda:

- La sicurezza dei dati trattati;
- Il rischio di distruzione o di perdita;
- Il rischio di accesso non autorizzato o non consentito;
- Il loro adeguato funzionamento anche in relazione all'evoluzione tecnologica.

Nel caso in cui esistano rischi evidenti, gli Amministratori di sistema devono informarne il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

Sono previste anche preventive misure di sicurezza qualora siano necessari interventi di manutenzione. Per scongiurare il caso di distruzione o danneggiamento, gli Amministratori di sistema vigilano sulla corretta gestione dei sistemi archiviazione dei dati.

Il processo di backup viene schedulato sulla base di un piano predisposto dagli amministratori di sistema che identificano le banche dati, gli archivi e i dati da copiare e i tempi nei quali effettuare l'operazione per non danneggiare l'operatività dei sistemi.

**Trattamenti affidati all'esterno**

Il Titolare del trattamento, relativamente ad alcuni trattamenti di dati, ha affidato la loro gestione a soggetti esterni designandoli formalmente con apposita lettera di nomina. In particolare, il Titolare del trattamento può decidere di affidare il trattamento dei dati in tutto o in parte a soggetti terzi, in outsourcing, nominandoli Responsabili esterni del trattamento, ai sensi dell'art. 28 GDPR. In questo

caso sono specificati nell'atto di nomina i soggetti interessati e i luoghi dove fisicamente avviene il trattamento dei dati stessi.
Nel caso i soggetti terzi che operano in outsourcing non vengano nominati espressamente come Responsabili esterni del trattamento, essi devono intendersi autonomi Titolari del trattamento e quindi soggetti ai relativi obblighi, e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni di legge.

**Procedura per l'accesso, la conservazione e la cancellazione**
Technogenetics Spa ha predisposto un'apposita procedura di esercizio dei diritti degli interessati, adottandola e diffondendola mediante apposita informativa a terzi.
La Procedura di esercizio dei diritti degli interessati comprende: la richiesta di esercizio dei diritti; la risposta in accettazione/diniego alla richiesta di esercizio suddetta.
In particolare, gli interessati possono richiedere la cancellazione senza ingiustificato ritardo dei dati personali o la limitazione del trattamento dei dati personali che li riguardano per i seguenti motivi:

- perché i dati non sono più necessari per la finalità per i quali erano stati raccolti;
- perché l'interessato ha revocato il consenso al trattamento dei dati;
- perché l'interessato si oppone al trattamento;
- perché i dati sono trattati illecitamente.

Technogenetics Spa ha previsto quindi che nei casi sopra citati il termine ultimo per la cancellazione sia di massimo 10 giorni lavorativi dal ricevimento della relativa richiesta da parte dell'interessato.
Sulle suddette procedure è stata svolta la formazione all'interno dell'organizzazione del titolare, come infra dettagliato.
Come già specificato, tutti i dati trattati sono accessibili al solo personale debitamente formato e autorizzato con apposita lettera di nomina e vengono gestiti elettronicamente. A livello cartaceo sono riposti in archivi specifici divisi per categoria di interessato; quindi, il Titolare del trattamento dei dati ha istruito il personale di riferimento sulla comunicazione immediata dei dati qualora ne venga fatta la richiesta da un interessato.
In tal senso viene consentito agli interessati di accedere ai propri dati per:

- Modificarli nel caso divengano inesatti;
- Integrarli anche con dichiarazione integrativa;
- Richiederne la cancellazione.

**Accesso ai dati personali:** l'accesso ai dati personali è libero per gli autorizzati al trattamento dei dati per quanto di loro competenza. È vietato, salvo comprovate esigenze di natura straordinaria, l'accesso ai dati personali nei confronti di soggetti non autorizzati al trattamento dei dati.

**Accesso ai dati sensibili o giudiziari:** l'accesso agli archivi contenenti dati sensibili o giudiziari è consentito esclusivamente al titolare del trattamento ed all'amministratore di sistema.

**Dati sanitari e/o comunque sensibili dei clienti:** eventuali dati sanitari e/o comunque sensibili comunicati all'Ufficio Risorse Umane, dai dipendenti e/o dal medico del lavoro, saranno trattati nel massimo rispetto della privacy e della riservatezza. La documentazione in formato cartaceo è riposta

in archivio, chiuso a chiave, nell'Ufficio Risorse Umane. Le idoneità mediche vengono inserite, in formato digitale, dallo stesso dottore all'interno di apposito gestionale, e sono accessibili solo dall'Ufficio Risorse Umane tramite password.

**Conservazione dei dati:** Il GDPR, include la "limitazione della conservazione" tra i principi fondamentali per il trattamento dei dati personali.

I dati personali "[…] 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 personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato" (art. 5, comma 1, lettera e), GDPR).

Limitare la conservazione dei dati personali al minimo periodo necessario permette di ridurre il rischio che questi diventino inaccurati, obsoleti o irrilevanti. Per questo motivo, il Titolare è tenuto a prevedere un tempo massimo di conservazione adeguato e limitato alle finalità del trattamento stesso.

La limitazione della conservazione è anche strettamente collegata al principio di minimizzazione del trattamento dei dati personali, che stabilisce che i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (art. 5, comma 1, lettera c), GDPR) ed al principio dell'esattezza, ai sensi del quale i dati devono essere esatti, aggiornati e devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (art 5, comma 1, lettera d), GDPR).

In ogni caso, Technogenetics Spa, conserverà i dati degli interessati in una forma che consenta l'identificazione degli stessi per un arco temporale non superiore al conseguimento delle finalità per le quali sono stati raccolti.

Technogenetics Spa ha adottato le procedure e policy necessarie per rispondere adeguatamente ai requisiti resi obbligatori dal contesto giuridico, tra i quali:

- prevedere, coerentemente alle previsioni dell'art. 13, comma 2, lettera a) GDPR, l'obbligo di informare il soggetto interessato in merito al periodo di conservazione dei dati personali oppure, se non è possibile, circa i criteri utilizzati per determinare tale periodo;
- permettere al Titolare del trattamento di comprovare il rispetto del principio della "limitazione della conservazione", come previsto dall'art. 5 cit., comma 1, lettera e) GDPR ed il rispetto del principio della "responsabilizzazione" (art. 5, comma 2, GDPR). In particolare, tenendo in considerazione il contesto normativo vigente e le peculiarità dei trattamenti effettuati, la policy di data retention ha i seguenti obiettivi:
  i. individuare i criteri per l'identificazione dei periodi di conservazione dei dati personali nell'ambito dei trattamenti effettuati, sia con l'ausilio di strumenti elettronici sia senza l'ausilio degli stessi;
  ii. definire la durata dei periodi di conservazione dei dati personali trattati nello svolgimento delle attività da parte del Titolare del trattamento;
  iii. fornire i requisiti operativi da implementare nei vari processi al fine di garantire l'applicazione della presente policy da parte degli incaricati del trattamento.

Si precisa che i dati strettamente necessari per gli adempimenti fiscali, contabili e per la gestione del rapporto di lavoro, venuta meno la finalità per la quale erano stati raccolti, verranno comunque

conservati per un periodo almeno pari a 10 anni e comunque secondo disposizioni di cui all'art. 22 del DPR n. 600/1973.
In particolare, I Girasoli S.r.l. ha individuato quali soggetti Interessati:

- Soggetti Candidati i cui i dati personali vengono trattati nel processo di ricerca e selezione del personale, dal momento dello screening dei curricula;
- Soggetti Dipendenti in possesso di un contratto di lavoro (a tempo determinato o a tempo indeterminato) o di stage;
- Soggetti Fornitori appartenenti a società terze aventi rapporti contrattuali di fornitura (o assimilabili);
- Soggetti Collaboratori legati alla Società Technogenetics Spa tramite un contratto di collaborazione, tra cui i consulenti esterni;
- Clienti della Società Technogenetics Spa

Per il computo del periodo di conservazione dei dati e per supplire alle carenze e alle lacune normative in materia, uno dei criteri ulteriori utilizzati è rappresentato dall'estensione analogica delle tempistiche di conservazione, atta a disciplinare casi equipollenti e non regolamentati applicando norme previste per fattispecie similari.
Il tempo di prescrizione per la proposizione di azioni giudiziarie (difesa in giudizio) ha costituito ulteriore elemento di valutazione per le categorie di atti passibili di una più consistente probabilità di coinvolgimento in procedure di contenzioso.
I tempi previsti sono riferibili sia a documenti su supporto tradizionale sia a quelli elettronici.
Il periodo temporale massimo indicato deve ritenersi applicabile a tutta la documentazione prodotta a seguito del conferimento dei dati personali e conservata nei luoghi di pertinenza (in caso di conservazione cartacea) o nei server o strumenti informatici (in caso di dati su supporto elettronico) il cui accesso è consentito solo al personale autorizzato dal Titolare del trattamento (incaricati o responsabili).

**Specifiche tempistiche di conservazione**
Di seguito, sono precisati i criteri per la conservazione dei dati personali con riferimento alle categorie precedentemente elencate e alle relative tempistiche individuate.

- Candidati: i dati personali dei candidati non selezionati sono conservati per il periodo strettamente necessario al perseguimento delle finalità di selezione ed assunzione del personale. In particolare, dopo 12 mesi dall'inizio del trattamento, ossia dallo screening dei curricula, dovranno essere cancellati i dati dei candidati in relazione ai quali non vi sia stato alcun evento per l'intero periodo di conservazione previsto (ad es.: modifica di dati personali, fissazione di un colloquio);
- Dipendenti: i dati personali riguardanti i dipendenti della Technogenetics Spa vengono conservati per la gestione del rapporto di lavoro e per l'adempimento degli obblighi di legge. Gli stessi dati saranno conservati per 10 anni successivi al termine del contratto di lavoro al fine di dare corso a richieste di tutela di diritti ed interessi, ad eccezione di particolari trattamenti che possono presentare tempi più stringenti come i dati di formazione e valutazione;
- Fornitori: i dati personali riguardanti i fornitori della Technogenetics Spa devono essere conservati per la gestione del rapporto e per l'adempimento degli obblighi di legge. Gli stessi dati saranno conservati per 10 anni successivi al termine del contratto al fine di dare corso a richieste di tutela di diritti ed interessi;

- Collaboratori: i dati personali riguardanti i collaboratori della Technogenetics Spa devono essere conservati per la gestione del rapporto di collaborazione e per l'adempimento agli obblighi di legge. Gli stessi dati devono essere per 10 anni successivi al termine del contratto di collaborazione al fine di dare corso a richieste di tutela di diritti ed interessi;
- Clienti: i dati personali forniti dai clienti saranno conservati per il periodo di prescrizione previsto dalle disposizioni normative, anche fiscali, applicabili.

**Gestione delle candidature**

Affinché il trattamento dei cv di possibili candidati o stagisti, provenienti da parte di soggetti Terzi (enti o società di reclutamento, enti di formazione o istituti scolastici, ecc.) sia conforme, è necessario che il titolare del trattamento ottenga dal Terzo una dichiarazione che attesti che i dati personali dei candidati sono e saranno raccolti, trattati e comunicati a Technogenetics Spa in conformità alla normativa di cui al GDPR, previa idonea informativa privacy e sempre sul presupposto di una valida base giuridica.

I cv consegnati direttamente dal candidato presso la struttura, non potranno essere accettati e dovrà essere comunicato l'indirizzo di posta elettronica o il sito a cui mandare il cv e presentare la propria candidatura.

I cv pervenuti per mezzo posta cartacea saranno consegnati al responsabile del trattamento designato ovvero al titolare del trattamento.

I cv caricati sul sito ovvero inoltrati alla casella di posta elettronica recruitment@technogenetics.it sono gestiti direttamente dal titolare del trattamento ovvero dagli amministratori di sistema, i quali provvederanno ad archiviare la candidatura ed a vuotare immediatamente la predetta casella mail.

In ogni caso, i cv senza autorizzazione al trattamento dei dati personali non potranno in alcun modo essere trattati.

Al primo colloquio, l'incaricato o il responsabile del trattamento dovrà far firmare al candidato copia della informativa privacy.

I cv dei candidati o stagisti non reclutati saranno distrutti a cura del responsabile del trattamento alla fine della selezione e comunque entro e non oltre 12 mesi.

I cv non potranno essere diffusi o trasmessi a paesi Terzi senza aver informato il candidato e senza aver adottato tutte le misure idonee previste dal Regolamento UE.

**Videosorveglianza**

La Technogenetics Spa, in relazione alle attività di business e alle esigenze di tutela della sicurezza e del patrimonio aziendale, ha provveduto all'installazione di impianti di videosorveglianza presso la propria struttura per finalità di protezione delle persone, della proprietà e del patrimonio aziendale attraverso un sistema di videosorveglianza con telecamere fisse posizionate sulla parete esterna dell'edificio e puntate verso gli ingressi dell'azienda.

Il trattamento rientra nelle finalità di legittimo interesse di tutela delle persone ed i beni rispetto ad atti di vandalismo, furti, rapine, aggressioni, danneggiamenti e per finalità di prevenzione incendi e sicurezza sul lavoro da parte della Società art 6 comma 1 lett. f, Reg. Ue 679/2016. Le immagini registrate sono cancellate dopo 24 ore, salvo festivi o altri casi di chiusura della struttura e comunque non oltre 7 giorni come previsto da normativa. La qualità delle immagini è appositamente degradata, a tutela

delle persone che, passando davanti all'azienda, rientrano nel campo visivo della telecamera. Non sono oggetto di comunicazione a terzi tranne nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

**Sistemi informatici aziendali**

Il personal computer, fisso o mobile, smartphone aziendale ed i relativi programmi e/o applicazioni affidati all'utente sono, come è noto, esclusivamente strumenti di lavoro, pertanto:

- tali strumenti vanno custoditi in modo appropriato;
- tali strumenti possono essere utilizzati solo per fini professionali (in relazione, ovviamente alle mansioni assegnate) e non anche per scopi personali, tantomeno per scopi illeciti;
- debbono essere prontamente segnalati alla Società il furto parziale o totale, il danneggiamento o lo smarrimento di tali strumenti.

Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, elevare i costi di manutenzione e, soprattutto, creare minacce alla sicurezza. Ai fini sopra esposti sono, quindi, da evitare atti o comportamenti contrastanti con le predette indicazioni, attenendosi anche a quanto in seguito esposto.

Per tale ragione, la Società ha approntato il Regolamento Informatico Aziendale, comunicato, accettato e sottoscritto da tutti i lavoratori dipendenti della stessa ed a cui ci si richiama integralmente.

Si evidenzia come a ciascun utente abilitato all'utilizzo dei computer aziendale siano state assegnate delle credenziali personali ed esclusive per accedere al pc. Tali credenziali devono essere custodite dall'utente con la massima diligenza e non divulgate a terzi.

È fatto espresso divieto di accesso al pc da parte di un utente mediante le credenziali di altro utente.

Per evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dei computer, è vietata l'installazione di programmi provenienti dall'esterno.

In particolare, tranne i casi di esplicita autorizzazione della Società, ai dipendenti non è consentito:

- utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- modificare le configurazioni impostate sul proprio PC;
- presso la sede aziendale, collegarsi a reti esterne mediante dispositivi wireless, modem telefonici, cellulari, palmari e apparati assimilabili;
- accedere direttamente ai servizi di base della rete mediante l'uso di programmi di utilità potenzialmente dannosi, se non espressamente autorizzati dalla società ("ping" e similari, network "probe", racket monitor, port scanner, ecc.);
- installare ed utilizzare, sui dispositivi aziendali, servizi di messaging, di scambio file, di "peer to peer" o simili (a titolo di esempio non esaustivo Skype, Netmeeting, e-mule, WEtransfer, ecc.), ad esclusione di Teams

L'utilizzo di dati e applicazioni aziendali su dispositivi personali è di norma vietato salvo specifiche autorizzazioni della società.

Al fine di evitare l'utilizzo da parte di terzi, senza che vi sia la possibilità di provarne in seguito l'indebito uso, il personal computer deve essere sempre spento al termine della propria attività lavorativa giornaliera; spento o disconnesso dalla propria sessione di lavoro e posto in stato di blocco, in particolar modo se collegato alla rete aziendale, nel caso di assenze prolungate dalla propria postazione di

lavoro. In quest'ultimo caso si raccomanda di porre il sistema in stand-by, al fine ridurre il consumo energetico e contribuendo alla salvaguardia dell'ambiente.
L'utilizzo delle porte USB per trasferire informazioni è proibito.
Eventuali dati e documenti privati dell'utente non possono essere conservati sul PC in dotazione.
Le unità di rete (server e dischi di rete) sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi; pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.
Il controllo delle stampe dei documenti è responsabilità degli utenti che devono ridurre al minimo il rischio che persone non autorizzate possano accedere alle stesse.
Il titolare del trattamento ovvero gli amministratori di sistema possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno pericolose per la sicurezza sia sui PC degli utenti e dei responsabili sia sulle unità di rete e/o altre risorse informatiche.
Per un utilizzo sicuro della rete interna, non sono ammessi accessi alla rete aziendale tramite PC o dispositivi non aziendali.

**Posta elettronica**
Generalmente, le informazioni trattate tramite posta elettronica sono trasmesse in "chiaro" e possono essere intercettate lungo la rete. Pertanto è necessario che tutti gli utenti utilizzino esclusivamente gli strumenti predisposti dalla Società, che garantiscono livelli di protezione adeguati.
La posta elettronica non va utilizzata per lo scambio di informazioni classificate riservate con soggetti esterni alla Società; in caso di comprovata necessità vanno adottati meccanismi di protezione o cifratura. Per quanto riguarda la sicurezza della posta in arrivo, tenuto conto delle caratteristiche di globalità della rete e dei problemi di sicurezza connessi, sono previsti meccanismi di protezione contro virus informatici e software malevoli.
Si consiglia di aprire gli allegati con cautela valutando con attenzione l'attendibilità del mittente; per quanto riguarda l'origine dei messaggi di posta, è opportuno considerare che è facile "impersonare" un mittente diverso da quello reale, soprattutto per i generatori di messaggi "malevoli".
È espressamente vietato l'uso di linguaggio o di immagini oscene, ingannevoli, diffamatorie, la creazione o la propagazione di mailing di massa (spamming) o delle cosiddette "catene di Sant'Antonio".
Non è consentito diffondere, all'esterno dell'azienda, account di posta elettronica senza l'esplicito consenso del proprietario. È vietato l'invio verso l'esterno di messaggi contenenti segreti aziendali o documenti contenenti know-how aziendali. Nel caso in cui ciò si renda necessario dovranno essere valutate le modalità trasmissive idonee e la sottoscrizione di opportuni accordi di riservatezza.
Per ottimizzare le infrastrutture tecniche e di trasmissione dati, occorre rispettare le seguenti regole:

- inviare allegati in formato compresso in caso di dimensioni importanti;
- limitare la dimensione del messaggio inviato. Un allegato di dimensioni eccessive potrebbe impedire l'arrivo del messaggio o richiedere un uso eccessivo delle risorse; a tal fine la dimensione massima, per gli allegati, non deve superare 25 MB;
- non aprire, ma cancellare, messaggi di posta elettronica provenienti da mittenti sconosciuti o non affidabili;

- svuotare periodicamente la propria casella elettronica, cancellando documenti inutili e soprattutto allegati ingombranti i quali, se è necessario conservarli, devono essere trasferiti al più presto nelle cartelle personali sul Sistema Informativo;
- evitare il più possibile di rispondere ad un messaggio allegando tutto il testo precedente;
- Non partecipare a forum e/o blog non professionali o registrarsi ad inutili liste di distribuzione, chat, gruppi di discussione, mailing commerciali o a guest book non professionali anche utilizzando pseudonimi (c.d. "nickname"); quando necessario, richiedere rapidamente la rimozione.

Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e ridurre al minimo l'accesso ai dati personali, nel rispetto del principio di necessità e di proporzionalità, il sistema in caso di assenze programmate, lunghe assenze e cambio gestione o cessazione del rapporto, potrà essere impostato in modo da inviare automaticamente messaggi di risposta contenenti le coordinate di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In caso di assenze lunghe o programmate, in caso di emergenza, o in caso di cessazione del rapporto di lavoro, è facoltà della Società di prendere visione della posta elettronica in entrata ed in uscita dell'account assegnato al dipendente, collaboratore, somministrato e stagista al fine di tutelare il patrimonio aziendale.
Si ricorda che la documentazione elettronica, che costituisce per la Società "know-how" aziendale tecnico o commerciale protetto (tutelato in base all'art. 6 bis del r.d. 29.6.1939 n. 1127) o che comunque viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto, a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Società.

**Internet**

La Società ha il compito non solo di incoraggiare, ma anche di sostenere, con ogni mezzo, un impiego appropriato di Internet.
È fatto divieto l'utilizzo di Internet per scopi non aziendali e detta violazione può comportare l'erogazione di sanzioni disciplinari.
La navigazione in Internet è consentita, per fini di lavoro, ai soli utenti abilitati.
L'accesso ad Internet richiede particolare attenzione, in quanto presenta alcuni rischi per la sicurezza, quali:

- il caricamento inconsapevole e l'esecuzione di codice malevolo (virus informatici, spyware, backdoor);
- la perdita di riservatezza individuale ed aziendale;
- il download di materiale soggetto a diritti di autore o comunque illecito.

Gli utenti sono tenuti ad osservare le seguenti norme:

- non trasferire sul proprio computer (download) file da siti sconosciuti se non per sole ragioni connesse all'attività lavorativa;
- non entrare tramite la connessione internet nei forum estranei al lavoro;
- non scaricare e non usare software gratuito o shareware prelevato da siti internet e ogni altro materiale coperto da copyright se non espressamente autorizzato dalla Società;
- non eseguire il codice mobile (applet Java, Activex) se non si conosce la provenienza;

- è vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simile salvo i casi direttamente autorizzati dalla Società e con il rispetto delle normali procedure di acquisto;
- è vietato l'accesso degli utenti ai social network, ad esclusione di Linkedin per le mansioni che ne richiedono l'utilizzo (es: Marketing, Risorse Umane);
- è vietata la diffusione di informazioni che possono avere effetto sul valore di mercato della Società o dei Clienti.

Fermo restando il divieto di accesso ad Internet per scopi non lavorativi, è altresì vietato, a titolo esemplificativo:

- visitare siti internet contenenti materiale osceno, oltraggioso o comunque non coerente con i valori etici sui quali si fonda la Società;
- svolgere o sollecitare attività economiche al fine di trarne profitti personali;
- rivelare o pubblicare informazioni confidenziali quali informazioni finanziarie, strategie di marketing, nuove attività economiche, elenchi Clienti, informazioni tecniche, composizione dei prodotti, contenuto di contratti e trattati, codici di accesso, ecc.;
- rappresentare idee personali come se fossero proprie della Società o dei Clienti;
- interferire con gli strumenti e con le normali operazioni di aggiornamento e gestione della rete aziendale che riducono il rischio di diffusione di virus informatici.

Per attenuare tali rischi, la Società predispone filtri sui siti ritenuti più critici.
Comunque la navigazione in Internet, effettuata su siti che esulano dall'attività lavorativa e che causi gli inconvenienti descritti sopra, è considerata dalla Società una responsabilità dell'utente, anche ai fini di una eventuale procedimento disciplinare.
Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, la Società rende nota l'adozione di uno specifico sistema di blocco o filtro automatico atto a prevenire determinate operazioni quali l'upload o l'accesso a determinati siti e/o categorie di siti inseriti in una black list o in specifiche categorie.

**Licenze software**

La Società ribadisce il proprio impegno ad utilizzare esclusivamente programmi originali e provvisti di licenza d'uso della casa produttrice.
Tutti i computer aziendali sono forniti, all'atto della consegna, di un corredo di programmi provvisti di licenza ufficiale o di utilizzo libero (es.: Sistema Operativo Windows, antivirus, ecc.).
Ogni personal computer è dotato di un software di protezione antivirus che non deve essere per nessun motivo disattivato.
Eventuali messaggi del software antivirus, siano essi inerenti anomalie del software stesso o la presenza di virus non eliminabili dovranno essere immediatamente comunicate dall'utente agli amministratori di sistema, prima di intraprendere qualsiasi azione.

## 3. Processo di Data Breach Management

La società Technogenetics Spa è obbligata ai sensi del Regolamento (UE) 2016/679, a mantenere i dati personali al sicuro ed a rispondere prontamente e in modo adeguato alle violazioni della sicurezza

dei dati, compresa la segnalazione di tali violazioni all'Autorità Garante per tutti gli obblighi previsti dal citato Regolamento.
È fondamentale adottare misure tempestive in caso di violazioni effettive, potenziali o sospette della sicurezza o della riservatezza dei dati personali per evitare il rischio di danni alle persone, alle attività operative e prevenire i gravi costi finanziari, legali e di reputazione.
Scopo della policy per la gestione dei Data Breach è quello di fornire all'organico di Technogenetics Spa gli indirizzi strategici e le linee guida per una gestione efficace ed efficiente degli incidenti di sicurezza che implicano la violazione dei dati personali.
Con il termine "violazione della sicurezza dei dati personali" si intende ogni evento 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, ai sensi dell'Art. 4 del Regolamento UE 2016/679 (GDPR).
Tali violazioni alla sicurezza dei dati personali possono essere identificate come segue:

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

Le cause più comuni si possono categorizzare in:

- Violazione involontaria ed accidentale: l'esempio più pratico è lo smarrimento di un supporto cartaceo, come un documento, o elettronico;
- Furto: con chiare intenzioni illecite, come ad esempio il furto dei detti supporti cartacei e/o elettronici;
- Volontarietà illecita da parte di dipendenti: avviene quando la violazione viene causata da un soggetto interno all'organizzazione, accedendo in maniera autorizzata alle informazioni, ma trattandole poi illegittimamente.
- Accesso non autorizzato/Alterazione dei dati: avviene quando viene condotto un attacco avente come fine l'accesso senza autorizzazioni ai sistemi informatici, l'acquisizione dei dati personali e/o l'alterazione/divulgazione degli stessi.

Gli Stakeholder coinvolti nel processo di Breach Management sono di seguito elencati:

- Autorità Garante
- Amministratore di Sistema
- Interessato
- Responsabile del Trattamento interessato dalla violazione
- Titolare del Trattamento
- Consulente

Le violazioni della sicurezza dei dati personali sono gestite dal responsabile del trattamento dei dati, la cui area di responsabilità è stata interessata dalla violazione; tale responsabile agisce per conto del titolare del trattamento, in collaborazione con l'amministratore di sistema.

Nel caso in cui si verifichi una violazione della sicurezza dei dati personali, è fondamentale garantire che questa venga gestita immediatamente ed in modo appropriato per ridurre al minimo l'impatto e le conseguenze della violazione ed evitare che essa si ripresenti.

**Resta inteso che, nel caso in cui la violazione presenti rischi elevati per i diritti e le libertà delle persone, la comunicazione all'Autorità Garante è obbligatoria.**

ii. Le persone interessate dalla violazione, a meno che:
   - Siano state poste in essere EX ANTE le misure tecniche e organizzative di protezione dei dati;
   - Siano state poste in essere EX POST tali misure in modo da prevenire il sopraggiungere del rischio elevato;
   - La comunicazione richieda degli sforzi eccessivamente onerosi per la Società. In tal caso, si procede ad una comunicazione pubblica.

**Resta inteso che, nel caso in cui la violazione presenti rischi elevati per i diritti e le libertà delle persone, la comunicazione agli interessati è obbligatoria.**

i. Altri organismi quali organismi di regolamentazione, finanziatori di sovvenzioni;
ii. La stampa o i media;
iii. Le società bancarie o di carte di credito;
iv. I sindacati;
v. I consulenti legali esterni.