FINPIEMONTE S.P.A.

REGOLAMENTO PER LA GESTIONE PRIVACY

AI SENSI DEL RGPD 679/2016 e s.m.i.

Versione 2.0 del 18/02/2022

INDICE

Oggetto

Il presente Regolamento stabilisce le politiche dell'azienda per garantire l'applicazione del Regolamento Generale sulla Protezione dei Dati 679/2016 (nel seguito RGPD 679/2016) in continuità con il D.Lgs. 196/2003, così come integrato e modificato dal D.Lgs. 101/2018, nell'ambito della propria organizzazione aziendale.
Il documento descrive le garanzie e le misure tecniche ed organizzative che vengono adottate in azienda nel trattamento dati, dalla raccolta fino alla sua conservazione e si completa con tutte le procedure e modulistiche redatte ed applicate dal personale deputato al trattamento dei dati.
Attraverso la diffusione capillare - anche mediante intranet aziendale - del presente documento e di tutta la documentazione implementata ed elaborata in ottica di conformità in ambito RGPD 679/2016, si intende perseguire la finalità di supportare tutti i soggetti autorizzati nel corretto svolgimento delle attività di trattamento dati, affinché le stesse si svolgano nel pieno rispetto sia della normativa privacy vigente, sia dei criteri di funzionalità ed efficienza cui deve essere improntata l'attività lavorativa.

Riferimenti normativi

La redazione del presente documento è stata effettuata sulla base delle seguenti fonti normative:

- Regolamento UE 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- Decreto Legislativo n. 196/2003 (Codice in materia di protezione dei dati personali) come integrato e modificato dal Decreto Legislativo n.101/2018;
- Atti, procedure e modelli aziendali;
- Norme comportamentali desunte dalla miglior prassi.

Destinatari

I destinatari del documento sono tutti i soggetti autorizzati dall'Azienda a svolgere operazioni di trattamento dei dati personali.
Al fine di garantirne l'efficace e corretta applicazione, l'Azienda procederà al periodico aggiornamento del presente documento.

1. DEFINIZIONI

Per Regolamento si intende il Regolamento UE 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Con riferimento al Regolamento, si specifica che la sua pubblicazione è avvenuta in data 4 maggio 2016 e che, a partire dal giorno della pubblicazione, gli Stati membro hanno avuto due anni di tempo per l'applicazione; quest'ultimo è divenuto obbligatorio a partire dal 25 maggio 2018.

Per "Titolare" del trattamento si intende 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 membro, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membro (art. 4, comma 7 del RGPD 679/2016).

Per "responsabile" del trattamento si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento (art. 4, comma 8 del RGPD 679/2016).

Per "autorizzato al trattamento" (*ex* Incaricato al trattamento) si intende chiunque agisce sotto l'autorità del titolare o del responsabile del trattamento che ha accesso ai dati personali e che è stato debitamente istruito su come effettuare il trattamento stesso.

Per "soggetto designato" si intende la persona fisica che opera sotto la responsabilità e nell'ambito dell'assetto organizzativo del titolare del trattamento o del responsabile, alla quale questi ultimi hanno attribuito specifici compiti e funzioni connessi al trattamento di dati personali.

Per "terzo" si intende 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 (art. 4, comma 10 del RGPD 679/2016).

Per "destinatario" si intende 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 (art. 4, comma 9 del RGPD 679/2016).

Per "trattamento" dei dati si intende qualunque operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate ai 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 (art. 4, comma 2 del RGPD 679/2016).

Esempi di trattamento svolti durante le attività Aziendali sono:

- l'introduzione dei dati anagrafici dei dipendenti/fornitori nel sistema informativo dell'Azienda;
- la visualizzazione (su video) di dati di dipendenti e fornitori (es. cedolino stipendiale, controlli contabili ecc.);
- la stampa di documenti contenenti dati personali o la loro consegna all'utente/destinatario;
- la consultazione, la riorganizzazione, l'archiviazione dei documenti e la loro gestione negli archivi;
- la registrazione di informazioni nei documenti aziendali.

Il trattamento è dunque qualunque tipo di gestione dei dati, dalla loro nascita (data input, scrittura su carta), utilizzo (visualizzazione, comunicazione, emissione, modifica, archiviazione), alla fine (cancellazione, distruzione).

Attraverso il termine "trattamento" il legislatore ha voluto estendere il RGPD dalle singole operazioni all'intero complesso di attività, ampliando in modo sostanziale l'ambito di applicazione della normativa.

Per "**dato personale"** si intende qualunque informazione relativa a 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, un identificativo on line o ad uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (articolo 4, comma 1 del RGPD 679/2016).
I principi di protezione non dovrebbero pertanto applicarsi al dato **"anonimo",** vale a dire informazioni che non si riferiscono ad una persona fisica identificata o identificabile, o a dati resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto, al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca. Al contrario i principi del RGPD si applicano al dato sottoposto a "pseudonimizzazione", i quali potrebbero essere attribuiti ad una persona fisica mediante l'utilizzo di ulteriori informazioni e quindi dovrebbero essere considerati informazioni su una persona fisica identificabile.

Per **"dati genetici**" si intendono 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 (articolo 4, comma 13 del RGPD 679/2016).

Per **"dati biometrici"** si intendono 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 (articolo 4, comma 14 del RGPD 679/2016).

Per **"dati relativi alla salute**" si intendono 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 (articolo 4 comma 15 del RGPD 679/2016).

Per "**dati particolari**" si intendono i dati personali che rilevano l'orige razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, biometrici e dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della personale (art.9, comma 1 del RGPD 679/2016).

Per "**dati relativi a condanne penali e reati"** i dati personali relativi alle condanne penali e reati o a connesse misure di sicurezza (art.10 del RGPD 679/2016).

Per "**Archivio**" si intende 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 (art.4, comma 6 del RGPD 679/2016).

2. TRATTAMENTO DEI DATI

2.1 Principi applicabili al trattamento dei dati personali

I dati personali devono essere:

- trattati in modo lecito, corretto e trasparente, nei confronti dell'interessato;
- acquisiti e trattati su idonea e pertinente base giuridica per scopi determinati, espliciti e legittimi;
- trattati solo per le finalità proprie dell'Azienda e in maniera non eccedente le predette finalità;

- trattati nel rispetto dei diritti e della dignità degli interessati;
- protetti dal rischio, anche solo potenziale, di distruzione, perdita, modificazione, rivelazione non autorizzata, accesso non autorizzato, non esattezza e non adeguatezza rispetto alle finalità per cui sono trattati.

2.2 Liceità del trattamento

I dati personali possono essere raccolti e trattati al ricorrere di una delle seguenti circostanze (base giuridica):

- l'interessato ha espresso il consenso al trattamento dei dati personali per una o più specifiche finalità;
- 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;
- il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Nel caso di dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute alla vita sessuale o all'orientamento sessuale della persona, sono ritenute valide basi giuridiche per il trattamento:

- il consenso dell'interessato, purché si tratti di consenso esplicito e per una o più finalità specifiche;
- il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- il trattamento è necessario per accertare, esercitare o difendere un diritto dell'Azienda in sede giudiziaria;
- il trattamento è necessario per motivi di interesse pubblico rilevante;
- il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale.

2.3 Informativa

L'informativa è lo strumento che rende esplicita e trasparente la gestione delle informazioni di carattere personale e particolari degli interessati, al fine di consentire agli stessi soggetti di prendere parte attiva alla difesa dei propri diritti nell'ambito della protezione dei dati personali.

L'azienda fornisce l'informativa agli interessati al momento del primo utilizzo dei loro dati, gli interessati vengono informati per iscritto tramite idonea informativa, che contiene tutte le informazioni richieste dall'art. 13 RGPD 679/2016:

- l'identità e i dati di contatto del Titolare del trattamento;
- dati di contatto del Responsabile della Protezione dei Dati;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- ove applicabile, l'intenzione del Titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma,

RGPD 679/2016, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), RGPD 679/2016, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo a un'Autorità di controllo;
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 del RGPD 679/2016, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati siano acquisiti da terzi, l'Azienda provvede a fornire l'informativa entro trenta giorni da quando i dati sono stati acquisiti.
In tali casi l'informativa deve anche indicare la fonte da cui sono stati acquisiti i dati personali e l'eventualità che i dati provengano da fonti accessibili al pubblico.
Si ricorda inoltre che qualora l'Azienda intenda utilizzare i dati raccolti per una finalità diversa da quella per cui sono stati ottenuti, prima di tale ulteriore trattamento, deve fornire all'interessato informazioni in merito a tale diversa finalità.

L'Azienda redige le seguenti informative:

- **Informativa per il trattamento dei dati personali dei dipendenti/collaboratori**
  Consegnata a tutti i dipendente/collaboratori all'atto dell'assunzione/collaborazione.
  La stessa viene firmata per accettazione e presa visione, ed inserita nel proprio fascicolo personale.

- **Informativa "opportunità di lavoro" nel sito web**
  Resa a tutti coloro che si registrano attraverso il sito web aziendale ai fini di ricerca e selezione del personale, i quali prendono visione dell'informativa nel corso della fase di registrazione attraverso il sito web aziendale; nel caso di candidatura presentata mediante altri canali (es. Società di ricerca e selezione) l'informativa viene consegnata al candidato/a, a mani per presa visione.

- **Informativa per il trattamento dei dati personali fornitore**
  Consegnata a tutti i fornitori al momento della stipula del contratto.

- **Informativa per il trattamento dei dati personali clienti/beneficiari**
  Tutti i beneficiari prendono visione dell'informativa attraverso il sito web aziendale richiamato nel bando di agevolazione per la realizzazione di progetti.

- **Informativa per il trattamento dei dati personali dei valutatori**
  Consegnata a tutti i valutatori al momento della stipula del contratto.

- **Informativa di verifica della certificazione verde COVID-19**
  Consegnata a tutti i dipendenti in ossequio all'entrata in vigore dell'obbligo normativo.

- **Informativa newsletter**
  Resa a coloro che fanno richiesta di ricevere la newsletter attraverso il sito web aziendale

- **Informativa Lavora con noi**
  Tutti i candidati prendono visione dell'informativa attraverso il sito web aziendale in ossequio alla normativa vigente.

- **Informativa Whistleblower per la segnalazione di illeciti**
  Tutti i segnalanti prendono visione dell'informativa attraverso il sito web aziendale in ossequio alla normativa vigente.

- **Policy privacy e Cookie policy**
  Resa agli utenti che hanno accesso e navigano sul sito web aziendale.

2.4 I diritti degli interessati

Ai sensi degli artt. 15 e ss. del RGPD 679/2016, il soggetto interessato, a cui si riferiscono i dati, ha il diritto di ottenere l'accesso ai dati personali ed informazioni in relazione a:

- alle finalità per cui i dati sono trattati;
- le categorie dei dati trattati;
- il periodo di conservazione dei dati;
- i destinatari dei dati personali;
- la logica cui risponde qualsiasi trattamento automatizzato di dati.

Inoltre, l'interessato ha il diritto di chiedere:

- rettifica;
- cancellazione ("diritto all'oblio");
- limitazione al trattamento;
- portabilità dei dati;
- opposizione;
- proporre reclamo ad un'Autorità di controllo.

L'Azienda ha adottato una procedura operativa per la gestione dei diritti degli interessati, denominata "Diritti degli interessati", approvata dal Consiglio di Amministrazione in data 19 dicembre 2019 e pubblicata nella intranet aziendale, che definisce le modalità per la gestione delle richieste avanzate dagli interessati; i soggetti interessati possono esercitare il diritto ad ottenere l'accesso ai dati personali e informazioni così come definito nella "Privacy policy" pubblicata sul sito istituzionale, utilizzando il modulo dedicato "Esercizio Diritti degli interessati".

3. ORGANIGRAMMA PRIVACY

3.1. Titolare del trattamento

Il Titolare del trattamento è 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.
Nel caso specifico è Finpiemonte S.p.a. ad essere Titolare del trattamento.

Il Titolare:

- decide sulle finalità del trattamento, sui mezzi e sul profilo delle misure di sicurezza;
- programma le misure di sicurezza tecniche ed organizzative adeguate per garantire che il trattamento effettuato sia conforme al RGPD;
- nel caso di violazione dei dati pone in essere misure effettive e tempestive e procede alla notifica al Garante e alla comunicazione all'interessato;
- fornisce istruzioni e forma adeguatamente il personale autorizzato al trattamento dei dati.

Il Titolare del trattamento inoltre, designa:

- il Responsabile della Protezione Dati – RPD, raggiungibile all'indirizzo rpd@finpiemonte.it;
- il Referente della sicurezza informatica;
- i Responsabili esterni del trattamento, i soggetti a cui affida operazioni di trattamento di dati in outsourcing;
- i Soggetti Autorizzati, cui affidare le operazioni di trattamento al suo interno;
- i Soggetti Designati
- gli Amministratori di sistema, ovvero i soggetti preposti alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, quali, gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

3.2 Responsabile della protezione dei dati – RPD

Il Titolare del trattamento nomina il Responsabile della Protezione dei Dati: tale nomina viene notificata al Garante Privacy.

La designazione del RPD avviene sulla base delle competenze professionali e personali, in particolare:

- conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati;
- conoscenza di norme e procedure amministrative applicabili all'azienda;
- conoscenza delle tecnologie informatiche e misure di sicurezza dei dati;
- conoscenza dello specifico settore di attività;
- conoscenza dell'organizzazione e dei processi aziendali;
- capacità organizzative, relazionali e di conseguenza capacità di promuovere una cultura della protezione dei dati all'interno dell'azienda.

Il RPD svolge il proprio compito in piena autonomia e con un supporto adeguato in termini di risorse finanziarie, infrastrutture e personale per svolgere in modo efficace i compiti cui è chiamato.

I dati di contatto del RPD sono comunicati:

- all'Autorità di controllo;
- all'utenza, mediante pubblicazione sul sito web aziendale;
- ai dipendenti attraverso la pubblicazione nella intranet aziendale.

Nell'esecuzione dei propri compiti il RPD provvede a:

- sorvegliare l'osservanza del RGPD, di altre disposizioni dell'Unione Europea o degli stati membro relativi alla protezione dei dati nonché delle politiche decise dal Titolare del trattamento, in materia di protezione dei dati personali;
- sensibilizzare sul tema trattamento dati, il personale che effettua operazioni di trattamenti;
- informare e fornire consulenza al Titolare del trattamento in merito agli obblighi derivanti dal presente Regolamento nonché da altre disposizioni dell'Unione Europea o degli stati membro relativi alla protezione dei dati;
- informare, indirizzare e fornire consulenza ai dipendenti che eseguono gli obblighi derivanti dal presente Regolamento nonché da altre disposizioni dell'Unione Europea o degli stati membro relativi alla protezione dei dati;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- cooperare con l'Autorità Garante;
- fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del RGPD ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Inoltre il RPD monitora l'applicazione del Regolamento e riporta con cadenza annuale al vertice dell'Azienda.

3.3 Referente della sicurezza informatica
Il Titolare del trattamento nomina il Referente della sicurezza Informatica con atto di nomina formale per iscritto, il quale ha la responsabilità del sistema informativo aziendale.

3.4. Amministratore di sistema
Gli amministratori di sistema, sono individuati in ambito informatico, in quanto figure specializzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l´elenco delle funzioni ad essi attribuite, vengono riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.
L'identità degli amministratori di sistema che riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, sono resi noti in azienda attraverso strumenti di comunicazione interna (es., intranet aziendale, ordini di servizio a circolazione interna o bollettini).
Le società terze nominate responsabili esterne dei trattamenti informatici si impegnano a mantenere un elenco aggiornato degli "amministratori di sistema" che possono avere accesso agli strumenti elettronici (server e client), database management system, applicativi complessi e apparati di rete del Titolare.

3.5 Soggetto Designato al trattamento dei dati personali, ex art. 2quaterdecies D.lgs. 196/2003 (di area/funzione)
Il Titolare del trattamento nomina il Soggetto Designato al trattamento dei dati personali (di area/funzione) con atto di nomina formale per iscritto. Il soggetto designato (di area/funzione), nell'ambito delle funzioni che è chiamato/a a svolgere e all'interno della struttura diretta e così come previsto da contratto, ha la responsabilità di trattare i dati ai fini dello svolgimento della propria attività lavorativa, sulla base delle attività assegnategli e successivi aggiornamenti.

In particolare, il soggetto designato al trattamento dei dati personali garantisce:
- che il trattamento dei dati personali e particolari, avvenga secondo le istruzioni impartite dal Titolare del trattamento nel pieno rispetto delle vigenti disposizioni in materia;
- che ogni dato, venga trattato per le sole finalità per le quali è stato raccolto;
- la correttezza, l'esattezza e la completezza di dati personali oggetto di trattamento sotto la sua responsabilità;
- che in fase di progettazione di nuovi trattamenti, ove necessario, venga richiesta una valutazione di impatto e di rischio, conforme alle direttive stabilite nel RGPD 679/2016, in continuità con il D.Lgs. 196/2003, così come integrato e modificato dal D.Lgs. 101/2018, informandone il Titolare del trattamento e il RPD;
- che nel caso in cui si verifichi una violazione di dati personali, informi tempestivamente il Titolare del trattamento e il RPD;
- che il personale autorizzato del trattamento operi in conformità alle disposizioni di legge e regolamenti loro impartiti;
- che i documenti contenenti dati personali/particolari vengano custoditi in modo da non essere accessibili a persone non autorizzate al trattamento;
- che i dati personali/particolari, vengano comunicati nel rispetto delle prescrizioni impartite; i documenti contenenti dati personali/particolari non devono essere condivisi, comunicati o inviati a persone non autorizzate;
- che l'informativa di cui all'art. 13 RGPD 679/2016 venga effettivamente resa;
- che gli autorizzati, deputati alla raccolta del consenso, nei casi previsti dalla legge, lo acquisiscano secondo le indicazioni impartite;

- che i dati personali/particolari raccolti su supporti cartacei ed informatici vengano trattati nel rispetto delle misure di sicurezza e delle istruzioni impartite dal Titolare del trattamento.

3.6 Soggetto Autorizzato al trattamento

Il Titolare del trattamento nomina, ogni dipendente dell'Azienda, preposto ad una determinata Area/Funzione che implichi il trattamento di dati personali, autorizzato al trattamento.
Le nomine, comprensive di istruzioni, vengono effettuate al momento dell'instaurarsi di un rapporto di lavoro dipendente con l'Azienda, per iscritto, e individuando il trattamento consentito.

Gli autorizzati al trattamento assicurano, in ogni operazione di trattamento, la massima riservatezza ed in particolare che i dati personali siano:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittimi;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per i quali sono trattati;
- esatti e, se necessario, aggiornati;
- conservati in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti e della perdita, della distruzione o dal danno accidentale.

Tutti gli autorizzati nelle operazioni di trattamento osservano le seguenti istruzioni:

<u>per la protezione dei documenti cartacei</u>:

- i documenti oggetto di trattamento sono affidati soltanto a soggetti appositamente autorizzati, nominati formalmente Autorizzato al trattamento e nel rispetto dei trattamenti loro affidati;
- durante il trattamento, i documenti devono essere custoditi e controllati in modo che ad essi non accedano persone prive di autorizzazione, in particolare non devono rimanere incustoditi su scrivanie o tavoli di lavoro;
- concluso il trattamento, i documenti devono essere collocati in una stanza presidiata dal personale autorizzato o, se la stanza non è presidiata, in un armadio chiudibile o nella stessa stanza chiudibile;
- gli accessi agli archivi contenenti dati particolari e giudiziari è controllato; le persone ammesse a qualunque titolo dopo l'orario di chiusura negli archivi contenenti dati particolari e giudiziari devono essere identificate e registrate;
- in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- in occasione della trasmissione dei documenti che avviene all'esterno dell'Azienda, devono essere adottati tutti gli accorgimenti necessari e idonei onde evitare che le informazioni riservate possano essere lette sia pure accidentalmente da chi non è autorizzato (ad esempio trasporto mediante cartelle chiuse);
- in occasione della trasmissione dei documenti agli interessati, gli stessi devono essere risposti in busta chiusa, priva all'esterno di informazioni particolari, da consegnarsi direttamente all'interessato o al terzo delegato per iscritto;
- i documenti non devono essere riciclati (ad esempio per carta da minuta o per le fotocopie) onde evitare il rischio che gli stessi possano essere letti da chi non è autorizzato;
- i documenti contenenti dati personali devono essere eliminati utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, sminuzzarli in modo da non essere più ricomponibili;
- raccogliere, registrare e conservare i dati presenti nella documentazione della Business Unit di appartenenza e nei supporti informatici, avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- è vietata la diffusione dei dati;
- è vietata la comunicazione dei dati senza la preventiva autorizzazione del Titolare del trattamento;

- l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro.

per la protezione dei documenti informatici:

- non bisogna lasciare incustodito il PC con l'utenza abilitata per impedirne l'utilizzo fraudolento; alla fine del lavoro bisogna scollegarsi dal PC eseguendo la "chiusura di sessione" indicata; non bisogna lasciare in vista le informazioni presenti sul monitor.
- utilizzare password riservate, personalizzate e con complessità adeguate per l'accesso ai sistemi informatizzati;
- nella password non devono essere immessi riferimenti agevolmente riconducibili alla propria persona (ad esempio nome, cognome, data di nascita, nome del coniuge);
- la password non deve essere trascritta su promemoria in vista (ad esempio biglietti dinanzi al pc) o comunicata a terzi;
- non installare e non scaricare da Internet programmi non pertinenti l'attività lavorativa né qualsiasi altro programma, senza la preventiva autorizzazione da parte dei Sistemi Informativi Aziendali (SIA);
- comunicare tempestivamente ai SIA, l'eventuale rilevazione di anomalie nell'utilizzo del sistema informatico che possono compromettere la sicurezza dei dati;
- verificare la provenienza dei messaggi di posta elettronica contenenti allegati e cancellare direttamente quelli di dubbia provenienza;
- utilizzare la posta elettronica e la connessione ad Internet esclusivamente per lo svolgimento dei propri compiti istituzionali;
- non diffondere messaggi di posta elettronica (es: catena di S. Antonio);
- informare tempestivamente l'RPD e/o il Soggetto Designato di area nel caso in cui si verifichi una violazione di dati personali.

3.7 Responsabile (esterno) del trattamento

I Responsabili (esterni) del trattamento sono individuati nelle persone fisiche o giuridiche, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto dell'Azienda (es. società di software, consulenti etc.).

La nomina a Responsabile (esterno) del trattamento, viene effettuata per i fornitori che presentino garanzie sufficienti di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche ed organizzative che soddisfino i requisiti del RGPD e per la sicurezza del trattamento.
La nomina è contenuta nel contratto stesso e stabilisce:

- la durata del trattamento;
- la natura e la finalità del trattamento;
- il tipo di dati personali e le categorie di interessati.

In particolare, stabilisce i doveri a cui è tenuto il Responsabile del trattamento, ovvero:

- attenersi e trattare i dati personali soltanto su istruzione documentata del Titolare del trattamento, solo per le finalità da quest'ultimo specificate e ai fini dell'esecuzione delle prestazioni contrattuali;
- prima del trattamento, informare il Titolare del trattamento in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale;
- assicurare specificamente che i dati trattati per conto del Titolare ai fini dell'esecuzione dell'attività oggetto del Contratto, non siano destinati a trattamenti diversi da quelli di cui all'incarico conferito ai sensi del Contratto;
- garantire l'applicazione dei principi (utilizzando i materiali, i prodotti, le applicazioni o i servizi) di protezione dei dati a partire da quando questi vengono progettati e della protezione dei dati di default.
- garantire la riservatezza dei dati personali trattati nell'ambito del contratto;
- provvedere alla nomina in forma scritta dei propri collaboratori (se presenti) "persone autorizzate al trattamento" ed impartire a questi ultimi, specifiche e dettagliate istruzioni dirette ad assicurare il

pieno rispetto delle disposizioni di legge, ai sensi dell'art. 29, comma 3, lett.b) del RGPD 679/2016, in particolare garantire che tali persone autorizzate si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

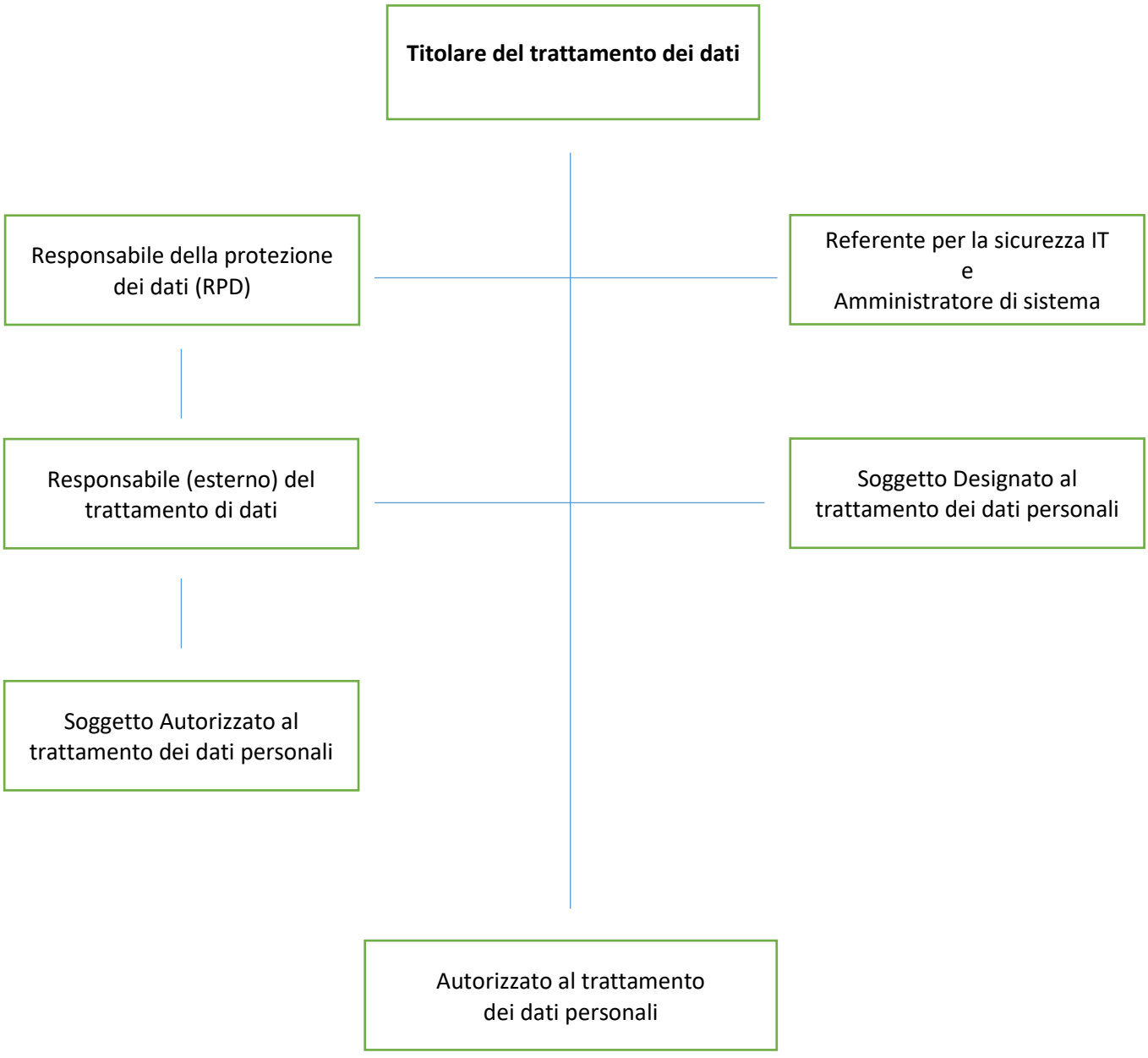
- adottare tutte le misure richieste ai sensi dell'art. 32 del RGPD 679/2016 (Sicurezza del trattamento);
- assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. da 32 a 36 (sicurezza del trattamento, notifica di una violazione di dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione d'impatto, consultazione preventiva);
- in caso di violazione o sospetta violazione di sicurezza dei dati personali, informare il Titolare senza ingiustificato ritardo, ed in ogni caso entro e non oltre 12 ore dopo esserne venuto a conoscenza. Il Responsabile fornirà immediatamente al Titolare una descrizione dettagliata della violazione e qualsivoglia ulteriore informazione che il Titolare possa richiedere in relazione ad essa, tra cui, a titolo esemplificativo ma non esaustivo, la natura della violazione, il numero approssimativo di interessati, le categorie in questione, il numero approssimativo di registrazioni di dati in questione, il nome e i dati di contatto del responsabile della protezione dei dati e le probabili conseguenze della violazione, nonché le misure intraprese per (i) rimediare alla violazione di dati, (ii) mitigare l'impatto sugli interessati, (iii) prevenire il ripetersi di violazioni.

  Il Responsabile adotterà le misure necessarie per proteggere i dati, per mitigare le possibili conseguenze negative per gli interessati e per prevenire il ripetersi di violazioni dei dati. Tali misure saranno intraprese in coordinamento con il Titolare. Il Responsabile non coinvolgerà né renderà comunicazione alcuna a terze parti (incluse le Autorità per la Protezione dei Dati) in merito ad alcuna violazione di dati senza la preventiva approvazione scritta da parte del Titolare.
- comunicare al Titolare del trattamento il nome ed i dati del proprio Responsabile della protezione dei dati, qualora ne abbia designato uno conformemente all'articolo 37 del Regolamento europeo sulla protezione dei dati.
- assistere il Titolare del trattamento nell'espletamento dei propri obblighi di far seguito alle domande di esercizio dei diritti delle persone interessate: diritto di accesso, di rettifica, di cancellazione e di opposizione, diritto alla limitazione del trattamento, diritto alla portabilità dei dati, diritto di non essere oggetto di una decisione individuale automatizzata (compresa la profilazione).
- cancellare o restituire tutti i dati personali dopo che è terminata la prestazione dei servizi, salvo che sia prevista per legge la conservazione, su richiesta del Titolare;
- mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al RGPD 679/2016;
- consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da altro soggetto da questi incaricato;
- assistere il Titolare con misure tecniche ed organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dar seguito alle richieste per l'esercizio dei diritti dell'interessato (informativa, diritto di accesso, di rettifica, di cancellazione, di limitazione, di portabilità dei dati, diritto di opposizione, etc.).

Qualora il Responsabile del trattamento ricorra ad altro Responsabile del trattamento ("sub-responsabile") per l'esecuzione di specifiche attività del trattamento per conto del Titolare del trattamento, è tenuto a richiedere al Titolare del trattamento un'autorizzazione scritta, specifica o generale. In tale ultima ipotesi, il Responsabile informa il Titolare di eventuali modifiche - aggiunta o sostituzione – di altri Responsabili del trattamento, dando la facoltà al Titolare di opporsi a tali modifiche.
Su tale - altro - responsabile del trattamento sono imposti gli stessi obblighi in materia di protezione dei dati contenuti nel presente documento tra il Titolare ed il responsabile, in particolare, garanzie sufficienti, per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del RGPD 679/2016. Qualora tale responsabile ometta di adempiere ai propri obblighi in materia di protezione

di dati, il responsabile iniziale conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dell'altro rappresentante.
Il Responsabile del trattamento informa immediatamente il Titolare, qualora, a suo parere un'istruzione violi il Regolamento in tema di protezione dei dati.
Il Responsabile del trattamento, se previsto dall'art. 30, comma 2 RGPD 679/2016, tiene un registro di tutte le categorie di attività relative al trattamento, svolte per conto del Titolare.
Gli obblighi relativi alla riservatezza devono essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro e la nomina a Responsabile cessa automaticamente con il venir meno del rapporto intercorrente tra il Titolare ed il Responsabile.

Di seguito si riporta lo schema organizzativo posto in essere dall'Azienda:



4. REGISTRO DEI TRATTAMENTI

Il Titolare del trattamento redige un registro delle attività di trattamento che contiene le informazioni di cui all'art. 30 del RGPD 679/2016, tra le quali:

- il nome e i dati di contatto del Titolare;
- le finalità del trattamento;
- la base giuridica del trattamento;
- una descrizione delle categorie degli interessati e delle categorie di dati personali trattati;
- le categorie di destinatari, a cui i dati personali sono stati o saranno comunicati;
- eventuali trasferimenti dei dati verso Paesi terzi o organizzazioni internazionali;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative mirate a garantire un livello di sicurezza adeguato al rischio, di cui all'art. 32, paragrafo 1 RGPD 679/2016.

Il registro è mantenuto aggiornato da parte del RPD. Come stabilito dall'Autorità garante il registro dei trattamenti può contenere elementi ulteriori rispetto al nucleo minimo previsto dall'art. 30 GDPR.

5. VALUTAZIONE DEI RISCHI E DPIA

Il Titolare effettua una valutazione dei rischi al fine di individuare eventuali aree critiche per attuare piani di miglioramento.
La valutazione viene condotta su tutti i trattamenti mappati nel Registro dei trattamenti analizzando le misure di protezione adottate e di potenziali rischi per le libertà degli interessati, pesandone probabilità e danno potenziale, al fine di generare un indice di rischio per ogni trattamento.
Qualora un rischio risulti "alto" viene definito un piano di miglioramento per agire sul danno o sulla probabilità, così da riportare l'indice di rischio ad un livello accettabile.
Nei casi specifici ove si verifichino rischi elevati per le libertà e i diritti degli interessati (persone fisiche) a seguito delle attività di trattamento in essere o pianificate, indipendentemente dalle misure di protezione messe in atto, il Titolare prescrive l'esecuzione di una DPIA.
La DPIA è prevista dall'articolo 35 del RGPD 679/2016 e mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli.
Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.
La DPIA è uno strumento importante in termini di responsabilizzazione (rif. principio di accountability) in quanto aiuta il Titolare non soltanto a rispettare le prescrizioni del RGPD 679/2016 ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, la DPIA è uno strumento che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali.
La DPIA è obbligatoria in tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ad esempio se include dati particolati, quali quelli sanitari ed è effettuato su larga scala, oppure dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, anziani, ecc.).
La DPIA deve essere condotta prima di procedere al trattamento e deve comunque esserne previsto un riesame continuo, ripetendo la valutazione a intervalli regolari.

6. POLITICHE DI SICUREZZA E PROCEDURE ORGANIZZATIVE DEI DATI AZIENDALI.

6.1 Gestione dei dati cartacei

I dati personali, oggetto di trattamento, sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnologico, in base alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di

distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non conforme alle finalità della raccolta.
Di seguito si riportano le misure di sicurezza ed i criteri tecnici ed organizzativi per la protezione dei locali e dei documenti cartacei dell'Azienda.
Il Titolare, individua nella propria organizzazione luoghi sicuri, stanze e/o gli uffici, in cui vengono svolte le operazioni di trattamento aventi ad oggetto i dati personali, nonché i locali e le stanze destinate alla loro conservazione/archiviazione.
L'accesso a tali locali deve essere consentito al solo personale autorizzato per l'espletamento della propria attività lavorativa ed esclusivamente negli orari di lavoro; ove risulta possibile, devono essere utilizzati anche schedari, armadi, cassetti e quant'altro dotati di serratura. Tali locali devono sempre essere presidiati dal personale autorizzato, e se non presidiati, i documenti devono essere collocati in armadi/schedari chiudibili o nella stessa stanza chiudibile. Sulle porte di ingresso di tali locali devono essere posizionati cartelli che vietano l'ingresso ai soggetti non autorizzati al trattamento dei dati.
I documenti oggetto di trattamento sono affidati soltanto a soggetti appositamente autorizzati (autorizzati del trattamento) che li trattano nel rispetto delle istruzioni fornite dal Titolare e/o dal soggetto designato (di area).
I documenti contenenti dati personali prelevati dagli archivi per l'attività quotidiana, devono essere ivi collocati al termine della giornata.
Durante il trattamento e per tutto il periodo che i documenti sono all'esterno del luogo sicuro, l'autorizzato non deve mai perderli di vista, adempiendo ad un preciso obbligo di custodia e controllo dei documenti stessi, per evitare che ad essi accedano persone prive di autorizzazione, in particolare non devono rimanere incustoditi su scrivanie o tavoli di lavoro.
In caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati.

Concluso il trattamento, l'autorizzato deve controllare che i documenti siano sempre completi, e deve collocarli nelle stanze/locali destinati all'archiviazione.
Inoltre:

- in occasione della trasmissione dei documenti sia all'interno che all'esterno dell'Azienda devono essere adottati tutti gli accorgimenti necessari e idonei onde evitare che le informazioni riservate possano essere lette sia pure accidentalmente da chi non è autorizzato (ad esempio trasporto mediante cartelle chiuse);
- i documenti non devono essere riciclati (ad esempio per carta da minuta o per le fotocopie) onde evitare il rischio che gli stessi possano essere letti da chi non è autorizzato;
- è vietata la fotocopiatura e/o duplicazione di documenti originali senza la preventiva autorizzazione del responsabile;
- è vietata la creazione di documenti "fai da te", bisogna attenersi ai soli documenti approvati dall'azienda ed alle relative procedure di compilazioni (es. attenendosi al principio di pertinenza e non eccedenza);
- i documenti contenenti dati personali devono essere eliminati utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, sminuzzarli in modo da non essere più ricomponibili;
- è vietata la diffusione dei dati;
- è vietata la comunicazione dei dati senza la preventiva autorizzazione del Responsabile.

6.2 Utilizzo della fotocopiatrice

Le fotocopiatrici devono essere ubicate in luoghi atti a limitare il rischio che i documenti (in originale o fotocopia) possano essere oggetto di accesso non autorizzato.
Quale ulteriore accorgimento è opportuno rispettare il seguente regolamento d'uso:

- l'uso delle fotocopiatrici è consentito ai soli soggetti autorizzati;
- le operazioni di fotocopiatura dei documenti contenenti dati personali sono svolte dai soggetti autorizzati nel rispetto del RGPD 679/2016;
- l'autorizzato non può utilizzare carta riciclata recante, sul retro del foglio, dati personali;

- l’autorizzato non può lasciare incustodita la documentazione durante lo svolgimento delle operazioni di fotocopiatura;
- l’autorizzato pone nel cestino una fotocopia recante dati personali solo previa adeguata distruzione della stessa;
- al termine delle medesime operazioni, l’autorizzato deve provvedere al ritiro tempestivo degli originali e delle copie dalla fotocopiatrice.

6.3 Utilizzo del fax

Il fax non deve essere utilizzato per trasmettere dati di tipo particolari (es. dati sulla salute); l’uso può essere consentito purché sia certo e conosciuto il destinatario.
Come la fotocopiatrice, anche il fax deve essere collocato in una zona non liberamente accessibile al pubblico onde evitare che informazioni riservate possano essere indebitamente lette da chi non è autorizzato.
Qualora si tratti di un numero faxato per la prima volta, è opportuno accertarsi con una preventiva telefonata in ordine al fatto che il documento sarà ritirato da un soggetto autorizzato.
I fax in “entrata” devono essere ritirati il prima possibile dagli autorizzati onde limitare al minimo il periodo di incustodita e quindi pericolosa giacenza degli stessi.

6.4 Utilizzo stampanti

Non deve essere utilizzata carta riciclata che abbia sull’altro lato dati personali.
In caso di stampa di documenti contenenti dati personali o particolari questi vanno immediatamente recuperati dalla stampante, a meno che non si utilizzi una stampante presidiata.

6.5 Archivi cartacei correnti

L’archivio corrente comprende i documenti attualmente in uso nelle varie Aree aziendali.
La gestione degli archivi cartacei correnti si ascrive alla competenza e responsabilità del soggetto designato di area. Lo stesso individua le tipologie dei documenti contenenti i dati sensibili e giudiziari e i dipendenti autorizzati dei relativi trattamenti. Il soggetto designato deve assicurare che la documentazione venga custodita in locali ad accesso selezionato e presidiato. In mancanza, in armadi dotati di serratura, le cui chiavi dovranno essere conservate in modo appropriato. Il personale addetto alle pulizie deve svolgere la propria attività con espressa autorizzazione ad accedere.

6.6 Archivi cartacei storici

L’archivio storico comprende i documenti che hanno esaurito il loro ciclo di trattamento (es. fascicoli del personale in pensione, pratiche amministrativa concluse etc…). L’accesso alla documentazione di tali archivi potrà avvenire esclusivamente da parte del personale autorizzato. La selezione e lo scarto della documentazione deve avvenire nel rispetto delle prescrizioni normative vigenti.
Le persone ammesse, a qualsiasi titolo, ad accedere agli archivi contenenti dati particolari e/o giudiziari fuori orario di lavoro, devono essere autorizzate identificate e registrate su apposito registro.

6.7 Modalità operative di utilizzo degli strumenti informatici

Per quanto attiene alle modalità di utilizzo degli strumenti informatici si rinvia al "Regolamento per l'utilizzo degli strumenti informatici" approvato dal Consiglio di Amministrazione in data 19 dicembre 2019, le cui previsioni si intendono integralmente richiamate.

7. VIOLAZIONE DEI DATI (DATA BREACH)

Con il termine Data Breach, o violazione dei dati personali, si intende (art. 4 comma 12 RGPD 679/2016) qualsiasi violazione della sicurezza che comporti, 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.

Nello specifico, potrebbero comportare violazione di dati eventi quali il furto o smarrimento di pc o chiavette usb, sottrazione o perdita di documenti cartacei, attacchi informatici, comunicazione di dati a soggetti non autorizzati.
Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivamente, provocare danni materiali e immateriali ai soggetti interessati quali, ad esempio, furto d'identità, perdite finanziarie, pregiudizio alla reputazione.
In ragione di quanto sopra è importante che tutto il personale autorizzato al trattamento di dati personali e particolari per conto dell'Azienda, presti sempre la massima attenzione nel prevenire eventuali violazioni, anche involontarie, rispettando le disposizioni ricevute e le procedure definite dal Titolare del trattamento.
L'Azienda ha adottato una procedura operativa di "Gestione delle violazioni dei dati personali (data breach)", approvata dal Consiglio di Amministrazione in data 19 dicembre 2019, successivamente aggiornata il 26 ottobre 2021 e pubblicata nella intranet aziendale, in cui sono delineate le linee guida per la gestione e valutazione delle violazioni di dati personali.
I soggetti interessati, in caso di sospetta violazione di dati personali, devono informare senza ritardo il Responsabile Protezione Dati e le figure apicali della società allo scopo designate, avendo cura di compilare il modulo interno "Allegato B_Data Breach interno".

8. POLITICHE DI SICUREZZA PER IL TRATTAMENTO DEI DATI PERSONALI DEI LAVORATORI

Il trattamento dei dati personali dei lavoratori individua la principale base giuridica nell'ambito del contratto con il quale viene instaurato il rapporto di lavoro. Il contratto deve contenere l'indicazione specifica dei trattamenti dei dati personali necessari all'esecuzione del rapporto di lavoro. Il medesimo contratto deve prevedere il diritto dell'Azienda di fondare il trattamento di dati personali del lavoratore:

- sulla necessità di adempiere ad un obbligo di legge o comunque previsto dal contratto collettivo vigente;
- sulla necessità di tutelare un interesse legittimo del Titolare con possibilità in questo caso del lavoratore di opporsi al trattamento per motivi preminenti rispetto a quelli del lavoratore;
- per la salvaguardia dell'interesse vitale del lavoratore con particolare riferimento ai trattamenti che riguardano la salute dei lavoratori.

In tutti i casi in cui non ricorra una delle ipotesi sopra indicate, all'atto di acquisire i dati personali deve essere richiesto il consenso del lavoratore con l'avvertenza che il rifiuto di prestarlo non ha nessuna conseguenza sul rapporto di lavoro né sulla sua prosecuzione.

8.1 Comunicazione e diffusione di dati personali

Ai dati personali dei lavoratori possono avere accesso unicamente gli autorizzati dello specifico trattamento per i quali sono raccolti.
I dati dei lavoratori non possono essere comunicati salvo il caso in cui:

- la base giuridica (contratto/legge) del trattamento ne richieda la trasmissione a soggetti determinati;
- vi sia il consenso dell'interessato.

Il consenso del lavoratore è sempre necessario per la diffusione: es. fotografie sulla intranet aziendale.

8.2 Dati particolari dei lavoratori

I documenti, anche informatici, di qualunque genere contenenti dati personali dei lavoratori idonei a rivelarne l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici, lo stato di salute, la vita o l'orientamento sessuale, devono essere conservati separatamente da ogni altro dato personale dell'interessato e comunque in modo da non consentirne una indistinta consultazione nel corso delle ordinarie attività amministrative e al fine di impedire ogni accesso a tali dati da parte di soggetti non previamente designati come autorizzati o responsabili del trattamento dati.

8.3 Sicurezza e igiene sul lavoro

Le cartelle sanitaria e di rischio contenenti gli accertamenti preventivi e periodici sui lavoratori eseguiti dal professionista medico competente è custodita presso l'Azienda ed è coperta da segreto professionale. La stessa può essere consultata esclusivamente dal medico competente ovvero consegnata alle autorità pubbliche nei casi previsti dalla legge.

All'Azienda è dato accesso alla sola valutazione finale circa l'idoneità sanitaria del dipendente ai fini dello svolgimento della mansione.

9. INTERVENTI INFORMATIVI E FORMATIVI

L'informazione e la formazione in materia di protezione dei dati sono fattori di rilievo per la gestione in sicurezza dei dati e sono finalizzate a fornire:

- la conoscenza degli elementi essenziali della normativa vigente;
- la sensibilizzazione sulle problematiche della protezione dei dati e sulla loro importanza;
- la conoscenza delle misure di sicurezza adottate e la loro gestione ai diversi livelli di responsabilità;
- la conoscenza delle regole di base per il trattamento dei dati;
- la conoscenza delle misure di sicurezza informatica da adottare per un corretto trattamento dei dati effettuato mediante l'utilizzo di strumenti informatici.

Per quanto riguarda le azioni informative, tutti i dipendenti/collaboratori nel momento stesso in cui si instaura il rapporto di lavoro, sono invitati a prendere visione del presente Regolamento diffuso sulla intranet aziendale in apposita sezione.

Per quanto riguarda le azioni formative, sono organizzati corsi di formazione per rendere edotti tutti gli autorizzati del trattamento in merito:

- a come devono essere trattati i dati personali e particolari;
- alle procedure da seguire per la raccolta, elaborazione, custodia ed archiviazione dei dati e dei documenti;
- ai rischi che incombono sui dati;
- alle misure da porre in essere per prevenire eventi dannosi;
- ai profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività;
- alle responsabilità che ne derivano.

In caso di entrata in vigore di nuove disposizioni legislative o in applicazione di aggiornamenti di prassi o procedure interne, il RPD provvede a darne informazione a tutto il personale coinvolto mediante specifiche mail/comunicazioni interne.