



sonepar
italia

POLICY PRIVACY

INDICE

1. Scopo e definizioni del documento	2
2. Principi, ambito di applicazione e destinatari della policy	3
3. Oggetto e modalità di applicazione	4
4. Organigramma e sistema di nomine e responsabilità	4
4.1 Titolare del Trattamento	4
4.2 Responsabile del Trattamento	5
4.3 Referenti privacy	6
4.4. Autorizzati al Trattamento	7
4.4 Referente esecutivo per la protezione dei dati personali (DPM)	8
4.5 Amministratore di sistema	9
5. Impegno alla riservatezza	10
6. Trattamento dei dati personali (definizione e mappatura dei trattamenti)	10
6.1 Dati dei dipendenti dei collaboratori e dei componenti degli Organi Aziendali	11
6.2 Dati dei clienti	11
6.3 Dati dei terzi	12
7. Misure di sicurezza e relativi controlli	12
7.1 La gestione della sicurezza: ruoli e responsabilità	12
7.2 Misure per garantire l'integrità a protezione dell'accesso ai dati	12
7.3 Clean Desk Policy	13
7.4 Misure per garantire la disponibilità dei dati	14
7.4.1 Processo di assunzione dei dipendenti	14
7.4.2 User ID Management	14
7.4.3 Processo di dimissione del dipendente	14
7.4.4. Review delle utenze	14
7.4.6. Dismissione dei dispositivi utilizzati dagli utenti di Sonepar Italia S.p.A.	14
7.5 Livelli di sicurezza	15
8. Informazione e formazione dei destinatari	15
9. Disposizioni interne per il corretto utilizzo degli strumenti informatici e telematici	16
9.1 Utilizzo del personal computer e internet	17
9.2 Gestione delle credenziali di accesso	18

1. Scopo e definizioni del documento

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

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

- **Regolamento:** Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (c.d. GDPR - Regolamento Generale sulla Protezione dei Dati);
- **Normativa:** D.Lgs. n. 169 del 2003 e Regolamento UE n. 679 del 2016, nonché ulteriori provvedimenti in materia di fonte normativa secondaria in vigore al momento dell'approvazione della seguente policy.
- **Codice Privacy:** Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";
- **Società:** Sonepar Italia S.p.A.
- **Affiliate:** società controllate o collegate da Sonepar Italia S.p.A. stabilite nel territorio dello Stato italiano o in un luogo comunque soggetto alla sovranità dello Stato italiano;
- **Titolare del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- **Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **Dati genetici:** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **Dati biometrici:** i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- **Dati relativi alla salute:** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- **Interessato:** la persona fisica cui si riferiscono i dati personali;
- **Responsabile del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

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

2. Principi, ambito di applicazione e destinatari della policy

Il presente documento si applica a tutti i trattamenti dei dati effettuati dagli uffici di Sonepar Italia S.p.A., automatizzati o svolti manualmente, in cui la predetta agisce in qualità di Titolare.

La presente Policy è di applicazione immediata per Sonepar Italia S.p.A. e dovrà essere recepita dalle sue Affiliate tempestivamente e comunque non oltre 90 giorni dalla sua emissione, tramite deliberazione del Consiglio di Amministrazione e ratifica da parte del Consiglio di Amministrazione delle Affiliate.

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

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati; a tal proposito sono state adottate misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Le presenti indicazioni sono valide anche, per tutti quei trattamenti di cui Sonepar Italia S.p.A. è nominata Responsabile esterno da altri Titolari, salvo la presenza di misure più restrittive in materia di protezione dei dati personali.

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

Tale policy si applica a tutti i Soci, ai dipendenti di Sonepar Italia S.p.A. e ai collaboratori esterni, che collaborano in modo continuo con quest'ultima.

3. Oggetto e modalità di applicazione

Oggetto della presente Policy è il trattamento dei Dati Personali, anche detenuti all'estero, effettuato da Sonepar Italia S.p.A. o da una sua Affiliata.

Le norme della presente Policy si applicano, inoltre, al trattamento dei Dati Personali effettuato da Società Controllate stabilite nel territorio di un Paese non appartenente all'Unione Europea che impiegano, per il Trattamento, strumenti situati nel territorio dello Stato italiano anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione Europea. Sono esclusi dall'ambito di applicazione:

- i Trattamenti dei Dati Personali effettuati da Società Controllate con sede nel territorio dell'Unione Europea, ma non in Italia. Tali Società Controllate dovranno attenersi alla specifica normativa in materia di privacy vigente nello Stato in cui la Società ha sede;
- i Trattamenti dei Dati Personali effettuati da persone fisiche per fini esclusivamente personali e nei casi in cui i dati non sono destinati ad una comunicazione sistematica o alla diffusione (anche se utilizzati ai fini di esigenze di lavoro: ad esempio, banca dati su PC accessibile ed utilizzata solo ed esclusivamente dall'utente - persona fisica per un'elaborazione personale - rubrica telefonica).

4. Organigramma e sistema di nomine e responsabilità

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

4.1 Titolare del Trattamento

Conformemente a quanto previsto dalla normativa, è Titolare del trattamento la società Sonepar Italia S.p.A. e quest'ultima si impegna a:

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

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

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

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

4.2 Responsabile del Trattamento

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

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

- osservare le procedure in materia di protezione dei dati personali adottate dal Titolare;
- organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni di legge e predisporre tutti i documenti nonché le misure tecniche organizzative richiesti dal Codice e dal Regolamento;

- adottare e verificare il rispetto delle misure di sicurezza indicate dal Codice e dal Regolamento e la conformità dei sistemi e delle misure di sicurezza;
- redigere e aggiornare il registro delle attività di trattamento, qualora venga adottato;
- informare il Titolare del trattamento di tutte le misure adottate e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato;
- nominare gli incaricati che svolgono le funzioni di amministratore di sistema, conservando i relativi estremi identificativi, definendo gli ambiti di operatività ai medesimi consentiti e verificando almeno annualmente il relativo operato per controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti il trattamento dei dati personali;
- inviare, con periodicità stabilita dal Titolare, una lista aggiornata dei nominativi e degli ambiti di operatività degli amministratori di sistema, in particolare al fine di consentire al Titolare l'adempimento dell'obbligazione posta a suo carico dal Provvedimento del Garante Privacy del 27.11.2008 circa il trattamento dei dati dei dipendenti;
- nominare gli autorizzati al trattamento dei dati ai sensi dell'art. 30 del Codice, conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione;
- controllare le operazioni di trattamento svolte dagli incaricati e la conformità all'ambito di trattamento consentito;
- redigere e aggiornare la lista dei nominativi degli autorizzati e verificarne almeno annualmente l'ambito del trattamento consentito ai medesimi;
- proporre al Titolare del trattamento dei dati la nomina di soggetti esterni quali Responsabile del trattamento dei dati in relazione all'affidamento agli stessi di determinate attività;
- attuare gli obblighi di informazione ed acquisizione del consenso, quando richiesto, nei confronti degli interessati;
- garantire all'interessato che ne faccia richiesta l'effettivo esercizio dei diritti previsti dalla normativa di settore;
- distruggere i dati personali alla fine dei trattamenti degli stessi nei casi previsti dal Regolamento, secondo le procedure atte a garantire la sicurezza degli stessi e provvedere alle formalità di legge e agli adempimenti necessari anche mediante comunicazione al Garante, se dovuta;
- comunicare immediatamente al titolare non oltre le 24 ore successive al loro ricevimento, ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità Giudiziaria;
- osservare le procedure in materia di protezione dei dati personali adottate dal Titolare;
- informare l'interessato del trasferimento dei dati all'estero.

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

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

4.3 Referenti privacy

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

I compiti del Referente privacy, autorizzato con apposito atto, sono di seguito sintetizzati:

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

4.4. Autorizzati al Trattamento

Il Titolare ha provveduto a nominare, presso le Unità Organizzative in cui vengono svolti i trattamenti, le persone autorizzate al trattamento dei dati, così come indicato dall'art. 30 del Codice Privacy e come indicato dal Garante Privacy¹.

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

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

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

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

- rilasciare all'interessato l'informativa e acquisire il consenso laddove necessario, secondo le istruzioni impartite dal Titolare.

4.4 Referente esecutivo per la protezione dei dati personali

Alla luce dell'analisi dei rischi aziendali in materia di trattamento dei dati personali, il Titolare ha ritenuto opportuno procedere alla nomina del Referente esecutivo per la protezione dei dati personali (DPM). A tal riguardo si precisa che le attività di trattamento, a monitoraggio regolare e sistematico, di dati personali non costituiscono il *core business* di Sonepar.

I compiti affidati al Referente esecutivo per la protezione dei dati personali (DPM) con espresso atto di designazione (cfr. allegato "B" al quale si rimanda per un più dettagliato elenco) sono i seguenti:

- sorvegliare l'osservanza della normativa in materia di privacy nonché delle politiche del Titolare del trattamento o del DPO di Gruppo, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti;
- vigilare sull'effettivo funzionamento delle prescrizioni adottate dalla Società in materia di Privacy;
- effettuare audit in materia di Privacy e controllare l'applicazione del principio di privacy by design e by default;
- informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla normativa in materia privacy;
- promuovere la cultura della protezione dei dati all'interno della società e contribuire a dare attuazione a elementi essenziali del Regolamento (es. principi fondamentali del trattamento, diritti degli interessati, privacy by design e by default, registro delle attività di trattamento, sicurezza dei trattamenti e data breach);
- conservare e aggiornare l'elenco dei Referenti privacy e autorizzati al trattamento dei dati;
- ricevere e dare esecuzione alle istruzioni e alle prescrizioni impartite dal DPO di Gruppo per la conformità della Società al Regolamento UE n. 679 del 2016;
- riportare direttamente al DPO le decisioni adottate dal Titolare in contrasto con la normativa privacy o in dissenso alle indicazioni ricevute dal DPO di Gruppo;
- predisporre e attuare adeguati flussi di comunicazione da e verso il DPO di Gruppo, ivi inclusi gli alert/data breach di sistema;
- fornire al DPO di Gruppo accesso alle informazioni necessarie per lo svolgimento dei compiti a quest'ultimo attribuiti;
- fungere da punto di contatto tra i referenti privacy/autorizzati al trattamento e il DPO di Gruppo;
- fungere da punto di contatto per l'interessato relativamente a tutte le questioni inerenti il trattamento dei loro dati personali e all'esercizio dei diritti;
- redigere una relazione annuale sulle proprie attività da sottoporre al DPO di Gruppo;
- tenere e aggiornare il Registro dei trattamenti;
- supportare il DPO di Gruppo nella DPIA, fornendo un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- coinvolgere il DPO di Gruppo in questioni di particolare complessità o che presentino i caratteri del monitoraggio regolare e sistematico su larga scala;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
- cooperare con l'autorità di controllo;
- informare tempestivamente il DPO di Gruppo in caso di data breach;

- garantire riservatezza in merito all'adempimento dei propri compiti, in conformità con il diritto previsto dall'UE o dagli Stati Membri.

4.5 Amministratore di sistema

La figura professionale che, in ambito informatico, mantiene, configura e gestisce (i) un sistema di elaborazione dati o sue componenti, ivi inclusi sistemi software complessi quali i sistemi Enterprise Resource Planning (system administrator), ovvero (ii) una base dati (database administrator), ovvero (iii) reti e apparati di telecomunicazione di sicurezza (network administrator) è nominata Amministratore di Sistema.

L'attribuzione delle funzioni di Amministratore di sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di Trattamento, ivi compreso il profilo relativo alla sicurezza.

La nomina ad amministratore di sistema deve essere individuale, formalizzata, con l'indicazione analitica degli ambiti di applicazione di operatività consentiti in base al profilo di autorizzazione assegnato.

In generale, l'Amministratore di sistema ha le seguenti responsabilità:

- sovrintendere alle risorse dei sistemi computerizzati al fine di consentirne una corretta ed efficiente utilizzazione;
- in accordo con il Manager della Protezione dei Dati personali, fornire guida e supporto ai Referenti e agli Incaricati in merito al trattamento dei dati personali;
- amministrare e gestire la sicurezza informatica operando anche come gestore e custode delle password;
- nell'ambito delle responsabilità assegnate, effettuare periodici controlli e verifiche tecniche, anche nei riguardi dei Responsabili e degli Incaricati in merito a quanto previsto dal presente documento;
- individuare l'eventuale soggetto/i esterno/i quale manutentore del sistema stesso. L'amministratore che provvede alla designazione dei soggetti incaricati alla manutenzione deve preventivamente informare il Titolare del Trattamento e deve formalizzare per iscritto l'attribuzione dell'incarico eventualmente specificando i limiti dell'intervento e le manutenzioni richieste. Per manutenzione s'intende non soltanto l'intervento tecnico diretto ad eliminare eventuali avarie hardware, ma anche gli interventi volti alla ricostruzione di archivi che dovessero in qualche modo risultare danneggiati o corrotti oltre all'intervento tecnico diretto ad eliminare eventuali avarie al software di sistema e all'applicativo utilizzato;
- per poter svolgere funzioni, allo stesso vengono concesse dal Titolare le "Autorità di sistema", che consistono nell'assegnazione di attributi, privilegi, o accessi che consentono la gestione delle "risorse critiche del sistema operativo", ovvero degli oggetti informatici necessari al funzionamento dei sistemi e del servizio di elaborazione dati (es. log di sistema, tabella di servizio, cataloghi dei dati, ecc.).
- L'elenco dei soggetti nominati Amministratori di sistema sono conservati presso il Reparto IT e consegnati in copia per la custodia al Manager della Protezione dei dati.
- Amministratori di sistema esterni: l'elenco dei soggetti nominati Amministratori esterni è conservato presso il Reparto IT e consegnato in copia per la custodia al Manager della Protezione dei dati, nonché presso l'Amministratore esterno a cui è rilasciata copia.

5. Impegno alla riservatezza

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

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

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

finalità connesse alla

- disciplina in tema di antiriciclaggio.

In relazione alle indicate finalità il trattamento dei dati avverrà in modo da garantire la sicurezza e la riservatezza e potrà essere effettuato attraverso strumenti manuali, informatici e telematici atti a memorizzare, gestire e trasmettere i dati stessi nel rispetto delle misure di sicurezza previste dal Codice. Tutti gli Amministratori e dipendenti di Sonepar italia S.p.A. sono tenuti al segreto previsto dall'art. 2407 del codice civile.

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

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

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

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

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

Il predetto registro deve contenere:

- a) il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del contitolare del trattamento, del Rappresentante esterno del trattamento, del DPO di Gruppo e del Referente esecutivo per la protezione dei dati personali;
- b) le finalità del trattamento;
- c) una descrizione delle categorie di interessati e delle categorie di dati personali;

- d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti, la documentazione delle garanzie adeguate;
- f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- g) ove possibile, una descrizione generale delle misure di sicurezza tecniche.

Nello svolgimento delle proprie attività, Sonepar Italia S.p.A. può svolgere trattamenti di dati che riguardano il personale dipendente, nonché candidati, i clienti o terzi fornitori/collaboratori.

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

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

Sonepar Italia S.p.A. al fine di adempiere ai propri obblighi di gestione del personale, raccoglie i dati dei componenti degli organi aziendali e dei propri dipendenti, informandoli dei propri diritti.

In particolare, il trattamento dei dati delle suddette categorie è previsto per finalità amministrativo-contabili, quali ad esempio:

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

Con riferimento al trattamento dei dati dei candidati, Sonepar Italia S.p.A. si impegna a verificare l'acquisizione del consenso al trattamento dei dati e a fornire adeguata informativa.

(Allegato 1 - registro dei trattamenti di Sonepar Italia S.p.A.)

6.2 Dati dei clienti

Sonepar Italia S.p.A. per mezzo dei propri Referenti o Autorizzati, può raccogliere i dati personali dei clienti direttamente presso la clientela ovvero presso terzi, al fine di perfezionare accordi contrattuali, per poter effettuare le necessarie valutazioni, le quali hanno ad oggetto prevalentemente la valutazione del rischio di credito.

I dati personali dei clienti potranno essere trattati nell'ambito della normale attività di Sonepar Italia S.p.A. per le seguenti finalità:

- prestare i servizi richiesti e gestire i rapporti con la clientela (es. acquisizione di informazioni preliminari alla conclusione di un contratto, esecuzione di operazioni sulla base degli obblighi derivanti dal contratto concluso con la clientela, ecc);
- adempiere ad obblighi previsti da un regolamento o dalla normativa comunitaria (es. centrale rischi, normativa in materia di antiriciclaggio ecc.), nonché per osservare disposizioni impartite dalle pubbliche Autorità ed organi di vigilanza e controllo a ciò legittimati dalla legge. In tal caso il conferimento dei dati personali è necessario e obbligatorio e per il trattamento di tali dati non è richiesto il consenso;

- svolgimento di indagini di mercato/customer satisfaction e marketing, tra cui rientrano indagini di mercato e rilevazione del grado di soddisfazione della clientela e promozione e vendita di prodotti e servizi di Sonepar Italia S.p.A. o di società terze con le quali possono essere stati conclusi accordi commerciali.

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

6.3 Dati dei terzi

Durante lo svolgimento dell'attività, Sonepar Italia S.p.A. può venire a conoscenza di dati che riguardano terzi, ovvero fornitori, collaboratori ecc.

In tali casi Sonepar Italia S.p.A. si impegna a sottoscrivere apposita clausola o accordo al fine di garantire la corretta applicazione delle presenti indicazioni anche nei rapporti con i terzi.

7. Misure di sicurezza e relativi controlli

7.1 La gestione della sicurezza: ruoli e responsabilità

La responsabilità dell'attività di impostazione e coordinamento dei sistemi che garantiscono la sicurezza e la tutela di tutti i dati oggetto di trattamento aziendale sia da un punto di vista logico che fisico, la loro gestione diretta o tramite fornitori, sono in carico al Responsabile della Direzione IT.

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

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

Sonepar Italia S.p.A., in qualità di Titolare del trattamento dei dati, è tenuta a proteggere i dati personali trattati in modo sicuro.

I dati in formato elettronico possono essere archiviati su: Cartelle in Cloud, cartelle su Server non cifrato, cartelle all'interno di PC non cifrato con password policy elevata.

Tali misure sono classificate da Sonepar Italia S.p.A. nell'allegato *Metodologia Data Protection Impact Assessment*

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

Sono le misure di sicurezza volte a minimizzare i rischi che le informazioni siano rivelate o modificate senza autorizzazione, ovvero perse o alterate accidentalmente o intenzionalmente.

Il sistema in atto prevede un sistema di autenticazione, basato su codice identificativo e password individuale segreta, per assicurare che la persona che accede al sistema, nelle sue diverse

articolazioni, sia identificata con certezza, nonché un sistema di autorizzazione, che prevede che a ciascuna persona che accede al sistema sia assegnato un profilo di accesso che definisce i dati ai quali l'utente è autorizzato ad accedere e, ove applicabile, le operazioni che per ciascun dato o gruppo di dati è autorizzato ad eseguire (consultazione, inserimento, modifica, cancellazione). Nessun dipendente di Sonepar Italia S.p.A. è amministratore di sistema della propria macchina, gli utenti che dispongono di un pc aziendale sono censiti all'interno dell'Active Directory.

7.3 Clean Desk Policy

La politica di "scrivania pulita" è una delle migliori strategie da attuare quando si cerca di ridurre il rischio di violazioni della sicurezza della postazione di lavoro.

Lo scopo di questa politica è di stabilire i requisiti minimi per adeguarsi non solo ai controlli della ISO 27001, ma anche per prevenire eventi di data breach e responsabilizzare i dipendenti aziendali. Di seguito sono elencati i comportamenti da applicare:

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

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

7.4 Misure per garantire la disponibilità dei dati

Sono le attività volte a ridurre i rischi di indisponibilità (parziale o totale) nell'accesso al sistema informatico di Sonepar Italia S.p.A..

7.4.1 Processo di assunzione dei dipendenti

Nel contesto di assunzione di una nuova risorsa in Sonepar Italia S.p.A., l'ufficio HR è tenuto ad inviare una mail almeno 7 giorni prima della data di ingresso della risorsa all'IT Support per la creazione dell'utenza in AD, in Office 365 e per la preparazione del PC e di eventuale telefono aziendale (Manager, Partner). Questi ultimi vengono consegnati al momento dell'ingresso della nuova risorsa.

Servizi IT:

- Con Office 365: la risorsa avrà in dotazione l'account di posta, OneDrive e Sharepoint per l'archiviazione ed il trasferimento delle carte di lavoro relativi ai progetti.
- Zucchetti: applicativo per visualizzazione e download del cedolino (profilo abilitato dalla funzione MAC).

7.4.2 User ID Management

Tutte le utenze hanno un unico ID ed un unico dominio. L'utenza è personale e non è concesso che essa sia condivisa con uno o più soggetti.

Sonepar Italia S.p.A. può modificare i diritti di accesso ai servizi e ai sistemi in qualsiasi momento e per qualsiasi ragione.

Tutti i dipendenti di Sonepar Italia S.p.A. non sono amministratori di macchina dei dispositivi rilasciati in dotazione.

7.4.3 Processo di dimissione del dipendente

Nel caso di dimissioni di una risorsa da Sonepar Italia S.p.A., l'ufficio HR è tenuto ad inviare una mail almeno 7 giorni prima della data di cessazione del rapporto di lavoro all'IT Support per la disabilitazione dell'utenza e per la riconsegna del PC e dell'eventuale telefono aziendale. L'IT Support disabilita immediatamente tutti i diritti di accesso del dipendente su Office 365 e rete aziendale.

7.4.4. Review delle utenze

L'IT Support verifica, con cadenza semestrale, insieme al dipartimento HR che la lista dei dipendenti cessati sia coerente con le utenze disabilitate.

7.4.6. Dismissione dei dispositivi utilizzati dagli utenti di Sonepar Italia S.p.A..

Tutti i dispositivi di Sonepar Italia S.p.A., rilasciati in dotazione ai dipendenti, vengono formattati a seguito delle dimissioni degli stessi al fine di rimuovere tutti i dati personali contenuti al loro interno.

Tutti i dipendenti di Sonepar Italia S.p.A. sono, quindi, tenuti ad assicurarsi che venga correttamente eseguito il passaggio di consegne tra i colleghi del team affinché venga assicurata la continuità dei servizi erogati e la conservazione delle carte di lavoro relative ai clienti.

7.5 Livelli di sicurezza

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

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

8. Informazione e formazione dei destinatari

L'obiettivo di garantire un corretto trattamento dei dati, conforme ai requisiti previsti dalla normativa², viene raggiunto dalla Società anche e soprattutto grazie alla particolare attenzione risposta nei confronti della formazione del proprio personale.

A tal proposito, fin dal momento di ingresso di una nuova risorsa, Sonepar Italia S.p.A. presenta a quest'ultima la Policy Privacy, nonché le comunica eventuali aggiornamenti con e-mail inviata a tutti i dipendenti. Tale policy viene comunque archiviata all'interno della intranet aziendale accessibile a tutti gli utenti di Sonepar Italia S.p.A..

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

Secondariamente, allo scopo di formare gli Incaricati e i Responsabili dei trattamenti, la Società:

1. adotta un piano formativo con l'obiettivo di alfabetizzazione in materia di protezione dei dati personali, destinato a tutto il personale della società;
2. prevede l'erogazione di un modulo relativo alla formazione privacy all'interno dei corsi organizzati all'atto dell'ingresso in servizio in Sonepar Italia S.p.A. o anche al momento del cambio di mansione, qualora tale cambio preveda l'utilizzo di un nuovo applicativo, sistema o software all'interno della quale vengono trattati dati personali;
3. prevede un piano di formazione programmato con cadenza annuale sulla formazione erogata in ambito privacy a tutti i dipendenti della società;
4. conserva la documentazione distribuita e la modulistica attestante la partecipazione agli interventi formativi.

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

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

La formazione deve essere:

- adeguata al proprio sistema di trattamenti dei dati;
- capace di trasmettere agli incaricati e responsabili del trattamento misure adeguate di sicurezza e protezione dei dati personali adottate dal Titolare;
- documentabile, in quanto la formazione dell'avvenuto training è parte integrante della policy privacy di Sonepar Italia S.p.A., e può essere richiesta in qualsiasi momento da enti specifici.

9. Disposizioni interne per il corretto utilizzo degli strumenti informatici e telematici

La Società si è dotata di procedure specifiche per l'uso dei sistemi informatici nonché l'accesso ad internet. Tali procedure, che vengono diffuse tra i dipendenti della Società e sono raccolte presso il Responsabile al trattamento, hanno lo scopo di ridurre i rischi di natura patrimoniale, di danneggiamento di immagine della Società nonché di incorrere in responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge.

Le regole che disciplinano l'utilizzo delle risorse informatiche e telematiche si ispirano al principio della diligenza e correttezza, principi che normalmente si adottano nell'ambito dei rapporti di lavoro. Per quanto non espressamente indicato, si rimanda alla normativa specifica in materia, adottata

dalla Società. Tali misure sono classificate da Sonepar Italia S.p.A. nell'allegato L "Regolamento Informatco Aziendale"

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

9.1 Utilizzo del personal computer e internet

Il Personal Computer affidato all'utente è uno strumento di lavoro, pertanto ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. È quindi assolutamente proibita la navigazione in Internet per motivi personali e diversi da quelli strettamente legati all'attività lavorativa.

Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

L'accesso alla intranet aziendale avviene solo attraverso specifiche credenziali di autenticazione, che devono essere custodite da parte dell'utente (v. *Regolamento Informatco Aziendale*).

Il personale incaricato del Reparto IT ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del Reparto IT per conto della Società né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.

L'inosservanza della presente disposizione espone la stessa Società a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico della società, come disposto dall'art. 25-nonies del D.lgs. 8 giugno 2001, n. 231, con applicazione di sanzioni pecuniarie ed interdittive.

Salvo preventiva espressa autorizzazione del personale del Reparto IT, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem ecc.).

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Reparto IT nel caso in cui siano rilevati virus.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo, salvo disposizioni e/o richieste specifiche da parte del Reparto IT.

In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Qualora, l'utente sia dotato di un PC portatile, egli è responsabile di custodirlo con diligenza sia se l'utilizzo avviene fuori sede sia durante l'utilizzo nel luogo di lavoro, in quest'ultimo caso bloccandolo con il relativo cavo di sicurezza.

I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, la Società rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che previene determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list.

Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

I supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dagli utenti in armadi chiusi. E' vietato l'utilizzo di supporti rimovibili personali.

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, ecc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione Aziendale, tramite il personale del Reparto IT o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

9.2 Gestione delle credenziali di accesso

Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Reparto IT, previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

Nel caso di collaboratori a progetto e coordinati e continuativi la preventiva richiesta, se necessaria, verrà inoltrata direttamente dalla Direzione aziendale ovvero dal Responsabile dell'ufficio/area con il quale il collaboratore si coordina nell'espletamento del proprio incarico.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal Reparto IT, associato ad una Password riservata che dovrà venir custodita dall'autorizzato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Reparto IT.

La Password, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'autorizzato. In ogni caso la Password dovrà soddisfare i requisiti delle singole applicazioni.

È necessario procedere alla modifica della parola chiave a cura dell'utente autorizzato del trattamento al primo utilizzo e, comunque, quando richiesto dall'applicazione e, successivamente, almeno ogni 2 (due) mesi.

Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale del Reparto IT.

Il soggetto preposto alla custodia delle credenziali di autenticazione è il personale autorizzato del Reparto IT.