Meridian s.r.l.
Viale Erminio Spalla, 9
00142 Roma (RM)
C.F.: 13693001003
E-mail: info@meridian-group.eu
PEC: meridiangroup@legalmail.it

Privacy Policy adottata da Meridian s.r.l.

Revisione del 23/04/2025

Meridian s.r.l.
Viale Erminio Spalla, 9
00142 Roma (RM)
C.F.: 13693001003
E-mail: info@meridian-group.eu
PEC: meridiangroup@legalmail.it

Indice

Premessa.

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, Tablet, Smartphone e più in generale ogni apparato in gradi di connettersi alla rete informatica del Titolare, espone Meridian s.r.l. (nel seguito "**il Titolare")** e gli utenti (dipendenti e collaboratori dello stesso) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e normativa sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine del Titolare stesso.

Premesso quindi che l'utilizzo degli strumenti di lavoro, nei quali sono compresi anche i sistemi e le risorse informatiche e telematiche, deve sempre ispirarsi al principio della diligenza e correttezza, propri del rapporto di lavoro, il Titolare ha adottato la presente Privacy Policy interna diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati nonché originare responsabilità in capo al Titolare ovvero ai singoli lavoratori.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni fornite a tutti i soggetti autorizzati in attuazione del Regolamento 2016/679/UE (nel seguito "GDPR") e del D. lgs. 30 giugno 2003 n. 196 (di seguito "Codice") come modificato dal D. lgs. 101/2018, relativamente alle prescrizioni non in contrasto con il GDPR, nonché integrano le informazioni fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse. Si è inoltre tenuto conto, sempre che non in contrasto con il GDPR, delle principali prescrizioni e le linee guida del Garante privacy in relazione al trattamento di dati personali effettuato dai datori di lavoro, (provvedimento "Linee-guida per il trattamento di dati dei dipendenti privati" del 23 novembre 2006) ai fini delle verifiche per il corretto utilizzo della posta elettronica e della rete Internet da parte dei dipendenti (provvedimento del 1° marzo 2007) nonché delle previsioni dell'art. 4 l. 300/70, come modificato dal D.lgs. 151/2015 relativamente ai controlli sugli "strumenti di lavoro", e tenendo presente le indicazioni fornite dal WP 29 con la "Opinion 2/2017 on data processing at work".

Dal contesto tracciato dal Garante nelle premesse dei citati provvedimenti emerge che:

1. compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;
2. spetta sempre ai datori di lavoro adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e dei dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;
3. è necessario tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;
4. l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di file di log, della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta dei file di log di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere fino alla

conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;

5. le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.

Alla luce delle premesse sopra riportate ed avendo in considerazione che il Titolare, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer desk-top e/o portatili, telefoni cellulari, etc.), sono state inserite nella presente Privacy Policy le opportune indicazioni ed istruzioni relative alle modalità ed ai doveri che ciascun lavoratore deve osservare nell'utilizzo di tale strumentazione.

1. Entrata in vigore della Privacy Policy e pubblicità.

Con l'entrata in vigore della presente Privacy Policy tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

Copia della presente Privacy Policy, oltre ad essere affissa nella eventuale bacheca, verrà resa disponibile nella intranet del Titolare, ed allegata alla comunicazione che ne ufficializza l'adozione nelle forme e con le modalità in uso presso il Titolare.

2. Campo di applicazione della Privacy Policy.

La Privacy Policy si applica a tutti i lavoratori, ossia ai dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori del Titolare a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.).
Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni lavoratore in possesso di specifiche credenziali di autenticazione. Tale figura sarà anche indicata e nominata quale "Soggetto Autorizzato al trattamento" nell'accezione propria dell'art. 29 del GDPR.

All'atto dell'assunzione e/o collaborazione del lavoratore, il Titolare, per lo svolgimento della specifica mansione e/o opera affidata, mette, ovvero può mettere, a disposizione tutta una serie di strumenti aziendali – ad esempio Personal Computer (fissi e/o portatili), periferiche, programmi applicativi, cavi, adattatori, telefoni cellulari, smartphone, tablet, chiavi USB, SIM, rete internet, account di posta elettronica ecc.

Tutti gli strumenti affidati sono da considerarsi strumenti di lavoro volti a rendere la propria prestazione lavorativa e funzionali alla stessa e sono di esclusiva proprietà del Titolare così come tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante detti strumenti.
Gli strumenti aziendali devono essere utilizzati esclusivamente per l'attività lavorativa e non è consentito farne uso diverso e/o improprio e/o personale.

3. Utilizzo del Personal Computer.

3.1 Quando si fa riferimento al PC aziendale, sia esso fisso che portatile, si intende il complesso delle risorse informatiche comprensive di tutti i suoi elementi (notebook, unità di sistema, mouse, tastiera, monitor), accessori, periferiche e componenti hardware e software.

3.2 Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di

manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer (PC) deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

3.3 Il personal computer dato in affidamento all'utente permette l'accesso alla rete del Titolare solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 4 della presente Privacy Policy.

3.4 Il Titolare per garantire la sicurezza del sistema informatico ha la facoltà, in qualunque momento, di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, come più specificatamente precisato al successivo punto 13.1 della presente Privacy Policy.

La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività del Titolare, si applica anche in caso di assenza prolungata od impedimento dell'utente. Analoghe verifiche possono essere effettuate sui siti internet acceduti dagli utenti abilitati alla navigazione esterna.

L'accesso, comunque, verrà effettuato con modalità tali da evitare qualsiasi forma di controllo a distanza.

In ogni caso, il Titolare garantisce la non effettuazione di alcun trattamento mediante sistemi *hardware* e *software* specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:

- lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
- riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
- la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- l'analisi occulta di computer portatili affidati in uso.

3.5 Il Titolare 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 o per attività di manutenzione.

3.6 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal Titolare 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 lo stesso Titolare 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 anche penalmente.

3.7 Salvo preventiva espressa autorizzazione del Titolare, 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, etc.). Non è consentito, inoltre, istallare, memorizzare e/o trattare file, programmi (ad es. di file sharing) documenti e/o informazioni personali o comunque non afferenti alle attività lavorative sul PC aziendale.

3.8 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Titolare nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 10 della presente Privacy Policy relativo alle procedure di protezione antivirus.

3.9 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. 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. Al fine di evitare tali evenienze si dovrà "bloccare" l'utilizzo del PC prima di allontanarsi o impostare la modalità "screen saver" che prevede la richiesta della password per riattivarne l'uso**.**

4. Gestione ed assegnazione delle credenziali di autenticazione.

- Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal Titolare. Nel caso di collaboratori e/o professionisti la preventiva richiesta, se necessario, verrà inoltrata dal Responsabile del trattamento competente per l'ufficio 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 Titolare, associato ad una parola chiave (password) riservata che dovrà venir custodita dal Soggetto Autorizzato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Titolare.
- La parola chiave, 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 al soggetto autorizzato. Per costruire e gestire la password:
  - Utilizzare lettere, numeri e almeno un carattere tra I seguenti:
    . ; $! @ - > <
  - non utilizzare date di nascita, nomi o cognomi propri o di parenti
  - non sceglierla uguale alla matricola o alla user-id
  - custodirla sempre in un luogo sicuro e non accessibile a terzi
  - non divulgarla a terzi e non condividerla con altri utenti
- È necessario procedere alla modifica della parola chiave a cura dell'utente, ove ciò non avvenga grazie a processi automatici del sistema informativo, al primo utilizzo e, successivamente, almeno ogni sei mesi (Ogni tre mesi nel caso invece di trattamento di dati particolari sensibili attraverso l'ausilio di strumenti elettronici).
- 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 Titolare.

5. Utilizzo della rete.

- Per l'accesso alla rete del Titolare ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

- È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le istruzioni impartite.
- Le cartelle utenti presenti nei server del Titolare sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del Titolare. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.
- Il Titolare può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC dei soggetti autorizzati sia sulle unità di rete.
- Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi del proprio PC, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6. Utilizzo e conservazione dei supporti rimovibili.

- Tutti i supporti magnetici rimovibili (CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati rilevanti dal punto di vista del business (classificabili come riservati e/o confidenziali) nonché informazioni costituenti know-how del Titolare, 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.
- Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il Titolare e seguire le istruzioni da questi impartite.
- In ogni caso, i supporti magnetici contenenti dati particolari/sensibili, secondo la definizione dell'art. 4 del GDPR, devono essere adeguatamente custoditi dagli utenti e risposti in armadi chiusi ad accesso controllato.
- È vietato l'utilizzo di supporti rimovibili personali.
- L'utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

7. Utilizzo di PC portatili.

- L'utente è responsabile del PC portatile assegnatogli dal Titolare e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
- Ai PC portatili si applicano le regole di utilizzo previste per i PC desktop.
- I PC portatili utilizzati all'esterno, se autorizzati, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.
- Tali disposizioni si applicano anche nei confronti di soggetti autorizzati esterni quali agenti, forza vendita, ecc.

8. Uso della posta elettronica.

- La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
- È fatto divieto di utilizzare le caselle di posta elettronica messe a disposizione dal Titolare per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:
  - l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
  - l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
  - la partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, è fatto obbligo di comunicarlo immediatamente al Titolare. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.
- La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili.
- Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per il Titolare ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere preventivamente visionata od autorizzata dal Responsabile d'ufficio.
- È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, …), possono richiedere l'autorizzazione e la firma dei Responsabili di ufficio, a seconda del loro contenuto e dei destinatari delle stesse.
- È obbligatorio controllare i file attachment di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
- Al fine di garantire la funzionalità del servizio di posta elettronica e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella, o malattia) invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In caso di assenze programmate la funzionalità deve essere attivata dall'utente; in caso di assenza non programmata (ad es. per malattia) verrà attivata a cura del Titolare.
- Al fine di ribadire agli interlocutori la natura esclusivamente istituzionale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, personale dipendente del Titolare debitamente nominato potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella propria policy. Si riportano di seguito i testi da utilizzare:

  Le informazioni contenute nella presente e-mail potrebbero essere confidenziali e sono dirette unicamente ai destinatari sopra indicati. In caso di ricezione da parte di persona diversa è

vietato qualunque tipo di distribuzione o copia. Chi riceva questo messaggio per errore è pregato di inoltrarlo al mittente e di distruggere questa e-mail.

This e-mail may contain confidential information and is intended only for the use of the addressee(s) named above. If the reader of this message is not the intended recipient of this message, please note that distribution or copying of this communication is forbidden. Anyone who receives this communication in error should return it immediately to the sender and destroy the message.

- Come anticipato al precedente punto 3.4 della presente Privacy Policy, il Titolare potrà accedere ai dati contenuti nelle caselle di posta elettronica di lavoro per le sole finalità ivi indicate.

- In caso di invio di messaggi con allegati contenenti dati personali, procedere in una delle seguenti modalità:

  - **Documenti Office (Word, Excel, etc.):**

    Per proteggere un file Office, completare i seguenti passaggi:

    - Aprire il file di Microsoft Office che si vuole proteggere
    - Fare clic su File
    - Fare clic su Informazioni
    - Fare clic su Proteggi documento o Password
    - Fare clic su Crittografa con password
    - Immettere una password (minimo 8 caratteri) e fare clic su OK
    - Confermare la password e fare clic su OK

  - **Altri formati (PDF, JPG, etc.): comprimere uno o più file con ZIP o RAR e proteggerli con Password.**

    Per proteggere il file ZIP, completare i seguenti passaggi:

    - Nella finestra di WinZip seleziona Azioni > Crittografia o fare clic sul pulsante Crittografia. Verrà visualizzata la schermata Crittografia.
    - Inserire la password (minimo 8 caratteri), e quindi confermarla ripetendo la password. Infine, fare clic su OK. Nella schermata di WinZip, in coda al nome del file apparirà un asterisco (*) a indicare che il file è stato protetto con password.
    - Selezionare File > Esci per chiudere la finestra di WinZip.

Per proteggere il file RAR, completare i seguenti passaggi:

- Selezionare con il mouse uno o più file che si vuole proteggere, usare il pulsante destro del mouse sui file evidenziati e poi selezionare la voce Aggiungi ad un archivio dal menù.

- Nella finestra che appare cliccare sul pulsante Imposta Parola chiave.

- Nella scheda successiva dovrete inserire per due volte la password, la seconda serve per la verifica.

- Chiudere le schede premendo il pulsante Ok. Verrà avviata la compressione dei file e per aprire il nuovo archivio occorrerà la password che è stata inserita.

In entrambi i casi, inviare la password al destinatario con un altro canale (SMS, Whatsapp, etc.).

9. Navigazione in Internet.

- La rete internet aziendale è di proprietà del Titolare.

- Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet, inoltre, costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.

- È assolutamente proibita, durante l'orario di lavoro, la navigazione in Internet per motivi personali e/o diversi da quelli strettamente legati all'attività lavorativa.

- In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare Internet per:
  - l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione;
  - l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal Titolare e comunque nel rispetto delle normali procedure di acquisto;
  - ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
  - navigare in siti con contenuti pornografici e pedo-pornografici o, comunque, che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile; è, altresì, vietata la navigazione nei siti di giochi e/o scommesse online;

- navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative ovvero siti che non contengano informazioni utili all'attività lavorativa ovvero che non forniscano idoneo supporto informativo professionale;
- accedere e/o navigare e/o postare e/o commentare e/o rispondere su sistemi di social networking e di chat/instant messaging personali sul luogo di lavoro o durante l'orario lavorativo;
- la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio;
- l'accesso, tramite Internet, a caselle webmail di posta elettronica personale, salvo specifica autorizzazione.

- Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, il Titolare può prevedere l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a specificati siti inseriti in una black list.
- In ogni caso, durante lo svolgimento dell'attività lavorativa, è vietato l'accesso nonché navigare e/o postare e/o commentare e/o rispondere su qualsivoglia account personale di *social network* sia mediante la rete internet aziendale sia mediante rete internet di dispositivi personali.
- In conformità al punto 3.5, il Titolare potrà procedere a controlli sulla navigazione finalizzati esclusivamente a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 6 mesi.

10. Protezione antivirus.

- Il sistema informatico del Titolare è protetto da software antivirus aggiornato periodicamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo.
- Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al Titolare.
- Ogni dispositivo magnetico di provenienza esterna al Titolare dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al Titolare.

11. Utilizzo dei telefoni, fax e fotocopiatrici.

- Il telefono affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita sempre che vengano rispettati i criteri di ragionevolezza ovvero nel caso di necessità ed urgenza. Si evidenzia che a fronte di volumi di traffico anomali saranno poste in essere le opportune analisi mirate a rilevare eventuali utilizzi impropri.

- Qualora venisse assegnato un cellulare (o smartphone, tablet, etc.) all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare si applicano le medesime regole sopra previste per l'utilizzo del telefono: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS e/o per accedere e/o navigare e/o postare e/o commentare e/o rispondere su sistemi di social networking e di chat/instant messaging personali o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal Titolare.
- È vietato l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Titolare.
- È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Titolare.

12. Gestione Archivi cartacei.

- Quando si tratta di applicare e adottare il GDPR, per i documenti cartacei come per qualsiasi informazione personale detenuta, i soggetti autorizzati devono esaminare le modalità di archiviazione delle informazioni e agire secondo le seguenti regole:
  - Stampare semplicemente un documento e dimenticarsi di averlo fatto può costituire un rischio per la sicurezza e bisogna considerare che dei soggetti non autorizzati potrebbero accidentalmente prendere quel documento stampato.
  - Ogni volta che si invia un documento da stampare tramite una stampante wireless o di rete, si corre il rischio di violazioni della sicurezza.
  - I documenti cartacei da conservare devono essere gestiti in modo da poter essere rintracciati e individuati facilmente. I documenti cartacei contenenti dati particolari sensibili o giudiziari devono essere conservati in armadietti chiusi a chiave il cui accesso è limitato soltanto alle persone autorizzate a quel trattamento.
- Lo smaltimento sicuro della carta deve essere una priorità, in particolare ora che l'UE ha aumentato le sue richieste in materia di protezione dei dati. I documenti cartacei non più necessari devono essere smaltiti in modo conforme. Bisogna utilizzare la macchina distruggidocumenti se presente o in mancanza agire manualmente spezzettando i fogli in piccole parti in modo da non essere più ricomponibili.
- I documenti cartacei contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone non autorizzate al trattamento (es. armadi o cassetti chiusi a chiave).
- I documenti cartacei che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti nel periodo di intervallo meridiano e a fine giornata e non devono rimanere incustoditi su scrivanie o tavoli di lavoro.
- I documenti cartacei contenenti dati particolari sensibili o giudiziari devono essere controllati e custoditi dai soggetti autorizzati in modo che non vi possano accedere persone prive di autorizzazione. La loro consultazione deve avvenire per il tempo strettamente necessario alla necessità di utilizzo e, subito dopo, i documenti devono essere nuovamente archiviati.

13. Data Breach.

Con il termine "**violazione dei dati personali**" (in inglese "**data breach**") si intende una situazione che può comportare, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso a informazioni qualificate dal Regolamento come dati personali trattati per mezzo di sistemi informatici o di altra natura.

La natura della violazione può essere classificata in base ai seguenti principi di sicurezza delle informazioni:

- "perdita di confidenzialità": comunicazione, diffusione, accesso non autorizzato o accidentale;
- "perdita di integrità": modifica non autorizzata o accidentale;
- "perdita di disponibilità": impossibilità di accesso, perdita, distruzione non autorizzata o accidentale.

Di seguito si riportano le principali possibili violazioni di dati personali identificate:

- furto o smarrimento di beni del Titolare, connesso ad un comportamento negligente di dipendenti/collaboratori, che può verificarsi nel caso in cui venga meno il controllo degli strumenti utilizzati per elaborare i dati personali (i.e. Server, PC/laptop, smartphone, device per l'archiviazione di dati esterni);
- accesso illegale da parte di soggetti terzi, ossia accesso abusivo da parte di terzi, non autorizzati, ai sistemi informatici, ad esempio, mediante:
  - un attacco ransomware, mirato al furto di documenti. Questo tipo di attacco di solito può essere classificato come violazione della disponibilità dei dati personali, ma spesso potrebbe verificarsi anche una violazione della riservatezza degli stessi;
  - attacchi *injection*. Tali attacchi mirano a copiare e abusare dei dati personali. Si tratta principalmente di violazioni della riservatezza, ma spesso potrebbe verificarsi anche una violazione dell'integrità degli stessi;
  - attacchi *phising*, ossia truffe informatiche effettuate inviando un'e-mail con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati, motivando tale richiesta con ragioni di ordine tecnico. Tali attacchi sono classificati come violazioni della riservatezza dei dati personali;
  - errore accidentale da parte di uno dei soggetti che trattano dati personali (i.e. invio di una mail contenente dati personali ad un destinatario errato);
  - furto di informazioni, può verificarsi nel caso in cui un dipendente/collaboratore (o ex dipendente/collaboratore) sfrutti la propria conoscenza o le proprie autorizzazioni per sottrarre dolosamente dati/informazioni di carattere personale;
  - vigilanza/adozione di misure di sicurezza, qualora, a causa di un'erronea valutazione sul livello di criticità dei dati e/o informazioni ministeriali, non siano state poste in essere le necessarie precauzioni volte alla salvaguardia dei dati medesimi, che sono stati perduti.

Alcuni possibili esempi di Data Breach sono:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;

- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

In qualità di Soggetti Autorizzati, preposti materialmente ad una o più attività di trattamento per cui sono stati autorizzati, in uno dei casi suddetti, sono obbligati a:

- avvertire immediatamente il referente Privacy del Titolare di eventuali violazioni di dati personali di cui sono a conoscenza, mediante l'invio di una comunicazione scritta;
- fornire supporto in fase identificazione dell'incidente, comunicando al referente Privacy informazioni utili per la classificazione delle violazioni verificatesi.

14. Osservanza delle disposizioni in materia di Privacy.

- È obbligatorio attenersi alle disposizioni in materia di protezione dei dati personali previste dal GDPR, e dal Codice, rispettando le misure di sicurezza adottate, nonché le istruzioni fornite con la designazione ad "Soggetto Autorizzato al trattamento dei dati", come previsto dall'art. 29 del GDPR, applicando puntualmente le disposizioni ivi contenute nonché ogni ulteriore indicazione comunicata, anche per le vie brevi, dal Responsabile d'ufficio.
- I Soggetti Autorizzati al trattamento o i Responsabili che sono addetti alle attività di amministrazione e gestione dei Sistemi, Data Base e della Infrastruttura di connessione (c.d. System Admin, DB Admin e Network Admin.) dovranno rispettare le specifiche istruzioni loro fornite al fine di rispettare i principi di necessità e di legittimità e correttezza nella effettuazione delle loro attività. I nominativi di coloro che hanno competenza sui sistemi che trattano dati personali dei dipendenti del Titolare potranno essere comunicati nelle modalità e con le forme previste dalla normativa applicabile.

15. Accesso ai dati trattati dall'utente.

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, etc.) o per finalità di controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad Internet, traffico telefonico, etc.), è facoltà del Titolare, direttamente o per il tramite degli addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

16. Sistemi di controlli graduali.

- In caso di anomalie e su mandato del Titolare, gli addetti alla manutenzione, effettueranno controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti messi a disposizione e si inviteranno gli utenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere computi solo in caso di successive ulteriori anomalie.

- In alcun caso, per gli strumenti aziendali, verranno compiuti controlli prolungati, costanti o indiscriminati.

17. Sanzioni.

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza della presente Privacy Policy. Il mancato rispetto o la violazione delle regole sopra ricordate possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice civile e sono perseguibili, in virtù dell'art. 4 dello Statuto dei lavoratori, nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal Contratto di lavoro sottoscritto ovvero dal vigente CCNL, nonché con tutte le azioni civili e penali consentite.

18. Aggiornamento e revisione.

- Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate della presente Privacy Policy. Le proposte verranno esaminate dal Titolare.
- La presente Privacy Policy è soggetta a revisione con frequenza periodica anche in funzione dell'introduzione di nuovi strumenti di lavoro e/o informatici, dell'evoluzione tecnologica o di cambiamenti normativi.