LAVORO A DISTANZA
INDICAZIONI OPERATIVE PER LA SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI

Lo svolgimento dell'attività lavorativa all'esterno della sede aziendale richiede da parte dei lavoratori la massima attenzione sui temi quali la riservatezza, nonché un comportamento corretto per proteggere anche l'operatività e la reputazione dell'Azienda.

Il lavoro in modalità a distanza non deve essere effettuato al di fuori di ambienti privati protetti ed il lavoratore deve predisporre una postazione di lavoro dedicata evitando che soggetti non autorizzati possano accedere, anche accidentalmente, alle informazioni e ai dati personali trattati.

Si forniscono, pertanto, le seguenti ulteriori istruzioni operative, ad integrazione di quelle già impartite in ordine al corretto trattamento dei dati nello svolgimento dell'attività lavorativa (documento reperibile sulla Intranet Aziendale – Sezione Comunicazioni Operative), al fine di garantire un livello di sicurezza adeguato al rischio connesso al trattamento dei dati effettuato a distanza mediante l'utilizzo di dispositivi aziendali e/o personali (PC/Tablet/Smartphone, etc.).

PROTEGGERE IL DATO DA ACCESSI NON AUTORIZZATI

Misure da adottare durante le conversazioni tra il/la dipendente e gli altri interessati.

Al fine di evitare l'acquisizione di informazioni da parte di soggetti non autorizzati, le conversazioni telefoniche tra il/la dipendente e gli altri interessati devono essere effettuate in modo tale da proteggere sempre la confidenzialità delle stesse.

Come garantire la confidenzialità delle comunicazioni

- evitando di effettuare colloqui ad alta voce in presenza di soggetti non autorizzati a conoscere il contenuto della conversazione;
- accertandosi che il coniuge o eventuali parenti e conoscenti non siano portati, anche involontariamente, a conoscenza di informazioni e processi attinenti l'attività lavorativa;
- non utilizzando familiari o terzi per veicolare informazioni, anche se ritenute "banali", afferenti l'attività lavorativa;
- accertandosi, nel caso di conversazioni telefoniche instaurate a seguito di chiamate inoltrate o ricevute, che l'interlocutore sia effettivamente un collega/utente/fornitore legittimato e autorizzato a conoscere le informazioni oggetto della comunicazione.

PROTEGGERE IL DATO
DA RISCHI DI DISTRUZIONE, PERDITA E ACCESSI NON CONSENTITI

Il Responsabile della Struttura deve adottare soluzioni organizzative idonee a ridurre il più possibile i rischi di distruzione, perdita e accessi non consentiti ai dati anche in ambiente privato eletto dal/dalla dipendente.

Misure da adottare durante il collegamento:

- per il trattamento di dati personali mediante l'ausilio di strumenti elettronici attenersi alle istruzioni fornite all'atto di nomina ad "autorizzato al trattamento dei dati", nonché alle Policy dell'Ente in materia di Privacy ;
- nel caso di utilizzo di propri dispositivi (pc, connessione, telefono), attenersi alle istruzioni tecniche fornite dai SII e garantire che tali strumenti rispettino i requisiti di sicurezza;
- garantire l'aggiornamento dei meccanismi di sicurezza, nonché il monitoraggio del rispetto dei livelli minimi di sicurezza dei dispositivi personali;
- la documentazione inerente all'attività lavorativa dovrà risiedere esclusivamente sulle cartelle di rete;
- conservare la password di accesso con diligenza in modo che resti riservata, evitando sotto la responsabilità del/della dipendente, che altri ne vengano a conoscenza;
- non lasciare incustoditi ed accessibili a persone non autorizzate il computer ed altri eventuali strumenti in dotazione e/o utilizzati per l'espletamento delle prestazioni di lavoro a distanza (P.C., smartphone, ecc.);
- in caso di allontanamento anche temporaneo dalla postazione di lavoro, disconnettere la sessione di lavoro bloccando l'operatività del computer ("ctrl-alt-canc") e/o l'accesso allo smartphone (password di blocco schermo);
- non utilizzare dispositivi di memorizzazione esterna (come sopra riportato la documentazione inerente all'attività lavorativa dovrà risiedere esclusivamente sulle cartelle di rete, poiché tale modalità operativa è ritenuta adeguata a garantire che il trattamento è effettuato conformemente al regolamento), né sul dispositivo privato.

Misure da adottare nella gestione della documentazione cartacea:

- per quanto concerne l'utilizzo di documenti cartacei contenenti dati personali e prelevati dagli archivi dell'Ente, il trasferimento di dati personali all'esterno deve essere giustificato da necessità strettamente correlate all'esercizio dell'attività lavorativa, agli obblighi di legge o alla difesa degli interessi della società;
- la circolazione dei dati personali cartacei, in situazione di mobilità deve essere ridotta al minimo indispensabile e in tal caso il lavoratore deve prestare particolare attenzione nel trasporto - mediante mezzi pubblici o privati o anche a piedi- dei documenti contenenti dati personali da un locale all'altro, da uno stabile all'altro, da un luogo ad un altro;
- i documenti utilizzati devono essere raccolti in porta documenti riportanti l'identificazione dell'utilizzatore (nominativo e recapito telefonico), della Struttura di appartenenza e dell'Azienda. In particolare i documenti cartacei:
    - devono essere utilizzati solo per il tempo necessario allo svolgimento dei compiti assegnati e poi riportiti negli archivi aziendali dedicati alla loro conservazione;
    - non devono essere lasciati incustoditi e deve essere ridotta al minimo la possibilità che terze persone possano avere accesso alle informazioni contenute nei documenti;
    - in caso di assenza, anche momentanea, dal luogo in cui si svolge la prestazione a distanza è necessario chiudere a chiave i locali che ospitano i dati ovvero riporli dentro un armadio/cassetto chiuso a chiave;
    - i documenti non devono restare, senza ragione, applicati su supporti (lavagne o simili) che possono essere visionati da persone non autorizzate;

- i documenti devono essere resi illeggibili prima di essere cestinati, qualora siano destinati a divenire rifiuti (ad es. strappando più volte la carta in modo che i contenuti diventino non decifrabili/non ricostruibili).

Comportamenti da adottare in caso di violazione dei dati personali.

Nel caso di violazione di dati personali, vale a dire nel caso di incidenti di sicurezza del dato che comportano accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati, si rimanda a quanto previsto nella procedura aziendale per la gestione del Data Breach, disponibile sulla Intranet aziendale –Sezione Privacy.

Data Firma del Dipendente

_____ _____