ISTRUZIONI OPERATIVE PER LA PROTEZIONE DEI DATI PER I LAVORATORI IN REGIME DI LAVORO A DISTANZA (LAVORO AGILE)

Nello svolgimento della prestazione lavorativa in modalità di lavoro a distanza (lavoro agile) è necessario prestare costante attenzione alla protezione dei dati personali e adottare, un comportamento improntato alla difesa della *privacy* degli interessati che entrano in relazione con l'Amministrazione.
Il presente documento contiene le **istruzioni operative** per i lavoratori del Ministero della Transizione Ecologica (MiTE), conformemente al Regolamento UE 2016/679 (GDPR) ed alla relativa normativa nazionale in vigore, da utilizzarsi nell'ambito dello svolgimento della prestazione lavorativa in modalità di lavoro a distanza (lavoro agile).

Nella fattispecie, è necessario, orientare atteggiamenti e comportamenti secondo le seguenti **istruzioni operative**:

- il trattamento dei dati deve essere improntato ai principi di necessità, pertinenza e non eccedenza rispetto alle finalità degli stessi, avere scopi espliciti, determinati e leciti;

- i dati trattati devono essere esatti e aggiornati, archiviati e conservati in modo tale da consentire l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati; ove necessario e compatibile, anonimizzati, pseudonimizzati o cifrati;

- nel trattamento dei dati soggetti a maggior tutela ovvero dati particolarmente sensibili per i diritti e le libertà degli interessati, il dipendente dovrà, altresì, adottare le cautele previste per legge (diritto all'oscuramento e anonimato);

- l'attività lavorativa dovrà essere effettuata in ambienti privati protetti, che garantiscano la necessaria riservatezza della prestazione e tali da consentire comunicazioni stabili, efficienti e non disturbate da rumori circostanti;

- adottare, in qualsiasi occasione, lavorativa e privata, un comportamento improntato alla difesa della *privacy* degli interessati che si relazionano con il Ministero;

- le **conversazioni** tra il dipendente e gli altri interessati non devono essere oggetto di ascolto da parte di soggetti non autorizzati, i quali devono essere mantenuti ad una distanza che consenta di proteggere la confidenzialità; pertanto, è obbligo:
  - evitare di effettuare colloqui ad alta voce, di persona o per telefono, in presenza di soggetti non autorizzati a conoscere il contenuto della conversazione;
  - accertarsi che il coniuge o eventuali parenti e conoscenti non siano portati, anche involontariamente, a conoscenza di informazioni e processi attinenti l'attività lavorativa;
  - non utilizzare familiari o terzi per veicolare informazioni, anche se ritenute "banali", afferenti l'attività lavorativa;
  - nel caso di conversazioni telefoniche instaurate in seguito di chiamate inoltrate o ricevute, accertare, con cura, che l'interlocutore sia effettivamente un collega/cliente/fornitore legittimato e autorizzato a conoscere le informazioni oggetto della comunicazione;

- è necessario ridurre al minimo indispensabile la circolazione di **documenti** cartacei contenenti dati personali. In ogni caso tali documenti:
  - devono essere utilizzati solo per il tempo necessario allo svolgimento dei compiti assegnati e poi immediatamente riposti negli archivi aziendali dedicati alla loro conservazione;

- non devono mai essere lasciati incustoditi; pertanto, nel caso di assenza, anche momentanea, dalla postazione di lavoro agile è necessario chiudere a chiave i locali che ospitano i dati ovvero riporli dentro un armadio/cassetto chiuso a chiave;
- devono essere resi illeggibili prima di essere cestinati, qualora siano destinati a divenire rifiuti;
- è necessario prestare particolare attenzione quando si trasportano da un locale all'altro, da uno stabile all'altro, da un luogo ad un altro (mediante mezzi pubblici o privati o anche a piedi) documenti contenenti dati personali;
- in situazione di mobilità, deve essere ridotta al minimo indispensabile la circolazione dei dati personali cartacei;

- per quanto riguarda l'utilizzo di **strumenti elettronici** (*Personal Computer*, *smartphon)*:
  - l'accesso all'infrastruttura di rete informatica aziendale avviene, per l'utente, mediante l'uso della piattaforma Citrix Virtual App & Desktop (VDI), come anche definito nel "Regolamento di disciplina del lavoro a distanza" del Ministero. Questo strumento consente di instaurare un canale di comunicazione protetto da opportuni meccanismi di sicurezza, che consente di accedere a tutte le risorse e funzionalità della rete aziendale messe a disposizione dall'Amministrazione. Le istruzioni per accedere alla postazione Citrix remota sono illustrate nella "Guida all'accesso e primo accesso alla piattaforma Citrix", condivisa con ogni lavoratore;
  - quale misura di sicurezza di *best practise*, si raccomanda di assicurarsi che i *software* di protezione del proprio sistema operativo (***Firewall, Antivirus***, ecc.) siano abilitati e costantemente aggiornati all'ultima versione disponibile; si raccomanda anche di utilizzare **sistemi operativi** per i quali sia garantito il supporto e che gli stessi siano costantemente aggiornati;
  - nel caso di utilizzo di **strumenti elettronici di proprietà del Ministero** gli stessi devono essere usati esclusivamente dal dipendente e non anche da altre persone (es. familiari e/o conviventi);
  - gli **strumenti elettronici di proprietà del dipendente** utilizzati per il lavoro a distanza dovrebbero essere utilizzati esclusivamente dal dipendente e non anche da altre persone (es. familiari e/o conviventi);
  - il personal computer ed gli altri eventuali strumenti in dotazione e/o utilizzati per l'espletamento delle prestazioni di "Lavoro a distanza" (PC, *smartphone*, personali e/o aziendali ecc.), non devono essere lasciati incustoditi ed accessibili a persone non autorizzate. In caso di allontanamento anche temporaneo dalla postazione di lavoro il/la dipendente è tenuto a disconnettere la sessione di lavoro bloccando l'operatività del computer (*ctrl-alt-canc*) e/o bloccare l'accesso allo smartphone (password di blocco schermo);
  - la documentazione in formato elettronico inerente all'attività lavorativa dovrà risiedere esclusivamente sulle **cartelle di rete internet del Ministero**, poiché tale modalità operativa è ritenuta adeguata a garantire che il trattamento è effettuato conformemente al Regolamento GDPR; non devono essere utilizzati dispositivi di memorizzazione esterna (es.: pennette *usb*, *hard disk*) per la gestione (es. archiviazione di *files*) della suddetta documentazione;
  - non utilizzare dispositivi *mobile* (*smartphone*) per memorizzare e gestire dati personali sensibili e riservati connessi all'attività lavorativa ed ai dati aziendali;
  - utilizzare l'accesso a connessioni *Wi-Fi* adeguatamente protette, non aperte;
  - effettuare sempre il *log-out* dai servizi/portali utilizzati dopo aver concluso la propria sessione lavorativa.
  - **al termine della sezione lavorativa "arrestare" sempre il PC utilizzato**;

- per quanto riguarda la gestione delle credenziali (**nome utente** e ***password***):
  - assicurare la custodia delle credenziali (***password***) di accesso ai sistemi informatici ed agli applicativi necessari per l'espletamento dell'attività lavorativa con diligenza, in modo tale da preservarne, sotto la propria responsabilità, la conoscibilità e l'utilizzo a soggetti terzi;
  - non rivelare e condividere le proprie credenziali, neppure con familiari, amici, colleghi di lavoro e servizi di assistenza dei servizi internet utilizzati;

- utilizzare ***password* diverse** per servizi informatici o siti internet diversi;
- utilizzare ***password* facili da ricordare ma**, allo stesso tempo, **difficili da indovinare**, come quelle che si possono ottenere utilizzando le iniziali delle parole che compongono una frase lunga ma nota;
- utilizzare diverse *password* sul pc utilizzato per lo smart working, ognuna avente un preciso obiettivo:
  - la password di accesso al computer per impedire l'utilizzo non autorizzato alla postazione a qualsiasi altro utente (es.: familiare e/o convivente);
  - la password del salvaschermo o di blocco della sessione, per impedire che una propri momentanea assenza consenta ad una persona non autorizzata di visualizzarne l'attività o di utilizzarne la postazione;

- per quanto riguarda l'utilizzo degli indirizzi ***e-mail*** forniti dal Ministero:
  - utilizzare l'*e-mail* di lavoro esclusivamente per registrazioni a servizi informatici o a siti internet connessi all'attività lavorativa istituzionale;
  - utilizzare il servizio di posta elettronica per comunicare con soggetti terzi, interni ed esterni al Ministero, esclusivamente per finalità lavorative istituzionali del Ministero;
  - nel caso di ricezione di *e-mail* da destinatari sconosciuti contenenti file di qualsiasi tipo o *link* a risorse esterne non procedere alla loro apertura o attivazione;
  - non cliccare su *link* o allegati contenuti in *e-mail* ritenute sospette.

Si richiamano, inoltre, i contenuti delle informazioni fornite ex artt. 13 e 14 Regolamento UE 2016/679, nonché la documentazione presente nella sezione "Privacy Policy" dell'Amministrazione con evidenza, altresì, dell'esercizio delle funzioni di Titolare del Trattamento da parte degli Autorizzati al Trattamento di cui agli artt. 1 e 2 del D.M. n. 237 del 17.06.2022 emanato dal Ministero in materia e, delle obbligazioni ivi riportate a carico dei dipendenti in relazione al ruolo ricoperto e in ottemperanza al principio dell'accountability (responsabilizzazione) previsto dal sopraccitato Regolamento.

Si evidenzia che è severamente sanzionata dal Regolamento (UE) 2016/679 la violazione dei dati personali, cioè la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati Tale violazione può afferire a una "violazione della riservatezza", in caso di divulgazione o accesso accidentale ai dati personali, alla "perdita della disponibilità"(comprese le ipotesi di sottrazione e/o furto), in caso di perdita o distruzione dei dati personali (accidentale o non autorizzata) e alla "violazione dell'integrità", in caso di alterazione non autorizzata o accidentale dei dati personali.
La violazione, in rapporto alla sua gravità, può comportare per l'Amministrazione la Notifica del *Data Breach*, cioè la comunicazione della violazione dei dati personali all'Autorità di Controllo (Garante per la protezione dei dati personali), nonché, qualora ne abbiano un danno, ai soggetti i cui dati sono stati violati.
A tal fine si ricorda l'obbligo del lavoratore di segnalare qualunque ipotesi di violazione dei dati personali al proprio responsabile e al Responsabile della Protezione dei Dati nominato ai sensi dell'art. 37 del Regolamento europeo 679/2016 dell'Amministrazione (Avv. Luca IADECOLA - rpd@mite.gov.it e rpd@pec.minambiente.it), tempestivamente al fine di consentire il rispetto dei termini di notifica all'Autorità di Controllo previsti dal Regolamento (UE) 2016/679, ove atto dovuto.

Restano ferme le disposizioni in materia di responsabilità, infrazioni e sanzioni contemplate dalle leggi, dal decreto del Presidente della Repubblica 16 aprile 2013, n. 62, recante il codice di comportamento dei dipendenti pubblici e dal decreto ministeriale n. 223 del 30.10.2020, recante il codice di comportamento dei dipendenti del Ministero della Transizione Ecologica, che trovano integrale applicazione anche ai lavoratori agili e che con la sottoscrizione dell'Accordo individuale il lavoratore in regime di lavoro a distanza accetta e si impegna ad adottare le presenti "istruzioni".