AGENZIA DELLE DOGANE E DEI MONOPOLI

PRIVACY POLICY DELL'AGENZIA SUL LAVORO A DISTANZA

1. LAVORO AGILE E TELELAVORO DOMICILIARE

Nella presente sono contenute le indicazioni aggiornate in ordine alla protezione dei dati personali che i/le dipendenti dell'Agenzia sono tenuti ad adottare qualora svolgano la propria attività lavorativa in modalità agile o in telelavoro domiciliare.

La modalità di lavoro agile nelle amministrazioni pubbliche è stata introdotta dall'art. 14 della legge 7 agosto 2015, n. 124 e successivamente disciplinata dall'art. 18 della legge 22 maggio 2017, n. 81.
Dal mese di marzo 2020, al fine di contrastare lo sviluppo della pandemia "Covid-19", tale modalità è stata utilizzata diffusamente sia per tutelare la salute del personale sia per garantire la prosecuzione dell'attività amministrativa.

La modalità di telelavoro domiciliare nelle amministrazioni pubbliche è stata introdotta dalla legge 16 giugno 1998, n. 191, ed, in particolare, dall'articolo 4 rubricato "Telelavoro". Attualmente tale modalità di lavoro è riconosciuta, altresì, dalla normativa contrattualistica e nello specifico dall'articolo 41, comma 2, lettera a) del CCNL Comparto Funzioni Centrali per il triennio 2019 – 2021.

L'Agenzia, per permettere al proprio personale di svolgere il lavoro in modalità agile o in telelavoro domiciliare ha:

- ✓ dotato i/le dipendenti, che ne abbiano fatto richiesta, ove ve ne fosse disponibilità, di una adeguata strumentazione hardware;
- ✓ dotato i/le dipendenti di V-APP per l'accesso ai sistemi informatici dell'Agenzia con le stesse credenziali utilizzate in ufficio;
- ✓ chiesto loro di poter trasferire sul proprio numero di telefono personale le chiamate in arrivo sul numero dell'ufficio.

Le istruzioni sui comportamenti e sulle verifiche che vengono effettuate da parte di ADM sui/sulle dipendenti che svolgono la propria attività in lavoro agile/telelavoro domiciliare sono contenute in appositi disciplinari approvati con Determinazioni Direttoriali.

1.1 ELEMENTI PER UNA CORRETTA GESTIONE DEL LAVORO AGILE E NEL TELELAVORO DOMICILIARE

La necessità di protezione dei dati personali dei quali il/la dipendente ha conoscenza nell'ambito dell'attività lavorativa, comporta alcuni accorgimenti che il/la medesimo/a deve assicurare laddove la prestazione lavorativa venga svolta in modalità agile o in telelavoro domiciliare.

Ai fini di una corretta politica di gestione della *privacy*, infatti, vanno garantiti alcuni aspetti:

- ✓ la correttezza della modalità di accesso al *desktop* remoto;
- ✓ la necessità di strumenti di protezione della strumentazione informatica da virus e *malware*;
- ✓ la sicurezza della comunicazione;
- ✓ la sicurezza della rete internet;
- ✓ la sicurezza del luogo nel quale il lavoro da remoto viene svolto;

- ✓ la limitazione dell'accesso alle informazioni da parte di soggetti non autorizzati, presenti nel luogo nel quale il lavoro da remoto viene svolto.

Strumenti di lavoro

Nel caso di *hardware* fornito dall'Agenzia, le configurazioni sono normalmente approntate dal personale tecnico addetto e pertanto il personale non dovrà modificare le impostazioni predefinite.

Nel caso in cui il/la dipendente utilizzi propri dispositivi, dovranno essere osservate le seguenti precauzioni:

- utilizzare i sistemi operativi per i quali è garantito il supporto;
- effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo utilizzato;
- assicurarsi che il *software* di protezione del sistema operativo utilizzato sia abilitato e costantemente aggiornato;
- utilizzare antivirus sicuri e adeguati;
- assicurarsi che gli accessi al sistema operativo siano protetti da *password* sicura e robusta;
- non utilizzare memorie USB di massa;
- nel caso si utilizzino *hotspot* o *dongle wifi*/4g assicurarsi di utilizzare un'autenticazione basata su sistema WPA2, avendo cura di modificare la *password* di *default* del *modem*/*router* per l'accesso in *wifi*;
- non salvare documenti di ufficio sul proprio pc;
- creare un *account* specifico per l'uso nei momenti di lavoro, se il pc è usato anche da familiari o conviventi.

Inoltre, il/la dipendente deve avere cura in ogni caso di:

- utilizzare l'accesso a connessioni Wi-Fi adeguatamente protette;
- non installare *software* provenienti da fonti non ufficiali;
- configurare la modalità di blocco automatico quando ci si allontana dalla postazione di lavoro;
- non aprire *link* o allegati contenuti in e-mail sospette;
- non navigare su siti non protetti;
- effettuare sempre il *log-out* dai servizi/portali utilizzati dopo aver concluso la sessione lavorativa;
- non tenere in evidenza (es. post-it sul pc) le proprie *password* per accedere agli applicativi di lavoro.

Luogo di lavoro

Il luogo nel quale viene svolta la prestazione lavorativa da remoto è normalmente la propria abitazione. Nel caso in cui l'attività di lavoro venga svolta presso l'abitazione di terzi, ovviamente

previa autorizzazione in tal senso, ricorre la necessità di utilizzo di particolari precauzioni proprio per la possibilità che altri possano venire a conoscenza di dati personali degli interessati.

In ogni caso il/la dipendente deve quantomeno:

- organizzare una postazione di lavoro dedicata, lontana da fonti di calore o acqua;
- rimuovere *listening devices* (ad esempio Alexa o Google Home) dal luogo in cui è adibita la postazione di lavoro;
- ridurre al minimo le interferenze di altri soggetti eventualmente presenti nell'abitazione;
- custodire con diligenza la documentazione, i dati e le informazioni relative alla prestazione lavorativa svolta;
- riporre, se risulta necessario trattenere presso la propria abitazione, materiale cartaceo contenente dati personali, in armadi, cassetti o altri contenitori muniti di serratura;
- evitare di rivelare al telefono informazioni che contengono dati personali di terzi interessati.

Nei casi in cui la prestazione venga svolta presso abitazione di terzi, il/la dipendente deve assicurarsi che il titolare della medesima e gli altri occupanti conoscano le regole di comportamento e non interferiscano con l'attività lavorativa nelle ore in cui viene svolta.

2. TELELAVORO DELOCALIZZATO (o COWORKING)

La modalità di telelavoro delocalizzato (o coworking) nelle amministrazioni pubbliche è stata introdotta dalla legge 16 giugno 1998, n. 191, ed, in particolare, dall'articolo 4 rubricato "Telelavoro". Attualmente tale modalità di lavoro è riconosciuta, altresì, dalla normativa contrattualistica e nello specifico dall'articolo 41, comma 1, lettera b) del CCNL Comparto Funzioni Centrali per il triennio 2019 – 2021.

Le istruzioni sui comportamenti e sulle verifiche che vengono effettuate da parte di ADM sul personale che svolge la propria attività in telelavoro delocalizzato sono contenute in apposito disciplinare approvato con Determinazione Direttoriale.

La necessità di protezione dei dati personali dei quali il/la dipendente ha conoscenza nell'ambito dell'attività lavorativa, comporta alcuni accorgimenti che il/la medesimo/a deve assicurare laddove la prestazione lavorativa venga svolta in telelavoro delocalizzato.

Il/La dipendente deve quantomeno:

- custodire con diligenza la documentazione, i dati e le informazioni relative alla prestazione lavorativa svolta;
- riporre, se risulta necessario trattenere presso l'ufficio presso cui svolge la prestazione in telelavoro delocalizzato, materiale cartaceo contenente dati personali, in armadi, cassetti o altri contenitori muniti di serratura;
- evitare di rivelare al telefono informazioni che contengono dati personali di terzi interessati se presenti altri soggetti;

Inoltre, il/la dipendente deve avere cura in ogni caso di:

- non installare *software* provenienti da fonti non ufficiali;
- configurare la modalità di blocco automatico quando ci si allontana dalla postazione di lavoro;
- non aprire *link* o allegati contenuti in e-mail sospette;
- non navigare su siti non protetti;
- effettuare sempre il *log-out* dai servizi/portali utilizzati dopo aver concluso la sessione lavorativa;
- non tenere in evidenza (es. post-it sul pc) le proprie *password* per accedere agli applicativi di lavoro.

3. PROCEDURA DATA BREACH

Nel caso in cui il/la dipendente abbia contezza o anche fondato sospetto di una violazione dei dati personali degli interessati, avvenuta durante la prestazione di lavoro a distanza, avvisa senza indugio (tenendo in considerazione il termine perentorio delle 72 ore consentito per l'intero processo) il/la proprio/a dirigente o persona delegata - per iscritto - utilizzando la casella di posta elettronica funzionale dell'Ufficio di appartenenza.

Per maggiori dettagli sulla procedura di *data breach* si rimanda al modello di gestione e segnalazione pubblicato sulla intranet al seguente link:
261820a1-f578-571d-2b6c-cfe90f987b84 (adm.gov.it)