

Indicazioni in materia di Riservatezza e Sicurezza Informatica

in contesto di Lavoro Agile (o *Smart Work*)

Gentile Lavoratore/Lavoratrice,

ricordando che il *lavoratore agile*, anche nelle giornate in cui svolge l'attività lavorativa da remoto al di fuori dei locali aziendali, è tenuto al rispetto delle norme di legge, di CCNL, dei regolamenti e delle procedure, delle indicazioni, istruzioni e direttive aziendali che normalmente si applicano durante lo svolgimento della prestazione lavorativa in presenza (in quanto compatibili), riportiamo di seguito le regole principali in materia di *Riservatezza e Sicurezza Informatica* alle quali dovrà attenersi durante lo svolgimento della prestazione lavorativa in modalità agile (in specie quando la prestazione è eseguita all'esterno dei locali aziendali) al fine di garantire la sicurezza e la riservatezza dei Suoi dati personali e dei dati dell'AOUP.

Alla luce di quanto precede si invita la S.V. a tenere un comportamento improntato alla massima diligenza, cautela e prudenza nella gestione dei dati ed informazioni trattati nello svolgimento dell'attività lavorativa e nell'utilizzo delle tecnologie fuori dai locali aziendali, ricordando l'obbligo di attenersi, oltre a quanto previsto nella presente informativa, alle disposizioni vigenti, anche interne, correlate al lavoro agile ed alle informazioni, istruzioni, indicazioni e relativi aggiornamenti che saranno prodotti dall'Azienda e resi noti anche tramite pubblicazione sulla INTRANET aziendale.

Premessa

Lo svolgimento dello *Smart Work* non fa venir meno gli obblighi generali derivanti dal contratto di lavoro e più precisamente:

- non violare il segreto e la riservatezza delle informazioni trattate;
- rispettare e applicare le misure di sicurezza fisiche, informatiche, organizzative, logistiche e procedurali indicate di seguito;
- adottare comportamenti adeguati atti a garantire l'integrità dei dati contro i rischi di distruzione, perdita e accesso non autorizzato;
- durante le giornate in lavoro agile, le ordinarie funzioni gerarchiche e/o di coordinamento naturalmente inerenti il rapporto di lavoro subordinato sono mantenute e pertanto è obbligatorio contattare senza ritardo il proprio superiore gerarchico nell'organizzazione¹ (anche telefonicamente) per qualsiasi dubbio, sospetto di incidente o di violazione, avendo cura di specificare se ha avuto ad oggetto dati personali, nonché qualsiasi altro evento significativo.

Dispositivi Aziendali

Se svolge la Sua attività di *Smart Work* utilizzando un dispositivo fornito da AOUP, questo è già configurato per un impiego sicuro.

Tuttavia, durante suo utilizzo, dovrà attenersi alle indicazioni che seguono:

- non utilizzare il dispositivo per scopi personali;
- mantenere il sistema operativo e l'antivirus aggiornati;
- non modificare le impostazioni pre-configurate da AOUP;
- non installare ulteriori software o applicativi non autorizzati;
- non conservare documenti personali sul dispositivo aziendale;

¹ Vedasi a tal riguardo anche quanto previsto nelle procedure aziendali o nelle indicazioni divulgate/pubblicate dall'Amministrazione: per esempio la PA 201 in materia di *Valutazione e Notifica delle Violazioni dei Dati Personali (Data Breach)* rinvenibile nella apposita sezione *Regolamenti e Procedure* della INTRANET.

- non incollare post-it sul dispositivo che lascino in evidenza password per accedere agli applicativi di lavoro o appunti su informazioni personali trattate per motivi di lavoro;
- in caso di anomalie o blocchi del sistema, sospendere ogni attività, chiudere ogni applicazione, arrestare il sistema ed informare immediatamente il Dirigente di riferimento (come definito ai sensi dell'art. 2, comma 2 del Regolamento aziendale in materia di lavoro agile) al fine di permettere a questi di effettuare le dovute valutazioni in ordine alle modalità di prosecuzione della giornata lavorativa. Laddove il problema tecnico non sia dipendente da mero malfunzionamento di apparati personali (quali per esempio la rete internet privata utilizzata per rendere la prestazione lavorativa da remoto), è necessario contattare altresì immediatamente senza ritardo le funzioni di *information technology*² aziendali al fine di procedere se possibile alla rapida soluzione del problema riscontrato.

Dispositivi personali

Se svolge la Sua attività di SmartWorking utilizzando un dispositivo personale, deve aver cura di:

- utilizzare un dispositivo che sia di Suo esclusivo uso personale (se possibile);
- utilizzare un dispositivo sul quale sia installato un sistema operativo per il quale sono ancora garantiti gli aggiornamenti ed il supporto;
- se il dispositivo è condiviso con i familiari/conviventi, creare un account appositamente dedicato al lavoro, ulteriore e diverso da quello personale, da utilizzare anche quando si connette al server aziendale tramite VPN, così da avere una partizione dedicata ad uso esclusivo;
- impostare una password forte (lunghezza minima di 8 caratteri, usando sia lettere minuscole e maiuscole, numeri arabi e caratteri non alfanumerici o speciali - ad esempio !?* o @) per accedere al dispositivo o alla partizione ad uso esclusivo;
- non condividere la password di accesso con i propri familiari/conviventi, password che dovrà essere conosciuta soltanto da Lei;
- se non già presente, installare un antivirus ed abilitare il firewall;
- configurare l'antivirus con la rilevazione delle minacce in tempo reale;
- mantenere il sistema operativo, l'antivirus ed il firewall costantemente aggiornati;
- non salvare i "documenti aziendali" nella memoria del proprio dispositivo o in altre periferiche personali laddove siano disponibili funzioni di salvataggio su server aziendali;
- non incollare post-it sul PC personale che lascino in evidenza password per accedere agli applicativi di lavoro o appunti su informazioni personali trattate per motivi di lavoro;
- durante la connessione in VPN, e più generalmente durante lo svolgimento dell'attività lavorativa, non accedere a siti, applicativi, piattaforme e simili non correlate a finalità istituzionali;
- in caso di anomalie o blocchi del sistema, sospendere ogni attività, chiudere ogni applicazione, arrestare il sistema ed informare immediatamente il Dirigente di riferimento (come definito ai sensi dell'art. 2, comma 2 del Regolamento aziendale in materia di lavoro agile) al fine di permettere a questi di effettuare le dovute valutazioni in ordine alle modalità di prosecuzione della giornata lavorativa. Laddove il problema tecnico non sia dipendente meramente da malfunzionamento del dispositivo personale, della rete privata o comunque degli strumenti personali adoperati per rendere la prestazione lavorativa da remoto, è necessario contattare altresì immediatamente senza ritardo le funzioni di *information technology*³ aziendali al fine di procedere se possibile alla rapida soluzione del problema riscontrato.

Regole di comportamento

Indipendentemente che Lei stia utilizzando un dispositivo aziendale o personale, Le chiediamo di rispettare queste semplici regole di comportamento durante lo svolgimento della Sua attività di SmartWorking:

² Istruzioni maggiori sono fornite sulla INTRANET aziendale nella sezione dedicata.

³ Vedi sub nota 2.

- non utilizzare altri dispositivi personali per svolgere la propria attività in SmartWorking (oltre a quello aziendale o a quello personale appositamente predisposto);
- evitare che altri soggetti possano accedere al dispositivo utilizzato;
- bloccare manualmente il dispositivo quando si allontana dalla postazione di lavoro, anche se per un breve periodo di tempo;
- custodire con diligenza informazioni, documenti e dati connessi alla Sua attività lavorativa;
- nel caso di stampa di documenti, conservarli in un luogo sicuro accessibile solo a Lei;
- non utilizzare i social network durante lo svolgimento dell'attività lavorativa e non navigare su siti di non stretta pertinenza con l'attività lavorativa;
- utilizzare solo chiavette USB o Hard Disk Esterni di cui si conosce la provenienza e comunque procedere ad una scansione della periferica con antivirus;
- cambiare la password di accesso al dispositivo nonché quella per accedere ad internet tramite WiFi almeno ogni 3 mesi;
- non installare software provenienti da fonti/repository non ufficiali;
- non aprire file, allegati o *link* che destino sospetti;
- non scaricare programmi e file di dubbia provenienza;
- disconnettersi sempre a fine sessione dagli applicativi aziendali;
- in caso di violazioni che possano riguardare dati personali – c.d. *Data Breach* –, come ad es. la loro perdita, distruzione, diffusione, informare subito il proprio responsabile ed attivare la procedura di Data Breach (PA-201 – “Valutazione e notifica delle violazioni dei dati personali (*data breach*)”);
- se il proprio dispositivo è stato infettato da virus, malware, ransomware, etc., disconnetterlo immediatamente da internet e spegnerlo (anche bruscamente, ad es. staccando la spina dell'alimentazione o forzando l'arresto);
- prestare sempre la massima attenzione prima di inviare una email, verificando correttamente l'indirizzo del destinatario per scongiurare il rischio di inviare per errore informazioni sensibili, coperte dal segreto professionale e/o dati personali a terzi che non sono autorizzati a riceverle.
- i documenti contenenti particolari categorie di dati (ad es. dati genetici o relativi all'HIV) devono essere inviati solo con modalità sicure (ad es. crittografandoli o proteggendo il documento con password da inviare al destinatario separatamente al documento e tramite altro canale).

Accesso da remoto alla rete aziendale tramite VPN

In regime di Smart Working, l'accesso da remoto alla rete aziendale AOUP può avvenire solo mediante VPN (Virtual Private Network), acronimo di “rete privata virtuale” che consente di creare un canale di comunicazione crittografato tra il Suo dispositivo e la rete aziendale AOUP.

Per utilizzare la VPN è necessario un accesso ad internet (tramite WiFi residenziale/privato o con collegamento tramite cavo al router DSL residenziale o mediante penna USB con SIM o tramite Internet Box).

Di seguito vengono fornite le indicazioni per adeguare le attrezzature a Sua disposizione ad un livello di sicurezza il linea con gli strumenti aziendali e per un corretto utilizzo della VPN.

- In caso di connessione ad Internet tramite WiFi, verificare che il router WiFi utilizzato non sia più vecchio di 5-7 anni, in modo da disporre del sistema di crittografia del segnale chiamato WPA2;
- non utilizzare reti WiFi con protocolli WEP o WPS, che devono essere disabilitati. La verifica può essere effettuata anche da cellulare, connesso alla rete residenziale, cliccando sul nome della rete WiFi alla quale si è connessi ed individuando il nome dei protocolli utilizzati.
- L'accesso alla rete residenziale via WiFi con protocollo WPA2 deve essere protetta da password, che dovrà essere impostata con una lunghezza di almeno 12 caratteri, utilizzando caratteri sia maiuscoli che minuscoli, numeri e simboli come !, @, & e così via (ad es., si può utilizzare una frase come *Il.s0le.s0rge.allal@* utilizzando lo “0” al posto delle “o” ed il simbolo @ al posto della “a” finale).
- Modificare la password di accesso al WiFi (almeno) dopo 6 mesi di Smart Working;
- Si raccomanda di modificare anche il nome della WiFi residenziale, che normalmente ha un nome predefinito.

- Disattivare il salvataggio automatico delle password nel browser e nel client VPN.
- Effettuare una scansione antivirus del computer prima di utilizzare la VPN.
- Non lasciare incustodito il computer con la VPN attiva.
- Chiudere la connessione VPN con la rete aziendale quando si compiono attività al computer che non richiedono il collegamento alla rete aziendale.
- Mantenere sempre attivo l'antivirus, anche quando la VPN non è attiva e si utilizza il computer per altre attività.
- Non utilizzare altri sistemi di collegamento remoto durante l'utilizzo della VPN.

Phishing

Il fenomeno del c.d. *phishing* fa riferimento a tentativi di frode basate sul carpire informazioni riservate e sensibili, come ad esempio dati di accesso di varia natura, numeri di carte di credito, etc.

Il *phishing* viene spesso realizzato tramite l'invio di e-mail apparentemente non sospette – ad es. riferibili ad istituti postali o bancari – che spingono l'utente a seguire le indicazioni in esse riportate (ad es. aprire un allegato od un link) così da fargli rivelare informazioni sensibili nella (errata) convinzione di rispondere ad una lecita richiesta del mittente.

Nel caso in cui riceva e-mail sospette, segua queste indicazioni prima di aprirle:

- verificare l'indirizzo di provenienza dell'e-mail;
- verificare che l'organizzazione / Ente cui appartiene il mittente esista davvero, tramite una ricerca sul web;
- leggere attentamente il testo della e-mail per rilevare sbavatura grammaticali o incongruenze logiche (di solito sintomo che il testo è stato tradotto con un traduttore automatico);
- se l'e-mail proviene da una persona conosciuta o da un indirizzo conosciuto, contattare telefonicamente la persona chiedendole conferma dell'invio dell'e-mail con il link e/o l'allegato;
- non aprire allegati o *link* fintanto che non si è certi della genuinità dell'e-mail.

Il Dipendente⁴

⁴ Il Dipendente firma l'informativa consegnatagli ai sensi e per gli effetti del Regolamento Aziendale in materia di lavoro agile atteso che la stessa è parte integrante e sostanziale dell'accordo individuale (anche di proroga) di lavoro agile e degli impegni assunti con lo stesso. L'originale dell'informativa firmata dal dipendente è conservata agli atti dell'Azienda ed una copia è consegnata allo stesso.