Informativa in materia di dotazione informatica per lo smart working

Premessa

Il presente documento descrive le linee guida e le regole di comportamento a cui si devono attenere i dipendenti nell'utilizzo degli strumenti informatici a supporto dello smart working, sia propri che assegnati dal datore di lavoro.

Risorse informatiche

Il personale in smart working deve disporre di una dotazione informatica adeguata alle mansioni svolte. Tali risorse possono essere di proprietà del dipendente o fornite dal datore di lavoro. La gestione delle risorse informatiche prevede due ruoli:

- gestore - gode del livello massimo di privilegio consentito per lo svolgimento delle operazioni eseguibili su una risorsa;
- utilizzatore - ha privilegi limitati per lo svolgimento di determinate operazioni eseguibili su una risorsa.

Una risorsa informatica deve avere almeno un gestore. Uno stesso soggetto può ricoprire entrambi i ruoli.

Nel caso della dotazione assegnata dall'amministrazione per smart working il ruolo di gestore è svolto da operatori incaricati dall'amministrazione, mentre quello di utilizzatore è ricoperto dal dipendente assegnatario.

Nel caso di apparecchiature di proprietà del dipendente i ruoli di gestore ed utilizzatore sono entrambi in capo al dipendente medesimo. In questo caso il dipendente è responsabile sia della corretta configurazione che dell'utilizzo in conformità alle presenti linee guida.

Dotazione di base della postazione di lavoro per smart working

Ai fini dello svolgimento dello smart working il dipendente deve disporre, come dotazione minima, di un personal computer e di una connessione ad Internet.

L'accesso a particolari applicazioni/servizi (es: protocollo, gestione delle Virtual Machine in housing) non accessibili dall'esterno può avvenire tramite VPN la cui attivazione va richiesta tramite il sito:

https://centroservizirsi.cnr.it/portale/login.php

Eventuali ulteriori dispositivi, necessari per specifiche mansioni, sono forniti dalla struttura di appartenenza, che ne disciplina l'uso in accordo con le presenti linee guida.

Norme di utilizzo dei dispositivi laptop, desktop e mobili

Gli utilizzatori dei dispositivi a supporto dello smart working devono rispettare le seguenti linee guida:

- nel caso di dispositivi di proprietà del dipendente, creare un account separato per le attività lavorative, le cui credenziali siano note unicamente al dipendente medesimo (è esclusa pertanto la condivisione di tali credenziali con i familiari);
- nel caso di dispositivi forniti dall'amministrazione, utilizzare solo l'account creato per il dipendente dal gestore della risorsa e solo per scopi di lavoro; è vietata la creazione di ulteriori account, se non

su specifica e motivata autorizzazione del responsabile della struttura di appartenenza; è altresì vietata la condivisione delle credenziali, anche con i familiari;
- i dati trattati durante l'attività lavorativa devono essere accessibili unicamente al dipendente;
- configurare la modalità di blocco automatico dell'accesso al sistema dopo un breve periodo di inattività o bloccare manualmente l'accesso al sistema quando il dispositivo non è in uso;
- utilizzare esclusivamente dispositivi removibili (pen drive, hd esterni, ecc.) di cui si conosce la provenienza;
- effettuare sempre il logout dai servizi Web una volta terminata la sessione lavorativa;
- custodire adeguatamente le credenziali di accesso e non condividerle con terzi;
- custodire con le debite cautele i dispositivi in uso;
- effettuare sempre il logout da programmi, VPN e piattaforme di lavoro al termine della sessione lavorativa;
- eseguire periodicamente il backup dei dati;
- non aprire allegati ricevuti via mail da mittenti sconosciuti oppure file scaricati da Internet che potrebbero contenere codice malevolo;
- non introdurre consapevolmente software malevolo sulla rete o sui dispositivi utilizzati per lo smart working;
- non collegare i dispositivi in uso a reti e VPN sconosciute;
- non utilizzare strumenti o tecniche che possano arrecare danni alle sottoreti o agli utenti dell'Ente (ad esempio port scanner, security scanner, network monitoring, honeypot, DoS, ecc.);
- collaborare con i gestori di rete al fine di garantire il corretto funzionamento della stessa;
- non tentare di aggirare i meccanismi di controllo degli accessi di qualsiasi risorsa informatica protetta.

Norme di utilizzo del software

I software di base per lo smart working sono:

- Sistema operativo (Microsoft Windows, Apple MacOS, Ubuntu 20.04),
- Strumenti di office automation (Microsoft Office, Libre Office, Only Office, iWork),
- Client di posta elettronica (Microsoft Outlook, Mozilla Thunderbird, Apple Mail),
- Browser Internet (Mozilla Firefox, Chrome, Safari, Microsoft Edge).

I responsabili di struttura autorizzano l'installazione e l'uso di eventuali altri software sulla base delle diverse mansioni svolte dal dipendente.

Di seguito è riportato un elenco non esaustivo di accorgimenti necessari per l'utilizzo delle "risorse software", del "codice sorgente" e delle "librerie di sviluppo software".

Per tutte le categorie citate precedentemente valgono le seguenti regole di comportamento:

- nel caso in cui il software richieda una licenza d'uso, questa dev'essere ottenuta attraverso canali ufficiali (rivenditore, apposito ufficio di Istituto, ecc.);
- ove possibile, deve sempre essere utilizzata la versione software più recente e in ogni caso non contenente vulnerabilità note;
- le versioni utilizzabili sono esclusivamente quelle mantenute dal produttore e per cui vengono ancora rilasciati aggiornamenti di sicurezza.

Per le risorse software:

- è consentita esclusivamente l'esecuzione di software ottenuto attraverso canali ufficiali e che rientri nella lista dei software di base per lo smart working sopra riportata o che sia autorizzato dal responsabile di struttura.

Per le librerie di sviluppo software e il codice sorgente utilizzati da personale adibito ad attività di sviluppo software:

- è consentito l'utilizzo di librerie o software reperibili su internet limitando il loro uso nell'ambito di tutte quelle attività che prevedano lo sviluppo di software autorizzato dal responsabile della struttura di afferenza e adottando tutte le necessarie cautele in ordine alla verifica della provenienza e dell'assenza di codice malevolo;
- è responsabilità del dipendente verificare che il codice sorgente e le librerie utilizzate non contengano vulnerabilità di sicurezza note;
- è responsabilità di chi sviluppa o utilizza il codice sorgente garantire che questo non introduca volontariamente vulnerabilità di sicurezza o arrechi danno ad altri.

Norme specifiche sull'utilizzo della posta elettronica

La presente sezione contiene indicazioni sull'utilizzo della posta elettronica aziendale, valide sia in condizioni di smart working che nel caso di lavoro in presenza.

Concetti generali:

- La casella di posta, assegnata dall'azienda all'utente, è uno strumento di lavoro.
- Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
- Ad ogni utente viene fornito un account e-mail nominativo con formato nome.cognome@cnr.it
- L'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi lavorativi, ed è assolutamente vietato ogni utilizzo di tipo privato.
- L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa.

Norme di comportamento:

- È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
- È obbligatorio controllare i file allegati di posta elettronica prima del loro utilizzo. In particolare, si deve evitare, secondo le regole di buona diligenza, l'apertura e la lettura di messaggi di posta elettronica in arrivo provenienti da mittenti di cui non si conosce con certezza l'identità o che contengano allegati del tipo .exe, .com, .vbs, .htm, .scr, .bat, .js, .pif.
- È vietato inviare catene telematiche (dette di Sant'Antonio). Se si ricevono messaggi di tale tipo, occorre comunicarlo tempestivamente all'amministratore di sistema. Non si devono in alcun caso attivare gli allegati di tali messaggi.
- L'iscrizione a mailing-list o newsletter esterne con l'indirizzo ricevuto è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.
- È vietato rispondere a messaggi in cui vengono chieste le credenziali dell'utente. Tutte le operazioni di gestione e manutenzione delle caselle di posta elettronica possono essere fatte dagli amministratori senza la necessità delle credenziali dell'utente.

Norme di utilizzo di smartphone e router wi-fi

I dispositivi smartphone e router wifi (con sim dati) assegnati dall'Amministrazione sono strumenti di lavoro utilizzabili unicamente a tale scopo. Non possono essere ceduti, condivisi con terzi o utilizzati per scopi personali. Entrambe le tipologie di dispositivo possono essere utilizzate per la connessione ad Internet in mobilità. Il relativo traffico dati può essere consumato solo per finalità connesse con l'attività lavorativa. Il dipendente è responsabile dell'uso corretto e lecito della connessione ad Internet ed è tenuto a restituire il dispositivo una volta cessato il rapporto di lavoro o revocata l'assegnazione da parte del Responsabile della struttura di afferenza.

Trattamento dei dati personali

La presente sezione contiene elenchi non esaustivi di definizioni e norme di comportamento relative ai trattamenti di dati personali. Tutti i trattamenti, ivi inclusi quelli operati in regime di smart working tramite strumenti informatici, devono essere effettuati in osservanza del Regolamento Generale per la Protezione dei Dati (Regolamento UE 2016/679) e adottando sempre la massima cautela. I trattamenti di dati personali avvengono su specifico incarico del datore di lavoro, che fornisce le istruzioni alle quali il personale autorizzato si deve attenere.

Definizioni

Dati personali

Informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.

Particolarmente importanti sono:

- i dati che permettono l'identificazione diretta - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);
- i dati rientranti in particolari categorie: si tratta dei dati c.d. "sensibili", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;
- i dati relativi a condanne penali e reati: si tratta dei dati c.d. "giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Interessato

Persona fisica alla quale si riferiscono i dati personali (articolo 4, paragrafo 1, punto 1 del Regolamento UE 2016/679).

Titolare

Persona fisica, autorità pubblica, impresa, ente pubblico o privato, associazione, ecc., che adotta le decisioni sugli scopi e sulle modalità del trattamento (articolo 4, paragrafo 1, punto 7 del Regolamento UE 2016/679). Nel caso delle presenti linee guida, Titolare dei trattamenti effettuati nell'ambito dell'attività lavorativa è **il CNR nelle sue articolazioni organizzative** (art. 19 bis Regolamento di Organizzazione e Funzionamento del CNR), salvo i casi in cui il CNR agisca in qualità di Responsabile del trattamento (ex art. 28 del Regolamento

UE 2016/679 – vd definizione successiva), sulla base di apposito contratto stipulato con soggetto terzo che detiene la titolarità del trattamento medesimo.

Nel caso di titolarità CNR, specifici compiti del Titolare sono demandati al responsabile della struttura nella quale il trattamento è svolto.

Responsabile
Persona fisica o giuridica alla quale il Titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo per suo conto del trattamento dei dati (articolo 4, paragrafo 1, punto 8 del Regolamento UE 2016/679). Il rapporto tra Titolare e Responsabile è regolato da apposito contratto.

Responsabile della protezione dei dati
Il responsabile della protezione dei dati è una figura che agisce alle dipendenze dirette del vertice gerarchico del Titolare, ed è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE 2016/679 nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza della normativa in materia di protezione dei dati personali e delle politiche adottate in questo ambito dal Titolare;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
d) cooperare con l'autorità di controllo (Garante Privacy);
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento.

Il Responsabile della Protezione dei Dati del CNR è contattabile all'indirizzo rpd@cnr.it.

Trattamento
Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4 par. 1 punto 2 del Regolamento UE 2016/679)

Data breach
Un data breach è una violazione di sicurezza che comporta - accidentalmente o per cause dolose - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità dei dati medesimi.

Norme di comportamento in caso di data breach

In caso di data breach il dipendente dovrà segnalare immediatamente la circostanza al suo responsabile di struttura per consentire l'espletamento di tutti gli obblighi del Titolare nei tempi previsti dalla legge.

Dovrà contestualmente fornire le seguenti informazioni

a) natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) probabili conseguenze della violazione dei dati personali;

c) eventuali misure adottate nell'immediatezza dell'evento o che si possono adottare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il dipendente dovrà rendersi contattabile per ogni ulteriore approfondimento e richiesta di informazioni.

Si sottolinea l'importanza della tempestività nel segnalare il data breach e nel fornire tutte le informazioni richieste, per consentire al Titolare di effettuare la segnalazione al Garante Privacy entro il termine di 72 ore dall'individuazione dell'incidente.