Raccomandazioni per la protezione dei dati nell'utilizzo di dispositivi personali ed in regime di lavoro agile

1. Premessa e finalità del documento

Come noto, con il perdurare della situazione di emergenza sanitaria, la maggior parte delle attività lavorative vengono svolte al di fuori delle strutture universitarie, presso l'abitazione del lavoratore e con l'utilizzo di dispositivi personali (cosiddetti BYOD, ovvero *bring your own device*).

Allo scopo di mantenere adeguati livelli di protezione dei dispositivi in dotazione e dei dati personali, il Centro InfoSapienza ha diramato tempestivamente, sin dall'avvio del lavoro agile (si veda la circolare AOS prot. n. 20438 del 6 marzo 2020), una serie di documenti (manuali d'uso, linee guida, comunicazioni diffuse a mezzo *mailing list*, ecc.) utili per il corretto svolgimento delle attività lavorative in *smart working*.

Le raccomandazioni qui illustrate intendono riassumere in un documento unico le indicazioni più rilevanti fornite nel tempo in materia, al fine di proteggere al meglio il patrimonio informativo dell'Ateneo, nel rispetto di quanto previsto dall'art. 32 del Regolamento (UE) 2016/679 (di seguito GDPR); la predetta disposizione normativa prevede infatti, tra l'altro, che il titolare del trattamento metta in atto "misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio".

2. Raccomandazioni

2.1. Misure generali

Nello svolgimento del lavoro agile, è opportuno predisporre ed ubicare la propria postazione lavorativa in modo da garantire la protezione dei dati personali trattati durante la sessione di lavoro ed evitare, pertanto, di lasciare incustoditi e accessibili i dispositivi informatici (o la documentazione

Sapienza Università di Roma
Area Affari Legali
Settore privacy
CF 80209930587 - PI 02133771002
p.le Aldo Moro 5
T (+39) 0649910166
www.uniroma1.it

cartacea) con i quali si stia svolgendo l'attività, specie durante una sessione di lavoro che comporti il trattamento di dati personali.

Al termine della sessione di lavoro occorre effettuare la procedura di disconnessione ("log off"/"log out"/"esci"); si consiglia di spegnere il dispositivo ove non sia indispensabile mantenerlo attivo (si pensi, ad esempio, alla connessione VPN - *Virtual Private Network*).

In caso di eventuali problemi o disfunzioni correlate alla postazione informatica assegnata dall'Ateneo, si raccomanda di richiedere il supporto a supportoDM@r1spa.it.

2.2. La sicurezza informatica

È importante che ogni lavoratore in regime di *smart working*, durante la prestazione lavorativa, osservi le linee guida in materia di sicurezza informatica adottate dall'Ateneo e, in particolare:

- Utilizzare sistemi operativi per i quali attualmente è garantito il supporto;
- Disporre di un pc con sistema operativo aggiornato;
- Assicurarsi che i *software* di protezione del sistema operativo (firewall, antivirus, ecc.) siano abilitati e costantemente aggiornati;
- Assicurarsi che gli accessi al sistema operativo siano protetti da una *password* sicura e, comunque, conforme alla *password policy* emanata dal Centro InfoSapienza;
- Bloccare l'accesso al sistema e/o configurare la modalità di blocco automatico quando ci si allontana dalla postazione di lavoro;
- Utilizzare l'accesso a connessioni Wi-Fi adeguatamente protette;
- Disconnettersi sempre dai servizi e dai portali della Sapienza dopo aver concluso la sessione lavorativa;
- Creare un *account* specifico per l'uso dei dispositivi nei momenti di lavoro, se gli stessi sono utilizzati anche da familiari o conviventi;
- Non visitare siti *web* poco attendibili o dal contenuto inappropriato e/o non sicuro;
- Controllare sempre e con la massima attenzione che l'indirizzo del sito *web* visitato corrisponda effettivamente alla risorsa ufficiale che si vuole consultare. Ad esempio, diffidare e non aprire mai indirizzi come www.uniroma1.com oppure www.uniromal.it;

- Prima di visitare una risorsa presente in una *email* ricevuta, accertarsi che il collegamento sia effettivamente quello dichiarato dal mittente;
- Non divulgare mai e per nessuna ragione le proprie credenziali di accesso ai servizi Sapienza, né inviare dati di accesso tramite *email* o altri canali di comunicazione (ad esempio, Whatsapp o Telegram);
- Effettuare regolarmente una copia di *backup* dei propri dati di lavoro sugli strumenti ufficiali messi a disposizione dal Centro InfoSapienza (cartelle condivise o Google Drive);
- Non caricare su dispositivi forniti in disposizione dal Centro InfoSapienza materiale di natura personale o privata;
- Qualora sia stato richiesto l'accesso in *Virtual Private Network*, utilizzare esclusivamente il software e la VPN forniti dal Centro InfoSapienza;
- Non condividere sui *social network* informazioni, immagini o *screenshot* inerenti la propria attività istituzionale;
- Abilitare la funzionalità di crittografia sui dispositivi utilizzati (notebook, tablet e smartphone personali e forniti dall'Ateneo), meccanismo grazie al quale vi è la garanzia di salvaguardia della protezione dei dati memorizzati – e di cui l'Ateneo è titolare – in caso di eventuale violazione dei dati stessi (ad esempio, alterazione, perdita, cancellazione e distruzione dei dati).

A tale ultimo riguardo, si ricorda che, ai sensi dell'art. 32, par. 1, del GDPR, la cifratura rientra tra le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio per i diritti e le libertà delle persone fisiche e che, se posta in essere, non occorre effettuare la comunicazione all'interessato in caso di violazione dei dati personali (c.d. *data breach*). Nel caso in cui si dovesse verificare una violazione di dati personali, si rimanda a quanto previsto dal vigente Piano di conformità *privacy*, diramato con nota prot. n. 37444 del 22.05.2020, e dalla nota circolare prot. n. 44407 del 25.05.2018.

2.3. L'archiviazione

Occorre porre l'attenzione in merito all'archiviazione, sui propri dispositivi, di documenti contenenti dati personali, che può avere implicazioni rispetto alle corrette modalità di trattamento previste dalla normativa vigente.

È, pertanto, altamente raccomandabile non salvare la documentazione su archivi personali, ma elaborarla e gestirla esclusivamente attraverso gli strumenti *web* proposti dall'Ateneo.

Nel caso in cui siano stati salvati documenti di ufficio sul pc personale (specie se contengono informazioni personali), quest'attività dovrebbe essere temporanea e, immediatamente dopo la fine dell'attività lavorativa, deve seguire la cancellazione dei documenti informatici.

2.4. La gestione dei documenti

Considerato che anche la gestione cartacea dei documenti può comportare rischi per la riservatezza dei dati personali, soprattutto se la prestazione lavorativa è svolta presso la propria abitazione, si raccomanda di gestire la predetta documentazione in modo tale da impedire l'accesso di soggetti terzi non autorizzati al trattamento dei dati personali.

Bisogna, pertanto, porre l'attenzione sulla corretta conservazione dei documenti che contengono dati personali; tali documenti, inoltre, devono essere archiviati con misure di sicurezza che permettano l'accesso solo ai soggetti formalmente autorizzati al relativo trattamento.

Si raccomanda, pertanto, di non lasciare in vista la documentazione che contiene dati personali e di custodirla all'interno di fascicoli che nascondano il contenuto dei documenti stessi.

Inoltre, si consiglia di operare solo con la documentazione necessaria e per il tempo strettamente necessario alla finalità lavorativa, al fine di limitare i rischi di violazione dei dati personali.

2.5. La distruzione dei documenti

Nel caso in cui siano stati utilizzati, per finalità lavorativa, documenti stampati, si raccomanda di porre attenzione alla distruzione di tali documenti, specie se contenenti dati personali, al termine dell'attività lavorativa, in modo da eliminare ogni dato personale contenuto nel documento e garantire il massimo livello di sicurezza, minimizzando i rischi.

3. Approfondimenti

Per ogni opportuno approfondimento delle materie trattate nelle presenti raccomandazioni, si rinvia alla documentazione reperibile alle seguenti pagine *web*:

[Configurazioni sicure dei dispositivi]
https://web.uniroma1.it/infosapienza/sites/default/files/Configurazione%20sicure%20dei%20dispositivi%20informatici.pdf

[Cifratura disco sistemi Windows]
https://web.uniroma1.it/infosapienza/cifratura-del-disco-windows-10-pro-tramite-bitlocker

[Cifratura smartphone Android]
https://web.uniroma1.it/infosapienza/crittografia-di-dati-su-smartphone-android

[Sapienza password policy]
https://web.uniroma1.it/infosapienza/sites/default/files/passwordpolicy.pdf

[Linee guida lavoro agile in sicurezza]
https://www.uniroma1.it/sites/default/files/field_file_allegati/linee_guida_lavoro_agile_in_sicurezza.pdf

[Linee_operative_smartworking]
https://www.uniroma1.it/sites/default/files/field_file_allegati/linee_operative_smartworking.pdf

[Funzione pubblica - "*Linee guida – Guida pratica al lavoro agile nella p.a.*"]
www.funzionepubblica.gov.it/lavoro-agile-e-covid-19/linee-guida
www.funzionepubblica.gov.it/articolo/dipartimento/12-03-2020/guida-pratica-al-lavoro-agile-nella-pa

[Agid - "*Smart working: vademecum per lavorare online in sicurezza*"]
https://www.agid.gov.it/index.php/it/agenzia/stampa-e-comunicazione/notizie/2020/03/17/smart-working-vademecum-lavorare-online-sicurezza