ISTRUZIONI PER TUTTO IL PERSONALE DIPENDENTE SUL TRATTAMENTO DEI DATI PERSONALI IN MODALITA' SMART WORKING / LAVORO AGILE

SOMMARIO

1. Premessa

Il "Lavoro Agile" impone la massima attenzione sui temi della sicurezza e presuppone che il dipendente dell'Ateneo, in particolare nello svolgimento delle attività lavorative da remoto, collabori attivamente al fine di mitigare i rischi di violazione di dati personali e di accesso non autorizzato ad informazioni e servizi che possano compromettere la sicurezza delle reti, dei sistemi informativi e dei servizi informatici dell'Università della Valle d'Aosta.

Di conseguenza, gli obiettivi di sicurezza da raggiungere risultano i seguenti:

- Riservatezza: assicurare che le comunicazioni ed i dati non possano essere letti da soggetti non autorizzati;
- Integrità: capacità di rilevare ogni cambiamento intenzionale o non intenzionale alla comunicazione remota;
- Disponibilità: assicurare che gli utenti possano avere accesso in condivisione alle risorse e ai dati necessari per svolgere la propria attività lavorativa.

Tra i rischi da considerare possono essere elencati i seguenti:

- Perdita o furto di strumenti informatici, comprensivi di dati memorizzati su di essi e di strumenti software di connessione autorizzati;
- Compromissione/perdita di riservatezza di informazioni e dati riservati anche tramite semplice osservazione da parte di persone non autorizzate;
- Introduzione di virus o malware dal Pc personale sulla rete informatica dell'Ateneo;
- In generale perdita di riservatezza, integrità e disponibilità di servizi informatici e dei dati.

2. Istruzioni per il dipendente

L'Università della Valle d'Aosta, in qualità di Titolare del trattamento dei dati, ai sensi dell'art. 24 c. 1 del Regolamento Generale sulla Protezione dei Dati (Reg. U.E. 2016/679), tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, in particolare nello svolgimento di attività lavorative da casa, mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al predetto Regolamento. Le seguenti istruzioni sono riesaminate e aggiornate qualora necessario.

In particolare, è obbligo del dipendente:

1. Assicurarsi che le conversazioni con terzi non siano oggetto di ascolto da parte di soggetti non autorizzati, i quali devono essere mantenuti ad una distanza che consenta di garantire la riservatezza delle comunicazioni;
2. Non utilizzare familiari o terzi per "veicolare" informazioni, anche se ritenute irrilevanti, afferenti l'attività lavorativa;
3. Accertarsi che il coniuge o eventuali parenti e conoscenti non siano portati, anche involontariamente, a conoscenza di informazioni e processi attinenti l'attività lavorativa;
4. Nel caso di conversazioni telefoniche instaurate a seguito di chiamate inoltrate o ricevute, accertare, con cura, che l'interlocutore sia effettivamente un collega/cliente/consulente/fornitore legittimato e autorizzato a conoscere le informazioni oggetto della comunicazione;
5. Limitare al massimo le stampe di documenti ove non indispensabili per motivi di lavoro;
6. Prelevare documentazione dagli archivi d'ufficio solo per comprovate necessità, per poi essere riposti a conclusione delle attività di lavoro agile, garantendo la massima riservatezza durante il trasporto;
7. In caso di assenza, anche momentanea, dal luogo in cui si svolge lo *smart working*, chiudere a chiave i locali che ospitano i dati ovvero riporli dentro un armadio/cassetto chiuso a chiave;
8. Rendere illeggibili i documenti cartacei prima di essere cestinati, qualora non più necessari (ad es. strappando più volte la carta in modo che i contenuti diventino non ricostruibili o attraverso l'uso di trita-documenti);
9. Custodire la password di accesso al Pc con diligenza in modo che resti riservata, evitando che altri ne vengano a conoscenza;
10. In caso di allontanamento anche temporaneo dalla postazione di lavoro, disconnettere la sessione di lavoro bloccando l'operatività del computer ("ctrl-alt-canc") e/o l'accesso allo smartphone o tablet (password di blocco schermo);
11. Non utilizzare dispositivi o sistemi di memorizzazione di tipo personale (pen drive, hard disk esterno o cloud storage) per conservare copie di dati istituzionali contenente dati personali, salvo per comprovate esigenze lavorative e con adeguate misure di sicurezza (ad es. cifratura dei dati o password all'apertura dei files);
12. Non trasmettere dati di lavoro via email a propri indirizzi di posta elettronica privati;
13. Connettersi da remoto alla rete informatica dell'Ateneo solo tramite la modalità VPN, seguendo le istruzioni impartite dai Sistemi Informativi Aziendali;
14. Rispettare il principio di necessità, pertinenza e non eccedenza rispetto alle finalità degli stessi, avere scopi espliciti, determinati e leciti, come da istruzioni fornite in punto all'atto dell'autorizzazione dell'Ateneo al trattamento dei dati personali.

Al fine di prevenire attacchi da virus, malware o altre fonti di rischio, è necessario osservare le seguenti disposizioni sui Pc personali, prima di collegarsi da remoto alla rete informatica dell'Ateneo o prima di utilizzare sistemi informatizzati disponibili sul cloud dell'Università:

- Installare sul Pc personale un sistema antivirus/antimalware, anche di tipo "free";

- Abilitare un Firewall personale.

Sui sistemi Windows sono disponibili le seguenti soluzioni:
- Antivirus Windows Defender (soluzione inclusa nel sistema operativo Ms Windows 10);
- Firewall di Windows (tutte le versioni del sistema operativo Ms Windows).

3. Browser web

- Utilizzare un browser specifico per attività di lavoro con strumenti dell'Ateneo ed utilizzarlo a fini esclusivi per tale scopo; tra le tipologie di browser sono presenti applicativi quali Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge;
- Impostare la configurazione per bloccare le finestre popup;
- Ove disponibile come opzione, abilitare il filtro contro i siti web considerati pericolosi (in genere disponibile come opzione per i sistemi antivirus-antimalware);
- Non consentire ai browser di memorizzare informazioni (ad esempio nei campi delle *form* compilabili)
- **Non consentire al browser di memorizzare credenziali** per accedere più velocemente ai siti protetti (es.: webmail dell'Ateneo).

4. Posta elettronica

- Utilizzare i client webmail per accedere alla posta elettronica dell'Ateneo;
- In caso di configurazione di client di posta elettronica, disabilitare la visualizzazione automatica dell'anteprima dei messaggi email;
- Nel caso sia disponibile come opzione, abilitare il filtro antispam.

5. Client di messaggistica istantanea

- Non trasferire documenti d'ufficio contenenti dati personali e sensibili tramite sistemi di messaggistica istantanea (es.: Skype, Whatsapp, Telegram etc…).

6. Software di Office Automation

- Disabilitare l'utilizzo delle macro: configurare almeno l'opzione di abilitazione su richiesta;
- Memorizzare i documenti d'ufficio in formato elettronico solo nelle condivisioni in cloud rese disponibili dall'Ateneo tramite piattaforma Ms Office 365 e solo temporaneamente sui dispositivi mobili personali.

7. Segnalazione violazioni

Si ribadisce l'obbligo del dipendente di segnalare qualunque ipotesi di violazione dei dati personali al proprio Dirigente Responsabile e al Responsabile della Protezione dei dati, tempestivamente e, comunque, non oltre 48 ore anche al fine di consentire il rispetto dei termini di notifica all'Autorità di Controllo, ove ritenuto necessario, ai sensi dell'art. 33 del Regolamento Generale sulla Protezione dei Dati - Reg. (UE) 2016/679.

E' obbligazione contrattuale del dipendente rispettare le istruzioni sopra riportate. Il dipendente per il quale venga accertata l'inosservanza delle istruzioni sopra elencate potrà essere soggetto ad azioni disciplinari. Per dettagli sulle modalità di trattamento dei dati personali, in conformità al Regolamento Generale sulla Protezione dei Dati, si rinvia al Regolamento interno dell'Ateneo in materia di protezione dei dati personali.