LINEE GUIDA IN TEMA DI PRIVACY E SICUREZZA INFORMATICA PER IL TRATTAMENTO DI DATI PERSONALI EFFETTUATO AL DI FUORI DELLA SEDE DI LAVORO E/O MEDIANTE LE MODALITÀ DI SVOLGIMENTO AGILE DELLA PRESTAZIONE LAVORATIVA

Le presenti linee guida forniscono le indicazioni operative per il trattamento di dati personali effettuato al di fuori della sede di lavoro e/o mediante le modalità di svolgimento agile della prestazione lavorativa, ad integrazione delle prescrizioni riportate nell'atto di incarico al trattamento (Art. 29 Regolamento UE 679/2016 GDPR, a garanzia di un livello di protezione adeguato delle dotazioni tecnologiche attraverso le quali svolge il lavoro smart e nel rispetto dei principi di integrità, riservatezza e disponibilità dei dati e delle informazioni ivi contenute, al fine di ridurre al minimo i rischi di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità oppure di distruzione o perdita dei dati stessi.

Principali prescrizioni

1. Proteggere l'accesso alla rete (LAN, WiFi) e alle dotazioni tecnologiche (PC, notebook, tablet, smartphone, ecc.) attraverso l'uso di password forti e diverse per ciascun servizio[1]. Allo scopo si prescrive il cambio delle password utilizzate abitualmente per l'accesso alle varie applicazioni in cloud. Si consiglia, inoltre, il cambio della password di accesso della propria linea ADSL. Laddove possibile, utilizzare l'autenticazione a due fattori. Ad esempio, gli applicativi Argo consentono l'attivazione del PIN di autenticazione in aggiunta alla password d'accesso. Medesima possibilità è garantita dagli account Google.

2. Garantire che i sistemi operativi installati sulle workstation (PC, notebook, tablet, smartphone) siano autentici e aggiornati all'ultima versione disponibile. Non è consentito lo smart working attraverso workstation dotate di sistemi operativi privi del supporto (ad esempio Windows 7) o peggio non autentici (privi della licenza d'uso). Le vulnerabilità proprie dei sistemi operativi non autentici o privi del supporto e quindi non aggiornati con le ultime patch di sicurezza è la prima causa di accesso non autorizzato alla rete e alle informazioni.

3. Nel caso di utilizzo di una workstation condivisa (PC, notebook, tablet) è obbligatorio implementare un nuovo account d'accesso al sistema, personale e riservato.

4. Garantire la presenza, sulla propria workstation, di un firewall e di un sistema antivirus. Il sistema antivirus deve essere sempre attivo e aggiornato in real time (va bene, ad esempio, anche Avira nella sua versione non commerciale). Il firewall (va bene anche quello integrato nel sistema operativo Windows) deve sempre essere attivo e non deve prevedere alcuna eccezione.

5. È assolutamente vietata la pratica di memorizzazione delle password dei vari account nel browser. È consigliabile evitare di memorizzare anche le user name. Pertanto, il completamento automatico deve essere disabilitato. Si consiglia di utilizzare, per l'accesso ai vari account in cloud, sempre lo stesso browser. La memorizzazione degli account in cloud può essere consentita solo in presenza di un gestore di password crittografico (ad esempio, l'applicazione "Password Manager" integrata nella suite gratuita di Avira).

6. Nel caso in cui si proceda a memorizzare in locale qualsivoglia tipologia di informazioni contenenti dati personali degli interessati, anche temporaneamente, le stesse non dovranno mai essere memorizzate

[1] La password deve essere sufficientemente lunga e complessa, ad esempio deve essere composta da almeno 8 caratteri, contenere almeno un carattere appartenente alle lettere maiuscole e almeno un carattere appartenente alle lettere minuscole, contenere almeno un carattere appartenente alle 10 cifre (0-9), contenere almeno un carattere appartenente ai caratteri non alfabetici (ad esempio !,$,#,%), essere diversa dall'ultima utilizzata e mai riconducibile alla propria sfera personale o professionale.

sull'hard disk della workstation, ma sempre in un dispositivo rimovibile (ad esempio pen drive, hard disk portatile) protetto su base crittografica. A tal proposito è possibile attivare la funzione "Attiva Bitlocker" fornita dal sistema operativo Windows.

7. Non meno importante, nello smart working, attuare una serie di misure organizzative per rendere l'ambiente domestico pari a quello lavorativo al fine di garantire la sicurezza e la riservatezza delle informazioni. Ad esempio, la normale cura della propria postazione di lavoro, non lasciare incustoditi i dispositivi e non condividere informazioni riservate con i propri familiari.

8. L'eventuale collegamento alla LAN (e quindi alla propria workstation) della scuola è consentito solo ed esclusivamente per mezzo di applicazioni conformi al GDPR e agli standar ISO/IEC 27001, ed ISO 9001:2015 (quali, ad esempio, Teamviewer). Ovviamente, in tal caso, valgono le prescrizioni definite ai punti precedenti.