Privacy. Le cautele dopo l'entrata in vigore del Regolamento Ue 2016/679 - Più garanzie con la doppia autenticazione

Dati da proteggere nel lavoro agile

È utile limitare l'accesso dello smart worker alle sole informazioni dell'azienda necessarie

Monica Lambrou

Conciliare il lavoro "agile", fuori dai locali dell'azienda, con la protezione dei dati (a volte riservati) che l'azienda mette a disposizione del lavoratore.

È una delle esigenze che si manifestano dopo l'entrata in vigore del Regolamento europeo 2016/679, che ha armonizzato le discipline degli Stati sulla privacy e ha introdotto nuove tutele. Sarà necessario, infatti, far coesistere due esigenze contrapposte:

- da un lato, il lavoro agile o smart working è utile per potenziare la competitività e conciliare i tempi di vita privata e vita professionale dei lavoratori;
- dall'altro lato, si presta a un incremento esponenziale dei rischi per il trattamento e, quindi, per la sicurezza dei dati delle aziende.

Il cosiddetto smartworker, infatti, con l'uso di strumenti tecnologici, entra in contatto quotidianamente con i database aziendali, con le informazioni relative ai clienti e, spesso, con dati sensibili. Il tutto, peraltro, avviene talvolta all'interno della propria abitazione, ma spesso anche in luoghi pubblici, con una moltiplicazione delle possibili minacce alla riservatezza.

Quali soluzioni è chiamato a individuare il datore per potersi avvalere del lavoro agile nel pieno rispetto della normativa ed evitare sanzioni?

Nonostante il Regolamento europeo sulla protezione dei dati personali non individui adempimenti specifici sullo smart working, dall'approccio generale adottato sui dati trattati con strumenti informatici è possibile trarre alcune considerazioni.

Il ruolo del Dpo

In primo luogo, un ruolo fondamentale sarà svolto dal Dpo (data protection officer). Il Responsabile della protezione dei dati nominato dall'azienda dovrà, infatti, prestare attenzione alla configurazione di un sistema di gestione dati che tenga in debita considerazione la presenza di lavoratori a distanza e, conciò, moderare e, possibilmente, limitare la condivisione delle informazioni allo stretto necessario per l'esecuzione della prestazione (si veda il principio di minimizzazione dei dati ex articolo 5 del regolamento 2016/679). Il Dpo sarà anche chiamato a istruire adeguatamente lo smart worker sull'uso corretto degli strumenti e, appunto, sui molteplici rischi.

Autenticazione a due vie

Sarà opportuno dotarsi di un sistema di autenticazione a due fattori, ossia un meccanismo che consenta al lavoratore di accedere ai dati non solo con la digitazione di una password ma anche con un passaggio identificativo ulteriore. Ciò consente, in particolare, di scongiurare illeciti accessi di terzi, anche in caso di furti o smarrimento del dispositivo utilizzato dallo smart worker. Lo stesso meccanismo dovrà, poi, permettere al datore di lavoro di riconoscere con precisione - a livello centralizzato - l'identità del lavoratore che abbia effettuato l'accesso e che sia dotato di autorizzazione. In base all'articolo 4 del Regolamento 2016/679, il dipendente deve essere preventivamente individuato quale «persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile», nel rispetto degli obblighi (già previsti dal Dlgs 196/2003) gravanti sull'incaricato del trattamento.

La sicurezza dei dispositivi

Sarà inoltre necessario garantire la sicurezza dei dispositivi che, nonostante l'uso al di fuori dei locali dell'azienda, rappresentano a tutti gli effetti strumenti di lavoro. In particolare, sia nel caso in cui questi siano offerti al lavoratore in dotazione (direttamente dal datore) sia ove lo smart worker utilizzi dispositivi propri, non c'è dubbio che questi debbano essere configurati in modo tale da prevenire possibili abusi e, quindi, con un adeguato software antivirus, certificati per connessioni cifrate, dotati di un meccanismo di backup periodico e di sistemi di comunicazione diretta con il server centrale aziendale. Ciò vale sicuramente per i Pc portatili, ma anche per tablet e smartphone.

Accesso limitato ai dati

Sempre in considerazione del principio di minimizzazione dei dati, poi, parrebbe opportuno che l'azienda si dotasse di un sistema per impedire allo smart worker di visualizzare ed entrare in contatto con le informazioni in possesso dell'azienda non pertinenti con lo svolgimento delle proprie mansioni e, quindi, estranee ai propri compiti.

Ulteriori e più efficaci soluzioni potranno - e dovranno - essere individuate, come detto, da piani gestionali ad hoc messi a punto dal Dpo, ovvero da adempimenti richiesti di volta in volta dalle pronunce del Garante della privacy. Le scelte qui richiamate possono prestarsi a rappresentare un modello di accorgimenti di base utili a dimostrare una tendenziale aderenza della policy aziendale alle prescrizioni del Regolamento Ue.

Gli esempi

	IL CASO	LA SOLUZIONE
VIOLAZIONE DEI DATI	Nell'esecuzione della prestazione lavorativa fuori dall'azienda da parte dello smart worker può accadere che i dispositivi usati siano smarriti o siano oggetto di accesso da parte di terzi. Come deve comportarsi il datore di lavoro nei confronti dei soggetti interessati?	**Il datore, come titolare del trattamento, è chiamato a notificare l'avvenuta violazione al Garante entro 72 ore dalla conoscenza del fatto e deve comunicarla senza ingiustificato ritardo agli interessati (articoli 33 e 34 del Regolamento)**
ACCESSO A DUE STEP	Come si realizza effettivamente l'autenticazione a due fattori? Quali strumenti specifici deve offrire il datore di lavoro allo smart worker per poterne identificare l'accesso?	**È bene prevedere un meccanismo di autenticazione e di successiva autorizzazione. Alla password si aggiunge un sistema di codici via sms sul telefono mobile dello smart worker o l'uso di hardware come chiavette (token Usb) o smart card.**
CONTROLLO A DISTANZA	Come si concilia l'esigenza di garantire la sicurezza dei dati personali trattati dallo smart worker con i limiti sul controllo a distanza dell'attività lavorativa? La riconducibilità al dipendente dell'accesso ai dati lede i suoi diritti?	**L'azienda deve poter dimostrare che l'eventuale monitoraggio non mira a controllare l'attività del lavoratore e che c'è un interesse concreto (come la protezione dei dati dei clienti) all'uso degli strumenti. Il lavoratore deve conoscere la policy aziendale**
MISURE A SCELTA	Quali misure di sicurezza informatica sono obbligatorie? Può il lavoratore agile trattare dati personali tramite il proprio dispositivo senza prevedere l'autenticazione a due fattori, la connessione cifrata e gli altri accorgimenti?	**In base al Regolamento (articolo 32), la scelta dei sistemi di sicurezza deve essere commisurata all'entità dei rischi e alla natura dei dati trattati. In caso di violazioni, il titolare dovrà dimostrare di aver previsto accorgimenti adeguati, per evitare sanzioni**
LE SANZIONI POSSIBILI	In caso di effettiva violazione dei dati personali di un soggetto da parte dello smart worker stesso o di eventuali altri terzi, chi è chiamato a rispondere? Qual è l'entità delle possibili sanzioni?	**Il datore di lavoro risponderà della violazione. Per l'inadeguatezza delle misure di sicurezza, la sanzione può raggiungere 10 milioni di euro. Il datore risponderà anche civilisticamente dei danni patiti dall'interessato.**