CIRCOLARE INFORMATIVA N. 8 DEL 02/05/2018

SMART WORKER
Trattamento dei Dati Personali.

Forme di lavoro agile come lo smart working stanno modificando la struttura organizzativa delle aziende anche nell'ottica della protezione dei dati. L'attenzione alla sicurezza dell'informazione deve essere mantenuta alta non solo all'interno dei muri dell'azienda, ma in tutti i luoghi dove i vari dispositivi mobili (laptop, tablet e smartphone) vengono utilizzati. La creazione di un ambiente "protetto" sul luogo di lavoro, dove le possibilità di incidenti siano ridotte al minimo e dove si impedisca in maniera automatica al lavoratore di effettuare operazioni che possano mettere in pericolo l'intero sistema, diventa un obiettivo sempre più complesso per le aziende. **Come fare fronte alle nuove sfide?**

Il documento dell'**Article 29 Data Protection Working Party** (opinion 2/2017) dell'8 giugno 2017 sul trattamento dei dati sul luogo di lavoro ha posto in evidenza numerosi vantaggi, sia in un'ottica organizzativa, sia in un'ottica di sicurezza, strettamente correlati alla società dell'informazione e al suo ingresso nel mondo del lavoro.

Protezione dei dati aziendali e del dipendente

Il cuore del documento è l'analisi del trattamento sistematico e sicuro, da parte di un ipotetico datore di lavoro, di dati personali dei dipendenti con particolare attenzione alla protezione dei dati degli interessati e alla ricerca di un bilanciamento necessario tra gli interessi legittimi del titolare (in questo caso: il datore di lavoro) e una ragionevole aspettativa di privacy e di protezione delle proprie informazioni in capo al dipendente, soprattutto nell'era dello smart working.

Sono molti i principi cardine che sono analizzati e sviluppati nel documento e che tracciano un quadro realistico (anche) del futuro dello smart working.

Un primo aspetto che i redattori del documento tengono a precisare punta alla consapevolezza di una necessaria protezione (che le tecnologie possono, in molti casi, facilitare), del flusso di comunicazioni aziendali elettroniche che sono quotidianamente (e necessariamente) diffuse per motivi correlati alla vita stessa dell'azienda e, in generale, per motivi lavorativi strettamente connessi alle mansioni dei dipendenti.

Di questo flusso elettronico di informazioni, e delle misure di sicurezza adottate, il datore di lavoro deve darne informazione ai lavoratori per renderli non solo consapevoli delle attività che sono svolte, ma anche per formarli e renderli più sicuri.

Dr.ssa ANGELA CUNZIO - Via A. Depretis n.19 - 80133 Napoli(NA) - Tel/Fax 081/19567178
E-mail: cunzioangela@gmail.com - ancunzio@tin.it - PEC: angela.cunzio@odcecnapoli.it

Smart working e flusso di comunicazioni

Il documento muove da alcune premesse che, a detta dei redattori, hanno completamente mutato il panorama del lavoro.

Innanzitutto, i costi per implementare strumenti accurati per la protezione dei dati e delle informazioni aziendali sono sensibilmente diminuiti, quindi la procedura diventa più semplice e, ormai, alla portata di tutti (anche delle piccole e medie imprese che, solitamente, non avevano grandi possibilità d'investimenti tecnologici).

Le attività online e sui device smart rendono, poi, il lavoratore molto più visibile e, in alcuni casi, molto più vulnerabile e, spesso, inconsapevole di che cosa realmente succeda nella gestione informatica del dato e alla potenza dei trattamenti (soprattutto quando i dati "viaggiano" tra sistemi, tra server cloud e, sempre più sovente, tra Nazioni).

Infine, i confini tra casa e lavoro sono stati eliminati, soprattutto quando i dipendenti lavorano da remoto o si trovano a dover viaggiare per lavoro. Non vi è più una comfort zone, un momento della giornata di assoluta privacy senza contaminazione tra vita privata e lavoro. Tutto, ora si mescola, soprattutto flusso di comunicazione e orari/tempi. E ciò comporta che l'attenzione alla sicurezza dell'informazione debba essere mantenuta alta non solo all'interno dei muri dell'azienda, ma in tutti i luoghi dove i vari dispositivi mobili (laptop, tablet e smartphone) vengano utilizzati.

Come creare un ambiente "protetto" sul luogo di lavoro

Una creazione di un ambiente "protetto" sul luogo di lavoro (per "protetto" intendiamo un luogo informatico dove le possibilità di incidenti siano ridotte al minimo e dove si impedisca in maniera automatica al lavoratore di effettuare operazioni che possano mettere in pericolo l'intero sistema) che sia nettamente separato dall'ambiente domestico diventa un obiettivo sempre più complesso nel momento in cui strumenti personali e strumenti professionali si fondono nella vita aziendale (si pensi alle attività dove è consentito al lavoratore di utilizzare il suo device).

Con le nuove tecnologie, però, e con policy o regolamenti specifici volti a "plasmare" il comportamento degli operatori anche quando non sono nell'ambiente "protetto" aziendale, è concretamente possibile equiparare il livello di sicurezza di qualsiasi operazione.

Le tecnologie, d'altro canto, possono permettere al datore di lavoro di raggiungere 3 obiettivi importanti in un'ottica produttiva e di incremento della sicurezza: evitare o prevenire perdite correlate ai beni dell'azienda (svolgendo attività di controllo preventive e difensive), aumentare la produttività dei dipendenti (fornendo strumenti deputati a ciò) e proteggere i loro dati personali(aumentando, così, il livello di privacy all'interno dell'azienda).

Crittografia e protezione by design

Per perseguire finalità di protezione dei dati personali, lo strumento principe è la crittografia, che dovrebbe cifrare sia le informazioni aziendali (statiche sui server e in transito nelle comunicazioni), sia le informazioni contenute in dispositivi forniti ai dipendenti (laptop, tablet, smartphone, chiavette) sia tutti i contatti di comunicazione tra i

dipendenti (magari lontani dalla sede aziendale o itineranti) e i punti di accesso della rete aziendale stessa. Lo stesso GDPR, e il documento in oggetto, citano spesso la crittografia e la pseudonimizzazione dei dati come due dei metodi più efficaci per proteggere un insieme di dati personali e sensibili che possa avere qualche valore (proprio come un tipico patrimonio aziendale).
Il rispetto della legge, nota il documento, non è dato soltanto dall'elevare simili misure di protezione, ma anche dal prestare attenzione, nello svolgimento delle quotidiane attività aziendali, a tre fattori molto specifici e considerati, dagli autori dell'Opinion, centrali.
Il primo fattore coinvolge le decisioni automatizzate che abbiano conseguenze giuridiche, ossia quelle modalità di trattamento dei dati che sono svolte unicamente da macchine ed algoritmi e che non prevedono un intervento dell'essere umano. Oltre a una adeguata informativa, va sempre prevista la possibilità di un intervento "umano" per poter verificare che la macchina abbia agito correttamente e all'interno dei parametri previsti dalla legge.
Il secondo fattore è l'attenzione a una protezione by design, ossia il patrimonio aziendale dei dati, e la sua gestione, devono sempre essere trattati con una attenzione "genetica" alla privacy, sia in un'ottica di protezione dei dati, sia con riferimento alla trasparenza dei processi.
Proprio un'idea diffusa di trasparenza, correlata alla protezione delle informazioni, è indicata come terzo e ultimo fattore essenziale: in ogni momento devono essere tracciabili le modalità di trattamento delle informazioni (tracking).
Posto che il trattamento deve sempre essere proporzionato e necessario, il documento conclude ribadendo come una comunicazione basata sulla trasparenza debba essere alla base di ogni attività di monitoraggio delle attività telematiche del dipendente, con nozioni chiare e immediatamente accessibili.
Al contempo, le misure adottate devono essere proporzionate, dovrebbero puntare all'anonimato del dipendente e dovrebbero configurare, allo stesso tempo, un trattamento dei dati ridotto al minimo.
Questo perché una reale protezione delle informazioni aziendali non si raggiunge soltanto con la creazione di un sistema "protetto" (immune sia da attacchi provenienti dall'esterno, sia da attacchi provenienti dall'interno), ma anche con un uso intelligente della crittografia (che garantisce non soltanto segretezza e riservatezza, ma anche integrità dei dati) e con una costante verificabilità e trasparenza dei processi, che vanno a beneficio sia dei diritti dei lavoratori, sia della protezione stessa (e accountability) dei processi aziendali.

Lo Studio Cunzio resta a disposizione per qualsiasi chiarimento in merito.

Distinti saluti
Dott.ssa Angela Cunzio

Dr.ssa ANGELA CUNZIO - Via A. Depretis n.19 - 80133 Napoli(NA) - Tel/Fax 081/19567178
E-mail: cunzioangela@gmail.com - ancunzio@tin.it - PEC: angela.cunzio@odcecnapoli.it