Aggiornamento Policy Utilizzo Beni Aziendali

L'articolo 23 del D.Lgs 151/2015 (Razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese) attuativo del Jobs Act è diventato il punto di riferimento normativo per quanto concerne la tutela del patrimonio aziendale.

STRUMENTI AZIENDALI (PC, CELL, TABLET…)
L'accordo sindacale o l'autorizzazione ministeriale non sono necessari per l'assegnazione ai lavoratori degli strumenti utilizzati per rendere la prestazione lavorativa, pur se dagli stessi derivi anche la possibilità di un controllo a distanza del lavoratore.

TELECAMERE
Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo sindacale con le Rsu o Rsa, ovvero con l'autorizzazione della Direzione territoriale del lavoro o, nel secondo caso, del ministero del Lavoro.

UTILIZZO DEI DATI RACCOLTI
I dati raccolti possono essere utilizzati «**a tutti i fini connessi al rapporto di lavoro**, a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli» sempre «nel rispetto» del Codice sulla privacy.

LINEE GUIDA
- Definizione di strumento aziendale
- Adeguata informazione
- Non eccedenza nel controllo
- Precisa informazione su modalità e descrizione dei controlli effettuati
- Security by design nel trattamento del dato (GDPR 2018)

RISULTATI

- Individuare frodi e comportamenti scorretti con maggiore tempestività
- Maggior numero di "sensori" a tutela del patrimonio aziendale
- Possibilità di gestire internamente all'azienda problematiche che precedente
- mente dovevano essere demandate a terzi per essere svolte nella legalità
- Maggior controllo sulle informazioni strategiche, anche in caso di uscita di persone in ruoli chiave

ESTRATTO DA UNA POLICY REALIZZATA

Riportiamo di seguito un paragrafo di policy da noi realizzata, che rispetta le prescrizioni contenute nel GDPR e nel D.Lgs 151/2015 e garantisce la possibilità di agire sia in caso di frode interna (white collar crime), sia in caso di attacco informatico (data breach).

X.X Nella gestione dei sistemi informatici aziendali, e degli strumenti di lavoro, il servizio ICT, o terzi incaricati dalla direzione, potranno acquisire informazioni generate dalle funzionalità insite negli stessi sistemi, quali: i log generati da Microsoft Windows/Android/iOS, gli accessi alla rete e ai dispositivi aziendali, la cancellazione, creazione o esportazione/trasferimento di file e informazioni, l'uso di file/software di carattere non lavorativo. I dati verranno conservati per 206 giorni (tempo medio statistico per la scoperta di un attacco informatico) e quindi cancellati. Tali informazioni potranno essere utilizzate in caso di attacco informatico, incidente informatico e ai sensi del successivo punto X, per tutti i fini connessi al rapporto di lavoro, sempre nell'ambito delle finalità individuate nel precedente punto Y, e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.