Lavoro agile

Aspetti privacy

Tutela dei dati personali e Smart working

Come la prestazione lavorativa agile incide sulla disciplina della tutela dei dati personali?

La prestazione lavorativa a distanza potrebbe comportare nuovi (o differenti nelle modalità) trattamenti di dati personali che richiedano:

- eventuale aggiornamento dell'informativa da rendere all'interessato;
- verifica dell'adeguatezza delle misure tecniche e organizzative a tutela dei dati personali trattati dal lavoratore (autorizzazione e istruzioni al trattamento).

Tutela dei dati personali e Smart working

Di quali dati personali parliamo in relazione al lavoro agile?

- dati personali **del lavoratore** trattati dall'azienda, raccolti tramite l'utilizzo dei dispositivi che consentono la connessione e la prestazione lavorativa a distanza
- dati personali **di terzi** (es. clienti, fornitori, colleghi di lavoro) trattati dal lavoratore per conto dell'azienda**,** che vanno protetti anche quando il loro trattamento è effettuato al di fuori della sede aziendale
- dati personali **di terzi** riferibili alla sfera privata del lavoratore (es. famigliari – amici-collaboratori domestici del lavoratore) eventualmente/accidentalmente raccolti dall'azienda, tramite i colleghi di lavoro, in relazione ai luoghi in cui avviene la prestazione (es. riprese durante una videoconferenza aziendale) o agli strumenti utilizzati (PC non aziendale utilizzato da più persone oltre al lavoratore)

La legge sul lavoro agile e i riflessi sulla disciplina privacy

La normativa privacy non viene espressamente citata nel testo della Legge 22 Maggio 2017 n.81.

Tuttavia sono richiamati due importanti principi alla base della *privacy compliance*:

Idonee misure di sicurezza tecniche e organizzative e relativa responsabilità

Il datore di lavoro «*è responsabile della sicurezza e del buon funzionamento degli strumenti tecnologici assegnati al lavoratore per lo svolgimento dell'attività' lavorativa*» [Art. 18 c.2]

La legge sul lavoro agile e i riflessi sulla normativa privacy

Corretta e trasparente informazione al lavoratore sui trattamenti di dati personali raccolti in relazione alla sua prestazione lavorativa

(Art. 21): L'accordo relativo alla modalità di lavoro agile disciplina l'esercizio del potere di controllo del datore di lavoro sulla prestazione resa dal lavoratore all'esterno dei locali aziendali nel rispetto di quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300, e successive modificazioni.

GDPR – Reg. UE 679/2016

Liceità, correttezza, trasparenza, necessità, limitatezza e pertinenza [art.5]

I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. I dati acquisiti devono essere strettamente **necessari, limitati e pertinenti** in relazione alle finalità perseguite**.**

Obbligo di istruire-autorizzare il trattamento [art.29]

Chiunque agisca sotto l'autorità del titolare (o responsabile) del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è **istruito** in tal senso dal titolare del trattamento

GDPR – Reg. UE 679/2016

Sicurezza del trattamento: le misure tecniche e organizzative «adeguate» [art.32]

Tenendo conto dello stato dell'arte e dei costi di attuazione (….) il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (….)

Si tiene conto in special modo dei rischi che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Codice Privacy – Dlgs.vo 196/2003

Art. 114 (Garanzie in materia di controllo a distanza)

1. Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n.300.

Quindi:

- Restano espressamente esclusi, anche per lo Smart working, controlli continuativi e sistematici non necessari e/o pertinenti ad una corretta gestione del rapporto di lavoro.
- La violazione delle disposizioni ex art.4 della legge 300/70 comporta anche una violazione sotto il profilo privacy (trattamento illecito di dati personali). E viceversa.

Protocollo nazionale sul lavoro in modalità agile

Promosso dal Ministro del Lavoro e delle Politiche Sociali e sottoscritto dalle Parti sociali il 7 dicembre 2021
Fornisce delle linee di indirizzo di riferimento per la prestazione lavorativa in smart working

Art. 5 Strumenti di lavoro

1 - Fatti salvi diversi accordi, il datore di lavoro, di norma, fornisce la strumentazione tecnologica e informatica necessaria allo svolgimento della prestazione lavorativa in modalità agile, al fine di assicurare al lavoratore la disponibilità di strumenti che siano **idonei** all'esecuzione della prestazione lavorativa e **sicuri per l'accesso ai sistemi aziendali**.

2 - Laddove le parti concordino l'utilizzo di strumenti tecnologici e informatici propri del lavoratore, provvedono a stabilire **i criteri e i requisiti minimi di sicurezza da implementare** e possono concordare eventuali forme di indennizzo per le spese.

Protocollo nazionale sul lavoro in modalità agile

promosso dal Ministro del Lavoro e delle Politiche Sociali e sottoscritto dalle Parti sociali

Art. 5 Strumenti di lavoro

4 - In caso di **guasto, furto o smarrimento** delle attrezzature e in ogni caso di impossibilità sopravvenuta a svolgere l'attività lavorativa, **il dipendente è tenuto ad avvisare tempestivamente** il proprio responsabile e, se del caso, attivare la procedura aziendale per la gestione del **data breach**. Laddove venga accertato un comportamento negligente da parte del lavoratore cui conseguano danni alle attrezzature fornite, quest'ultimo ne risponde. Qualora persista l'impossibilità a riprendere l'attività lavorativa in modalità agile in tempi ragionevoli, il dipendente e il datore di lavoro devono concordare le modalità di completamento della prestazione lavorativa, ivi compreso il rientro presso i locali aziendali.

Protocollo nazionale sul lavoro in modalità agile

promosso dal Ministro del Lavoro e delle Politiche Sociali e sottoscritto dalle Parti sociali

Art. 12 Protezione dei dati personali e riservatezza

1. Il lavoratore in modalità agile è tenuto a trattare i dati personali cui accede per fini professionali in **conformità alle istruzioni fornite dal datore di lavoro**. Il lavoratore è tenuto, altresì, alla riservatezza sui dati e sulle informazioni aziendali in proprio possesso e/o disponibili sul sistema informativo aziendale.

2. Il datore di lavoro **adotta tutte le misure tecnico-organizzative adeguate** a garantire la protezione dei dati personali dei lavoratori in modalità agile e dei dati trattati da questi ultimi.

3. Resta ferma la normativa vigente sul trattamento dei dati personali e, in particolare, il Regolamento UE n. 679/2016 (GDPR).

Protocollo nazionale sul lavoro in modalità agile

promosso dal Ministro del Lavoro e delle Politiche Sociali e sottoscritto dalle Parti sociali

Art. 12 Protezione dei dati personali e riservatezza

4. Il datore di lavoro informa il lavoratore agile in merito ai trattamenti dei dati personali che lo riguardano, anche nel rispetto di quanto disposto dall'art. 4 Stat. Lav. e s.m.i. Il datore di lavoro fornisce al lavoratore agile **le istruzioni e l'indicazione delle misure di sicurezza che lo stesso deve osservare** per garantire la protezione, segretezza e riservatezza delle informazioni che egli tratta per fini professionali. Spetta al datore di lavoro/titolare del trattamento **l'aggiornamento del registro del trattamento** dei dati connessi alle attività svolte anche in modalità di lavoro agile. Al fine di verificare che gli strumenti utilizzati per il lavoro in modalità agile siano conformi ai principi di privacy by design e by default, è sempre raccomandata l'esecuzione di **valutazione d'impatto (DPIA)** dei trattamenti.

Protocollo nazionale sul lavoro in modalità agile

promosso dal Ministro del Lavoro e delle Politiche Sociali e sottoscritto dalle Parti sociali

Art. 12 Protezione dei dati personali e riservatezza

5. Il datore di lavoro promuove l'adozione di **policy aziendali** basate sul concetto di security by design, che prevedono la gestione dei **data breach** e l'implementazione di misure di sicurezza adeguate che comprendono, a titolo meramente esemplificativo, se del caso la **crittografia, l'adozione di sistemi di autenticazione e VPN, la definizione di piani di backup e protezione malware**. Il datore di lavoro favorisce iniziative di formazione e **sensibilizzazione** dei lavoratori sia **sull'utilizzo, custodia e protezione degli strumenti** impiegati per rendere la prestazione, sia sulle cautele comportamentali da adottare nello svolgimento della prestazione lavorativa in modalità agile, compresa la gestione dei data breach.

Gli adempimenti

Dall'analisi della normativa applicabile, il rispetto della disciplina privacy si traduce, nel caso di prestazione lavorativa in Smart working, nei seguenti adempimenti:

- **informare** il lavoratore sulle peculiarità che il trattamento dei suoi dati personali comporta quando la sua prestazione è effettuata a distanza
- garantire l'estensione delle **istruzioni e policy aziendali** in essere anche al caso in cui l'attività lavorativa non sia svolta nella sede aziendale
- assicurare che le **misure di sicurezza** adottate dall'azienda siano **idonee** anche nel caso di attività di trattamento dei dati personali svolte a distanza

Consigli operativi

Predisporre un documento, da sottoporre allo smart worker, che funga da estensione e complemento dei tre documenti di cui il lavoratore è già in possesso:

- **informativa ai dipendenti** (nel caso di ulteriore raccolta di dati personali riferibili al lavoratore)
- **autorizzazione/istruzioni** al trattamento dei dati personali da parte del lavoratore (per fornire istruzioni o autorizzazioni aggiuntive)
- **regolamento aziendale** sull'utilizzo dei dispositivi e degli strumenti informatici (in relazione all'utilizzo da remoto)
- se, necessario, integrare il **registro dei trattamenti** e**, i**n caso di trattamenti particolarmente invasivi per la privacy dei lavoratori, effettuare una **DPIA** (valutazione d'impatto dei trattamenti)

Consigli operativi

In alternativa: integrare i tre documenti con istruzioni/prescrizioni specifiche per la prestazione in remoto.

Sul sito di Confindustria Vicenza è disponibile, per le imprese associate, una bozza del documento all'interno della modulistica della Guida «Privacy in Azienda»:

https://www.confindustria.vicenza.it/guide/Privacy-in-azienda.-La-transizione-verso-il-Regolamento-europeo-(GDPR)-1748

Criticità

Alcuni spunti di riflessione rivolti, in particolare alle PMI:

- Il PC utilizzato dal lavoratore è aziendale o personale?
  Se personale:
  - è sufficientemente aggiornato e protetto da software maligno?
  - è utilizzato anche da altre persone? Se si, sono implementate sessioni distinte ad accesso riservato per i diversi utilizzatori?
- I dati vengono salvati sul server aziendale o sul PC? Sono coperti da backup?

Criticità

- Il PC del lavoratore come si connette alla rete aziendale? E' stata implementata una connessione protetta? (es. desktop remoto via VPN)
- La profilazione autorizzativa personale degli utenti è garantita anche in Smart working? Le password per accedere al PC e al server aziendale sono «robuste»?
- I dispositivi di rete per la connessione da casa (router) sono adeguatamente protetti/aggiornati?

Criticità

- Il lavoratore è informato di avvisare tempestivamente il responsabile IT in caso di anomalie che possano far sospettare una violazione del dispositivo o in caso di furto in abitazione?
- I software utilizzati per il lavoro in remoto e per il lavoro in team offrono garanzie di sicurezza e di conformità al GDPR?
- Viene gestita e limitata la fuoriuscita di documenti cartacei aziendali riservati e la loro temporanea custodia presso il domicilio del lavoratore?

Considerazione finale:
l'importanza di tutelare i segreti commerciali

Le misure di sicurezza tecniche e organizzative non sono solo necessarie per conseguire la conformità aziendale alla normativa privacy, ma sono utili anche per **proteggere le informazioni tecniche e commerciali che costituiscono rilevante know-how** dell'azienda e dei propri clienti/fornitori.

Grazie

Luca Grifalconi

Area Legale e Urbanistica

legale@confindustria.vicenza.it