STUDIO LEGALE DELFINO E ASSOCIATI
WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PALO ALTO SAN FRANCISCO CHICAGO LOS ANGELES PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

LA DISCIPLINA A TUTELA DEI DATI PERSONALI ANCHE IN UN'OTTICA DI MITIGAZIONE DEI RISCHI DI ATTACCHI CYBER

Avv. Marilena Hyeraci

22 marzo 2022

INDICE DEGLI ARGOMENTI

- Uno sguardo d'insieme
- Obblighi di lavoratore e datore di lavoro
- La cd. valutazione di impatto
- *Privacy by design* e *privacy by default*
- *Data breach* e misure di sicurezza
- *Take-aways* e buone prassi applicative
- Pari opportunità e inclusività

UNO SGUARDO D'INSIEME

- Centralità di tutela dei dati personali e sicurezza:
  - ✓ Premessa
  - ✓ Protezione di dati personali e riservatezza (artt. 2 e 12)
  - ✓ Violazione dei dati - *data breach* (art. 5, comma 5)
  - ✓ Sicurezza *by design* (artt. 6 e 12)
  - ✓ *Privacy by design* e *privacy by default* (art. 12)
  - ✓ Valutazione d'impatto - *data privacy impact assessment/DPIA* (art. 12)
  - ✓ Formazione e informazione (artt. 2 e 13)

- Parità di trattamento e inclusività:
  - ✓ Parità di trattamento e pari opportunità (art. 9)
  - ✓ *Welfare* e inclusività (art. 11)

QUALCHE DATO

- Il ricorso al lavoro agile è più che raddoppiato rispetto al periodo pre-pandemico (Gruppo di Studio, **Premessa al Protocollo**)
- Prima della pandemia: lavoro da remoto in Italia 3.6% (vs media europea 6% e14% Paesi Bassi e Finlandia), nel 2020 in Italia il 40% dei lavoratori ha iniziato a lavorare da casa, a fronte della media europea del 37% (**Eurostat**)
- Oltre 6,6 milioni i lavoratori da remoto attivi a marzo 2020 in Italia (**Osservatorio sullo *Smart working* Politecnico Mi**)
- Forte incremento nell'utilizzo della modalità di Lavoro Agile vs consapevolezza di rischi e vulnerabilità da parte di datore di lavoro e lavoratore agile
- "*Per il primo semestre 2021 sono stati analizzati 1.053 gli attacchi cyber gravi, ovvero con un impatto sistemico in diversi aspetti della società, della politica, dell'economia e della geopolitica. Si tratta del 24% in più rispetto allo stesso periodo del 2020, per una media mensile di attacchi gravi pari a 170, contro i 156 del 2020" (*Rapporto della Associazione Italiana per la Sicurezza Informatica - **Clusit 2021**)

OBBLIGHI DI DATORE DI LAVORO E LAVORATORE (ARTT. 12-13)

- Il datore di lavoro deve dare al lavoratore agile **istruzioni** chiare e precise sulle modalità di trattamento dei dati personali che effettua nell'ambito della propria attività lavorativa

- Lo *smart worker* é vincolato a **riservatezza e confidenzialità**

- **Informativa** dettagliata (sezione *ad hoc* sui controlli)

- **Formazione:**
  - ✓ "*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***" (art. 12, comma 5)
  - ✓ Formazione obbligatoria (art. 13, comma 5)

LA C.D. VALUTAZIONE DI IMPATTO (ART.12)

- «*Quando un trattamento di dati personali può presentare un 'rischio elevato' per i diritti e le libertà delle persone, prima di iniziare il trattamento, deve essere effettuata una cd. valutazione di impatto sulla protezione dei dati personali» (*art. 35 GDPR)

- La valutazione di impatto è 'sempre raccomandata' nel caso di Lavoro Agile, quindi anche in caso di 'rischio non elevato' (Protocollo, Autorità Nazionali per la Protezione dei Dati Personali)

- La valutazione di impatto è raccomandata per verificare che siano rispettati i principi di ***privacy by design e by default*** previsti dal GDPR

PRIVACY BY DESIGN E *PRIVACY BY DEFAULT* (ART. 12)

- "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento* ***stesso****"* devono essere messe in atto *"****misure tecniche e organizzative adeguate****, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati*" (art. 25, comma 1, GDPR)

- Le misure tecniche e organizzative devono essere tali da garantire che siano trattati, '**per impostazione predefinita**', solo i dati personali necessari per ogni specifica finalità del trattamento e "*per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*" (art. 25, comma 2, GDPR)

DATA BREACH (ART. 5) E MISURE DI SICUREZZA (ART. 12)

- Le Parti sociali dedicano molta attenzione a ***data breach*** e **misure di sicurezza**:
  - ✓ "*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"* (art. 5, comma 4)
- "*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*" (art. 12, comma 5)

TAKE-AWAYS E BUONE PRASSI APPLICATIVE

- Consultare i referenti di tutte le aree aziendali potenzialmente coinvolte (Risorse umane, Legale/*Compliance*, IT, *Privacy*, eventuale DPO, RSPP)
- Aggiornare - periodicamente - tutta la documentazione collegata al Lavoro Agile
- Privacy e sicurezza non solo nei documenti, ma anche nei processi
- Coordinamento con il modello di organizzazione gestione e controllo *ex* d.lgs. 231/2001

PARITÀ DI TRATTAMENTO E INCLUSIVITA' (1/2)

- Parità di trattamento tra lavoratore agile e lavoratore in presenza (art. 9, comma 1):
  - ✓ «*mansioni*
  - ✓ *inquadramento professionale*
  - ✓ *retribuzione*
  - ✓ *premi di risultato*
  - ✓ *percorsi di carriera*
  - ✓ *iniziative formative*
  - ✓ *forme di welfare aziendale*
  - ✓ *benefit*»

PARITÀ DI TRATTAMENTO E INCLUSIVITA' (2/2)

- *«Le Parti sociali promuovono lo svolgimento del lavoro in modalità agile, garantendo:*
  - ✓ *la parità tra i generi,*
  - ✓ *anche nella logica di favorire l'effettiva* ***condivisione delle responsabilità genitoriali****, e*
  - ✓ *accrescere in termini più generali la conciliazione tra i tempi di vita e i tempi di lavoro…*

- *…A tal fine si impegnano a rafforzare i servizi e le misure di equilibrio tra attività professionale e vita familiare per i genitori e i* ***prestatori di assistenza****»* (art. 9, comma 2)

- «*Le Parti sociali, a fronte dei cambiamenti che l'estensione del lavoro agile può determinare nelle dinamiche personali di ciascun dipendente, si impegnano a sviluppare nell'ambito degli strumenti di* welfare *aziendale e di bilateralità, un più ampio e concreto supporto anche in ambito di* ***genitorialità****,* ***inclusione e conciliazione vita-lavoro****, anche mediante* ***misure di carattere economico*** *e/o* ***strumenti di welfare*** *che supportino l'attività di lavoro in modalità agile da parte del lavoratore*» (art. 11)

MARILENA HYERACI

MILANO

Litigation Department

Milano
+39 02 76 36 31
mhyeraci@delfinowillkie.com

Marilena Hyeraci è *Senior Associate* del dipartimento di contenzioso dello studio di Milano.

Vanta consolidata esperienza in *compliance*, *white collar cimes*, e *data protection*. Assiste i clienti anche in situazioni di pre-contenzioso, e nelle indagini interne, in contesti nazionali e *cross border*.

Marilena supporta le aziende nella valutazione dei rischi legali, nella redazione e revisione dei modelli organizzativi e di *compliance* aziendale. Presta consulenza in materia di protezione dei dati personali, nella gestione dei *data breach* e procedure di *disclosure* alle Autorità. Tiene inoltre corsi di formazione sul decreto legislativo n. 231/2001, in materia di *compliance* e protezione dei dati personali, per i membri dei consigli di amministrazione e prime linee aziendali.

In oltre 15 anni di esperienza, ha assistito primarie società italiane e multinazionali, sviluppando un *focus* particolare su corruzione nazionale ed internazionale, reati informatici e frodi nazionali e internazionali.

Marilena ha fondato una *community* in materia di *diversity&inclusion* ed è tra le 10 *TopVoices* in Italia riconosciute da LinkedIn sui temi di parità e inclusione.

Interviene regolarmente a convegni ed è autrice di numerose pubblicazioni; è inserita nei principali *ranking* internazionali, quali *Chambers&Partners, Legal 500 e Who's Who Legal.*