Spett.le
GIMAV
Via Petitti, 16
20149 MILANO (MI)
c.a Ing. Laura Biason

Milano, 27 Marzo 2018

Oggetto: Brevi note esplicative ed operative sull'attività di assistenza relativa all'*assessment privacy – compliance* (di seguito: "GDPR").

Spetta.le Gimav,

facciamo seguito alla integrazione della convenzione in essere per inviare delle brevi note esplicative ed operative sul lavoro di assistenza legale che il nostro Team può offrire agli associati relativamente all'*assessment privacy*, con specifico riguardo al GDPR.

Indichiamo qui di seguito i temi più rilevanti.

1. Note introduttive

a. Definizioni e ambito di applicazione della normativa in materia di privacy

Le definizioni più rilevanti, da tenere in considerazione ai fini dell'attività di *assessment*, sono le seguenti:

- **Dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("**interessato**"). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **Trattamento**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- **Titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- **Responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

b. Il GDPR (General Data Protection Regulation)

Il GDPR è il Regolamento Europeo n. 679/2016, entrato in vigore il 27 aprile 2016 e che sarà efficace a partire dal 25 maggio 2018 (*deadline* per l'adeguamento).

Si tratta di una normativa **unica** per tutti gli Stati Membri dell'Unione Europea.

Le principali novità introdotte dal GDPR sono costituite da:

- Il principio di **responsabilizzazione** (***accountability***): chi tratta dati deve essere in grado di dimostrare di rispettare il GDPR;

  es. analisi dei rischi, predisposizione dei trattamenti e delle misure di sicurezza a tutela dei dati adeguati rispetto ai rischi

- I nuovi **adempimenti** per quanto concerne il livello organizzativo interno delle realtà coinvolte;

  es. registri dei trattamenti, procedura di analisi di impatto in caso di trattamenti che presentano forti rischi, nomina di un Data Protection Officer con funzione di vigilanza

- Le nuove **sanzioni**, che possono arrivare sino al 2% o 4% del fatturato globale annuo mondiale, con possibilità di "modulazione" da parte dell'Autorità Garante.

2. Attività di assessment

a. Mappatura

Il primo passaggio dell'*assessment* è la **mappatura** delle tipologie e della mole di **dati** trattati, dei **soggetti** coinvolti nel trattamento e della strutturazione dei **sistemi** utilizzati per trattare tali dati.

Ai soggetti coinvolti può essere richiesto di **partecipare** a questa fase tramite

- completamento di un **questionario** relativo ai trattamenti di dati realizzati (accompagnato da eventuale integrazione documentale);
- completamento di un documento descrittivo dei trattamenti di dati realizzati nell'ambito delle attività svolte.

Entrambi i documenti di cui sopra sono accompagnati da un **glossario**, **note** di accompagnamento, **domande** di supporto ed **esempi** pratici.

Via San Vittore al Teatro 1/3
20123 – Milano
(Piazza Affari)
Ph. +39 02 21117645
Fax +39 02 87182231
e.mail: gfbonacci@elrlex.it

Entrambi i documenti necessari per la mappatura richiedono sia un'attività di **descrizione** e **compilazione** da parte dei soggetti coinvolti che un'attività di raccolta e consegna della documentazione richiesta al *Team compliance aziendale ELR LEX*.

Esempio: Estratto del Questionario:

Sezione "Risorse Umane"

- ***Soggetti coinvolti:*** *HR unit*

INFORMATIVA E CONSENSO

1) È stata fornita a tutti i dipendenti/collaboratori un'informativa privacy contenente tutti gli elementi richiesti dall'art. 13 del Codice Privacy e dall'art. 13 del Regolamento?	*☐ No* *☐ Sì* *Si prega di fornire l'informativa privacy, se esistente.*
2) In caso affermativo, è possibile provare di aver fornito l'informativa privacy ai dipendenti/collaboratori?	*☐ No* *☐ Sì, grazie a: _____*

- *Potrebbe essere richiesto, ad esempio all'HR Manager, di rispondere a questa sezione del questionario, trattandosi di trattamenti di dati di sua competenza*
- *All'HR Manager potrebbe poi essere sottoposta una richiesta di integrazione documentale (es. fornire l'informativa di cui alla domanda **1.**)*

b. Analisi

Terminata la prima fase dell'*assessment* ("**Mappatura**"), il *Team compliance aziendale ELR LEX* provvede ad analizzarne le risultanze e quindi:

- le **risposte** alle varie sezioni del Questionario;
- la **documentazione** eventualmente fornita;
- l'eventuale **documento di descrizione dei trattamenti** realizzato relativamente alle attività svolte.

Laddove le informazioni reperite risultino incomplete e/o lacunose il *Team compliance aziendale ELR LEX* provvede ad approfondire quanto rilevato tramite **interviste mirate** ai singoli soggetti/funzioni

- a tale fase partecipano esclusivamente il *Team compliance aziendale ELR LEX* e, soltanto nel caso si ritenga necessario procedere con le interviste, sono coinvolti anche i soggetti appartenenti alle funzioni interessate.

c. Remediation Plan

Sulla base dell'esame svolto nel corso del secondo passaggio dell'*assessment* ("**Analisi**") si predispone un Piano di Remediation, che Vi verrebbe sottoposto ai fini dell'approvazione.

Via San Vittore al Teatro 1/3
20123 – Milano
(Piazza Affari)
Ph. +39 02 21117645
Fax +39 02 87182231
e.mail: gfbonacci@elrlex.it

Il piano di Remediation riporta le risultanze dell'attività di *assessment* e quindi

- un fedele *report* di tutti i trattamenti e i ruoli *privacy* al momento in essere all'interno della realtà analizzata;
- l'identificazione dei principali gap rispetto a quanto previsto dal GDPR e delle aree in merito alle quali risulta più urgente intervenire, in termini di processo e presidi tecnologici, rispetto a quanto previsto dal GDPR stesso;
- l'identificazione delle principali azioni da avviare, in termini di processo e metodologie;
- le possibili proposte in relazione ad eventuali scelte strategiche da fare, nonché le relative tempistiche specifiche per attuare le stesse.

d. Implementazione

L'ultima fase dell'*assessment* prevede, infine, un'attività di supporto - sulla base di quanto sviluppato nei precedenti passaggi - nell'implementazione degli strumenti organizzativi *privacy* necessari alla *compliance* della società, non solo relativamente al Regolamento ma anche agli orientamenti del Garante sviluppati in relazione alla applicazione dello stesso. In particolare si provvede alla:

- predisposizione di un modello standard della documentazione privacy;

A titolo esemplificativo e non esaustivo si procederebbe a redigere i seguenti documenti:

a) autocertificazione sostitutiva del DPS;

b) nomina/e responsabili del trattamento;

c) nomina/e incaricati del trattamento;

d) Informativa privacy per dipendenti e collaboratori;

e) Informativa privacy per tirocinanti e stagisti;

f) Informativa privacy per clienti;

g) Informativa privacy per fornitori;

h) Nomina standard responsabile esterno del trattamento attiva (quando una nominate un soggetto terzo);

i) Nomina standard responsabile esterno del trattamento passiva (quando un soggetto terzo Vi nomina);

l) Nomina standard responsabile esterno del trattamento con funzioni di amministratore di sistema attiva (quando Voi nominate qualcuno);

m) Nomina di Amministratore di Sistema;

n) Nota informativa Amministratori di Sistema per dipendenti;

o) Disciplinare interno per email e Internet;

p) Disclaimer email.

Via San Vittore al Teatro 1/3
20123 – Milano
(Piazza Affari)
Ph. +39 02 21117645
Fax +39 02 87182231
e.mail: gfbonacci@elrlex.it

- definizione di linee guida/procedure/documentazione *privacy* per la gestione dei dati personali, sulla base di quanto definito nell'ambito del GDPR, con particolare riferimento ai seguenti ambiti: gestione del ciclo di vita dei dati personali (ad es. raccolta, utilizzo, condivisione), gestione dei trasferimenti, data *protection by design* e *by default*, *data protection impact assessment*, gestione dei *data breach*, notificazione, monitoraggio e controllo.

3. Tempistiche

A partire dall'affidamento dell'incarico, l'attività di *assessment* potrebbe richiedere un lavoro di circa un mese e mezzo.

Confidiamo nel fatto che le presenti note possano essere utili con le Vostre esigenze e aspettative. Rimaniamo in ogni caso a disposizione per chiarire, approfondire e discutere i contenuti delle stesse.

Infine, con riguardo ai costi di assistenza, tenuto conto della convenzione in essere con GIMAV, consapevoli della tipologia di società (aziende industriali) a cui fanno capo gli associati e forti della nostra esperienza (avendo già provveduto ad adeguare oltre 200 aziende) siamo in grado di offrire la massima competitività ed efficienza.

Per qualunque maggiore informazione non esitate a contattarci ai recapiti che trovate in calce alle presenti note.

Cordiali saluti.

Avv. Giuseppe F. Bonacci

(Coordinatore e Responsabile Team Compliance aziendale ELR LEX)

Via San Vittore al Teatro 1/3
20123 – Milano
(Piazza Affari)
Ph. +39 02 21117645
Fax +39 02 87182231
e.mail: gfbonacci@elrlex.it