- GRUPPO ZELARI -

DOCUMENTO DI SINTESI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI: LINEE GUIDA E *BEST PRACTICES*

Il quadro normativo di riferimento

- In data 25 maggio 2018 è entrato in vigore il nuovo Regolamento dell'UE, n. 679/2016, in materia di protezione dei dati personali, c.d. **GDPR, General Data Protection Regulation**;
- In data 19 settembre è entrato in vigore il **D.lgs. n. 101/2018**, di raccordo della normativa italiana con il GDPR;
- È rimasto in vigore il **D.lgs. 196/2003**, c.d. Codice della privacy, con le necessarie modifiche apportate dal D.lgs. 101/2018.

Le linee guida

- Ogni realtà professionale o aziendale deve adeguarsi alle nuove previsioni nel settore privacy e riservatezza dei dati personali;
- Il GDPR, in particolare, promuove la **responsabilizzazione** dei titolari del trattamento e l'adozione di politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati;
- Centrale il concetto di **analisi dei rischi**, con conseguente adeguamento delle misure di sicurezza da adottare, e monitoraggio costante di tale livello di adeguatezza;
- La tutela dei dati personali deve ora avvenire per impostazione predefinita dell'organizzazione aziendale: c.d. "**privacy by default**", e l'obiettivo è quello di prevenire i potenziali danni che potrebbero derivare dai trattamenti effettuati, anziché correggerli a posteriori, quindi di valutare i possibili problemi già in fase di progettazione ("**privacy by design**"). La privacy viene così incorporata nei processi e nei progetti aziendali, garantendo la sicurezza del trattamento durante tutto il ciclo del prodotto o servizio.

Individuazione degli adeguamenti minimi necessari nella realtà Gruppo Zelari

Tanto premesso, le azioni da intraprendere sono le seguenti:

1) La redazione e l'utilizzo delle nuove informative, da sottoporre ai clienti e ai fornitori, pubblicate anche sul **sito web**, conformi ai contenuti minimi previsti dal GDPR.

Fondamentale, inoltre, nell'informativa, la corretta indicazione dei **diritti che competono all'interessato** (accesso, rettifica, oblio, cancellazione, limitazione, opposizione), che questi potrà esercitare attraverso comunicazione scritta alla società di riferimento e/o segnalazione all'Ufficio Legale del Gruppo.

Il consenso al trattamento dei dati personali deve essere sempre richiesto all'interessato al quale si intendono indirizzare comunicazioni aventi carattere commerciale e/o promozionale, prima dell'invio di tali comunicazioni. Per ***consenso*** deve intendersi la manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento, attraverso apposita informativa per il trattamento dei dati personali per finalità di marketing.

2) La redazione e l'utilizzo di informative destinate ai dipendenti del gruppo.

3) La corretta individuazione e nomina dei soggetti del trattamento dei dati personali.

Posto che il **Titolare del trattamento** è necessariamente ciascuna delle società del gruppo stesso, è opportuno individuare uno o più **Responsabili del trattamento**, intesi come soggetti che trattano dati per conto del Titolare del trattamento. Per raggiungere tale finalità possono essere utilizzati idonei contratti di nomina a Responsabile del trattamento ai sensi dell'art. 28 GDPR, che possono essere personalizzati da ciascuna realtà in ordine a: oggetto e durata del trattamento; doveri e compiti del responsabile del trattamento; ambito di rischi; natura e finalità del trattamento; modalità di svolgimento delle attività di trattamento; tipo di dati personali trattati; categorie di persone fisiche coinvolte; obblighi e diritti del titolare del trattamento.

Allo stesso modo, è opportuna la designazione, sempre da parte del Titolare, di **Incaricati del trattamento** (o "**Autorizzati**", ai sensi del GDPR), ossia soggetti che svolgano qualunque tipo di trattamento di dati personali, anche di carattere materiale, esecutivo. Si consiglia di designare come tali tutti i dipendenti degli uffici che vengano a contatto coi dati personali trattati dall'ufficio stesso. In particolare, agli incaricati dovranno essere fornite idonee **istruzioni** da osservare nell'esecuzione delle operazioni di trattamento, contenuta nella cd. "lettera di incarico".

Da segnalare inoltre che il contratto (scritto) di **Contitolarità del trattamento (accordo di Contitolarità)**, deve essere firmato e conservato da ciascuna società del Gruppo.

La presenza di Contitolari del trattamento è indicata nelle informative.

Si fa presente, fin da ora, che l'individuazione e la nomina dei soggetti deputati a trattare dati personali, all'interno dell'organizzazione aziendale, e la relativa ripartizione di competenza, rappresenta un'importante **misura di sicurezza di tipo organizzativo**, in grado, insieme ad altri elementi, di garantire la *compliance* alla nuova normativa.

4) La nomina dei Responsabili esterni del trattamento.

I Responsabili del trattamento possono essere soggetti **esterni all'organizzazione aziendale**, a cui il Titolare affida taluni trattamenti (es. trattamenti di dati dei propri dipendenti o clienti).

Questa situazione ben può verificarsi all'interno del gruppo: ad es. se una società interna al gruppo si avvale, per la redazione dei contratti di lavoro e/o la predisposizione delle buste paga di un Consulente del lavoro. Lo stesso nell'ipotesi in cui ci si avvalga di collaboratori esterni, quali ad es. commercialisti per la preparazione di fatture. Negli atti di nomina a Responsabili del trattamento sono individuati alcuni soggetti che possono essere nominati da ciascuna realtà: tali nomine possono essere inviate ai soggetti individuati via email o PEC, con richiesta di reinvio firmate, dopodiché devono essere conservate.

5) La tenuta ed aggiornamento di appositi Registri dei trattamenti.

E' necessaria l'adozione, *ex* art. 30 GDPR, da parte di ciascuna Società, di un Registro dei trattamenti, una sorta di "**giornale di bordo**" riepilogativo dei trattamenti effettuati, contenente una serie di informazioni (quali ad es. il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del DPO, una descrizione delle categorie di interessati e delle categorie di dati personali trattati, le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi extra UE, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate). I Registri dovranno essere **aggiornati periodicamente**.

6) La nomina di un DPO.

La nomina di un Data Protection Officer è obbligatoria non solo per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, ma anche per i **soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche**.

Come precisato dall'Autorità Garante della Privacy, è comunque possibile, ed anzi utile e consigliabile, la designazione su base volontaria. Vista la complessità dei trattamenti effettuati dal Gruppo Zelari, e l'ingente quantitativo di dati trattati, si raccomanda la nomina di un DPO.

Le *best practices*

In termini di *best practices*, buone pratiche da osservare all'interno degli uffici, si suggerisce l'adozione delle seguenti condotte, in relazione agli aspetti problematici rilevati.

a) Un primo aspetto problematico riguarda, all'interno degli uffici, le modalità di **conservazione dei dati in cartaceo**: in proposito, si suggerisce un ricorso costante alle chiusure di armadi e cassetti in cui riporre i documenti, nonché delle porte delle stanze adibite ad archivi.

Si raccomanda inoltre di non lasciare documenti recanti dati personali, anche meramente anagrafici, in giro per scrivanie, soprattutto quando ci si rapporta con clienti e fornitori.
Si consiglia poi di non lasciare **mai incustodite le proprie postazioni di lavoro**, e di non lasciare mai aperte e potenzialmente accessibili a chiunque le zone di lavoro durante le pause pranzo.
b) Ancora, sempre con riguardo alle modalità cartacee di trattamento dei dati personali, si è riscontrato il **mancato controllo sui periodi di conservazione dei dati trattati**, che, talvolta, finiscono a giacere dimenticati in archivi. È invece fondamentale limitare la conservazione al periodo strettamente necessario (tendenzialmente coincidente con il termine prescrizionale decennale), e poi procedere allo smaltimento dei documenti contenenti dati il cui trattamento non è più necessario. Un trattamento prolungato oltre il necessario potrebbe configurarsi come illecito, con le relative conseguenze anche sul versante sanzionatorio.
c) In generale, è necessaria da parte di tutti i dirigenti/dipendenti/collaboratori la presa d'atto dell'**importanza dell'adozione di misure fisiche di sicurezza, anche minimali** - quali ad es. non lasciare fogli con scritte su le password in giro, voltare i fascicoli quando ci si relaziona con un cliente, allontanarsi dai colleghi quando si fanno telefonate di particolare delicatezza, limitare al minimo la divulgazione di dati personali anche all'interno dello stesso ufficio – finalizzate a realizzare trattamenti di dati personali pienamente legittimi e conformi alle nuove normative.

Focus **sul versante informatico**

Dal punto di vista informatico, si riepilogano in generale i comportamenti da tenere:
-**Analisi periodica dello stato della strumentazione informatica**, sia nella sede centrale del Gruppo che negli Uffici periferici. Il gruppo deve essere infatti in grado di garantire, secondo il GDPR, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi informatici su base permanente, nonché la capacità di ripristinare tempestivamente l'accesso dei dati personali in caso di incidenti fisici o tecnici;
-**Controllo degli accessi**, in particolare ogni utente deve avere proprie credenziali di accesso sia agli strumenti informatici (all'avvio del sistema e in *stand-by*) che ai programmi utilizzati, con password che rispettino gli standard di sicurezza (8 o più caratteri alfanumerici), da reimpostare almeno ogni 90 giorni. E' consigliato l'affidamento della custodia delle credenziali di accesso a una persona specificamente individuata per ciascuna area, che garantisca un livello di sicurezza elevato nella custodia stessa. Ogni area di lavoro deve poter accedere alle cartelle di file, contenenti dati personali facenti capo alla stessa, che siano di sua competenza e pertinentemente all'attività svolta. Si auspica un controllo delle attuali *permissions* sulle cartelle, limitando la

condivisione a quanto strettamente necessario alle finalità di organizzazione del lavoro. Ove talune cartelle di file contengano categorie particolari di dati (come documenti scansionati recanti riferimenti a informazioni sensibili degli interessati quali stato di salute, appartenenza sindacale, ovvero dati giudiziari, il cui trattamento, si ricorda, è vietato tranne qualora vi sia la presenza di un consenso esplicito), si consiglia, quale misura di sicurezza informatica, l'adozione di tecniche di cifratura;

-**Adottare Antivirus e Antimalware su licenza** su ogni computer utilizzato, con un efficace sistema di filtraggio della navigazione in Internet e della posta elettronica, onde evitare possibili rischi;

-**Impostare un Firewall**;

-**Implementare un efficace sistema di backup dei dati personali**;

-**Assicurare una conservazione** dei dati personali limitata al minimo necessario e stabilire **un termine per la cancellazione** e la verifica periodica, attraverso politiche uniformi per tutto il personale che rispettino quanto stabilito dalle leggi vigenti;

-**Impostare termini di conservazione delle immagini raccolte attraverso l'utilizzo del sistema di videosorveglianza** che non superino le 24-48 ore, ed assicurarsi che l'accesso alle immagini avvenga esclusivamente da parte di personale autorizzato e dietro effettiva e comprovata necessità;

-**Prestare estrema attenzione alle fonti di provenienza dei dati personali ed alle finalità dei trattamenti**. In particolare, per quanto concerne il trattamento dei dati contenuti in carte di identità, eccetto per quanto concerne i documenti di riconoscimento dei dipendenti del Gruppo trattati dall'Ufficio Personale, si fa presente che la normativa vigente autorizza a richiedere legittimamente tale documento esclusivamente determinati soggetti (Pubblica Amministrazione; gestori di utenze pubbliche; soggetti che erogano schede SIM). Il Garante Privacy, con proprio provvedimento, ha chiarito che l'identificazione di una persona, da parte di altri soggetti al di fuori di quelli citati, può essere necessaria per eseguire obblighi derivanti dal contratto e che quindi la richiesta di esibizione del documento di identità sarebbe legittima, ma non altrettanto la richiesta di copia e di conservazione del documento di identità. E', quindi, nel legittimo interesse della Società richiedere l'esibizione del documento per comprovare l'identità di una persona ma l'interessato può altrettanto legittimamente rifiutare l'esibizione in quanto non è un obbligo previsto dalla legge nei confronti della Società. E' possibile quindi richiedere l'esibizione della carta d'identità, o di una copia (nel caso del soggetto delegato da un legale rappresentante) ma è sconsigliabile che venga pretesa una copia della stessa, per un rischio di violazione dei principi di

proporzionalità, pertinenza e non eccedenza nel trattamento dei dati personali, al di fuori naturalmente dei casi in cui la legge lo consenta espressamente.

-**Utilizzo di strumenti informatici portatili (PC e/o Smartphone) ad uso "promiscuo".** Nei casi in cui dipendenti e/o soci utilizzino, per lo svolgimento di attività inerenti le rispettive Società, strumenti personali (uso cd. "promiscuo"), l'analisi dei rischi informatici coinvolge anche tale strumento. Ne consegue che debba essere effettuata una valutazione sulle misure di sicurezza informatiche e sull'adeguatezza delle stesse e che, ove si verifichi un qualunque evento accidentale e/o illecito che coinvolga tale strumento debba essere effettuata la notifica all'Autorità Garante per la protezione dei dati personali (*infra*).

Notifica della violazione all'Autorità Garante Privacy e comunicazione all'interessato in caso di gravi rischi per i suoi diritti

Nel caso in cui si verifichi un qualunque evento accidentale (es. perdita di dati) o illecito (es. furto di documenti o di strumenti informatici) che coinvolga dati personali trattati, vige l'obbligo di messa in atto della procedura di notifica della violazione all'Autorità Garante Privacy. Ogni dipendente che venga a conoscenza di un evento di tale tipo, deve senza ritardo informare il responsabile dell'Ufficio al quale appartiene e l'Ufficio Legale del Gruppo e, nel caso, eseguire dietro autorizzazione del legale rappresentante, entro 72 ore dalla conoscenza della violazione, la notifica.