BREVE GUIDA SUL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (REGOLAMENTO UE 2016/679)

Il Regolamento UE 679/2016 (in seguito anche GDPR) è divenuto pienamente applicabile dal 25 maggio 2018.

Un Regolamento Europeo è un atto vincolante che gode di diretta applicabilità; ciò vale a dire che entra simultaneamente in vigore in tutti gli Stati membri, senza atti nazionali di recepimento.

Il quadro giuridico nazionale, tuttavia, si è voluto adeguare alle regole comunitarie, con la conseguente modifica e integrazione del vigente codice della protezione dei dati personali di cui al DLgs. 30.6.2003 n. 196 (codice della *privacy*). La modifica del D. lgs. 196/2003 è avvenuta con il D. Lgs. 10 agosto 2018 n. 101 "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*".

Le novità apportate sono rilevanti:

ACCOUNTABILITY: In virtù del principio di accountability, il Regolamento dispone che il titolare del trattamento adotta politiche e attua misure adeguate che gli consentano di garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme allo stesso Regolamento.

In particolare il GDPR recepisce tale principio all'**art. 24** il quale prevede che tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. Inoltre, se ciò è proporzionato rispetto alle attività di trattamento, le predette misure includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

VALUTAZIONE D'IMPATTO E ACCOUNTABILITY DI TITOLARE E RESPONSABILI DEL TRATTAMENTO

Il regolamento pone l'accento sul principio di responsabilizzazione (accountability) di titolari e responsabili, in base ai criteri di privacy by default e by design, in base alla necessità di prevedere fin dall'inizio i requisiti necessari per rispettare il regolamento e tutelare i diritti degli interessati. In questo senso, il responsabile dovrà svolgere valutazioni d'impatto sui rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di adottare per mitigare i rischi.

PRIVACY BY DESIGN E PRIVACY BY DEFAULT: La privacy by design impone al titolare di adottare e attuare misure tecniche e organizzative sin dal momento della progettazione (oltre che nell'esecuzione) del trattamento; tali misure devono essere informate alla tutela dei principi di protezione dei dati.

La privacy by default prevede che le impostazioni di tutela della vita privata relative ai servizi e ai prodotti, rispettino i principi generali della protezione dei dati, quali la **minimizzazione** dei dati e la limitazione delle finalità.

La privacy by default richiede che in un corretto approccio di progettazione di sistemi informatici che possa risultare funzionale alla tutela della privacy, determinate informazioni debbano essere protette in modo rafforzato. Dall'altra parte, comporta l'utilizzo di determinate impostazioni in automatico di maggiore tutela per l'utente e che son scelte da chi costruisce il sistema informatico con la possibilità di cambiamento da parte dell'utente dell'opzione prescelta.

RESPONSABILE DELLA PROTEZIONE DATI (RPD)

Tale figura deve essere tempestivamente ed adeguatamente coinvolta, dal titolare e dai responsabili del trattamento, in tutte le questioni riguardanti la protezione dei dati personali. Al Responsabile Protezione Dati devono essere fornite le risorse necessarie per lo svolgimento dei compiti menzionati nell'art. 39 del Regolamento UE (informare e fornire consulenza al titolare e ai

responsabili del trattamento; sorvegliare l'osservanza del Regolamento UE e della ulteriore normativa in tema di protezione dei dati nonché le politiche del titolare del trattamento su tale tematica, anche in ordine alla formazione e sensibilizzazione del personale; fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento; cooperare con l'autorità di controllo; fungere da punto di contatto con l'autorità garante).
Il titolare e il responsabile del trattamento sono tenuti ad assicurarsi che il RPD non riceva alcun istruzione per l'esecuzione dei compiti sopra menzionati. Il RPD, inoltre, non può essere rimosso o penalizzato per l'adempimento dei propri compiti.

INFORMATIVA: I contenuti dell'informativa sono più ampi rispetto al Codice Privacy. Il titolare deve sempre specificare, oltre ai propri, i dati di contatto del RPD-DPO (Responsabile della Protezione Dati – Data Protection Officer) ove esistente; le finalità e la base giuridica del trattamento; se trasferisce i dati in Paesi terzi e, se lo fa, con quali strumenti. Il titolare deve specificare il periodo di conservazione dei dati (o almeno i criteri utilizzati per determinarlo); il diritto di presentare reclamo all'autorità di controllo. L'informativa deve specificare se il trattamento prevede processi decisionali automatizzati (compresa la profilazione), indicando la logica dei processi automatizzati e le conseguenze previste per l'interessato.
In linea di principio, l'informativa deve essere data per iscritto e preferibilmente in formato elettronico.

DIRITTI DELL'INTERESSATO: L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in questo caso, di ottenere l'accesso ai dati personali e alle informazioni concernenti le finalità del trattamento, le categorie dei dati personali trattati, i destinatari o categorie di destinatari a cui i dati sono stati o saranno comunicati, ove possibile il periodo di conservazione dei dati o almeno i criteri utilizzati per determinarlo, l'esistenza della possibilità di chiedere al titolare del trattamento la rettifica, la cancellazione o la limitazione del trattamento dei dati personali e la possibilità, in talune circostanze, di opporsi allo stesso, il diritto di proporre reclamo all'autorità garante.

DIRITTO ALLA PORTABILITA' DEI DATI Si tratta di un nuovo diritto previsto dal regolamento, che per certi versi richiama la number portability nell'ambito delle Telecomunicazioni. Sono portabili soltanto i dati automatizzati (la data portability non si applica agli archivi o registri cartacei) e trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato e forniti dall'interessato al titolare (ad esempio in ambito bancario). Il titolare deve essere in grado di trasmettere i dati ad un altro titolare, se tecnicamente possibile, per questo dovrà mettersi nelle condizioni di poter produrre i dati in formato interoperabile.

DATA BREACH (importante):

Per data breach (violazione dei dati personali) si intende la violazione di sicurezza che comporta **accidentalmente o in modo illecito** la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Il data breach non si concretizza solo a seguito di un accesso abusivo a sistemi informatici, ma anche in casi che sono, purtroppo, molto più frequenti: furto o smarrimento di device (Pc portatili, tablet, smartphone, chiavette USB sulle quali sono memorizzati dati) o di documenti cartacei, perdita o sottrazione di credenziali di accesso a device, perdita/smarrimento/furto di credenziali di accesso ad applicazioni centrali (Titulus, Esse3, posta elettronica UNICAM).
Il Responsabile Protezione Dati, Dott. Maurizio Sabbieti, sta mettendo a punto, assieme al proprio gruppo di supporto, una procedura che consenta a chi incorre in qualcuna delle sopra indicate situazioni (che mettono a rischio i dati personali del soggetto stesso e di altri interessati) di comunicare al titolare e al RPD stesso il potenziale data breach, affinché possano essere messi in atto gli step successivi (valutazione del data breach, individuazione delle misure correttive, eventuale segnalazione al Garante e agli interessati, a seconda se emergano o meno significativi rischi per le libertà e i diritti degli individui).

La notifica di eventuali violazioni di dati dovrà avvenire possibilmente senza ingiustificato ritardo e, ove possibile, **entro 72 ore**, dal momento in cui si è venuti a conoscenza della violazione, a meno

che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. L'eventuale ritardo dovrà essere motivato.