studio legale
tributario associato

corso magenta, 56
20123 milano

tel. +39 02 4801 3990
fax +39 02 4819 5206

mbc
masotti berger cassella

A: Clienti Studio

Da: Masotti Berger Cassella

Data: 9 maggio 2018

Oggetto: **Gli adempimenti privacy e il nuovo Regolamento UE 2016/679**

1 Introduzione

Il presente *memorandum* si prefigge l'obiettivo di individuare le principali novità introdotte dal Regolamento UE 2016/679, **obbligatorio per gli Stati Membri entro e non oltre il 25 maggio 2018**, e le differenze rispetto alla normativa oggi vigente in Italia in materia di Privacy e di Protezione dei dati personali (D. Lgs. 196/2003, c.d. Codice per la protezione dei dati personali).

Lo scopo del lavoro è, infatti, quello in evidenziare gli ambiti ed i profili in cui il Regolamento UE è destinato ad avere un maggior "impatto" e le principali novità per le imprese e per gli enti.

Pertanto, in relazione a ciascun "profilo di indagine", si eporranno sinteticamente gli aspetti più rilevanti ai sensi dell'attuale normativa (il "**Codice**") e, contestualmente, le novità imposte dal nuovo Regolamento UE 2016/679 (il "**Regolamento UE**").

L'ordine degli argomenti selezionati è il seguente:

1.1.1 Il trattamento dei dati

1.1.2 I soggetti del trattamento

1.1.3 Le principali regole per un corretto trasferimento dei dati

1.1.4 Comunicazione e trasferimento dei dati all'estero

1.1.5 Il nuova logica della protezione dei dati personali

1.1.6 Le sanzioni

2 Il trattamento dei dati

Per trattamento si intende qualsiasi **operazione** o complesso di operazioni (con o senza l'ausilio di strumenti elettronici) che hanno per oggetto **dati**.

2.1.1 Le operazioni che hanno per oggetto dati personali sono: raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione, distruzione.

2.1.2 I dati che possono oggetto di trattamento sono: dati personali, dati identificativi, dati sensibili, dati giudiziari e dati anonimi.

Cosa cambia con il Regolamento UE?

2.1.3 Il Regolamento UE contiene qualche novità in merito al:

(i) **diritto di cancellazione (o oblio)**: nel Regolamento UE ha un campo di applicazione più ampio rispetto a quello previsto nel Codice. Ad esempio, l'interessato ha il diritto di chiedere la cancellazione dei propri dati anche dopo revoca del consenso al trattamento.

(ii) **diritto di limitazione del trattamento**: nel Regolamento UE tale diritto ha un ambito di applicazione più ampio rispetto a quello previsto nel Codice. Infatti tale diritto è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), ma anche in caso di rettifica dei dati (in attesa di tale rettifica da parte del titolare) o di opposizione al loro trattamento (in attesa della valutazione da parte del titolare).

(iii) **diritto alla portabilità dei dati**: è un nuovo diritto, previsto per la prima volta dal Regolamento UE. In particolare:

(a) è il diritto che consente all'interessato **di ricevere i dati personali forniti a un titolare** (in un formato strutturato, di uso comune e leggibile da dispositivo automatico) e **di trasmetterli (eventualmente) ad un altro titolare del trattamento** senza impedimenti da parte del titolare che li ha forniti,

(b) si applica soltanto per i dati personali riferibili all'interessato (quindi con esclusione dei dati anonimi),

(c) il titolare deve prevedere un'informativa sul diritto alla portabilità dei dati,

(d) facilita il passaggio da un fornitore di servizi all'altro,

(e) consente di ricevere i dati su un sopporto personale o un *cloud* privato in vista di un utilizzo ulteriore per scopi personali senza necessariamente trasmetterli ad un altro titolare,

(f) offre la possibilità di “riequilibrare” il rapporto tra interessati e titolari del trattamento perchè di fatto consente ai primi un controllo sui dati personali che li riguardano,

(g) l’esercizio di tale diritto non pregiudica nessuno degli altri diritti dell’interessato che può, ad esempio, continuare a fruire del servizio del primo titolare (anche dopo un’operazione di portabilità) oppure esercitare il diritto di cancellazione (o diritto all’oblio).

2.1.4 Rispetto al Codice, il Regolamento prevede delle **novità per l’esercizio dei diritti** da parte dell’interessato.

(i) Il titolare del trattamento ha un **termine** per rispondere all’interessato: 1 mese dal ricevimento della richiesta. Tale termine può essere prorogato di due mesi, se necessario, in casi di particolare complessità. Il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

(ii) Il titolare può stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato soltanto se si tratta di richieste manifestamente infondate o eccessive (in particolare per il loro carattere ripetitivo).

(iii) Il titolare deve dare riscontro all’interessato in forma scritta o con altri mezzi, anche elettronici. Il riscontro può essere dato oralmente solo se richiesto espressamente dall'interessato stesso (purchè sia comprovata con altri mezzi l’identità dell’interessato).

(iv) La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, e deve essere espressa con un linguaggio semplice e chiaro.

3 I soggetti del trattamento

Il Codice distingue tra **soggetti attivi** e **soggetti passivi** del trattamento dei dati.

I **soggetti attivi** sono quelli che eseguono il trattamento dei dati.

3.1.1 Il **titolare del trattamento** è il soggetto a cui competono le decisioni in ordine a:

(i) finalità del trattamento dei dati,

(ii) modalità del trattamento dei dati,

(iii) strumenti per il trattamento dei dati, compreso il profilo della sicurezza.

Il titolare può essere:

(a) persona fisica,

(b) persona giuridica,

(c) pubblica amministrazione,

(d) qualsiasi altro ente, associazione o organismo.

Nelle ipotesi di cui alle lettere (b), (c) e (d), il titolare è l'entità nel suo complesso oppure l'unità o l'organismo periferico che esercita un potere decisionale del tutto autonomo in relazione alle decisioni da prendere in merito al trattamento dei dati.

In sintesi. Il titolare è il soggetto che deve adempiere agli obblighi previsti dal Codice e che deve rispondere delle eventuali sanzioni in caso di inadempimento.

Pertanto, l'elemento che consente di individuare tale figura è il potere decisionale di cui dispone.

3.1.2 Il **responsabile del trattamento** è il soggetto a cui compete assicurare il costante e puntuale rispetto della disposizioni del Codice.

Il responsabile:

(i) è una figura "facoltativa" (e quindi non c'è alcun obbligo di designazione),

(ii) è nominato dal titolare del trattamento,

(iii) deve ricevere i compiti "analiticamente specificati per iscritto",

(iv) deve attenersi ai compiti e alle istruzioni impartiti dal titolare,

(v) è soggetto a verifiche periodiche da parte del titolare,

(vi) può essere solo uno oppure possono essere nominati più di uno (con eventuale suddivisione dei compiti).

Il responsabile può essere:

(a) persona fisica,

(b) persona giuridica,

(c) pubblica amministrazione,

(d) qualsiasi altro ente, associazione o organismo.

In sintesi. Il titolare **può** avvalersi della facoltà di delegare i propri compiti in materia di privacy ad un diverso soggetto denominato responsabile.

Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare, il quale vigila sulla puntuale osservanza delle disposizioni.

3.1.3 L'**incaricato del trattamento** è il soggetto autorizzato a compiere operazioni di trattamento dei dati.

L'incaricato:

(i) è una figura obbligatoria (quindi, la sua nomina è obbligatoria),

(ii) è designato dal titolare e/o dal responsabile (se designato),

(iii) è designato per iscritto,

(iv) è autorizzato al trattamento dei dati nel solo ambito puntualmente individuato nella designazione (cioè natura dei dati ai quali accede e tipologia del trattamento consentita),

(v) opera sotto la diretta autorità del titolare o del responsabile,

(vi) si attiene rigorosamente alle istruzioni impartite,

(vii) possono essere più di uno.

L'incaricato può essere soltanto:

(a) una persona fisica.

In sintesi. Gli incaricati (solitamente sono più di uno) sono gli esecutori materiali del trattamento dei dati. La loro nomina, da parte del titolare e/o del responsabile (se designato), è obbligatoria.

3.1.4 L'**amministratore di sistema** è la figura professionale dedicata all gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati i trattamenti dei dati, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di dicurezza, nella misura in cui consentano di intervenire sui dati personali.

I **soggetti passivi** sono quelli a cui si riferiscono i dati oggetto del trattamento (c.d. "interessati").

Cosa cambia con il Regolamento UE?

3.1.5 Il Regolamento UE non prevede espressamente la figura dell'incaricato del trattamento ma non ne esclude nemmeno la presenza. Il Regolamento UE parla, infatti, più genericamente di "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile".

3.1.6 In aggiunta al titolare, al responsabile a gli incaricati, il Regolamento UE prevede una nuova figura: **il Data Protection Officer (il "DPO").**

Il DPO ha il compito di:

(i) informare e consigliare il titolare o il responsabile, se designato, nonchè i dipendenti in merito agli obblighi derivanti dal Regolamento e da altre disposizioni dell'Unione o degli Stati Membri relative alla protezione dei dati,

(ii) verificare l'attuazione e l'applicazione del Regolamento e delle altre disposizioni dell'Unione o degli Stati Membri relative alla protezione dei dati,

(iii) fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti,

(iv) fungere da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei dati o all'esercizio dei loro diritti,

(v) fungere da punto di contatto per il Garante e consultare il Garante di propria iniziativa.

Il DPO deve essere designato **sistematicamente:**

(i) quando il trattamento è effettuato da un'autorità pubblica o un organismo pubblico (fatta eccezione per le autorità giudiziarie),

(ii) quando le attività principali del titolare del trattamento o del responsabile consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati **su larga scala**,

(iii) quando le attività principali del titolare o del responsabile consistono nel trattamento, **su larga scala**, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Il DPO:

(a) può essere designato anche su base volontaria,

(b) viene designato dal titolare e dal responsabile, i quali dovranno mettere a disposizione del DPO le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti,

(c) deve possedere un'adeguata conoscenza delle normativa e delle prassi nazionali ed europee di gestione dei dati personali,

(d) deve agire in piena indipendenza ed in assenza di conflitti di interesse,

(e) deve operare alle dipendenze del titolare oppure sulla base di un contratto di servizio.

In sintesi. Il DPO è una nuova figura che si va ad aggiungere a quelle già esistenti.

Il DPO deve essere indipendente e deve agire in assenza di conflitti di interesse.

Il DPO può sempre designato facoltativamente ma deve essere necessariamente designato nelle ipotesi specificatamente individuate nel Regolamento. In particolare, quando il trattamento dei dati avviene su larga scala.

In mancanza di una definizione, il Garante ha definito 4 principali fattori da tenere in considerazione per considerare un trattamento su larga scala:

- il numero di soggetti al trattamento dei dati,
- il volume dei dati e/o i vari dati trattati,
- la durata del trattamento,
- l'estensione geografica del trattamento.

Esempi di trattamenti su larga scala:

- trattamento dati da parte di struttura sanitaria,
- trattamento dati da parte di assicurazioni,
- trattamento dati da parte di banche,
- trattamento dati da parte di motori di ricerca a fini pubblicitari.

3.1.7 Il Regolamento UE disciplina il fenomeno della **contitolarità del trattamento.** I titolari operanti congiuntamente (due o piu) devono definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti con particolare riguardo all'esercizio dei diritti degli interessati. Gli interessati possono accedere al contenuto dell'accordo e possono rivolgersi indifferentemente a uno qualsiasi dei titolari.

3.1.8 Il Regolamento UE fissa più dettagliatamente, rispetto al Codice, le **caratteristiche dell'atto con cui il titolare designa il responsabile del trattamento**. In particolare:

(i) deve trattarsi, infatti, di un contratto (o altro atto giuridico conforme al diritto nazionale),

(ii) deve avere il contenuto tassativamente indicato all'art. 28, terzo comma, del Regolamento UE. In particolare, deve indicare la natura, durata e finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in generale, delle disposizioni contenute nel Regolamento.

3.1.9 Il Regolamento UE prevede che il responsabile, per specifiche attività di trattamento, possa nominare un **sub-responsabile**. In particolare:

(i) l'atto con, cui il responsabile designa il sub-responsabile deve essere un contratto (o un atto giuridico conforme al diritto nazionale),

(ii) gli obblighi contrattuali tra responsabile e sub-responsabile sono i medesimi che legano il titolare ed il responsabile,

(iii) il responsabile del trattamento è responsabile nei confronti del titolare del trattamento dell'inadempimento del sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile.

3.1.10 Il Regolamento UE prevede **obblighi specifici in capo al responsabile del trattamento** e tali obblighi sono distinti ed ulteriori rispetto a quelli gravanti in capo al titolare. Ad esempio, il responsabile ha l'obbligo:

(i) di tenere un registro dei trattamenti svolti,

(ii) di adottare idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti,

(iii) di nominare un DPO (nei casi in cui la designazione sia obbligatoria),

(iv) di designare un rappresentante del trattamento in Italia se in Italia si trovano gli interessati, i cui dati personali sono trattati nell'ambito dell'offerta di beni o servizi o il cui comportamento è monitorato.

4 Le principali regole per un corretto trattamento dei dati

4.1.1 Sintenticamente, il Codice prevede:

(i) l'essenzialità dei dati trattati (cioè che siano trattati i soli dati essenziali per le finalità per le quali è previsto il trattamento),

(ii) l'esattezza, la pertinenza, la non eccedenza e la necessità dei dati rispetto alle finalità perseguite con il loro trattamento,

(iii) che il trattamento dei dati avvenga solo da parte degli incaricati nei limiti delle istruzioni loro impartite,

(iv) che il titolare fornisca l'informativa all'interessato,

(v) che l'interessato presti il suo consenso,

(vi) che in limitati casi, specificatamente individuati, il consenso dell'interessato non è necessario (ad es. obbligo previsto per legge o regolamento, dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque ecc),

(vii) che, in caso di dati sensibili, il consenso deve essere manifestato in forma scritta e previa autorizzazione del Garante. I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante:

(I) quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, per il perseguimento di scopi determinati e legittimi, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo,

(II) quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo,

(III) quando il trattamento è necessario per lo svolgimento delle investigazioni difensive o comunque per far valere o difendere in sede giudiziari un diritto,

(IV) quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge (ad esempio, per la gestione del rapporto di lavoro, anche in amteria di igiene e sicurezza del lavoro),

(viii) che, ottenuto il consenso e prima di dare inizio al trattamento, il titolare deve notificare al Garante l'esistenza di un'attività di raccolta e di utilizzazione dei dati personali. Tutte le notificazioni sono conservate in un "registro dei trattamenti" accessibile al pubblico gratuitamente per via telematica,

(ix) che il consenso sia richiesto solo quando non sia possibile avvalersi di uno dei presupposti equipollenti al consenso,

(x) che siano rispettate le prescrizioni contenute nelle autorizzazioni rilasciate dal Garante, se si trattano dati sensibili o giudiziari,

(xi) che siano adottate le misure di sicurezza idonee a prevenire alcuni eventi.

4.1.2 Prima del 2012, il Codice imponeva l'adozione di un documento che raccogliesse e riassumesse tutte le procedure e le misure di sicurezza adottate dal titolare del trattamento: il c.d. Documento Programmatico di Sicurezza ("DPS").

A partire dal 2012 è venuto meno l'obbligo legale di redigere il DPS ma rimane l'opportunità della sua adozione al fine di una più agevole dimostrazione degli adempimenti effettuati.

Cosa cambia con il Regolamento UE?

4.1.3 Ai sensi del Regolamento UE l'**informativa** ha un **contenuto** più ampio rispetto a quello previsto dal Codice. In particolare, l'informativa deve necessariamente indicare:

(i) i dati di contatto del DPO, se esistente,

(ii) la base giuridica del trattamento,

(iii) il periodo di conservazione dei dati oppure i criteri seguiti per stabilire tale periodo di conservazione,

(iv) il diritto di proporre reclamo all'autorità di controllo,

(v) l'esistenza di un processo decisionale automatizzato, la logica di tale processo decisionale e le conseguenze previste per l'interessato.

4.1.4 Il Regolamento UE prevede un **termine** per fornire l'**informativa** nel caso di dati non raccolti direttamente presso l'interessato: 1 mese (dalla raccolta dei dati) oppure al momento della prima comunicazione dei dati all'interessato o ai terzi (e non dalla registrazione, come prevede ora il Codice).

4.1.5 Il Regolamento UE prevede requisiti parzialmente diversi per **l'esonero dall'informativa** rispetto a quanto previsto dal Codice. Ad esempio, l'informativa non è dovuta se l'interessato dispone già delle informazioni, oppure se, secondo la valutazione del titolare, l'informativa risulti impossibile o implichi uno sforzo sproporzionato (in caso di dati non ottenuti presso l'interessato).

4.1.6 Ai sensi del Regolamento UE, il **consenso** deve essere necessariamente **esplicito** in caso di:

(i) trattamenti di dati sensibili,

(ii) trattamenti automatizzati dei dati.

4.1.7 A differenza del Codice, ai sensi del Regolamento UE, il consenso non deve essere necessariamente documentato per iscritto, né è richiesta la forma scritta. Semplicemente la forma scritta è la modalità più idonea a garantire un consenso esplicito.

5 Comunicazione e trasferimento di dati all'estero

5.1.1 Il trasferimento di dati **da Paesi UE a Paesi UE** è consentito, senza eccezioni.

5.1.2 In linea di principio, il trasferimento di **da Paesi UE a Paesi extra UE** è vietato, a meno che il Paese ricevente non garantisca un livello di protezione adeguato.

In una **serie tassativa di casi** è consentito il trasferimento anche verso Paesi extra UE quando:

(i) l'interessato ha manifestato il proprio consenso espresso (in forma scritta, in caso di dati sensibili),

(ii) il trasferimento è necessario per:

(a) dare esecuzioni ad obblighi contrattuali,

(b) la salvaguardia di un interesse pubblico, della vita o dell'incolumità fisica di un terzo,

(c) le esigenze difensive in sede giudiziaria,

(d) finalità storiche, scientifiche o statistiche.

Cosa cambia con il Regolamento UE?

5.1.3 Con il Regolamento UE viene meno il requisito dell'autorizzazione nazionale del Garante. Tuttavia, l'autorizzazione del Garante sarà ancora necessaria:

(i) se il titolare utilizza clausole contrattuali non riconosciute come adeguate tramite decisione della Commissione Europea,

(ii) in caso di accordi amministrativi tra autorità pubbliche.

5.1.4 Al fine di legittimare trasferimento dei dati verso Paesi terzi, il Regolamento UE consente di ricorrere anche a codici di condotta ovvero a schemi di certificazione (laddove disciplinino anche o esclusivamente i trasferimenti di dati verso Paesi terzi).

5.1.5 Il Regolamento UE vieta trasferimenti di dati verso titolari o responsabili in un Paese terzo sulla base di decisioni giudiziarie o ordinanze amministrative emesse da autorità di tale Paese terzo, a meno dell'esistenza di accordi internazionali tra gli Stati.

5.1.6 Ai sensi del Regolamento UE è lecito, in deroga al divieto generale, trasferire dati personali verso un Paese terzo non adeguato "per importanti motivi di interesse pubblico", purchè si tratti di un “interesse pubblico” riconosciuto dal diritto dello Stato membro del titolare o dal diritto dell'UE.

6 Regolamento UE: il cambio di prospettiva

Cosa cambia con il Regolamento UE?

Con il Regolamento UE si assiste ad un cambio di prospettiva rispetto al Codice: si passa dall’obbligo di applicazione delle misure di sicurezza previste nel Codice ad un più generale **obbligo di responsabilizzazione del titolare** (c.d. principio di accountability).

Si tratta di una grande novità in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali.

In applicazione del principio di accountability, il Regolamento UE prevede le seguenti regole.

6.1.1 Il titolare dovrà, **sin dall’inizio**, “**strutturare**” il trattamento dei dati in modo tale da prevedere le garanzie indispensabili al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati, tenendo condo del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati (“protezione dei dati fin dalla progettazione” e “protezione per impostazione predefinita”).

6.1.2 La designazione del DPO riflette l'approccio responsabilizzante che è proprio del Regolamento UE essendo finalizzata a facilitare l'attuazione del Regolamento UE da parte del titolare e del responsabile. Per tale ragione, anche laddove la designazione del DPO non sia obbligatoria, una designazione volontaria del DPO sarebbe potrebbe comunque garantire:

(i) maggiore rispetto della compliance aziendale attraverso DPIA e audit,

(ii) maggiore competitività aziendale,

(iii) maggiore mediazione tra i principali stakeholders (Garanti, interessati al trattamento e unità operative interne all’azienda).

6.1.3 Il Regolamento UE introduce il DPIA (Data Protection Impact Assessment) ovvero un Piano di Valutazione di impatto sui dati personali che dovrà essere adottato ogni qualvolta ci sarà un mutazione nell'asset di trattamento (il "**Piano di Valutazione**").

Il DPIA è obbligatorio in caso di:

(i) **trattamenti di dati su larga scala,** che mirano al trattamento di una notevole quantità di dati personali e che potenzialmente presentano un rischio elevato,

(ii) **trattamenti derivanti dall'impiego di nuove tecnologie o che presentano un rischio elevato per i diritti e le libertà degli interessati,**

(iii) dati trattati per adottare **decisioni riguardanti determinate persone fisiche**, in seguito ad una valutazione sistematica e globale degli aspetti personali (quali ad esempio quelle operate in ambito sanitario),

(iv) **trattamenti basati sulla profilazione o su trattameni automatici dei dati stessi**, e che vanno ad avere effetti giuridici o incidono significativamente sulle persone fisiche,

(v) **trattamenti di particolari categorie di dati personali** (dati biometrici, genetici o relativi a condanne penali, nonchè I reati o le misure di sicurezza ad essi connesse),

(vi) **sorveglianza sanitaria sistematica su larga scala di zone accessibili al pubblico.**

Il processo di DPIA è così riassumibile:

(a) indicazione delle motivazioni del DPIA e identificazione dei responsabili del processo di valutazione,

(b) analisi organizzativa dei processi aziendali nell'ambito dei quali sono trattati i dati,

(c) identificazione degli interessati del trattamento (ad es. dipendenti, fornitori, ecc),

(d) identificazione delle tipologie del trattamento (ad es. dati anagrafici, sanitari, ecc),

(e) identificazione della categoria del trattamento (dati comuni, sensibili e giudiziari),

(f) specificazione delle finalità del trattamento,

(g) modalità del trattamento,

(h) funzioni coinvolte (in qualità di responsabile o di incaricato),

(i) necessità del trattamento e proporzionalità nell'uso dei dati,

(j) valutazione dei rischi in termini di probabilità ed impatto,

(k) valutazione dell'efficacia del sistema di controllo interno privacy (misure di sicurezza, porocedure, informative, consensi, formazione, nomine, flussi informativi al DPO),

(l) valutazione del rischio privacy residuo,

(m) monitoraggio e riesame per la valutazione delle confromità del trattamento in relazione alla valutazione di impatto effettuata.

6.1.4 Tutti i titolari e i responsabili di trattamento (con l'eccezione di alcuni specifici casi) devono tenere, in forma scritta, un **registro delle operazioni di trattamento** il cui contenuto è tassativamente indicato nel Regolamento UE e che deve essere esibito su richiesta al Garante. E' uno strumento fondamentale sia ai fini dell'eventuale supervisione da parte del Garante, sia allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda.

6.1.5 A differenza di quanto previsto nel Codice, le **misure di sicurezza** devono garantire un livello di sicurezza adeguato al rischio del trattamento. Di conseguenza:

(i) la lista delle misue di sicurezza previste nel Regolamento UE è una lista aperta e non esaustiva,

(ii) non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure minime di sicurezza poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati,

(iii) l'adeguatezza delle misure di sicurezza adottate può essere attestata attraverso l'adesione a specifici codici di condotta o a schemi di certificazione.

6.1.6 Parimenti a quanto attualmente previsto nel Codice, tutti i titolari dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati. In più, però, il Regolamento UE introduce per la prima volta **l'obbligo della Data Breach Notification**, ossia la notifica in caso di violazioni di dati.

(i) In caso di violazione dei dati personali, il titolare del trattamento deve **notificare** all'autorità di controllo (cioè al Garante della Privacy) **senza giustificato ritardo e, ove possibile, entro 72 ore** dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà degli interessati.

La notifica deve indicare:

(a) la natura della violazione dei dati,

(b) le probabili conseguenze,

(c) le misure adottate per porvi rimedio.

(ii) Quando la violazione comporta un rischio elevato per i diritti e le libertà dei soggetti interessati, **la violazione deve essere comunicata a ciascun**

soggetto coinvolto individualmente o, laddove una comunicazione individuale richieda sforzi sproporzionati, tramite una comunicazione pubblica..

In sintesi. Il Regolamento UE prevede, in determinate ipotesi di violazioni dei dati, un obbligo di notifica da parte del titolare.

Tutto dipende dal livello di rischio per i diritti e le libertà degli interessati.

Se il livello di **rischio** è **trascurabile** (cioè nessun rischio di pregiudizio), non c'è obbligo di notifica.

Se il livello di **rischio** è **basso** (cioè nessun rischio significativo), c'è l'obbligo di notifica al Garante.

Se il livello di **rischio** è **medio** (cioè c'è possibilità di pregiudizio), c'è l'obbligo di notifica al Garante + comunicazione al cliente.

Se il livello di **rischio** è **alto** (cioè c'è possibilità di significativo pregiudizio), c'è obbligo di notifica al Garante + comunicazione al cliente.

Se il livello di **rischio** è **molto alto** (cioè c'è possibilità di grave pregiudizio), c'è l'obbligo di notifica al Garante + comunicazione al cliente.

6.1.7 L'intervento delle autorità di controllo sarà principalmente *ex post*, cioè si collocherà successivamente alle determinazioni assunte autonomamente dal titolare. Pertanto, il Regolamento UE prevede **l'abolizione di alcuni istituti previsti dal Codice**, quali ad esempio:

(i) la notifica preventiva dei trattamenti all'autorità di controllo, e

(ii) il c.d. prior checking (o verifica preliminare).

Tali istituti sono sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e di effettuazione di valutazioni di impatto in piena autonomia.

In conclusione, con il Regolamento UE, il ruolo del titolare del trattamento diviene, pertanto, più attivo.

Il titolare del trattamento avrà la responsabilità di costruire un vero e proprio "modello privacy" in relazione alle peculiarità delle propria struttura organizzativa.

Ancor più che sotto il vigore del Codice, con il Regolamento UE non è possibile identificare un "modello universale" ideale al quale ispirarsi: difatti, le modalità di adempimento ai dettami del Regolamento UE dovranno essere costruite in relazione a ciascuna singola attività aziendale e alle sue specifiche problematiche.

Vale a dire che in ogni impresa la costruzione di un "modello privacy" efficace dovrà essere quanto più possibile "personalizzata".

Inoltre, il Regolamento UE, sempre per agevolare il titolare nella dimostrazione che il trattamento dei dati è stato "strutturato" in maniera tale (i) da rispettare gli obblighi e i requisiti previsti dalle disposizioni comunitarie e (ii) da garantire la sicurezza dei dati, incoraggia l'adesione ai codici di condotta e ai meccanismi di certificazione. L'adesione a tali meccanismi di certificazione, sigilli e marchi di protezione dati consente, dall'altro lato, agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi.

La certificazione sarà, quindi, su base volontaria.

7 Le sanzioni

Cosa cambia con il Regolamento UE?

Il Regolamento UE contempla un notevole inasprimento delle sanzioni: fino ad un massimo di Euro 20.000.000 o al 4% del fatturato mondiale annuo.

* * *

Il nostro studio è a Vostra disposizione per qualunque supporto in merito ai contenuti di cui al presente *memorandum*.