CIRCOLARE n. 11 / 2018

Gentili clienti
Loro sedi

Modena, 20 aprile 2018

LA NUOVA DISCIPLINA DELLA PRIVACY (REGOLAMENTO UE 679/2016)

Con il regolamento UE 27.4.2016 n. 679 sono state introdotte alcune novità in materia di *privacy*. Tale regolamento è entrato in vigore il 24.5.2016, ma sarà **applicabile dal prossimo 25.5.2018**. Ad oggi mancano ancora le norme di coordinamento rispetto alla disciplina prevista dal vigente Codice della *privacy* (di cui al DLgs. 196/2003), che, quindi, alla data del 25.5.2018, rimarrà in vigore, compatibilmente con le nuove previsioni.

1.1 OGGETTO E FINALITÀ DEL REGOLAMENTO

Le disposizioni contenute nel reg. UE 679/2016 (art. 1 par. 1) riguardano la protezione delle **persone fisiche** (così come per il Codice della *privacy*, che esclude il trattamento dei dati relativi a persone giuridiche) con riferimento:

- al trattamento dei dati personali;
- alla circolazione di tali dati (intesa come qualsiasi manipolazione di dati, anche per semplice lettura accidentale).

1.2 AMBITO DI APPLICAZIONE *MATERIALE*

Il reg. UE 679/2016 (art. 2) trova applicazione con riferimento ai seguenti trattamenti:

- trattamento automatizzato, in maniera parziale o totale, di dati personali;
- trattamento non automatizzato di dati personali contenuti in un archivio o destinati ad essere ivi inclusi.

Sono **esclusi** i trattamenti di dati personali effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico. Sono inoltre esclusi dall'applicazione del regolamento anche i *dati trattati in forma anonima* e che non consentono l'identificazione del soggetto interessato.

1.3 AMBITO DI APPLICAZIONE *TERRITORIALE*

Il reg. UE 679/2016 (art. 3) è applicabile alle imprese stabilite nell'Unione Europea, indipendentemente da dove venga gestito il trattamento dei dati (ad esempio per le imprese che aderiscono ai *servizi in cloud* i dati potrebbero essere trattati fuori dall'UE ma le imprese sono comunque tenute al rispetto delle norme previste nel regolamento).

2 FIGURE PROFESSIONALI

Nell'ambito dei **soggetti coinvolti** nel trattamento dei dati personali, il reg. UE 679/2016 (Capo IV, artt. 24 - 43) richiama le figure del **titolare del trattamento** dei dati e del **responsabile del trattamento** dei dati e introduce la nuova figura del **responsabile per la protezione dei dati personali (RPD/DPO)**.

2.1 TITOLARE, RESPONSABILE E INCARICATO DEL TRATTAMENTO DEI DATI

Il reg. UE 679/2016 definisce in maniera più precisa ruoli e compiti del titolare e del responsabile del trattamento dei dati. Tali qualifiche possono essere assunte da una *persona fisica o giuridica*, unâautorità pubblica, un servizio o altro organismo (art. 4 n. 7 e 8). A queste figure potrebbe poi affiancarsi quella dellâincaricato del trattamento, quale ñ*persona autorizzata al trattamento dei dati personali sotto lâautorità diretta del titolare o del responsabile*ò (art. 4 n. 10).

Titolare del trattamento

Il **titolare** del trattamento è il soggetto che, singolarmente o insieme ad altri, ***determina le finalità e i mezzi*** del trattamento di dati personali (artt. 24, 26 e 27 del reg. UE 679/2016). Eôil soggetto che **risponde del corretto trattamento dei dati** acquisiti dagli interessati.

Il nuovo regolamento disciplina la possibilità che vi sia una contitolarità del trattamento, identificata come *compresenza di due o più titolari* del trattamento che determinano ñ*congiuntamente*ò finalità e mezzi, definendo ï tramite un **accordo scritto** - le rispettive responsabilità e compiti, oltre che i rispettivi ruoli e rapporti con gli interessati. Il *contenuto essenziale* dellâaccordo è *messo a disposizione dellôinteressato*, il quale è libero di esercitare i propri diritti nei confronti e contro ciascun titolare del trattamento.

In caso di trattamento dei dati personali di interessati che si trovano nellôUnione da parte di un titolare del trattamento (o da un responsabile del trattamento) che non è stabilito nellôUnione, il titolare del trattamento (o il responsabile del trattamento) deve nominare per iscritto un ***rappresentante che abbia sede nellôUnione***.

Responsabile del trattamento

Il **responsabile** del trattamento è il soggetto che tratta dati personali per conto del titolare del trattamento (art. 28 del reg. UE 679/2016) e viene **nominato dal titolare** sulla base di un accordo contrattuale.

Il responsabile del trattamento può ricorrere a sua volta ad un altro responsabile, ma **solo su autorizzazione scritta** (specifica o generale) del titolare del trattamento; nel caso di nomina di un *sub-responsabile*, per specifiche attività di trattamento, occorre definire anche tali rapporti mediante un contratto o altro atto giuridico.

La violazione del regolamento da parte del responsabile del trattamento, determinando finalità e mezzi del trattamento stesso, comporta lâassunzione diretta della qualifica di titolare del trattamento.

Contenuto del contratto stipulato tra titolare e responsabile del trattamento	
Aspetti generali	• materia disciplinata ï dati da trattare; • la durata del trattamento; • la natura e finalità del trattamento; • il tipo di dati personali trattati; • le categorie di interessati; • gli obblighi e diritti del titolare del trattamento.
Aspetti specifici	• obbligo per il responsabile di procedere al trattamento dei dati solo su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un Paese terzo o unôorganizzazione internazionale, salvo sussista un obbligo giuridico e previa informativa al titolare (salvo divieto per rilevanti motivi di interesse pubblico); • il responsabile deve garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

segue	• il responsabile deve adottare tutte le misure di sicurezza per evitare una violazione dei dati trattati; • il responsabile deve rispettare le condizioni stabilite per la nomina di un eventuale sub-responsabile del trattamento; • il responsabile deve assistere il titolare, tenuto conto della natura del trattamento, con misure tecniche e organizzative adeguate per lôadempimento da parte del titolare alle richieste dellôinteressato per lôesercizio dei suoi diritti; • il responsabile deve assistere il titolare, tenuto conto della natura del trattamento e delle informazioni a disposizione, nel garantire il rispetto degli obblighi per la sicurezza dei dati personali e per la valutazione dôimpatto sulla protezione dei dati e la consultazione preventiva; • in caso di richiesta del titolare del trattamento, il responsabile si impegna a cancellare o restituire tutti i dati personali una volta terminata la prestazione dei servizi relativi al trattamento, e deve cancellare le copie esistenti, salvo sia prevista dal diritto dellôUnione o degli Stati membri la conservazione dei dati; • il responsabile deve mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto dei sopra esposti obblighi, consentendo e contribuendo alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

2.2 RESPONSABILE DELLA PROTEZIONE DEI DATI - DPO

Il reg. UE 679/2016 (artt. 37 - 39) introduce la nuova figura professionale del responsabile della protezione dei dati - RPD (o *Data Protection Officer* - DPO), si tratta di un **organo di vigilanza** (interno o esterno) che supervisiona i trattamenti dei dati, monitora le fasi e indica cosa dovrebbe essere fatto.

Tale soggetto deve essere **nominato per iscritto** e **comunicato** al Garante della Privacy **entro il 25.05.2018**.

Obbligo di Nomina	• le Pubbliche Amministrazioni (salvo i casi in cui il trattamento dei dati sia effettuato dalle autorità giurisdizionali nellôesercizio delle funzioni giurisdizionali); • i soggetti la cui attività principale consiste nel trattamento di dati che, per loro natura, ambito di applicazione e/o finalità, richiedono il un monitoraggio regolare e sistematico degli interessati su larga scala (es. sistemi di videosorveglianza su suolo pubblico); • i soggetti la cui attività principale consiste nel trattamento, su larga scala, di categorie particolari di dati personali (nellôambito dei quali sono compresi i dati ñsensibiliò, i dati genetici e biometrici) e i dati relativi a condanne penali e reati (artt. 9 e 10 del reg. UE 679/2016) (es. sistemi di domotica e telecontrollo).
Qualifica e designazione	LôRPD viene designato dal titolare del trattamento e dal responsabile del trattamento: • in base alle qualità professionali (conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati) e alla capacità di assolvere i propri compiti; non sono necessarie attestazioni formali o titoli professionali specifici ma devono essere rispettati gli obblighi formativi (almeno 40 ore); • ricorrendo a un proprio dipendente (RPD interno) o a un soggetto esterno (RPD esterno), in questôultimo caso mediante il ricorso ad un contratto di servizi. È possibile per un gruppo di imprese o di soggetti pubblici nominare un unico RPD.

Compiti	Lô RPD deve svolgere i seguenti compiti minimi: • informare e fornire consulenza al titolare o al responsabile del trattamento, nonché ai dipendenti, in merito agli obblighi derivanti dal regolamento; • verificare lôattuazione e lôapplicazione della normativa, oltre alla sensibilizzazione e formazione del personale e dei relativi *auditors*; • fornire, se richiesto, pareri in merito alla valutazione di impatto sulla protezione dei dati e sorvegliare i relativi adempimenti; • fungere da punto di contatto con lôautorità di controllo o, eventualmente, consultarla di propria iniziativa; • riferire con cadenza almeno annuale al titolare del trattamento le attività formative specialistiche e di aggiornamento seguite periodicamente dal personale oltre alle novità normative, amministrative e tecnologiche che interessano i singoli trattamenti; • inviare comunicazioni periodiche, promuovere iniziative ed eventi di sensibilizzazione sul tema della protezione dei dati delle persone fisiche. Nellôesecuzione di tali compiti, lô RPD: • deve essere ñ*sostenuto*ò, mediante il rilascio delle risorse necessarie che deve comunque gestire evitando esborsi superflui e rendicontando le spese sostenute al titolare del trattamento; • non deve ricevere alcuna istruzione; • non è rimosso o penalizzato.
Obblighi	È tenuto al segreto o alla riservatezza in merito allôadempimento dei propri compiti (che possono essere anche altri, purché non integrino un conflitto di interessi).
Adempimenti	I dati di contatto del responsabile della protezione dei dati devono essere pubblicati e comunicati allôautorità di controllo da parte del titolare del trattamento e dal responsabile del trattamento.

3 ADEMPIMENTI DEL TITOLARE DEL TRATTAMENTO E DEL RESPONSABILE DEL TRATTAMENTO

In capo al titolare del trattamento e al responsabile del trattamento sono stati:

- **dettagliati e/o modificati alcuni adempimenti** già previsti dalla normativa precedente, ad esempio la modalità di trattamento dei dati, di acquisizione del consenso e di rilascio dellôinformativa;
- introdotti **nuovi compiti**, fra i quali tenere un registro delle attività di trattamento ed effettuare una valutazione di impatto sulla protezione dei dati.

3.1 MODALITÀ DI TRATTAMENTI DEI DATI

Il **titolare del trattamento** deve istruire tutti coloro che sono autorizzati ad accedere e trattare i dati personali, *compreso il responsabile* del trattamento (art. 29 del reg. UE 679/2016).

Costituiscono **principi generali del trattamento** (art. 5 del reg. UE 679/2016):

- la liceità, la correttezza e la trasparenza nei confronti dellôinteressato (previa adeguata informativa e acquisizione del consenso dellôinteressato, ovvero in base a forme contrattuali o per obbligo, ad esempio per salvargli la vita);
- la limitazione delle finalità ï stabilire lo scopo della raccolta dei dati dellôinteressato (determinate, esplicite e legittime);

- la proporzionalità - minimizzare i dati da acquisire, che devono essere adeguati, pertinenti e limitati a quanto strettamente necessario rispetto alle finalità per le quali sono trattati (ad esempio per l'accesso al caveau di una banca sarà necessaria l'acquisizione dei dati biometrici, mentre per l'accesso ad un ufficio potrebbe essere sufficiente un badge);
- l'esattezza con aggiornamento dei dati (se necessario);
- la limitazione della conservazione ai soli dati necessari e per un periodo limitato di tempo, definire nell'incarico il termine ultimo di conservazione dei dati e le condizioni per il ritiro dei documenti, cosa accade in caso di mancato ritiro. Nell'ipotesi in cui si rendesse necessaria un'estensione del periodo di conservazione rispetto alle pattuizioni iniziali sarà opportuno redigere una nuova informativa;
- l'integrità e la riservatezza ï tutela dei dati conservati;
- la responsabilizzazione del titolare del trattamento, il quale è competente per il rispetto dei principi sopra esposti e sul quale grava l'onore di prova.

3.2 ACQUISIZIONE DEL CONSENSO

Come già previsto dalla normativa precedente, il consenso deve essere libero, specifico rispetto alle finalità del trattamento (o per finalità compatibili), informato e inequivocabile. In tal senso la novità riguarda il fatto che il regolamento non precisa le modalità di espressione del consenso, infatti potrebbe avvenire anche mediante la selezione di apposita casella in un sito web. Infatti si richiede il **consenso ñesplicitoò** (per iscritto) solo per:

- categorie particolari di dati (in particolare i dati definiti ñsensibiliò);
- le decisioni basate su trattamenti automatizzati (compresa la profilazione).

La richiesta di consenso, *qualora inserita all'interno di una dichiarazione scritta*, deve essere chiaramente **distinguibile** da altre richieste o dichiarazioni rivolte all'interessato e deve essere resa in **forma comprensibile e facilmente accessibile**, con linguaggio semplice e chiaro.

Il consenso dei minori è valido a partire dai 16 anni, mentre prima occorre il consenso dei genitori o di chi ne fa le veci.

Non è normativamente previsto l'obbligo di consenso tramite la forma scritta, si consiglia comunque l'uso di tale modalità per l'inequivocabilità del consenso, il titolare è infatti chiamato a dimostrare che l'interessato ha prestato il consenso ad uno specifico trattamento in caso di verifica.

Categorie particolari di dati personali

Sono inclusi nella nuova definizione di ñcategorie particolari di datiò quelli classificati come **dati ñsensibiliò**, quindi i dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oltre ai dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 del reg. UE 679/2016 e art. 4 co. 1 lett. d) del Codice della *privacy*), i dati genetici e dati biometrici (intesi a identificare in modo univoco una persona fisica).

Per il trattamento dei suddetti dati è, in generale, prescritto il *divieto generale di trattamento*. Costituiscono eccezione, oltre al consenso, fra l'altro, l'esecuzione di un contratto di lavoro e le connesse esigenze di sicurezza/protezione sociale, nonché la difesa di un diritto in sede giudiziaria.

Dati personali relativi a condanne penali e reati

Il trattamento dei dati personali relativi a condanne penali e reati ï sostanzialmente corrispondenti a quelli oggi definiti ñgiudiziariò ï deve avvenire, in maniera alternativa, sotto il controllo della autorità pubblica o previa autorizzazione proveniente da norme dell'Unione e del singolo Stato membro, che prevedano garanzie

appropriate per i diritti e le libertà degli interessati (art. 10 del reg. UE 679/2016 e art. 4 co. 1 lett. e) del Codice della *privacy*).

Processi decisionali automatizzati

Il reg. UE 679/2016 (art. 22) codifica espressamente il diritto dell'interessato a non essere sottoposto ad una decisione basata unicamente su un trattamento automatizzato dei dati che produca effetti giuridici che lo riguardano o che comunque incida significativamente sulla sua persona.

In tale ambito, viene ricompresa anche la profilazione, definita come "*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali, in particolare per analizzare o prevedere il rendimento professionale, la situazione economica, la salute, le preferenze personali (intesi anche come abitudini di consumo), gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*" (art. 4 n. 4 del reg. UE 679/2016).

Il trattamento è vietato salvo l'acquisizione del consenso "*esplicito*" dell'interessato, o nei casi in cui tali operazioni siano necessarie per l'esecuzione di un contratto con l'interessato o sia autorizzata dal diritto dell'Unione o del singolo Stato membro.

Rimane comunque l'obbligo di apprestare garanzie adeguate ad assicurare il rispetto dei diritti dell'interessato, riguardanti la specifica informazione all'interessato, e del diritto di ottenere l'intervento umano, nonché di esprimere la propria opinione e di contestare la decisione.

Nell'informativa devono essere esplicitate le modalità e le finalità della profilazione. Inoltre, deve essere chiarita la logica inerente il trattamento e le conseguenze previste per l'interessato a seguito di tale tipo di trattamento (art. 13 del reg. UE 679/2016).

Trattamento dei dati nell'ambito dei rapporti di lavoro

Per quanto riguarda il trattamento dei dati nell'ambito dei rapporti di lavoro (art. 88), viene riconosciuta la possibilità per gli Stati membri di prevedere (con legge o tramite contratti collettivi) norme più specifiche "*per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro*".

3.3 INFORMATIVA

Il reg. UE 679/2016 (artt. 13 e 14) sancisce l'obbligo di informativa, da tenere sempre distinto dalla raccolta dei dati presso l'interessato, prevedendo però un contenuto maggiormente dettagliato.

L'informativa deve:

- avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile e deve essere utilizzato un linguaggio chiaro e semplice;
- essere data per iscritto o con "*altri mezzi*" anche elettronici (ad esempio, nel caso di servizi *on line*), oralmente se richiesto dall'interessato; è ammesso l'uso di icone;
- essere fornita all'interessato prima della raccolta dei dati dall'interessato. Se la *raccolta avviene tramite soggetti terzi*, l'informativa deve contenere anche le categorie dei dati personali oggetto di trattamento.

Qualora i dati personali siano raccolti presso l'interessato, le informazioni devono essere fornite nel momento in cui i dati personali sono ottenuti.

Nel caso di dati personali non ottenuti presso l'interessato, le informazioni devono essere fornite:

- entro un termine ragionevole dall'ottenimento dei dati personali, comunque entro un mese, tenuto conto delle specifiche circostanze di trattamento dei dati;
- qualora i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato (l'attuale norma consentiva l'acquisizione al più tardi al momento della registrazione, quindi vengono *ridotti i tempi* per la raccolta dei dati personali);
- qualora sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

Qualora le finalità cambino, occorre informarne l'interessato prima di procedere al trattamento ulteriore.

In entrambi i casi di informativa per dati raccolti presso l'interessato o meno, la stessa non va resa se e nella misura in cui l'interessato abbia già le informazioni.

Contenuto dell'informativa	
Informativa per il trattamento di dati raccolti presso l'interessato	Occorre rendere noto: • l'identità e i dati di contatto del **titolare del trattamento** e, ove applicabile, del suo rappresentante; • i dati di contatto del **responsabile della protezione dei dati**, se nominato; • le **finalità del trattamento** cui sono destinati i dati personali e la base giuridica del trattamento; • i legittimi **interessi perseguiti** dal titolare del trattamento o da terzi, qualora costituisca la base giuridica del trattamento; • gli eventuali **destinatari** o le eventuali categorie di destinatari dei dati personali; • l'intenzione del titolare del trattamento di **trasferire dati personali a un Paese terzo** o a un'organizzazione internazionale il riferimento alle garanzie appropriate od opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili; • il **periodo di conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; • l'esistenza del **diritto** dell'interessato di chiedere al titolare del trattamento l'**accesso** ai dati personali e la **rettifica** o la **cancellazione** degli stessi o la **limitazione** del trattamento che lo riguardano o di **opporsi** al loro trattamento, oltre al **diritto alla portabilità** dei dati; • l'esistenza del **diritto di revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca, anche di categorie particolari di dati; • il **diritto di proporre reclamo** a un'autorità di controllo; • se la comunicazione di dati personali è un **obbligo** legale o contrattuale o un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali, oltre alle possibili conseguenze circa la mancata comunicazione di tali dati; • l'esistenza di un **processo decisionale automatizzato**, compresa la profilazione e, in tali casi, le informazioni significative sulla logica utilizzata, oltre all'importanza e alle conseguenze previste di tale trattamento per l'interessato.

Contenuto dellôinformativa	
Informativa per il trattamento di dati non ottenuti presso lôinteressato	Occorre rendere noto le informazioni di cui sopra (con esclusione del riferimento alla comunicazione dei dati personali come obbligo legale o contrattuale), con lôaggiunta: • delle **categorie di dati personali** oggetto di trattamento; • della **fonte** da cui hanno origine i dati personali e, se del caso, dellôeventualità che i dati provengano da fonti accessibili al pubblico.

3.4 DIRITTI DEGLI INTERESSATI

Nellôambito dei **diritti previsti in capo allôinteressato**, vengono riproposti, rispetto alla normativa precedente, oltre allôinformativa sul trattamento dei dati personali, i seguenti (artt. 12 - 23 del reg. UE 679/2016):

- diritto di accesso;
- diritto di rettifica;
- diritto di cancellazione (diritto allôoblio in forma rafforzata);
- diritto di opposizione.

Viene previsto, poi, il diritto alla limitazione al trattamento dei dati, che costituisce un diritto diverso e più esteso rispetto al ñbloccoò del trattamento di cui al Codice della *privacy* (art. 7 co. 3 lett. b)).

Viene introdotto, infine, il nuovo diritto alla portabilità dei dati, che riguarda i trattamenti:

- basati sul consenso o su un contratto stipulato con lôinteressato;
- effettuati con *mezzi automatizzati*, non si applica quindi agli archivi o registri cartacei.

Inoltre, si deve trattare di dati forniti direttamente dallôinteressato al titolare del trattamento.

Modalità per lôesercizio dei diritti

Quanto alle modalità per lôesercizio dei diritti, rispetto al Codice della *privacy* (artt. 9 e 10):

- il **termine per la risposta** allôinteressato è, per tutti i diritti, di **un mese** dal ricevimento della richiesta, estendibile fino a due mesi in casi di particolare complessità; il titolare deve **comunque dare un riscontro allôinteressato, anche in caso di diniego**;
- il riscontro alle richieste presentate dagli interessati deve avvenire in forma scritta, anche elettronica; se la richiesta avviene con mezzi elettronici, nella medesima forma sono rese le informazioni (ove possibile e salva diversa indicazione dellôinteressato). Il riscontro può essere dato **oralmente solo se** così **richiesto** dallôinteressato;
- in generale le informazioni vanno rese in maniera *gratuita*; spetta al titolare, però, stabilire lôammontare dellôeventuale contributo da chiedere allôinteressato qualora si tratti di richieste manifestamente infondate o eccessive, anche ripetitive, e, nellôambito del diritto di accesso, nel caso di richiesta di più copie dei dati personali (tenuto conto dei costi amministrativi sostenuti).

3.5 PRINCIPIO DI ñ*ACCOUNTABILITY*ò

Viene introdotto il principio della c.d. ñresponsabilizzazioneò (*accountability*) di titolari (e responsabili) del trattamento, che sono tenuti a **mettere in atto misure tecniche e organizzative adeguate** per garantire e per dimostrare lôapplicazione del regolamento, con gli aggiornamenti necessari (art. 24 del reg. UE 679/2016).

Pertanto, è il titolare che decide in maniera autonoma modalità, garanzie e limiti del trattamento dei dati personali, nel rispetto del regolamento e di alcuni criteri previsti di seguito trattati.

3.6 PRINCIPIO DELLA *PRIVACY* ñ*BY DESIGN*ò E ñ*BY DEFAULT*ò

Viene richiesto al **titolare** del trattamento di impostare da subito lôattività e la stessa organizzazione secondo i principi c.d. di ñ*privacy by design*ò e ñ*privacy by default*ò, riducendo i trattamenti non necessari (art. 25 del reg. UE 679/2016).

In particolare:

- ñ*privacy by design*ò occorre attuare adeguate misure tecniche e organizzative sin dallôatto della progettazione (quindi, prima di procedere al trattamento dei dati) e comunque al momento dellôesecuzione del trattamento; fra le misure vengono indicate espressamente la pseudonimizzazione e la minimizzazione;
- ñ*privacy by default*ò i dati vengano trattati, per impostazione predefinita, esclusivamente per le finalità previste e per il periodo strettamente necessario (in maniera similare a quanto già previsto dal principio di necessità); le misure devono garantire che i dati personali non siano resi accessibili a un numero indefinito di persone fisiche senza lôintervento della persona fisica.

La conformità ai requisiti richiesti può essere dimostrata mediante il ricorso a meccanismi di certificazione.

3.7 REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

I titolari e i responsabili del trattamento devono **tenere un registro delle operazioni di trattamento**, in forma scritta, anche in *formato elettronico* (art. 30 del reg. UE 679/2016), e deve essere esibito su richiesta del Garante per la privacy.

Sono **obbligate** alla tenuta del registro le imprese o le organizzazioni con 250 o più dipendenti, e tutti coloro che:

- Trattano dati sensibili per i quali possa presentarsi un rischio per i diritti e le libertà dellôinteressato;
- Offrono consulenze non occasionali;
- Trattano categorie particolari di dati o dati personali relativi a condanne penali e a reati.

Contenuto del registro	
Titolare del trattamento	• nome e dati di contatto del **titolare del trattamento** e, ove applicabile, del **contitolare** del trattamento, del **rappresentante** del titolare del trattamento e del **responsabile della protezione dei dati** (se nominato); • **finalità** del trattamento; • categorie di **interessati** e categorie di **dati personali**; • categorie di **destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali; • **trasferimenti dei dati personali** verso un Paese terzo o unôorganizzazione internazionale, compresa lôidentificazione del Paese terzo o dellôorganizzazione internazionale e la documentazione delle **garanzie adeguate**; • **termini ultimi previsti per la cancellazione** delle diverse categorie di dati (la conservazione deve necessariamente essere fatta in luoghi idonei ad evitare il deperimento dei documenti); • descrizione generale delle **misure di sicurezza** tecniche e organizzative.
Responsabile del trattamento	• nome e dati di contatto del **responsabile o dei responsabili del trattamento**, di ogni **titolare del trattamento per conto del quale agisce** il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati; • **categorie dei trattamenti** effettuati per conto di ogni titolare del trattamento;

Contenuto del registro	
segue	• **categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali; • **trasferimenti di dati personali** verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate; • descrizione generale delle **misure di sicurezza** tecniche e organizzative.
Incaricati del trattamento	• informativa sugli **incaricati** al trattamento dei dati: collaboratori e dipendenti con incarico interno che nello svolgimento delle attività professionali si trovano a gestire i dati per conto del titolare o del responsabile; • definizione da parte del titolare e del responsabile delle **mansioni e procedure** che devono seguire nell'attività lavorativa.

3.8 MISURE DI SICUREZZA "ADEGUATE"

Il nuovo regolamento non prevede delle misure minime di sicurezza, ma è il **titolare del trattamento** che insieme al responsabile devono definire le **misure tecniche e organizzative "*adeguate*"** al fine di "*garantire un livello di sicurezza idoneo in base all'analisi del rischio*" del trattamento (art. 32 del reg. UE 679/2016).

Sarà, quindi, il titolare a valutare le misure necessarie, caso per caso, rispetto ad una serie di elementi, di seguito indicati:

- stato dell'arte;
- costi di attuazione;
- natura, oggetto, contesto e finalità del trattamento;
- rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

3.9 VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La valutazione di impatto sulla protezione dei dati (DPIA) costituisce un ulteriore adempimento derivante dal principio introdotto della responsabilizzazione (*accountability*) dei titolari nei confronti dei trattamenti da questi effettuati (artt. 35 e 36 del reg. UE 679/2016).

La valutazione, da effettuare *ex ante* al trattamento ad opera del titolare del trattamento consultandosi con il responsabile della protezione dei dati personali, ricorre come **obbligo** in caso di **trattamento molto rischioso per i diritti e le libertà delle persone fisiche**. La valutazione di impatto sulla protezione dei dati è richiesta, nello specifico, nei casi seguenti:

- valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano "*decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche*";
- trattamento, su larga scala, di categorie particolari di dati personali o dei dati relativi a condanne penali e a reati;
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Contenuto minimo della valutazione di impatto sulla protezione dei dati (DPIA)
• una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; • una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone.

Per i professionisti / consulenti tale valutazione può essere sostituita da una relazione dove vengono descritti i rischi al trattamento dei dati individuati.

3.10 VIOLAZIONE DEI DATI (ñ*DATA BREACH*ò)

Il regolamento sancisce lôobbligo di notifica, da parte del **titolare** del trattamento, di **ogni violazione** dei dati trattati allôautorità competente **entro 72 ore** dal momento in cui ne venga a conoscenza (e comunque senza ingiustificato ritardo) e, in casi gravi, anche allôinteressato. Tale adempimento è necessario **solo se** si ritiene probabile che da tale violazione derivino **rischi per i diritti e le libertà degli interessati** (artt. 33 e 34 del reg. UE 679/2016), ad esempio in caso di attacco da parte di un virus informatico.

Una volta ricevuta la segnalazione, il Garante provvede ad avviare unôindagine sulle misure di sicurezza adottate, partendo dal registro della privacy (nel quale vengono esposte le analisi svolte e le valutazioni dei rischi).

3.11 LôAMMINISTRATORE DI SISTEMA

Il nuovo regolamento non prevede questa figura ma sarebbe opportuno identificarlo tramite **nomina per iscritto** e prevederlo nella documentazione redatta dal titolare. Eôil soggetto che amministra la rete aziendale e ha i massimi privilegi di accesso (inteso nel senso che è custode delle password di rete). Eônecessario che venga redatta una relazione con cadenza almeno annuale sulle attività poste in essere e sui controlli che lôamministratore di sistema svolge per verificare il corretto funzionamento dei sistemi di sicurezza.

4 COSA FARE PER METTERSI IN REGOLA?

Il **titolare** del trattamento deve procedere allôorganizzazione in modo che vengano rispettati tutti gli adempimenti previsti dal regolamento, in caso contrario è lui il **responsabile ultimo** delle violazioni o omissioni. (si pensi ad esempio al fatto che le SIM aziendali devono essere riferibili al singolo dipendente oppure alla necessità prevedere password di accesso differenziate per ogni postazione di lavoro conservate in luoghi non accessibili a persone estranee).

Al contempo, ricade sempre sul titolare del trattamento lônere di **provare lôavvenuto adeguamento alla normativa** in materia di protezione dei dati tramite la predisposizione delle ñproveòdi aver agito con la massima diligenza.

4.1 IL DOSSIER PRIVACY

In questo documento vengono **esplicitati i ragionamenti e le analisi** che hanno indotto il titolare del trattamento a compiere determinate scelte dichiarandone le motivazioni. Tale documento è quello che consente di adempiere rapidamente alle eventuali richieste di informazioni e ispezioni da parte degli organi competenti.

Il *dossier privacy* potrebbe seguire la seguente struttura:

1. introduzione ï dove viene fatta una descrizione dellôimpresa, dellôattività svolta precisando eventuali trattamenti di dati su larga scala, ovvero con monitoraggio sistematico ovvero con profilazione; si specifica lôambito territoriale di trattamento e le categorie dei soggetti interessati;

2. disciplina normativa di riferimento ï dove si indicano i riferimenti al regolamento ovvero a codici di condotta cui si aderisce o a regolamenti adottati allôinterno dellôimpresa;
3. politica di protezione dei dati ï dove si precisano le finalità del trattamento dei dati, i piani di azione e si esplicitano i processi seguiti ed eventuali accorgimenti particolari;
4. organigramma ï in questa sezione viene fatta una descrizione delle categorie di responsabili (interni ed esterni), degli incaricati e di eventuali contitolari del trattamento in qualità di attori chiamati a gestire i dati acquisiti dagli interessati;
5. adempimenti interni ï vengono descritte le procedure interne adottate nel trattamento dei dati, precisando i protocolli seguiti nei rapporti tra gli attori indicati nellôorganigramma e le misure di sicurezza adottate;
6. adempimenti verso gli interessati ï include il modello relativo allôinformativa data agli interessati e la raccolta del consenso al trattamento dei dati, precisando i casi in cui lo stesso non sia obbligatorio e in base a quale norma; vengono esplicitate lôorganizzazione e le procedure che gli interessati possono porre in essere per lôesercizio dei propri diritti;
7. misure di sicurezza ï contiene lôanalisi dei rischi e le misure seguite per farvi fronte, le verifiche sulla corretta attuazione dei sistemi di sicurezza previsti e la descrizione del piano di formazione del personale.

4.2 IL REGISTRO DEI TRATTAMENTI

Tale documento, già descritto al paragrafo 3.7 cui si rimanda per il contenuto, ha una mera funzione descrittiva delle operazioni di trattamento dati poste in essere.

Poiché si tratta di un documento utile per dimostrare le valutazioni svolte in merito ai processi e alle procedure adottati, ne viene consigliata la tenuta anche ai soggetti che non sono obbligati dal regolamento. Questo perché in ogni caso si dovrebbe tenere una traccia delle analisi svolte e questo strumento è fondamentale per disporre di un quado aggiornato dei trattamenti.

4.3 SICUREZZA

Questo è un obiettivo necessario per garantire lôintegrità dei dati trattati e la difesa da attacchi esterni. Si compone di diversi adempimenti e in particolare della necessaria **formazione del personale** nellôuso degli strumenti e alla sensibilizzazione in merito alla tutela della riservatezza.

Il primo passaggio fondamentale parte dallôanalisi dei rischi: per ogni rischio individuato occorre stimare le misure di sicurezza implementate, i costi delle stesse, verificare la loro applicabilità nel tempo stimando anche eventuali costi aggiuntivi di manutenzione. Il regolamento richiede lôidentificazione delle misure tecniche e organizzative adottate precisando la periodicità di aggiornamento (almeno con cadenza annuale) oltre a richiedere di precisare i tempi di ripristino.

4.4 DISCIPLINA DEI RAPPORTI CON I CONTITOLARI E I RESPONSABILI DEL TRATTAMENTO

Occorre predisporre documenti scritti nei quali vengono espressamente identificati i contitolari e i responsabili del trattamento e questi dati devono poi essere comunicati agli interessati. Questi soggetti sono chiamati a rispettare lôobbligo di riservatezza che deve essere inserito negli accordi stipulati con il titolare.

4.5 INFORMATIVA E CONSENSO

Tutti gli obblighi di informativa sono invariati rispetto a quelli previsti dalla precedente normativa senonché occorre integrare i dati con i riferimenti del DPO (se nominato) e deve essere resa obbligatoriamente per

iscritto, anche con mezzi elettronici. Il contenuto dovrà anche essere integrato con i tempi di conservazione, precisando il termine ultimo, cosa accade se non vengono recuperati i dati conservati entro tale data e implementando un sistema di controllo sulla mancata conservazione di dati non più utilizzabili.

5 SANZIONI

Il titolare del trattamento risponde in prima persona del danno subito dall'interessato.

Il responsabile del trattamento risponde del danno causato dal trattamento solo se non ha adempiuto gli obblighi del regolamento o ha agito in maniera difforme rispetto alle istruzioni del titolare del trattamento.

Entrambi sono *esonerati* dalla responsabilità se dimostrano di aver rispettato tutti gli adempimenti previsti dalla normativa e pertanto il danno non è a loro imputabile.

Per quanto attiene le sanzioni amministrative, che verranno comminate dal Garante della privacy tenendo conto delle dimensioni del trasgressore, si differenziano come segue:

- sanzione per la violazione degli obblighi ï fino 10 milioni di Euro o il 2% del fatturato dell'impresa;
- sanzione per violazione dei diritti degli interessati o delle condizioni di trattamento ï fino a 20 milioni di Euro o il 4% del fatturato dell'impresa.

Il Garante ha comunque il potere di decidere se *ammonire il titolare*, senza prevedere alcuna sanzione amministrativa pecuniaria, nel caso in cui in sede di prima segnalazione, ritenga che tale comportamento possa essere sufficiente ad evitare il ripetersi delle violazioni riscontrate ovvero se voglia semplicemente dare un avvertimento sul fatto che i trattamenti previsti possano violare il regolamento.

Per ogni ulteriore chiarimento potrete rivolgervi direttamente alla Dott.ssa Elisa Simoni.
Cordiali saluti.

Lo Studio