Euroconference
Editoria

LA CIRCOLARE DI LAVORO E PREVIDENZA

Periodico di aggiornamento ed approfondimento professionale in area giuslavoristica

venticinque 2016
SETTIMANALE

Da leggere

23 giugno 2016

La nuova *privacy* europea: il Regolamento (Ue) 2016/679

di Piergiovanni Cervato - avvocato

Il 4 maggio 2016 è stato pubblicato il nuovo Regolamento Ue 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Si tratta del nuovo Regolamento privacy Ue, che detta una serie di nuovi adempimenti (dal registro dei trattamenti alle valutazioni di impatto) e prevede nuove figure di controllo e responsabilità (tra cui spicca il "responsabile della protezione dei dati", il c.d. Data Privacy Officer - DPO), oltre a consacrare a livello normativo il diritto all'oblio e a prevedere un'estensione territoriale e soggettiva di applicazione ben più ampia rispetto al passato.

Introduzione

Il 4 maggio 2016 è stato pubblicato il 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, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE.

Si tratta del Regolamento generale sulla protezione dei dati personali, ossia del *c.d. Regolamento privacy europeo*.

> Il Regolamento armonizza – *rectius*, cerca di armonizzare – la disciplina della protezione dei dati personali che a livello comunitario era stata dettata appunto dalla Direttiva 95/46/CE, variamente trasposta nei diversi Stati membri dell'Unione.

Per quanto riguarda l'Italia sappiamo che la materia era stata dapprima governata dalla non troppo felice L. n.6758/96, quindi dal D.Lgs. n.196/03, *c.d. Codice privacy*, entrato definitivamente in vigore a colpi di proroghe nell'arco dei successivi due anni.

Come si intuisce, da un lato la disciplina della protezione dei dati personali a livello comunitario era dettata nei vari Stati membri da normative che, pur operanti sotto l'ombra formale della medesima direttiva 95/46/CE, spesso invece presentavano sfumature, anche rilevanti, che le distinguevano tra di loro e creavano dei solchi tra Stato e Stato; dall'altro era divenuta sempre più anacronistica solo raffrontando il dato testuale con l'esponenziale sviluppo delle tecnologie di comunicazione, in primissimo luogo di *internet* e delle tecnologie *mobile*.

Si consideri inoltre come negli ultimi tempi la Corte di Giustizia fosse intervenuta con pronunce strategiche nei delicati temi del trattamento dei dati personali da parte dei motori di ricerca in relazione al *c.d. diritto all'oblio* (caso Costeja Gonzalez/Google Spain) e nel trasferimento dei dati personali al di fuori dell'Unione (*in primis* verso gli Usa), sostanzialmente sancendo l'illegittimità del *c.d. regime del Safe Harbor*, ossia di quel regime di "autocertificazione" per cui determinati sistemi nazionali extraeuropei potevano attestare che i propri operatori (ad esempio le società statunitensi) operassero autoconformando le proprie condotte a una disciplina analoga a quella comunitaria in tema di *privacy*.

Ancora, l'introduzione della riforma sui *cookie*, ossia sui *file* di testo che vengano a installarsi sui dispositivi degli utenti durante la navigazione *web* e che permettono una serie di tracciature (da quelle più semplici, di natura tecnica, a quelle statistiche, a quelle di una vera e propria profilazione commerciale), nell'ultimo paio d'anni aveva ulteriormente fatto irruzione nel sistema europeo (per l'Italia con la riforma dell'art.122 del Codice *privacy*, in vigore dal 2 giugno 2015).

A livello comunitario non era quindi più possibile affidarsi unicamente a una direttiva (cioè a uno strumento normativo di non diretta applicazione, ma richiedente la trasposizione nei singoli Stati), soprattutto nel momento in cui il sistema sociale stesso, in particolare nella *c.d. società dell'informazione* (*internet* e nuove tecnologie in genere), stava mutando e venendo a configurare ormai un *unicum* territorialmente inscindibile (*internet* è per definizione a-territoriale), per cui era divenuta ormai impellente l'adozione di una nuova disciplina uniforme e in particolare di diretta applicazione: appunto il Regolamento.

Entrata in vigore

Si ritiene utile invertire l'ordine di esposizione e anticipare fin da subito che il Regolamento, entrato in vigore il ventesimo giorno successivo alla sua pubblicazione, si applica dal 25 maggio 2018.

Ciò in quanto il Regolamento demanda ai singoli Stati membri la facoltà di adeguare le rispettive normative interne nazionali in senso più stringente rispetto alle proprie disposizioni "minime".
I singoli Stati membri hanno quindi l'onere di valutare l'eventuale introduzione interna di un sistema più protezionista entro il prossimo biennio, decorso il quale il Regolamento costituirà comunque esso stesso la disciplina di immediata e diretta applicazione in materia.

Ambito di applicazione

Ambito di applicazione soggettivo

Il Regolamento disciplina la protezione dai dati personali quale diritto fondamentale dell'Unione e, in particolare, mira a creare uno spazio di libertà, sicurezza e giustizia teso al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche (considerando 2), a prescindere dalla loro nazionalità e residenza.

Fin dai primi considerando e, in seguito, dalle prime disposizioni, in primo luogo il Regolamento chiarisce come la disciplina, dal lato dei destinatari della protezione, sia dettata esclusivamente a tutela delle persone fisiche, in quanto il "dato personale" è una qualsiasi informazione riguardante appunto (solo) una persona fisica identificata o identificabile (il *c.d. interessato*).

I dati delle persone diverse (persone giuridiche e assimilate) non rientrano quindi nell'alveo generale di applicazione della normativa e in ciò il Regolamento ha mantenuto quella linea che a livello comunitario – e anche in Italia, dal 2012 – aveva negli ultimi anni ristretto l'oggetto della protezione, appunto, solo alle persone fisiche.

Ambito di applicazione territoriale

Dal lato degli obblighi attivi alla protezione, il Regolamento ha invece innovato, introducendo anche nel sistema *privacy* il concetto di "stabilimento", per cui la disciplina si applica:

- sia al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione,
- sia al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
  - l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato;
  - oppure il monitoraggio del loro comportamento, nella misura in cui tale comportamento ha luogo all'interno dell'Unione;
- sia al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico (considerando 22 ss. e art.3).

Ambito di applicazione oggettivo

Il Regolamento chiarisce poi di applicarsi al trattamento automatizzato, e non di dati personali, e di non applicarsi invece ai trattamenti:

a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, Tue;
c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

Il Regolamento esplica, infine, di non voler pregiudicare in ogni caso l'applicazione della direttiva 2000/31/CE su taluni aspetti della società dell'informazione, con particolare riferimento ai profili di responsabilità (e relative esclusioni di responsabilità) dei prestatori intermediari di servizi, ossia dei *c.d. Internet Service Provider* (responsabilità per l'attività di *mere conduit*, *caching* e *hosting*).
Per il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione, il Regolamento rinvia infine al Regolamento (CE) n.45/01.

I principi della *privacy*: principi consolidati e principi di nuova introduzione

Il Regolamento ha riservato una particolare attenzione ai principi informatori della materia, utilizzati in modo rilevante anche dalla recente giurisprudenza della Corte di Giustizia in fase di interpretazione della vecchia direttiva del 1995, ad esempio laddove ha enucleato l'ormai noto diritto all'oblio proprio sulla base dei principi di "*pertinenza*" e "*non eccedenza*".
Accanto a tali due principi basilari, per cui il dato deve essere trattato negli stretti limiti e contesti per cui esso effettivamente serve allo scopo ("*minimizzazione dei dati*"), nonché a quelli generali di "*liceità, correttezza e trasparenza*", oltre che di "*esattezza*" e aggiornamento e di "*integrità e riservatezza*", la riforma comunitaria ha introdotto o chiarito altri importanti principi, come tali:

- quello della "*limitazione della finalità*", secondo cui il trattamento è lecito fintantoché non sia incompatibile con l'originaria finalità per cui esso era stato concesso (e in questo il principio si avvicina molto alla pertinenza e non eccedenza);
- quello della "*limitazione della conservazione*", per cui i dati personali possono essere conservati per il tempo necessario al raggiungimento dello scopo ed eccezionalmente possono essere conservati per periodi più lunghi, a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, venendo detti interessi di natura lato senso pubblicistica a compensare nel bilanciamento l'interesse privato alla riservatezza.

Le condizioni di liceità del trattamento: il consenso al trattamento, i casi di sua esclusione e l'informativa

I casi di consenso e di sua esclusione per necessità del trattamento

A norma del Regolamento, viene mantenuta la condizione minima di liceità del trattamento, rappresentata ordinariamente dal consenso dell'interessato, ovviamente informato e specifico per singole finalità (e qui rinviamo al tema dell'informativa, a seguire).
Altrettanto ovviamente, il consenso è revocabile e l'eventuale revoca non inficia la liceità del trattamento passato, intervenendo solo per il futuro.
Tale consenso può invece essere sostituito dal requisito della necessità del trattamento, che può configurarsi nei seguenti casi:

- quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- quando il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- quando il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- quando il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- quando il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Sul punto il Regolamento, come già anticipato, demanda agli Stati membri la possibilità di mantenere o introdurre disposizioni più specifiche nei propri ambiti nazionali.

La specificità del consenso

Nei casi in cui il consenso sia condizione per la liceità del trattamento, esso deve risultare da apposita dichiarazione scritta, che, laddove la richiesta riguardi anche altre questioni, sia chiaramente distinguibile dalle altre materie, comprensibile e facilmente accessibile, esposta in un linguaggio semplice e chiaro.
Norme particolari sono dettate per l'offerta diretta di servizi della società dell'informazione (servizi *web* e simili) ai minori, per cui in questi casi il consenso è lecitamente prestato dal minore stesso ove egli abbia almeno 16 anni: una sorta di "maggiore età" ai fini *privacy* per il trattamento di dati *on-line* e assimilati.
Per età inferiori il consenso deve invece provenire da chi rappresenti la potestà genitoriale.
Anche in questo caso gli Stati Membri possono peraltro derogare alle disposizioni regolamentari, in senso anche più liberale, abbassando il suddetto limite di età a 13 anni.

Il trattamento dei dati sensibili e giudiziari

L'art.9 del Regolamento detta inoltre tutta una serie di regole specifiche per trattamenti particolari, con specifico riferimento ai dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzio-

ni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (ossia i dati già conosciuti come "dati sensibili").

Per questi dati la regola ordinaria è quella del divieto di trattamento, tranne le eccezioni ivi disciplinate, tra cui è il caso di menzionare, oltre a quella dell'avvenuto consenso per una o più finalità specifiche, le seguenti:

- trattamento necessario in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, conformemente al diritto dell'Unione o degli Stati membri o al contratto collettivo;
- trattamento necessario per la tutela di un interesse vitale;
- trattamento effettuato da organizzazione senza scopo di lucro nell'ambito delle legittime attività perseguite per finalità politiche, filosofiche, religiose o sindacali, in relazione ai dati degli membri (attuali ed *ex*) e delle persone con cui tali enti abbiano contatti legittimi;
- trattamento necessario per l'esercizio di un diritto in sede giudiziaria;
- trattamento necessario per motivi di interesse pubblico rilevante;
- trattamento necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali;
- trattamento necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici;
- trattamento necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Anche in questo caso gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, biometrici o relativi alla salute.

Analoghe regole sono dettate per il trattamento di dati giudiziari.

L'informativa

Il trattamento è inoltre lecito qualora sia rispettata la condizione, minima e indispensabile oltre che generalmente preventiva, dell'informativa.

L'informativa deve riguardare quanto già previsto dalla legislazione attuale (per l'Italia, dall'art.13 codice *privacy*, di recente in abbinamento con l'art.122 per quanto riguarda la gestione dei *cookie*), ossia:

- le generalità del titolare;
- le finalità del trattamento;
- i destinatari nel caso di comunicazione dei dati;
- il legittimo interesse perseguito nei casi applicabili (cioè quando il trattamento è legittimato dal suo perseguimento).

Le novità introdotte dal Regolamento riguardano invece la previsione di specifiche informazioni:

- circa la base giuridica del trattamento, per cui quindi l'informativa dovrà espressamente descrivere il quadro normativo all'interno del quale il trattamento andrà ad eseguirsi, ciò al fine di poter comprendere se esso sia legittimo o meno in relazione al diritto dell'Unione e degli Stati membri, tenuto conto in particolare delle eventuali restrizioni che essi potranno apportare a singole parti della disciplina applicabile;
- circa l'intenzione del titolare di trasferire dati personali a un Paese terzo o a un'organizzazione internazionale e circa l'esistenza o l'assenza di una decisione di adeguatezza della Commissione (ossia di una decisione analoga a quella già adottata agli inizi degli anni 2000 per il *c.d. Safe Harbor*, poi in realtà ritenuta illegittima dalla Corte di Giustizia), con il riferimento alle opportune garanzie e relativi mezzi per ottenere una copia di tali dati o il luogo dove essi sono disponibili;
- circa i dati di contatto del responsabile della protezione dei dati, ossia del *c.d. Data Privacy Officer* (per cui rinviamo a seguire).

Il Regolamento introduce altresì un nuovo regime di informativa, che potremmo definire consequenziale al conferimento dei dati e che si pone in abbinamento all'ordinario regime di informativa, generalmente preventivo e, quindi, precedente la raccolta dei dati.

Esso riguarda le seguenti informazioni:

- il periodo di conservazione dei dati personali o i criteri di calcolo temporale;
- il diritto dell'interessato di accesso ai dati ovvero di rettifica o cancellazione o limitazione o opposizione (invero già previsti attualmente per l'Italia dall'art.7 Codice *privacy*), oltre al nuovo "*diritto alla portabilità*" dei dati (per cui rinviamo a seguire);

- il diritto dell'interessato di revocare il consenso in qualsiasi momento;
- il diritto di proporre reclamo a un'autorità di controllo;
- la necessità o meno del trattamento e le conseguenze di un eventuale rifiuto (invero attualmente previsto nell'informativa preventiva ai sensi dell'art.13 Codice *privacy*);
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, con informazioni specifiche sulla logica informatrice del trattamento e sulle conseguenze previste.

Tutta una serie di informazioni ulteriori sono altresì previste per il caso in cui i dati personali non siano ottenuti presso l'interessato, per cui si rinvia nel dettaglio all'art.14 del Regolamento.

I diritti dell'interessato

Tra i diritti dell'interessato, oltre a quelli già previsti attualmente e consolidati dal Regolamento agli artt.15 (diritto di accesso), 16 (diritto di rettifica) e 21 (diritto di opposizione), si segnalano alcune novità introdotte dal Regolamento, ancora in scia alla produzione giurisprudenziale soprattutto della Corte di Giustizia.

> Il Regolamento ha infatti normato specificamente, in primo luogo, il diritto alla cancellazione nella forma del *c.d. diritto all'oblio* (facendo eco al famoso caso pilota Costeja Gonzalez/Google Spain).

Secondo tale previsione l'interessato ha il vero e proprio diritto ad essere "dimenticato" (*right to be forgotten*) qualora i dati personali non siano più necessari rispetto alle finalità per le quali erano stati raccolti o altrimenti trattati, ovvero qualora abbia revocato il consenso e non sussista altro fondamento giuridico per il trattamento, ovvero, infine, nei casi di opposizione al trattamento e insussistenza di altri interessi legittimi, oltre che per l'adempimento di un obbligo legale e infine – ed ecco la peculiare novità – allorquando i dati personali siano stati raccolti relativamente all'offerta di servizi della società dell'informazione (quindi per i trattamenti *on-line*).

Naturalmente tale diritto deve essere soppesato nel bilanciamento degli interessi con altri diritti contrapposti, tra cui ovviamente spicca il diritto alla libertà di espressione e di informazione, oltre all'adempimento degli obblighi legali, ai motivi di interesse pubblico e alle finalità di tutela dei diritti in ambito giudiziario.

L'interessato ha anche il diritto di limitazione del trattamento allorquando egli contesti l'esattezza dei dati personali, per il periodo necessario alle verifiche del caso, ovvero quando il trattamento sia illecito e l'interessato chieda appunto la limitazione in luogo della cancellazione, oppure i dati non servano più alle esigenze del titolare, ma l'interessato abbia invece interesse a limitarli per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

L'ulteriore novità riguarda il diritto alla portabilità dei dati personali, ossia il diritto dell'interessato ad ottenere la loro trasmissione da un titolare a un altro senza impedimenti, allorquando il trattamento sia effettuato con mezzi automatizzati e se tecnicamente fattibile.

Le figure attive nel trattamento dei dati: in particolare il responsabile del trattamento e il responsabile della protezione dei dati (*Data Privacy Officer*)

Il responsabile del trattamento

Il Regolamento mantiene immutata l'attuale configurazione dei soggetti attivi del trattamento, come tali il titolare (ossia il soggetto cui i dati sono conferiti e che ne ha la responsabilità diretta di gestione) e il responsabile (ossia il soggetto che opera detta gestione per conto del titolare), nonché implicitamente anche gli Incaricati (esecutori materiali del trattamento).

La novità riguarda invece le modalità di designazione del responsabile, che deve ora promanare da un contratto, o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, il quale disciplini la materia e la durata del trattamento, la sua natura e finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento e che preveda in particolare che il responsabile:

- tratti i dati personali soltanto su istruzione documentata del titolare del trattamento;
- garantisca che le persone autorizzate al trattamento dei dati personali (gli incaricati) si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adotti tutte le misure richieste;
- assista il titolare del trattamento con misure tecniche e organizzative adeguate, anche nella conformazione e per il rispetto degli obblighi di sicurezza dettati dal Regolamento;
- gestisca il trattamento dopo la cessazione del rapporto, in particolare cancelli o restituisca i dati personali al termine della prestazione;

- comprovi al titolare il rispetto dei propri obblighi.

Come si vede, dall'attuale designazione del Responsabile sostanzialmente unilaterale (prevista per l'Italia dall'art.29 codice *privacy*) si è passati ad una previsione di natura contrattuale, si immagina foriera di contrattazioni economiche e quindi anche di una formazione sempre più professionale e specifica di tale figura.

Il responsabile della protezione dei dati

Da non confondere con il responsabile del trattamento, il Regolamento introduce la nuova figura del responsabile della protezione dei dati, ossia del *c.d. Data Privacy Officer*.

Tale nuova figura deve essere designata sistematicamente quando:

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali sensibili o giudiziari.

Come si può comprendere, il *Data Privacy Officer* (DPO) interessa quindi principalmente o i trattamenti in ambito pubblico (o eseguiti da Enti pubblici o operanti in ambito pubblico) o i trattamenti eseguiti su larga scala con monitoraggio sistematico dei dati.

Il DPO può essere un dipendente o agire sulla base di un contratto di servizi ed essere, quindi, un professionista autonomo.

Per i gruppi imprenditoriali il DPO può essere anche nominato nella medesima persona, purché sia accessibile facilmente dai vari stabilimenti. Analogamente, per l'ambito pubblico un unico DPO può essere designato per più autorità/Enti.

Negli altri casi la nomina del DPO è facoltativa, a meno che gli Stati membri non deroghino anche in questo caso con discipline nazionali più restrittive.

Nella sostanza dei compiti, delle funzioni e delle responsabilità, il DPO deve essere coinvolto in tutte le questioni privacy da parte del titolare/responsabile, e in particolare deve:

- informare e fornire consulenza al titolare o al responsabile nonché agli incaricati in merito alla disciplina *privacy*, pertanto nella veste di "formatore" interno oltre che di consulente specifico;
- sorvegliare l'osservanza della normativa;
- 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, fungendo da punto di contatto.

I registri delle attività di trattamento

Venendo alle modalità pratiche di protezione, il Regolamento introduce l'adozione dei registri delle attività di trattamento, che ogni titolare (o suoi rappresentanti) deve tenere e che devono avere ad oggetto:

- il nome e i dati di contatto del titolare e/o del contitolare del trattamento, del suo rappresentante, del titolare del trattamento e del responsabile della protezione dei dati (DPO);
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari per il caso di comunicazione dei dati, anche di tipo internazionale;
- gli eventuali trasferimenti verso aree *extra* Ue;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

In sostanza, il registro assomiglia molto a un DPS sintetico, ossia alla sintesi di quel famoso Documento Programmatico sulla Sicurezza che era stato introdotto con la vecchia disciplina e che era rimasto in vigore (per l'Italia) fino al 2012.

Analogo registro deve essere tenuto dal responsabile del trattamento o dai suoi rappresentanti.

Tali registri possono essere tenuti anche in formato elettronico.

La valutazione d'impatto sulla protezione dei dati personali

Per quanto concerne invece specificamente i trattamenti con uso di nuove tecnologie che, alla luce della natura, dell'oggetto, del contesto e delle finalità del trattamento, possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Regolamento richiede al titolare di effettuare, preliminarmente al trattamento, una valutazione di impatto sulla protezione dei dati personali, consultando in proposito il DPO.

Detto incombente è richiesto in particolare quando:

- vi sia una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, su cui si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- il trattamento sia eseguito su larga scala su categorie particolari di dati sensibili o giudiziari;
- vi sia una sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La valutazione di impatto deve contenere almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità, comprese l'interesse legittimo perseguito;
- 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 dettato normativo.

Anche in questo caso il documento si avvicina molto per funzioni e specifiche al vecchio DPS, con qualche assonanza anche al regolamento richiesto per il trattamento dei dati sensibili eseguito da Enti pubblici per il perseguimento di interessi pubblici.

Codici di condotta e certificazioni di corretto trattamento

Il Regolamento prevede (e gli Stati, i garanti e la Commissione devono incoraggiare) l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione della disciplina, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle PMI.

Tali codici di condotta possono essere elaborati dalle associazioni rappresentative e avere ad oggetto informazioni e istruzioni per la corretta applicazione del Regolamento, ad esempio con riferimento al trattamento corretto e trasparente dei dati, alla raccolta dei dati personali e alla loro pseudonimizzazione, alle informazioni da fornire agli interessati e all'esercizio dei loro diritti, alle misure di sicurezza, alla disciplina del *c.d. data breach* (notifica della violazione dei dati personali), al trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali, alle procedure stragiudiziali di composizione delle controversie.

In stretta relazione all'adozione dei codici di condotta, il Regolamento prevede anche (e gli Stati, i garanti e la Commissione devono ulteriormente incoraggiare) l'istituzione di meccanismi di certificazione della protezione dei dati, nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità normativa dei trattamenti effettuati dai titolari e dai responsabili, tenute sempre in considerazione le esigenze specifiche delle PMI.

La certificazione può essere rilasciata da organismi specificamente autorizzati, per un periodo massimo di tre anni, rinnovabile alle stesse condizioni purché continuino ad essere soddisfatti i requisiti pertinenti. Tali organismi di certificazione, per poter operare, devono essere accreditati dall'autorità di controllo o dall'organismo nazionale di accreditamento designato in forza del regolamento (CE) n.765/08.

Autorità di controllo e regime sanzionatorio

Ogni Stato membro deve disporre che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del Regolamento nella veste di "autorità di controllo": trattasi in sostanza dei Garanti nazionali.

Alle autorità di controllo sono demandate le funzioni di sorveglianza, promozione, consulenza, gestione dei reclami, incoraggiamento ed esame dei codici di condotta, indagine, ingiunzione e gli altri poteri di natura accertativa e sanzionatoria, il tutto in cooperazione con le altre autorità e con il comitato europeo per la protezione dei dati, istituito quale organismo dell'Unione dotato di personalità giuridica.

Il regime sanzionatorio è più stringente rispetto all'attuale previsione normativa, avendo specificamente funzione effettiva e dissuasiva.

Sono previste infatti, tra le altre, varie sanzioni amministrative non pecuniarie e pecuniarie, espresse queste ultime non solo in termini nominali, ma anche in misura proporzionale rispetto al fatturato, oltre a ordinarie regole di responsabilità e di accesso al diritto al risarcimento degli interessati lesi da illeciti trattamenti e da altre violazione delle norme del Regolamento.

Tornando alle sanzioni pecuniarie si menziona un esempio per tutti: la violazione delle disposizioni inerenti i principi di base del trattamento, comprese le condizioni relative al consenso, ovvero i diritti degli interessati, è soggetta a sanzioni amministrative pecuniarie fino a € 20.000.000,00 o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Ricorsi

Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, il Regolamento prevede che l'interessato che si ritenga leso nei propri diritti alla protezione dei dati personali possa proporre reclamo all'autorità di controllo dello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione.

Fatto sempre salvo ogni altro ricorso amministrativo o stragiudiziale, il Regolamento dispone altresì che ogni persona fisica o giuridica ha inoltre il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda, al pari dell'interessato che ha analogo diritto qualora l'autorità di controllo competente non tratti il reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto.

Ogni interessato ha infine il diritto di proporre un ricorso giurisdizionale davanti alle autorità giurisdizionali dello Stato membro in cui il titolare o il responsabile ha uno stabilimento, ovvero, in alternativa, dello Stato membro in cui l'interessato risiede abitualmente, qualora ritenga che i propri diritti alla protezione dei dati personali siano stati violati a seguito di un trattamento.