Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo I

Avv. Michele Iaselli

M1.1.Ambiti di applicazione della norma

La privacy è un termine inglese traducibile all'incirca con riservatezza, è il diritto alla riservatezza delle informazioni personali e della propria vita privata: *the right to be let alone* (lett. "il diritto di essere lasciati in pace"), secondo la formulazione del giurista statunitense Louis Brandeis che fu probabilmente il primo al mondo a formulare una legge sulla riservatezza.

In realtà comunemente per privacy si intende il diritto della persona di impedire che le informazioni che la riguardano vengano trattate da altri, a meno che il soggetto non abbia volontariamente prestato il proprio consenso.

Con l'introduzione dei primi strumenti tecnologici gli studiosi si sono posti il problema della necessità o meno di una specifica tutela avuto riguardo al rapporto tra "riservatezza-computer"; l'impiego dell'elaboratore elettronico, infatti, consente di impadronirsi ed archiviare informazioni che riguardano l'individuo, comprese quelle della sua vita privata sottoponendolo, così, ad una nuova forma di dominio, che si potrebbe chiamare "*il potere informatico*".

Il "*right to privacy*" ha quindi acquistato un nuovo significato ed una nuova ampiezza, che non poteva avere un secolo fa: questo ora consiste nel diritto, riconosciuto al cittadino, *di esercitare anche un controllo sull'uso dei propri dati personali inseriti in un archivio elettronico*.

Il diritto alla riservatezza, per effetto della nuova dimensione acquisita, non viene, infatti, più inteso in un senso puramente negativo, come facoltà di ripulsa delle intromissioni di estranei nella vita privata, o di rifiutare il consenso alla diffusione di informazioni sul proprio conto, di rinuncia alla partecipazione nella vita sociale; ma in senso positivo, come affermazione della libertà e dignità della persona, e come potere di limitare il potere informatico, controllandone i mezzi ed i fini.

e dal punto di vista normativo?

Da un punto di vista normativo già la Convenzione europea dei diritti dell'uomo, all'art. 8, stabiliva che non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui.

Oltre che negli Accordi di Schengen, il concetto è stato riportato nella Carta dei diritti fondamentali dell'Unione europea all'art. 8, che recita:

Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.

Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.

Per quanto attiene alla legislazione italiana, al di là della normativa fondamentale, i fondamenti costituzionali sono ravvisabili negli art. 14, 15 e 21 Cost., rispettivamente riguardanti il domicilio, la libertà e segretezza della corrispondenza, e la libertà di manifestazione del pensiero; ma si può fare anche riferimento all'art. 2 Cost., incorporando la riservatezza nei *diritti inviolabili dell'uomo*.

La nuova dimensione della privacy

Il progressivo sviluppo delle comunicazioni elettroniche ha determinato la crescita esponenziale di nuovi servizi e tecnologie. Se ciò ha comportato, da un lato, indiscutibili vantaggi in termini di semplificazione e rapidità nel reperimento e nello scambio di informazioni fra utenti della rete Internet, dall'altro, ha provocato un enorme incremento del numero e delle tipologie di dati personali trasmessi e scambiati, nonché dei pericoli connessi al loro illecito utilizzo da parte di terzi non autorizzati.

Si è così maggiormente diffusa l'esigenza di assicurare una forte tutela dei diritti e delle libertà delle persone, con particolare riferimento all'identità personale e alla vita privata degli individui che utilizzano le reti telematiche.

Lo sviluppo di moderne tecnologie e di nuovi servizi di comunicazione elettronica ha reso, quindi, necessario un ulteriore adeguamento della normativa sulla protezione dei dati personali in ambito italiano ed internazionale.

Sul punto, in Italia, il Codice per la protezione dei dati personali ha compiuto una ricognizione innovativa delle preesistenti norme sul trattamento dei dati nel settore delle telecomunicazioni (d.lgs. n. 171/1998, come modificato dal d.lgs. n. 467/2001), completando nello stesso tempo il recepimento della direttiva n. 2002/58/CE, relativa alla tutela della vita privata nel settore delle comunicazioni elettroniche.

La disciplina introdotta in materia dal Codice, riproponendo un criterio già presente nella normativa comunitaria, adotta un approccio "tecnologicamente neutro", ossia valido ed applicabile a tutte le forme di comunicazione elettronica a prescindere dal mezzo tecnico utilizzato.

Ma tale processo di adeguamento normativo ha compiuto un altro passo importante con il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016.

Come è noto il Regolamento UE 2016/679 (GDPR) 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 e che abroga la direttiva 95/46/CE è stato pubblicato il 4 maggio 2016 nella Gazzetta Ufficiale dell'Unione Europea.

L’iter di questo Regolamento, che è entrato direttamente in vigore nei singoli Stati membri dell'UE, è stato molto sofferto e sono passati ben quattro anni dalla prima proposta della Commissione Europea. Un testo inizialmente molto severo è stato reso più “digeribile” nel corso degli anni, anche se rimangono confermati i principi fondamentali del provvedimento europeo.

Perché un Regolamento Europeo?

La necessità di emanare un Regolamento Europeo in materia di privacy nasce dalla continua evoluzione degli stessi concetti di privacy e protezione dei dati personali e quindi della relativa tutela dovuta principalmente alla diffusione del progresso tecnologico.

Originariamente la direttiva 95/46/CE, pietra angolare nell'impianto della vigente normativa dell'UE in materia di protezione dei dati personali, è stata adottata nel 1995 con due obiettivi: salvaguardare il diritto fondamentale alla protezione dei dati e garantire la libera circolazione dei dati personali tra gli Stati membri.

Successivamente incalzanti sviluppi tecnologici hanno allontanato le frontiere della protezione dei dati personali. La portata della condivisione e della raccolta di dati è aumentata in modo vertiginoso.

La tecnologia attuale consente alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività e, sempre più spesso, gli stessi privati rendono pubbliche sulla rete mondiale informazioni personali che li riguardano. Le nuove tecnologie non hanno trasformato solo l'economia, ma anche le relazioni sociali.

È diventato, quindi, necessario instaurare un quadro giuridico più solido e coerente in materia di protezione dei dati nell'Unione che, affiancato da efficaci misure di attuazione, consentirà lo sviluppo dell'economia digitale nel mercato interno, garantirà alle persone fisiche il controllo dei loro dati personali e rafforzerà la certezza giuridica e operativa per i soggetti economici e le autorità pubbliche.

M1.2 Principi Generali

Trasparenza

Accountability

Privacy by design e by default

L'art. 3 del Regolamento rivede la concezione tradizionale del principio di stabilimento del territorio e sancisce che il Regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento 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.

Inoltre il Regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione effettuato da un titolare del trattamento o responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato, oppure
b) il controllo del loro comportamento, quest'ultimo inteso all'interno dell'Unione europea.

Infine il Regolamento si applica anche al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto nazionale di uno Stato membro in virtù del diritto internazionale pubblico.

M1.3 Liceità del trattamento

Principi da applicare al trattamento dei dati personali

L'art. 5 del Regolamento ribadisce i classici principi da applicare al trattamento dei dati personali già propri della precedente normativa e cioè che i dati devono essere:

a) trattati in modo lecito, equo e trasparente nei confronti dell'interessato ("liceità, equità e trasparenza");

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità ("limitazione della finalità");

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");

d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; ("limitazione della conservazione");

f) trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza").

Altro principio di fondamentale importanza ribadito nel Regolamento è quello di liceità e l'art. 6 sancisce che il trattamento dei dati personali è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali prese su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) 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;
f) 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. Ciò non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

M1.4 Le categorie di dati personali

Gli artt. 9 e 10 del Regolamento sulla scorta di quanto già determinato dalla precedente normativa individuano rispettivamente i dati sensibili (e non solo) ed i dati giudiziari.

L’art. 9 parte dalla premessa del divieto di trattamento dei dati personali che rivelino l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l’appartenenza sindacale, come pure trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona o dati relativi alla salute o alla vita sessuale e all'orientamento sessuale.

Tale divieto, da considerare, quindi, come principio di carattere generale, non si applica quando ricorrono determinati casi previsti dalla disposizione e cioè quando:
a) l'interessato ha prestato il proprio consenso;
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri;
h) il trattamento è 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 sulla base del diritto dell'Unione o degli Stati membri;
i) il trattamento è 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, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;
j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

L’art. 10, invece, dispone che il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

M1.5 Informazioni e consenso

Il principio di Trasparenza

(art. 12)

Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano facilmente accessibili e di facile comprensione e che sia utilizzato un linguaggio semplice e chiaro. Ciò è particolarmente utile in situazioni quali la pubblicità on line, in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se vengono raccolti dati personali, da chi e a quale scopo. Dato che i minori necessitano di una protezione specifica, quando il trattamento dati li riguarda specificamente, qualsiasi informazione e comunicazione deve utilizzare il linguaggio semplice e chiaro che un minore possa capire facilmente.

Si fa, inoltre, riferimento in particolare all'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento equo e trasparente con riguardo agli interessati e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano.

In particolare, sempre nel rispetto del principio di trasparenza ed avuto riferimento alla Rete, viene favorito l'utilizzo dei c.d. formati multistrato. Difatti, le politiche in materia di protezione dei dati sono documenti complessi che contengono una grande quantità di informazioni orientate a situazioni specifiche.

L'obiettivo delle comunicazioni multistrato consiste nel contribuire a migliorare la qualità delle informazioni sulla protezione dei dati ricevute focalizzando ciascun strato sulle informazioni di cui l'interessato necessita per comprendere la propria posizione e prendere decisioni. Di conseguenza, l'interessato può con un'occhiata alle semplici icone scoprire se e in quale modo i propri dati vengono utilizzati.

In virtù del principio di trasparenza l'art. 12 del Regolamento sancisce che il titolare del trattamento debba adottare misure appropriate per fornire all'interessato tutte le informazioni necessarie e le comunicazioni relative al trattamento dei dati personali in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, se del caso in formato elettronico. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Nello specifico gli artt. 13 e 14 elencano le informazioni che bisogna fornire all'interessato.

L'art. 13 prevede che in caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:
a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione……

Inoltre sempre l'art. 13 chiarisce che nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento equo e trasparente:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali……..;

c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il diritto di proporre reclamo a un'autorità di controllo;

e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto.

f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4…….

L’art. 14, chiarisce che qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le medesime informazioni di cui all’art. 13 ad eccezione del punto d) dove al posto dei legittimi interessi perseguiti dal titolare del trattamento o da terzi nel caso in cui il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), dovrà indicare le categorie di dati personali in questione.

Anche le ulteriori informazioni che il titolare dovrà fornire all'interessato per garantire un trattamento equo e trasparente sono sostanzialmente analoghe a quelle di cui all'art. 13.

Se il consenso dell'interessato è espresso nel contesto di una dichiarazione scritta che riguarda anche altre materie, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

Nessuna parte della dichiarazione cui l'interessato abbia dato il consenso e che costituisca una violazione del Regolamento è vincolante.

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento.
La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca.
Prima di esprimere il proprio consenso, l'interessato viene informato di ciò.
Il consenso è revocato con la stessa facilità con cui è accordato.

Particolari condizioni sono poi dettate dall'art. 8 del Regolamento nell'interesse dei minori il quale chiarisce che il trattamento di dati personali di minori al di sotto dei 16 anni - o, se previsto dal diritto degli Stati membri, di un'età inferiore ma non al di sotto di 13 anni - è lecito soltanto se e nella misura in cui tale consenso è espresso o autorizzato dal titolare della responsabilità genitoriale sul minore.

Il 12 dicembre 2017 il Gruppo Articolo 29 (WP29) ha pubblicato una bozza di linee guida in materia di consenso dell'interessato ora in consultazione pubblica. Il documento vuole fornire maggiori indicazioni a livello interpretativo delle problematiche relative al consenso, anche affiancando ai concetti le esemplificazioni più adatte o ricorrenti nei casi concreti.

L'articolo 4, paragrafo 11, stabilisce che il consenso dell'interessato, in modo inequivocabile, deve essere:

- libero;
- specifico;
- informato.

Il consenso deve essere innanzitutto libero: se l'interessato non compie una scelta reale e si sente obbligato a prestare il proprio consenso anche per evitare conseguenze negative nel caso rifiutasse, allora il consenso non potrà essere considerato come valido.
Per esempio se il consenso è inserito in una parte non negoziabile di termini e condizioni si presume che lo stesso non sia stato fornito liberamente.

Inoltre il consenso non potrà considerarsi libero se utilizzato per giustificare molteplici trattamenti: se un servizio comporta più operazioni di elaborazione o più scopi, il consenso deve essere dato liberamente per ciascuno. Gli interessati devono essere in grado di scegliere per quali scopi acconsentono il trattamento.
Il Gruppo di lavoro individua tre componenti per garantire questo requisito:
- indicazione esatta dello scopo, come salvaguardia contro l'abuso di trattamento;
- granularità nelle richieste di consenso;
- chiara separazione delle informazioni relative all'ottenimento del consenso per le attività di elaborazione dati da informazioni su altri argomenti.

Senza informazioni accessibili, gli interessati non possono prendere decisioni informate e quindi, chiarisce il WP29 "il controllo dell'utente diventerebbe illusorio e il consenso non valido per l'elaborazione".
Il Gruppo ha identificato sei categorie di informazioni minime necessarie:
- l'identità del titolare;
- lo scopo di ciascuna delle operazioni di trattamento per le quali è richiesto il consenso;
- quale tipo di dati saranno raccolti e trattati;
- l'esistenza del diritto di revocare il consenso;
- informazioni sull'uso dei dati per le decisioni basate esclusivamente sull'elaborazione automatica (inclusa la profilazione);
- se il consenso riguarda trasferimenti, circa i possibili rischi di trasferimenti di dati verso paesi terzi in assenza di una decisione di adeguatezza / garanzie appropriate.

Nelle situazioni, poi, in cui emergono "gravi rischi per la protezione dei dati", è richiesto un consenso esplicito: un diverso livello di consenso rispetto a quello ordinario appena sopra descritto. Ci si riferisce in particolare ai dati relativi all'articolo 9 (categoria speciale), ai trasferimenti verso Paesi o organizzazioni privi di una decisione di adeguatezza e al processo decisionale individuale automatizzato (compresa la profilazione).

Il Gruppo di lavoro suggerisce per esempio che il consenso dato attraverso una espressa e formale dichiarazione scritta (firmata dall'interessato) è da considerarsi esplicito.
Sono previste altre modalità, in particolare nel contesto elettronico che includono il coinvolgimento dell'interessato: compilare un modulo elettronico; inviare una mail; caricare un documento scansionato con firma; registrare una dichiarazione orale, o verificare il consenso tramite un processo di autenticazione a due fasi (come un'e-mail seguita da un messaggio SMS).

Il gruppo di lavoro fornisce anche importanti indicazioni in merito al mantenimento della prova del consenso.
I responsabili ed i titolari del trattamento terranno prova del consenso per tutta la durata dell'attività connessa all'elaborazione dei dati; quando questa termina la prova del consenso deve essere mantenuta soltanto al fine di adempiere agli obblighi di legge o per stabilire, esercitare o difendere i diritti legali.

Infine, secondo i garanti europei, il consenso pre-Regolamento conforme alla legge nazionale non deve essere necessariamente riformulato e riottenuto. Il Gruppo di lavoro riconosce che "il consenso … ottenuto fino ad oggi continua ad essere valido nella misura in cui è in linea con le condizioni stabilite nel GDPR".

M1.6 Diritti dell'interessato

Diritto di accesso

Diritto di rettifica

Diritto di limitazione

Diritto di opposizione

Diritto all'oblio

Diritto alla portabilità

Diritto di accesso dell'interessato

Nel Regolamento ritroviamo anche il diritto di accesso dell'interessato che viene disciplinato dall'art. 15 laddove viene sancito che l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, se è in corso tale trattamento, l'accesso ai dati ed a determinate informazioni.

Tali informazioni sono:
a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare questo periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo ad un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata.

Il titolare del trattamento deve fornire all'interessato le informazioni relative all'azione intrapresa riguardo ad una richiesta di accesso, ai sensi degli articoli da 15 a 20, senza ingiustificato ritardo e al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato per un massimo di altri due mesi, se necessario, tenuto conto della complessità della richiesta e del numero di richieste.

Qualora si applichi la proroga, l'interessato è informato dei motivi del ritardo entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta in formato elettronico, le informazioni sono fornite, ove possibile, in formato elettronico, salvo indicazione diversa dell'interessato.
Se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.

Inoltre gli artt. 16, 17 e 18 del Regolamento prevedono ulteriori importanti diritti dell'interessato che già sono pacifici nel nostro ordinamento, quali il diritto di rettifica, il diritto di cancellazione e il diritto di limitazione del trattamento, quando naturalmente ricorrono determinati casi.

Il diritto di rettifica

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.
Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Diritto di limitazione di trattamento

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Se il trattamento è limitato i dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

Diritto di opposizione

Viene ribadito nel Regolamento anche il diritto di opposizione dell'interessato, sempre nell'ottica della nuova dimensione acquisita dal diritto alla riservatezza, che, non viene, infatti, più inteso in un senso puramente negativo, come facoltà di ripulsa delle intromissioni di estranei nella vita privata, o di rifiutare il consenso alla diffusione di informazioni sul proprio conto, di rinuncia alla partecipazione nella vita sociale; ma in senso positivo, come affermazione della libertà e dignità della persona, e come potere di limitare il potere informatico, controllandone i mezzi ed i fini.

L'art. 21 attribuisce però a tale diritto una rilevanza autonoma sancendo che l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento non tratta più i dati personali salvo che egli dimostri l'esistenza di motivi legittimi preminenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Inoltre qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

Qualora, poi, i dati personali siano trattati per finalità di ricerca scientifica e storica o per finalità statistiche a norma dell'articolo 83, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento dei dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Processo decisionale automatizzato

Anche nel Regolamento il legislatore pone una particolare attenzione al trattamento automatizzato dei dati personali che possa sfociare in decisioni che sono proprie della macchina e non dell'uomo.
L'art. 22, quindi, ribadisce come principio generale che l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida allo stesso modo significativamente sulla sua persona.

Tale disposizione non sia applica quando la decisione:
a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, oppure
b) sia autorizzata dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato, oppure
c) si basi sul consenso esplicito dell'interessato.

M1.7 Diritto all'oblio (art. 17)

Ogni persona deve avere il diritto di rettificare i dati personali che la riguardano e il "diritto alla cancellazione e all'oblio", se la conservazione di tali dati non è conforme al regolamento.

In particolare, l'interessato deve avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al Regolamento.

Tale diritto è particolarmente rilevante se l'interessato ha dato il consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare questo tipo di dati personali, in particolare da Internet.

Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica e storica o finalità statistiche o per accertare, esercitare o difendere un diritto in sede giudiziaria.

Per rafforzare il "diritto all'oblio" nell'ambiente on line, è opportuno che il diritto di cancellazione sia esteso in modo da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i responsabili del trattamento che stanno trattando tali dati affinché cancellino qualsiasi link verso tali dati personali o copia o riproduzione di detti dati.

Il diritto all'oblio è un concetto tornato prepotentemente alla ribalta in ambito internazionale e principalmente europeo con l'avvento della Rete e diverse sono le definizioni fornite dalla dottrina.

Secondo la nota enciclopedia della Rete Wikipedia "il diritto all'oblio è una particolare forma di garanzia che prevede la non diffondibilità di precedenti pregiudizievoli, per tali intendendosi propriamente i precedenti giudiziari di una persona". In base a questo principio, non è legittimo diffondere dati circa condanne ricevute o comunque altri dati sensibili di analogo argomento, salvo che si tratti di casi particolari ricollegabili a fatti di cronaca. Questa garanzia è variamente riconosciuta ed applicata a seconda degli ordinamenti.

Secondo un'altra impostazione dottrinaria (Finocchiaro) il diritto all'oblio è il diritto di un individuo ad essere dimenticato, o meglio, a non essere più ricordato per fatti che in passato furono oggetto di cronaca. Il suo presupposto è che l'interesse pubblico alla conoscenza di un fatto è racchiuso in quello spazio temporale necessario ad informarne la collettività, e che con il trascorrere del tempo si affievolisce fino a scomparire.

Secondo altri (Palermo) il diritto all'oblio è quindi la naturale conseguenza di una corretta e logica applicazione dei principi generali del diritto di cronaca. Come non va diffuso il fatto la cui diffusione (lesiva) non risponda ad un reale interesse pubblico, così non va riproposta la vecchia notizia (lesiva) quando ciò non sia più rispondente ad una attuale esigenza informativa.

Il diritto all'oblio secondo Corasaniti è il diritto a non restare indeterminatamente esposti ai danni ulteriori che la reiterata pubblicazione di una notizia può arrecare all'onore e alla reputazione, salvo che, per eventi sopravvenuti, il fatto precedente ritorni di attualità e rinasca un nuovo interesse pubblico all'informazione. «Non è tanto inibire il dato – afferma Corasaniti – quanto la circolazione non autorizzata del dato».

Altra dottrina più recente (SCORZA) sostiene che per diritto all'oblio, si intende il diritto a che nessuno riproponga nel presente un episodio che riguarda la nostra vita passata e che ciascuno di noi vorrebbe, per le ragioni più diverse, rimanesse semplicemente affidato alla storia.

Un concetto più moderno ed attuale del diritto all'oblio in rete che ha portato il noto studioso e blogger Peter Fleisher ad individuare gli 8 punti cardinali per la privacy online:

1. Se posto qualcosa sul web, ho poi il diritto di cancellarlo?
2. Se qualcuno copia il mio contenuto, ho il diritto di cancellarlo anche dall'altro sito?
3. Se qualcun altro posta qualcosa su di me, ho il diritto di cancellarlo?
4. Le piattaforme online hanno l'obbligo di cancellare le informazioni personali?
5. Se si dopo quanto tempo?
6. Internet deve imparare a dimenticare?
7. Internet deve essere ripensato per essere più vicino alla mente umana?
8. Chi ha il compito di decidere cosa può essere ricordato e cosa deve essere dimenticato?

L'oblio è un diritto che va oltre la tutela della privacy e che, a oggi, non trova legittimazione nell'ordinamento nazionale ed europeo.
Frutto di elaborazioni dottrinarie, giurisprudenziali e principalmente delle Autorità Garanti europee è da intendersi quale diritto dell'individuo ad essere dimenticato; diritto che mira a salvaguardare il riserbo imposto dal tempo ad un notizia già resa di dominio pubblico.
In Italia assumono rilevanza alcune decisioni della Corte di Cassazione come Cass., 9/4/1998, n. 3679; Cass., 25/6/2004, n. 11864; Cass., 05/04/2012, n. 5525; Cass. 26/5/2013 n. 16111 e da ultimo Cass. 24/6/2016, n. 13161.

Nonostante la stretta contiguità tra riservatezza e oblio, i due concetti però non coincidono. Il diritto all'oblio può essere considerato in qualche misura speculare rispetto al diritto alla riservatezza, dal momento che il problema del diritto all'oblio si pone relativamente a situazioni che, per loro natura, nel momento in cui si sono verificate, non rientravano nell'ambito della tutela della riservatezza.

Il problema del diritto all'oblio nasce storicamente in rapporto all'esercizio del diritto di cronaca giornalistica. Difatti, presupposto perché un fatto privato possa divenire legittimamente oggetto di cronaca è l'interesse pubblico alla notizia. La collettività va informata con tempestività, in modo da poter conoscere l'accaduto in tempo reale e con completezza, così da fornirle una chiara visione del fatto.

Ma una volta che del fatto il pubblico sia stato informato con completezza, cessa l'interesse pubblico in quanto la collettività ha ormai acquisito il fatto. Non vi è più una notizia. Riproporre l'accadimento sarebbe inutile, poiché non vi sarebbe più un reale interesse della collettività da soddisfare. Non solo inutile per la collettività, ma anche dannoso per i protagonisti in negativo della vicenda.

Il diritto all'oblio è quindi la naturale conseguenza di una corretta e logica applicazione dei principi generali del diritto di cronaca.

Nel testo del Regolamento il diritto all'oblio è recepito dall'art. 17 dove viene sancito che l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato ritira il consenso su cui si basa il trattamento e non sussiste altro motivo legittimo per trattare i dati;

c) l'interessato si oppone al trattamento dei dati personali e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;

d) i dati sono stati trattati illecitamente;

e) i dati devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento;

f) i dati sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.

M1.8 Diritto alla portabilità (art. 20)

L’art. 20 del Regolamento parla di diritto alla portabilità dei dati per cui l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti ad un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e

b) il trattamento sia effettuato con mezzi automatizzati.

Inoltre, nell'esercitare i propri diritti relativamente alla portabilità dei dati l'interessato ha il diritto di ottenere la trasmissione diretta dei dati da un titolare del trattamento all'altro, se tecnicamente fattibile.

Il diritto dell'interessato di trasmettere o ricevere dati personali che lo riguardano non comporta l'obbligo per i titolari del trattamento di adottare o mantenere sistemi di trattamento dei dati tecnicamente compatibili.
Qualora un certo insieme di dati personali riguardi più di un interessato, il diritto di ricevere i dati non deve pregiudicare i diritti degli altri interessati in ottemperanza del Regolamento.

Sul diritto alla portabilità sono state elaborate dal Gruppo di lavoro ex art. 29 delle linee guida adottate il 13 dicembre 2016 ed emendate il 5 aprile 2017.

Nel parere si offrono indicazioni sull'interpretazione e sull'attuazione del diritto alla portabilità dei dati introdotto dal Regolamento europeo.
L'obiettivo è analizzare questo nuovo diritto e il suo ambito di applicazione, chiarendo le condizioni di applicabilità alla luce della base legale del trattamento (consenso dell'interessato o adempimento di obblighi contrattuali) nonché nell'ottica della limitazione relativa ai dati personali forniti dall'interessato stesso.

Innanzitutto si chiarisce che il nuovo diritto alla portabilità intende promuovere il controllo degli interessati sui propri dati personali, facilitando la circolazione, la copia o la trasmissione dei dati da un ambiente informatico all'altro (che si tratti dei propri sistemi, dei sistemi di soggetti terzi fidati, o di quelli di un diverso titolare del trattamento).

Le componenti del diritto alla portabilità

Il diritto di ricevere dati personali

In primo luogo, la portabilità dei dati comprende il diritto dell'interessato di ricevere un sottoinsieme dei dati personali che lo riguardano trattati da un titolare, e di conservarli in vista di un utilizzo ulteriore per scopi personali. Tale conservazione può avvenire su un supporto personale o su un cloud privato, senza comportare necessariamente la trasmissione dei dati a un altro titolare.
In questo senso, il diritto alla portabilità costituisce un'integrazione del diritto di accesso.

Il diritto di trasmettere dati personali da un titolare del trattamento a un altro titolare del trattamento

In secondo luogo, l'art. 20, primo paragrafo, dà agli interessati il diritto di trasmettere dati personali da un titolare del trattamento a un altro titolare del trattamento "senza impedimenti".
In questo senso, il considerando 68 promuove lo sviluppo di formati interoperabili da parte dei titolari così da consentire la portabilità dei dati, ma non configura un obbligo in capo ai titolari stessi di introdurre o mantenere sistemi di trattamento tecnicamente compatibili.

In sostanza, questa componente del diritto alla portabilità configura per gli interessati la possibilità non soltanto di ottenere e riutilizzare i dati forniti a un titolare, bensì anche di trasmettere questi dati a un diverso fornitore di servizi.

Titolarità del trattamento

Diritto alla portabilità e altri diritti degli interessati

Necessità dell'informativa

Qual è la tempistica per ottemperare a una richiesta di portabilità?

E’ possibile opporre diniego a una richiesta di portabilità o addebitare un contributo per ottemperarvi?

Quali sono gli strumenti che il titolare dovrebbe predisporre al fine di fornire i dati richiesti?

L'art. 20, paragrafo 2, del Regolamento prevede che gli interessati hanno il diritto di trasmettere i dati a un diverso titolare senza impedimenti da parte del titolare cui li hanno forniti.
Gli impedimenti in questione possono consistere in ostacoli di natura giuridica, tecnica o finanziaria con cui il titolare evita o rallenta l'accesso, la trasmissione o il riutilizzo da parte dell'interessato o di un diverso titolare.

Sul piano tecnico, i titolari dovrebbero esplorare e valutare due approcci diversi e complementari per mettere a disposizione degli interessati o di altri titolari dati che siano portabili:

- trasmissione diretta dell'intero insieme di dati portabili (o di più estratti di parti del set complessivo di dati);
- utilizzo di uno strumento automatizzato che consenta l'estrazione dei dati pertinenti.

M1.9 Privacy by design
M1.10 Privacy by default

Il principio della privacy by design richiede che la tutela dei diritti e delle libertà degli interessati con riguardo al trattamento dei dati personali comporti l'attuazione di adeguate misure tecniche e organizzative al momento sia della progettazione che dell'esecuzione del trattamento stesso, onde garantire il rispetto delle disposizioni del Regolamento.

Il principio della privacy by design prevede che la protezione dei dati sia integrata nell'intero ciclo di vita della tecnologia, dalla primissima fase di progettazione fino alla sua ultima distribuzione, all'utilizzo e all'eliminazione finale.
Il principio della privacy by default prevede che le impostazioni di tutela della vita privata relative ai servizi e prodotti rispettino i principi generali della protezione dei dati, quali la minimizzazione dei dati e la limitazione delle finalità.

La privacy by design può essere definita la nuova dimensione della privacy che trae le sue origini dall'innovazione tecnologica e dal progresso delle comunicazioni elettroniche.
In particolare, con riferimento alla tecnologia dell'informazione si afferma, come già evidenziato, che la tecnologia non può costituire una minaccia per la privacy, ma un ausilio per la riduzione dei rischi. Per le pratiche commerciali responsabili, viene evidenziato come la privacy non va interpretata come un onere, un costo che appesantisce l'attività imprenditoriale ma, al contrario, come un vantaggio per una migliore competitività.

Il principio è recepito dall'art. 25 del Regolamento il quale sancisce che tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare i principi di protezione dei dati, quali la minimizzazione, in modo efficace e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati.

Lo stesso titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, di default, solo i dati personali necessari per ogni specifica finalità del trattamento; ciò vale per la quantità dei dati raccolti, l'estensione del trattamento, il periodo di conservazione e l'accessibilità. In particolare dette misure garantiscono che, di default, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Le figure soggettive del mondo della protezione dei dati personali

M1.11 Titolare del trattamento: obblighi e responsabilità

Il titolare del trattamento (art. 4) è definito come la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità, le condizioni e i mezzi del trattamento sono determinati dal diritto dell'Unione o dal diritto di uno Stato membro, il titolare del trattamento o i criteri specifici applicabili alla sua nomina possono essere designati dal diritto dell'Unione o dal diritto dello Stato membro.

Nell'ambito dell'organizzazione dell'ente o dell'azienda il titolare del trattamento rimane una figura fondamentale e tale figura assume una rilevanza tale da coincidere con lo stesso concetto di titolare del trattamento di cui al nostro codice. Egli é tenuto ad adottare politiche e attuare misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme alla normativa.

Molte di queste ultime misure sono nuove rispetto alla precedente normativa. Difatti oltre alla legittima conservazione della documentazione ed all'attuazione dei necessari requisiti di sicurezza dei dati, è prevista l'esecuzione della valutazione d'impatto sulla protezione dei dati (concetto del tutto nuovo), il rispetto dei requisiti di autorizzazione preventiva o di consultazione preventiva dell'autorità di controllo e del responsabile della protezione dei dati, la designazione di un responsabile della protezione dei dati e la definizione di informazioni e comunicazioni trasparenti da fornire all'interessato.

Il titolare del trattamento deve essere in grado di dimostrare l'efficacia di tali misure e ciò nel rispetto dell'importante principio di accountability che viene recepito dal Regolamento europeo. Per lo stesso motivo il Regolamento intende definire una responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che abbia effettuato direttamente o altri abbia effettuato per suo conto. In particolare, il titolare del trattamento deve garantire ed essere in grado di dimostrare la conformità di ogni trattamento con il Regolamento.

Altra importante novità connessa alla figura del titolare del trattamento è il recepimento dei principi della privacy by design per cui lo stesso titolare tenuto conto dell'evoluzione tecnica e dei costi di attuazione, deve mettere in atto adeguate misure e procedure tecniche e organizzative in modo tale che il trattamento sia conforme al Regolamento e assicuri la tutela dei diritti dell'interessato. In particolare, se all'interessato è lasciata facoltà di scelta relativamente al trattamento dei dati personali, il titolare del trattamento garantisce che siano trattati, di default, solo i dati personali necessari per ciascuna finalità specifica del trattamento e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non vadano oltre il minimo necessario per le finalità perseguite.

M1.12 Responsabile del trattamento

Il responsabile del trattamento (art. 4) è definito come la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che tratta dati personali per conto del titolare del trattamento.
Tale figura è di tutt'altra rilevanza rispetto al passato in quanto il responsabile assume nell'ambito del Regolamento una connotazione quasi professionale.

Difatti, dice la norma (art. 28) che "qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato". Quindi non viene scelta una persona fisica o giuridica qualsiasi, ma chi possieda già determinate competenze, per cui appare evidente che anche il responsabile del trattamento debba avere una formazione specifica.

Inoltre il Regolamento sancisce che l'esecuzione dei trattamenti su commissione è disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento, in cui siano stipulati la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Il contratto deve prevedere, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento;
b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste ai sensi dell'articolo 32;
d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36;
g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento
h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all’art. 28.

Di conseguenza lo stesso accordo tra titolare ed responsabile del trattamento deve avere un fondamento giuridico in quanto deve essere oggetto di contratto o altro atto giuridico che preveda tutta una serie di obblighi del responsabile che dipende direttamente dal titolare, può impiegare soltanto personale che si sia impegnato alla riservatezza e principalmente viene considerato anch'esso titolare del trattamento qualora tratti dati personali diversamente da quanto indicato nelle istruzioni dal titolare del trattamento.

Ciò è quanto si intuisce da quanto disciplinato dall'art. 26 del Regolamento che parla anche di contitolari del trattamento quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito al rispetto degli obblighi derivanti dal Regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato.

E' evidente, quindi, che la figura del responsabile del trattamento è connessa ad un soggetto che grazie al possesso di determinate competenze collabora concretamente con il titolare per la creazione di quelle condizioni tecniche e organizzative necessarie per l'adempimento dell'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato, assumendo peraltro determinate responsabilità derivanti dalla stipula di un accordo contrattuale.

Proprio per questi motivi lo stesso Regolamento specifica che il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento.
Tra i vari obblighi, inoltre, il Regolamento pone a carico del responsabile, ma anche del titolare del trattamento l'obbligo di conservazione della documentazione di tutti i trattamenti effettuati sotto la propria responsabilità. Conservazione che se riferita a documenti informatici ovviamente implica necessarie competenze inerenti la conservazione sostitutiva.

Inoltre l'art. 28 del GDPR chiarisce che quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

Non va confusa con tale figura quella prevista dall'art. 2-quaterdecies del codice in materia di protezione dei dati personali introdotto dall'art. 2 del d.lgs. n. 101/2018 che reca una serie di disposizioni volte a precisare taluni poteri e obblighi in capo al titolare e al responsabile, tra cui la possibilità di delegare compiti e funzioni a persone fisiche operanti sotto la loro autorità e responsabilità.

Tale disposizione assume una particolare rilevanza proprio perché risolve in parte le diverse problematiche sorte a seguito di quanto stabilito dall'art. 28 del GDPR che concepisce il solo responsabile esterno del trattamento.
Viene poi precisato che ogni qualvolta il titolare intende effettuare un trattamento connesso all'esecuzione di un compito di pubblico interesse che presenta rischi particolarmente elevati, deve obbligatoriamente chiedere la previa autorizzazione del Garante (cfr. art. 36, comma 5, Reg).

M1.13 Incaricato al trattamento

Nulla dice il Regolamento in merito alla figura dell'incaricato così come la conosciamo nel nostro Codice per la protezione dei dati personali e l'arcano è presto chiarito. Difatti la figura dell'incaricato scompare a seguito della traduzione-interpretazione in lingua italiana proposta dalla nostra Autorità Garante alla Commissione Europea ed accettata da quest'ultima. Difatti secondo l'ormai superata Direttiva 95/46/CE il "controller" era il nostro "responsabile de trattamento", mentre il "processor" era il nostro "incaricato". A seguito, invece, della proposta del Garante, alla luce dell'attuale Regolamento, per "controller" bisogna intendere "titolare del trattamento", mentre per "processor" bisogna intendere "responsabile del trattamento".

Comunque è pacifico che a prescindere da aspetti di carattere terminologico l'incaricato debba necessariamente continuare ad esistere, anche se sarebbe preferibile chiamarlo in modo diverso, ad esempio autorizzato al trattamento.

M1.14 Documentazione obbligatoria: il principio dell'accountability (Registro del trattamento)

Il termine anglosassone "accountability" non è facilmente traducibile e difatti nella traduzione del regolamento europeo si parla impropriamente di "responsabilità". Al massimo la traduzione più corretta, anche se poco pratica, potrebbe essere quella di "rendicontazione".

In realtà il termine "accountability" richiama almeno due accezioni o componenti fondamentali:
1. da un lato il dar conto all'esterno e in particolare al complesso degli stakeholder, in modo esaustivo e comprensibile, del corretto utilizzo delle risorse e della produzione di risultati in linea con gli scopi istituzionali;
2. dall'altro, l'esigenza di introdurre logiche e meccanismi di maggiore responsabilizzazione interna alle aziende e alle reti di aziende relativamente all'impiego di tali risorse e alla produzione dei correlati risultati.

In un ambito pubblicistico il concetto di accountability è sicuramente collegato a quello di trasparenza. Difatti le istituzioni pubbliche compiono (o non compiono) quotidianamente atti rilevanti per la comunità nazionale. Ma proprio una tale responsabilità, mette i cittadini nelle condizioni di formulare domande e osservazioni sul rendimento degli uffici pubblici e dei dirigenti che li guidano. I cittadini chiedono che il potere amministrativo adotti delle decisioni, ma, allo stesso tempo, chiedono che queste decisioni risolvano i loro problemi e che siano comprensibili e trasparenti. In altre parole, chiedono di "rendere conto".

L'accountability si compone di almeno tre elementi:

1. La "trasparenza" intesa come garanzia della completa accessibilità alle informazioni, in primo luogo per i cittadini, anche in quanto utenti del servizio.
2. La "responsività" intesa come la capacità di rendere conto di scelte, comportamenti e azioni e di rispondere alle questioni poste dagli stakeholder.
3. La "compliance" intesa come capacità di far rispettare le norme, sia nel senso di finalizzare l'azione pubblica all'obiettivo stabilito nelle leggi, che nel senso di fare osservare le regole di comportamento degli operatori della PA.

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

Registro delle attività di trattamento

L’art. 30 del Regolamento prevede che ogni titolare del trattamento e il suo eventuale rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.

Il registro contiene le seguenti informazioni:
a) il nome e i dati di contatto del titolare del trattamento e di ogni contitolare del trattamento, del rappresentante del titolare del trattamento e dell'eventuale responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Anche ogni responsabile del trattamento e il suo eventuale rappresentante tengono un registro di tutte le categorie di attività di trattamento dei dati personali svolte per conto di un titolare del trattamento, contenente:

a) 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 dell'eventuale responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative.

Su richiesta, il titolare del trattamento o il responsabile del trattamento e l'eventuale rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

Registro dei trattamenti

Titolare del trattamento	**Indirizzo** **Numero di telefono** **Indirizzo mail** **Indirizzo pec**
Responsabile del Trattamento	Indirizzo Numero di telefono Indirizzo mail Indirizzo pec

Trattamento	Ufficio	Finalità	Tipi di dati personali	Categorie di interessati	Consenso	Informativa	Conservazione	Misure di sicurezza	Destinatari delle comunicazioni dei dati personali

Più nello specifico, a seguito anche di quanto consigliato dall'Autorità Garante nelle proprie FAQ datate 8 ottobre 2018, si precisa:

a) nel campo "finalità del trattamento" oltre alla precipua indicazione delle stesse, distinta per tipologie di trattamento (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini), sarebbe opportuno indicare anche la base giuridica dello stesso (v. art. 6 del GDPR; in merito, con particolare riferimento al "legittimo interesse", si rappresenta che il registro potrebbe riportare la descrizione del legittimo interesse concretamente perseguito, le "garanzie adeguate" eventualmente approntate, nonché, ove effettuata, la preventiva valutazione d'impatto posta in essere dal titolare (v. provv. del Garante del 22 febbraio 2018). Sempre con riferimento alla base giuridica, sarebbe parimenti opportuno: in caso di trattamenti di "categorie particolari di dati", indicare una delle condizioni di cui all'art. 9, par. 2 del GDPR; in caso di trattamenti di dati relativi a condanne penali e reati, riportare la specifica normativa (nazionale o dell'Unione europea) che ne autorizza il trattamento ai sensi dell'art. 10 del GDPR;

(b) nel campo "descrizione delle categorie di interessati e delle categorie di dati personali" andranno specificate sia le tipologie di interessati (es. clienti, fornitori, dipendenti) sia quelle di dati personali oggetto di trattamento (es. dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, ecc.);

(c) nel campo "categorie di destinatari a cui i dati sono stati o saranno comunicati" andranno riportati, anche semplicemente per categoria di appartenenza, gli altri titolari cui siano comunicati i dati (es. enti previdenziali cui debbano essere trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi). Inoltre, si ritiene opportuno che siano indicati anche gli eventuali altri soggetti ai quali – in qualità di responsabili e sub-responsabili del trattamento– siano trasmessi i dati da parte del titolare (es. soggetto esterno cui sia affidato dal titolare il servizio di elaborazione delle buste paga dei dipendenti o altri soggetti esterni cui siano affidate in tutto o in parte le attività di trattamento). Ciò al fine di consentire al titolare medesimo di avere effettiva contezza del novero e della tipologia dei soggetti esterni cui sono affidate le operazioni di trattamento dei dati personali;

(d) nel campo "trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale" andrà riportata l'informazione relativa ai suddetti trasferimenti unitamente all'indicazione relativa al Paese/i terzo/i cui i dati sono trasferiti e alle "garanzie" adottate ai sensi del capo V del GDPR (es. decisioni di adeguatezza, norme vincolanti d'impresa, clausole contrattuali tipo, ecc.);

(e) nel campo "termini ultimi previsti per la cancellazione delle diverse categorie di dati" dovranno essere individuati i tempi di cancellazione per tipologia e finalità di trattamento (ad es. "in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall'ultima registrazione – v. art. 2220 del codice civile"). Ad ogni modo, ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a criteri (es. norme di legge, prassi settoriali) indicativi degli stessi (es. "in caso di contenzioso, i dati saranno cancellati al termine dello stesso");

(f) nel campo "descrizione generale delle misure di sicurezza" andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell'art. 32 del RGDP tenendo presente che l'elenco ivi riportato costituisce una lista aperta e non esaustiva, essendo rimessa al titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere. Tale lista ha di per sé un carattere dinamico (e non più statico come è stato per l'Allegato B del d. lgs. 196/2003) dovendosi continuamente confrontare con gli sviluppi della tecnologia e l'insorgere di nuovi rischi. Le misure di sicurezza possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (es. procedure organizzative interne; security policy ecc.).

Può essere riportata nel registro qualsiasi altra informazione che il titolare o il responsabile ritengano utile indicare (ad es. le modalità di raccolta del consenso, le eventuali valutazioni di impatto effettuate, l'indicazione di eventuali "referenti interni" individuati dal titolare in merito ad alcune tipologie di trattamento ecc.).

In merito, poi, al registro del responsabile del trattamento il Garante nelle proprie Faq ha precisato che:

a) nel caso in cui uno stesso soggetto agisca in qualità di responsabile del trattamento per conto di più clienti quali autonomi e distinti titolari (es. società di software house), le informazioni di cui all'art. 30, par. 2 del GDPR dovranno essere riportate nel registro con riferimento a ciascuno dei suddetti titolari. In questi casi il responsabile dovrà suddividere il registro in tante sezioni quanti sono i titolari per conto dei quali agisce; ove, a causa dell'ingente numero di titolari per cui si operi, l'attività di puntuale indicazione e di continuo aggiornamento dei nominativi degli stessi nonché di correlazione delle categorie di trattamenti svolti per ognuno di essi risulti eccessivamente difficoltosa, il registro del responsabile potrebbe riportare il rinvio, ad es., a schede o banche dati anagrafiche dei clienti (titolari del trattamento), contenenti la descrizione dei servizi forniti agli stessi, ferma restando la necessità che comunque tali schede riportino tutte le indicazioni richieste dall'art. 30, par. 2 del GDPR;

b) con riferimento alla "descrizione delle categorie di trattamenti effettuati" (art. 30, par. 2, lett. b) del GDPR) è possibile far riferimento a quanto contenuto nel contratto di designazione a responsabile che, ai sensi dell'art. 28 del GDPR, deve individuare, in particolare, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati oggetto del trattamento, nonché la durata di quest'ultimo;

c) in caso di sub-responsabile, parimenti, il registro delle attività di trattamento svolte da quest'ultimo potrà specificatamente far riferimento ai contenuti del contratto stipulato tra lo stesso e il responsabile ai sensi dell'art. 28, paragrafi 2 e 4 del GDPR.

L'art. 30, però, chiarisce che l'obbligo della tenuta di questi registri non si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati come quelli di cui all'art. 9 del GDPR (particolari) o all'art. 10 del GDPR (dati relativi a condanne penali, reato o connessi a misure di sicurezza.

In particolare (sulla scorta di quanto evidenziato anche dall'Autorità Garante nelle proprie FAQ datate 8 ottobre 2018), in ambito privato, i soggetti obbligati sono così individuabili:

- imprese o organizzazioni con almeno 250 dipendenti;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che possano presentare un rischio – anche non elevato – per i diritti e le libertà dell'interessato;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti non occasionali;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle categorie particolari di dati di cui all'articolo 9, paragrafo 1 GDPR, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10 GDPR.

Alla luce di quanto detto sopra, sono tenuti all'obbligo di redazione del registro, ad esempio:

- esercizi commerciali, esercizi pubblici o artigiani con almeno un dipendente (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);
- liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);
- associazioni, fondazioni e comitati ove trattino "categorie particolari di dati" e/o dati relativi a condanne penali o reati (i.e. organizzazioni di tendenza; associazioni a tutela di soggetti c.d. "vulnerabili" quali ad esempio malati, persone con disabilità, ex detenuti ecc.; associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull'orientamento sessuale, politico o religioso ecc.; associazioni sportive con riferimento ai dati sanitari trattati; partiti e movimenti politici; sindacati; associazioni e movimenti a carattere religioso);
- il condominio ove tratti "categorie particolari di dati" (es. delibere per interventi volti al superamento e all'abbattimento delle barriere architettoniche ai sensi della L. n. 13/1989; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all'interno dei locali condominiali).

Al di fuori dei casi di tenuta obbligatoria del Registro, anche alla luce del considerando 82 del GDPR, il Garante ne raccomanda la redazione a tutti i titolari e responsabili del trattamento, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di accountability e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso.

Nella realtà, come sostenuto dai Garanti europei nelle linee guida, sono spesso i DPO a realizzare l'inventario dei trattamenti e tenere un registro di tali trattamenti sulla base delle informazioni fornite loro dai vari uffici o unità che trattano dati personali.

È una prassi consolidata e fondata sulle disposizioni di numerose leggi nazionali nonché sulla normativa in materia di protezione dati applicabile alle istituzioni e agli organismi dell'UE.

Diventa, quindi, un'attività fondamentale dello stesso DPO per monitorare tutti i trattamenti della realtà organizzativa di riferimento.

Modalità di compilazione del registro

Lo stesso art. 30 del GDPR prevede che il registro debba rispettare la forma scritta anche in formato elettronico. In realtà l'aspetto formale poco conta (cartaceo, elettronico, struttura schematica, descrittiva, foglio di calcolo, tabella) ciò che rileva è l'esistenza di tutti gli elementi richiesti dall'art. 30 del Regolamento e l'indicazione verificabile della data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) unitamente a quella dell'ultimo aggiornamento. In quest'ultimo caso il registro dovrà recare una annotazione del tipo:
"- scheda creata in data XY"
"- ultimo aggiornamento avvenuto in data XY.

Come precisato dal Garante nelle proprie FAQ il registro dei trattamenti è un documento di censimento e analisi dei trattamenti effettuati dal titolare o responsabile.
In quanto tale, il registro deve essere mantenuto costantemente aggiornato poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Di conseguenza, qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

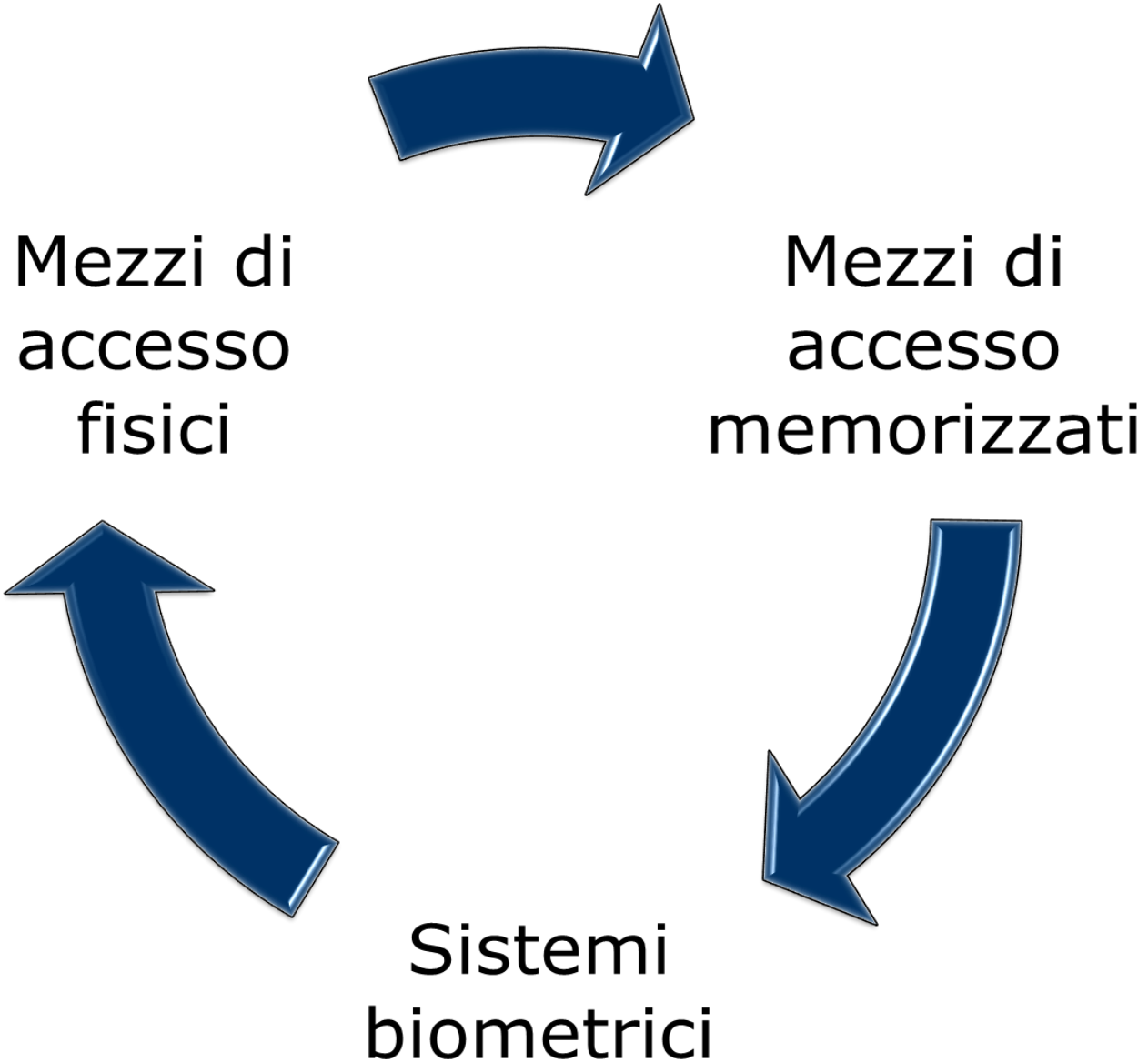
M1.15 Sicurezza dei dati e necessità di misure adeguate

La sicurezza nell'informatica equivale ad attuare tutte le misure e tutte le tecniche necessarie per proteggere l'hardware, il software ed i dati dagli accessi non autorizzati (intenzionali o meno), per garantirne la riservatezza, nonché eventuali usi illeciti, dalla divulgazione, modifica e distruzione.
Si include, quindi, la sicurezza del cuore del sistema informativo, cioè il centro elettronico dell'elaboratore stesso, dei programmi, dei dati e degli archivi.

Questi problemi di sicurezza sono stati presenti sin dall'inizio della storia dell'informatica, ma hanno assunto dimensione e complessità crescenti in relazione alla diffusione e agli sviluppi tecnici più recenti dell'elaborazione dati; in particolare per quanto riguarda i data base, la trasmissione dati e la elaborazione a distanza (informatica distribuita).

Riguardo l'aspetto "sicurezza" connesso alla rete telematica essa può essere considerata una disciplina mediante la quale ogni organizzazione che possiede un insieme di beni, cerca di proteggerne il valore adottando misure che contrastino il verificarsi di eventi accidentali o intenzionali che possano produrre un danneggiamento parziale o totale dei beni stessi o una violazione dei diritti ad essi associati.

Come può essere garantita la sicurezza?


Mezzi di accesso fisici
Mezzi di accesso memorizzati
Sistemi biometrici

La sicurezza nel GDPR

Non poteva, ovviamente, mancare nel Regolamento un chiaro riferimento alle misure di sicurezza che già vengono menzionate nell'art. 24 quando si chiarisce che il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento (principio di accountability).

Più nello specifico, l'art. 32 del Regolamento ne parla a proposito della sicurezza del trattamento. Tenuto conto, quindi, dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Tali misure comprendono:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
d) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel recente passato si è assistito ad una rapida evoluzione della minaccia cibernetica ed in particolare per quella incombente sulla pubblica amministrazione, che è divenuta un bersaglio specifico per alcune tipologie di attaccanti particolarmente pericolosi.

I pericoli legati a questo genere di minaccia sono particolarmente gravi per due ordini di motivi:
Il primo è la quantità di risorse che gli attaccanti possono mettere in campo, che si riflette sulla sofisticazione delle strategie e degli strumenti utilizzati.
Il secondo è rappresentato dal fatto che il primo obiettivo perseguito è il mascheramento dell'attività, in modo tale che questa possa procedere senza destare sospetti.

La combinazione di questi due fattori fa sì che misure tecniche adeguate, pur tenendo nella massima considerazione le difese tradizionali, quali gli antivirus e la difesa perimetrale, pongano l'accento sulle misure rivolte ad assicurare che le attività degli utenti rimangano sempre all'interno dei limiti previsti.
Infatti elemento comune e caratteristico degli attacchi più pericolosi è l'assunzione del controllo remoto della macchina attraverso una scalata ai privilegi.

Naturalmente le misure preventive, destinate ad impedire il successo dell'attacco, devono essere affiancate da efficaci strumenti di rilevazione, in grado di abbreviare i tempi, oggi pericolosamente lunghi, che intercorrono dal momento in cui l'attacco primario è avvenuto e quello in cui le conseguenze vengono scoperte.

In questo quadro diviene fondamentale la rilevazione delle anomalie operative e ciò rende conto dell'importanza data agli **inventari dei dispositivi e dei software**, che costituiscono le prime due classi di misure, nonché la **protezione della configurazione** (di hardware e software), che è quella immediatamente successiva.

La quarta classe deve la sua priorità alla duplice rilevanza **dell'analisi delle vulnerabilità**.
In primo luogo le vulnerabilità sono l'elemento essenziale per la scalata ai privilegi che è condizione determinante per il successo dell'attacco; pertanto la loro eliminazione è la misura di prevenzione più efficace.
Secondariamente si deve considerare che l'analisi dei sistemi è il momento in cui è più facile rilevare le alterazioni eventualmente intervenute e rilevare un attacco in corso.

La quinta classe è rivolta alla gestione degli utenti, in particolare con riferimento **all'attività degli amministratori** ed ad un uso appropriato dei relativi privilegi.

La sesta classe rappresentata dalle **difese contro i malware** deve la sua considerazione al fatto che anche gli attacchi complessi prevedono in qualche fase l'installazione di codice malevolo e la sua individuazione può impedirne il successo o rilevarne la presenza.

Le **copie di sicurezza**, settima classe, sono alla fine dei conti l'unico strumento che garantisce il ripristino dopo un incidente.
L'ultima classe, la **Protezione dei Dati**, deve la sua presenza alla considerazione che l'obiettivo principale degli attacchi più gravi è la sottrazione di informazioni.

M1.16 Data Breach: Violazione dei dati personali

I dati personali conservati, trasmessi o trattati da aziende e pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la privacy degli interessati cui si riferiscono i dati.

L'art. 33 del Regolamento dispone che in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente ai sensi dell'articolo 51 senza ingiustificato ritardo, 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 delle persone fisiche. Qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo è corredata di una giustificazione motivata (Data breach).

Tale notifica deve come minimo:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il Garante per la protezione dei dati personali già per il passato aveva adottato una serie di provvedimenti che introducevano in determinati settori l'obbligo di comunicare eventuali violazioni di dati personali *(data breach*) all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati.

- Provvedimento del Garante n. 161 del 4 aprile 2013 con il quale viene prescritto l'obbligo di comunicazione al Garante (mediante un apposito modello di comunicazione) da parte dei fornitori di servizi telefonici e di accesso a Internet (e non, ad esempio, i siti internet che diffondono contenuti, i motori di ricerca, gli internet point, le reti aziendali).
- Provvedimento n. 513 del 12 novembre 2014 dove viene previsto che entro 24 ore dalla conoscenza del fatto, i titolari del trattamento (aziende, amministrazioni pubbliche, ecc.) comunicano al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.

- Provvedimento n. 331 del 4 giugno 2015 dove viene sancito che entro 48 ore dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.
- Provvedimento del 2 luglio 2015 "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche" con il quale il Garante prescrive, ai sensi dell'articolo 154, comma 1, lett. c), del Codice in materia di protezione dei dati personali, che le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 devono comunicare all'Autorità, entro quarantotto ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possono avere un impatto significativo sui dati personali contenuti nelle proprie banche dati e che tali comunicazioni dovevano essere redatte secondo uno schema specifico allegato al provvedimento e inviate tramite posta elettronica o posta elettronica certificata.

L'art. 34, invece, prevede un'altra importante incombenza collegata alla precedente e cioè la comunicazione di una violazione dei dati personali all'interessato. Difatti, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

La predetta comunicazione descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e non è richiesta se:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

M1.17 Data Protection Impact Assessment

L'art. 35 del Regolamento europeo n. 2016/679 sulla protezione dei dati personali (GDPR) parla di valutazione d'impatto sulla protezione dei dati che deve essere effettuata dal titolare del trattamento quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei seguenti casi:
a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata sul trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono allo stesso modo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
c) la sorveglianza sistematica di una zona accessibile al pubblico su larga scala.

La valutazione contiene almeno:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, se del caso, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;
d) 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 presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Come già accaduto in Italia, l'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati. La stessa Autorità comunica tali elenchi al Comitato europeo per la protezione dei dati.
L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. Anche tali elenchi sono comunicati dall'Autorità al Comitato europeo per la protezione dei dati.

Prima di adottare tali elenchi l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 del Regolamento (che richiede una operazione delle Autorità di controllo per un'applicazione coerente del Regolamento) se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al controllo del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili si tiene debito conto, anche, del rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

Di recente (per l'esattezza il 4 aprile 2017 con primo emendamento avvenuto il 4 ottobre 2017), in materia, sono state pubblicate delle linee guida dei Garanti europei che hanno cercato di fornire utili chiarimenti in una materia sicuramente molto complessa.

In realtà nelle linee guida viene precisato che l'obbligo di condurre una DPIA, in determinate circostanze, deve essere collocato nel contesto del più generale obbligo imposto ai titolari di gestire correttamente i rischi connessi al trattamento di dati personali.

Per "rischio" si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità. D'altro canto, la "gestione del rischio" è definibile come l'insieme coordinato delle attività finalizzate a guidare e monitorare un ente o organismo nei riguardi di tale rischio.

Quando si parla di approccio basato sul rischio nel contesto giuridico della protezione dei dati, il riferimento ai "diritti e le libertà" degli interessati va inteso in primo luogo come relativo al diritto alla privacy, ma può riguardare anche altri diritti fondamentali quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione.

Coerentemente con l'approccio basato sul rischio che informa il GDPR, non è obbligatorio condurre una DPIA per ogni singolo trattamento. Viceversa, la DPIA è obbligatoria solo se una determinata tipologia di trattamenti "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35, paragrafo 1).*

Tuttavia, la semplice circostanza per cui non siano soddisfatte le condizioni che generano un obbligo di condurre la DPIA non riduce in alcun modo l'obbligo più generale cui soggiacciono i titolari di mettere in atto misure finalizzate a gestire in modo idoneo i rischi per i diritti e le libertà degli interessati.

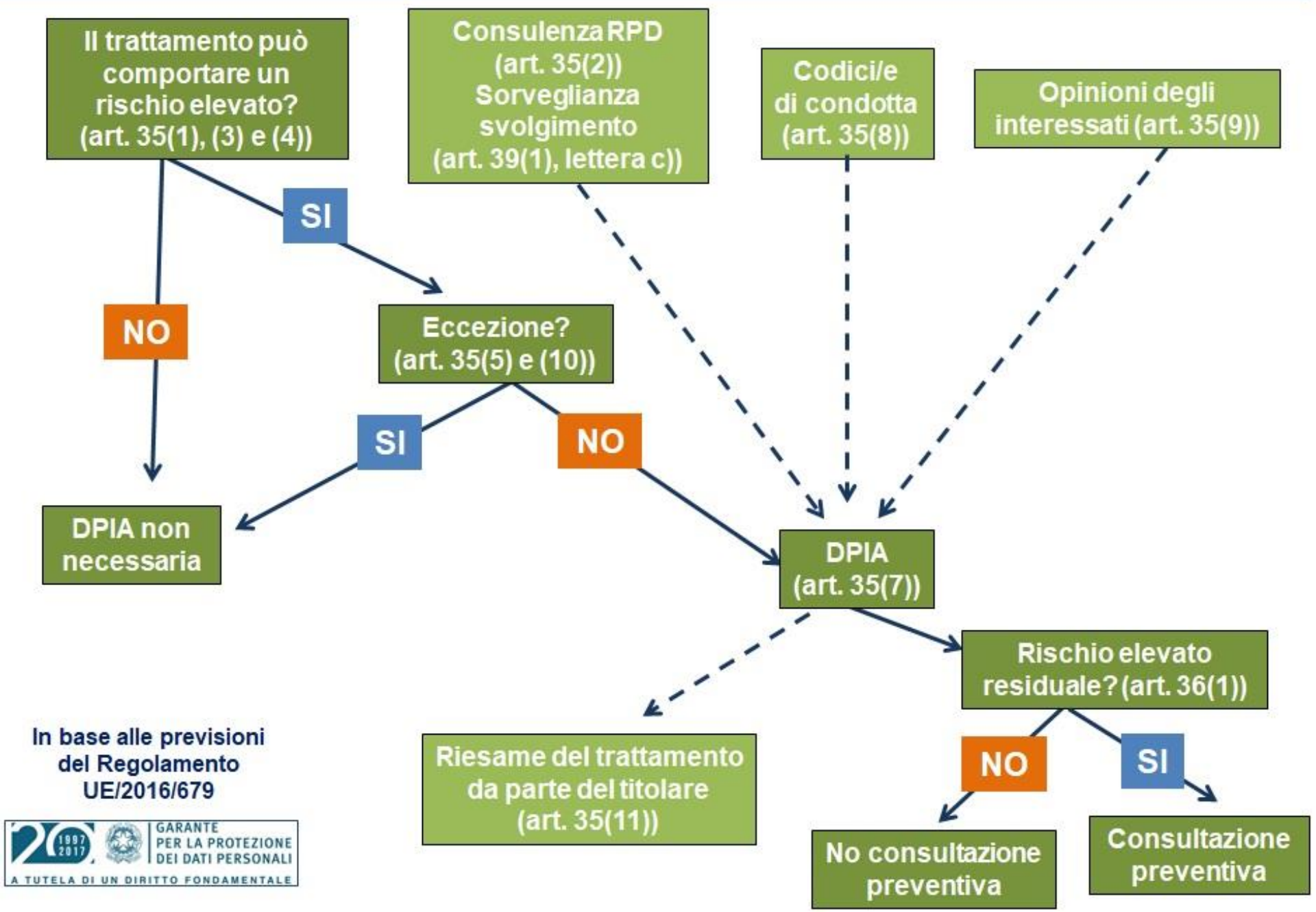
Nelle linee guida viene innanzitutto precisato che una singola DPIA per quanto può riguardare una sola operazione di trattamento dei dati potrebbe essere utilizzata per valutare molteplici operazioni di trattamento che sono simili in termini di rischi presentati, purché adeguatamente considerate la specifica natura, portata, contesto e finalità del trattamento.

Si può fare riferimento, quindi, a tecnologie simili utilizzate per raccogliere lo stesso tipo di dati per le medesime finalità. Ad esempio, un gruppo di autorità municipali in cui ciascuno predisponga un simile sistema TVCC potrebbe effettuare un' unica DPIA che copra l'elaborazione di questi titolari separati, o un operatore ferroviario (singolo titolare) potrebbe 'coprire' la videosorveglianza in tutte le sue stazioni con una DPIA.

Quando un trattamento è svolto in contitolarità, è necessario che ciascun contitolare definisca con precisione gli obblighi rispettivamente incombenti. La DPIA dovrebbe stabilire chi ha la responsabilità delle singole misure finalizzate alla gestione dei rischi e alla tutela dei diritti e delle libertà degli interessati. Ciascun titolare dovrebbe indicare con chiarezza le rispettive esigenze e condividere tutte le informazioni utili senza pregiudicare quanto coperto da segreto (per esempio, informazioni tutelate dal segreto commerciale, soggette a diritti di proprietà intellettuale, informazioni economiche riservate) né rivelare eventuali vulnerabilità.

Una DPIA può anche essere utile per valutare l'impatto di protezione di dati di un prodotto tecnologico, per esempio un componente hardware o software, qualora ciò sia suscettibile ad essere utilizzato da altri titolari per effettuare diversi trattamenti.
Naturalmente, il titolare del trattamento che distribuisce il prodotto, rimane obbligato a svolgere la propria DPIA per quanto riguarda l'attuazione specifica, ma questo può essere messo al corrente della DPIA preparata dal fornitore del prodotto, se del caso.

Valutazione di impatto sulla protezione dei dati (DPIA). Quando effettuarla?



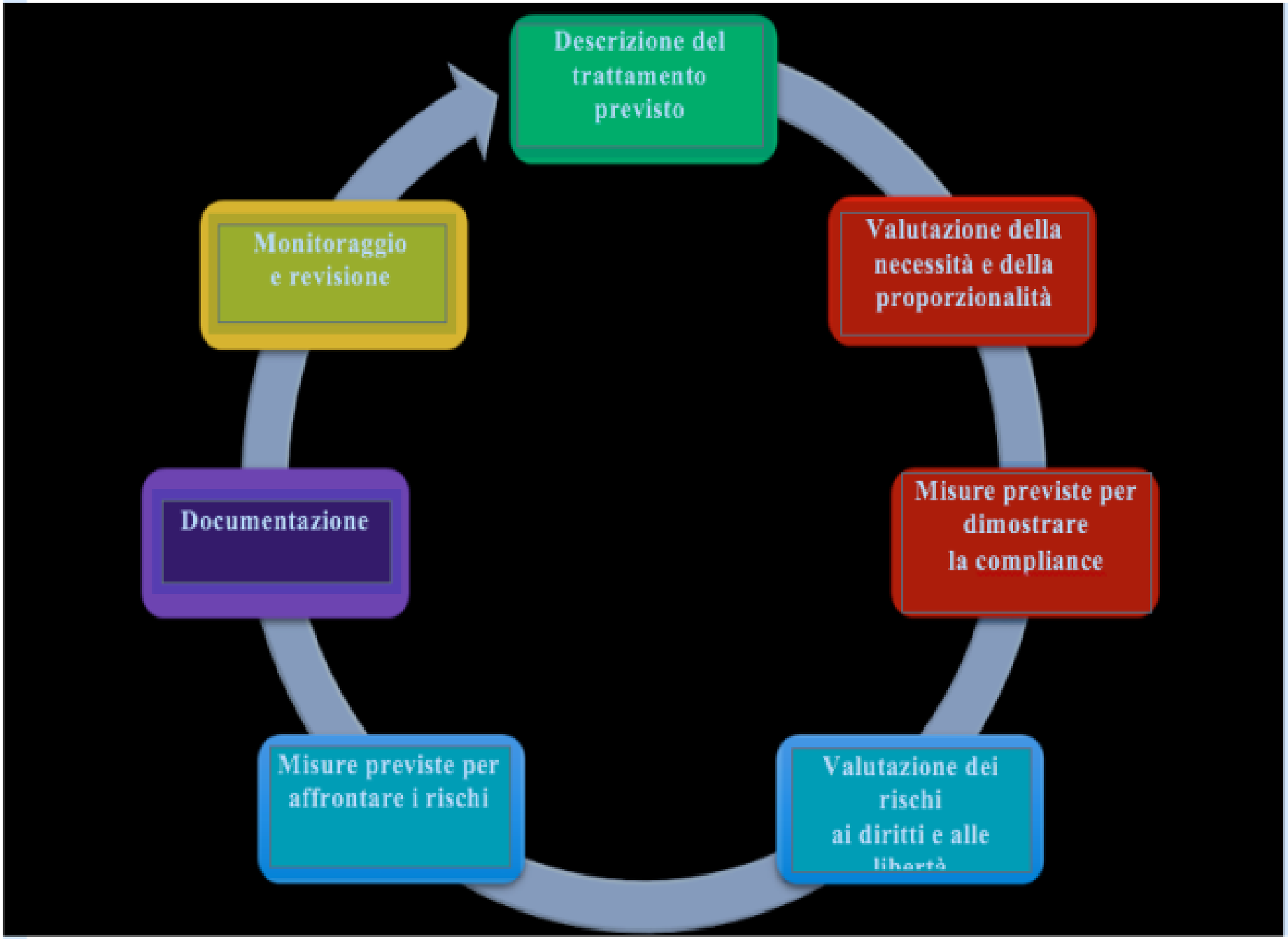
In base alle previsioni del Regolamento UE/2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
1997 2017
A TUTELA DI UN DIRITTO FONDAMENTALE

Esempi di lavorazione	Possibili criteri	DPIA richiesta?
Il trattamento dei dati genetici e di salute dei pazienti in un ospedale (sistema informativo dell'ospedale).	I dati sensibili Dati relativi interessati vulnerabili	Si
L'uso di un sistema di telecamere per monitorare il comportamento di guida in autostrada. Il titolare prevede di utilizzare un sistema di analisi video intelligente per individuare autoveicoli e riconoscere automaticamente le targhe.	Il monitoraggio sistematico L'uso innovativo o l'applicazione di soluzioni tecnologiche o organizzative	
Una società che monitora le attività dei suoi dipendenti inclusa la loro postazione di lavoro, attività internet, ecc	Il monitoraggio sistematico I dati relativi interessati vulnerabili	
La raccolta di dati dai profili social usate da compagnie private per generare profili per database di contatti	Valutazione o assegnazione di un punteggio I dati trattati su larga scala	
Una rivista online utilizza una mailing list per inviare un sommario giornaliero generico ai suoi abbonati.	Nessuno	Non necessariamente
Un sito di e-commerce visualizza annunci pubblicitari di auto d'epoca includendo una limitata profilazione ispirata al passato comportamento d'acquisto su alcune parti del proprio sito Web.	Valutazione o assegnazione di un punteggio, ma non sistematica o estesa	

Metodologia della DPIA

Le linee guida suggeriscono, inoltre, diverse metodologie per effettuare una DPIA anche se i criteri naturalmente devono essere comuni.
In merito è stata predisposta una specifica norma internazionale ISO/IEC 29134 dal titolo "*Privacy Impact Assessment – Methodology*" di prossima pubblicazione che propone: un processo molto articolato in 12 passi, a cui ne vanno aggiunti 2 di riesame periodico o ad hoc e di attuazione degli eventuali cambiamenti necessari; un indice in 6 punti per il rapporto di valutazione ed un esempio per la stima degli impatti.


Descrizione del trattamento previsto
Valutazione della necessità e della proporzionalità
Misure previste per dimostrare la compliance
Valutazione dei rischi ai diritti e alle
Misure previste per affrontare i rischi
Documentazione
Monitoraggio e revisione

Nel considerando 90 del GDPR sono elencati alcuni elementi della DPIA che risultano sovrapponibili a elementi ben noti di schemi esistenti per la gestione del rischio (per esempio, ISO 31000). In termini di gestione del rischio, una DPIA mira a "gestire i rischi" per i diritti e le libertà delle persone fisiche attraverso i processi di seguito indicati:

- Definizione del contesto: "*tenendo conto della natura, dell'ambito, del contesto e delle finalità del trattamento e delle fonti di rischio*";
- Valutazione dei rischi: "*valutare la particolare probabilità e gravità del rischio elevato*";
- Gestione dei rischi: "*attenuare tale rischio*" "*assicurando la protezione dei dati personali*" e "*dimostrando la conformità al regolamento*".

Il regolamento dà ai titolari un margine di flessibilità nello stabilire la struttura e la forma della valutazione di impatto in modo da consentirne l'inclusione nelle prassi lavorative in essere.
Vi sono già oggi alcuni schemi definiti nell'Ue e a livello mondiale che tengono conto degli elementi descritti al considerando 90; tuttavia, qualunque sia la forma prescelta, la DPIA deve configurare una vera valutazione dei rischi e consentire ai titolari di adottare misure per affrontare tali rischi.

Una corretta analisi dei rischi dovrebbe, quindi, tener conto:

- la tipologia dei dati trattati, la loro appetibilità, nonché la loro pericolosità per la privacy dei soggetti cui essi si riferiscono;
- i comportamenti degli operatori, gli eventi relativi agli strumenti utilizzati per il trattamento dei dati, gli eventi relativi al contesto.

Il WP29 incoraggia, inoltre, lo sviluppo di quadri DPIA settoriali. Questo perché essi possono attingere a conoscenze specifiche di settore, il che significa che la DPIA si può indirizzare alle specifiche di un particolare tipo di operazione di trattamento (es.: particolari tipi di dati, beni aziendali, le potenziali ripercussioni, minacce, misure). In questo modo la DPIA può risolvere i problemi che sorgono in un particolare settore economico, o se si utilizzano particolari tecnologie o si effettuano particolari tipi di operazioni di trattamento.

La pubblicazione della DPIA non costituisce un obbligo formale ai sensi del regolamento, ed è quindi rimessa alla discrezionalità del titolare. Tuttavia, sarebbe opportuno che i titolari valutassero di rendere pubbliche almeno parti della DPIA, quali una sintesi o le conclusioni: così facendo si promuoverebbe la fiducia nelle attività di trattamento svolte da quei titolari dando prova di un approccio responsabile e trasparente. La pubblicazione della DPIA appare particolarmente indicata se il trattamento produce effetti su una parte della popolazione, il che vale soprattutto nel caso sia un'autorità pubblica a condurre la DPIA.

I trattamenti necessariamente soggetti alla DPIA

Come già si è avuto modo di specificare la DPIA è obbligatoria solo qualora un trattamento "*possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35, paragrafo 1),* come meglio chiarito dal paragrafo 3 dell'art. 35 e integrato da quanto prevede il paragrafo 4 dello stesso articolo. Si tratta di un requisito particolarmente pertinente qualora si intenda introdurre una tecnologia di trattamento innovativa.

Con il provvedimento n. 467 dell'11 ottobre 2018 pubblicato sulla G.U. n. 269 del 19 novembre 2018 il Garante per la protezione dei dati personali ha previsto, ai sensi dell'art. 35 comma 4 del Regolamento UE n. 2016/679, l'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati.
Come precisato dalla stessa Autorità nel proprio provvedimento, non si tratta di un'iniziativa autonoma, ma nel rispetto di quanto previsto dal Regolamento e, quindi, dallo stesso principio di coerenza, tale elenco è stato condiviso in ambito comunitario e comunicato al Comitato Europeo per la protezione dei dati, che ha espresso, in merito, specifico parere recepito dall'Autorità.

Analizzando, nello specifico, i trattamenti previsti dal Garante, peraltro non esaustivi, si nota come vengono ripresi e precisati quei trattamenti già indicati dai Garanti europei (WP29) nelle loro linee guida e del resto non poteva essere diversamente in quanto una base condivisa a livello comunitario si rendeva necessaria.

Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato".

Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).

Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.

Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).

Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).

Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev.01.

Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.

Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).

Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.

Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

M1.18 Prior Check

L’art. 36 del Regolamento prevede la c.d. consultazione preventiva quando il titolare del trattamento, prima di procedere al trattamento dei dati personali, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

Se l'Autorità di controllo ritiene che il trattamento previsto non sia conforme al Regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, entro un periodo massimo di otto settimane dalla richiesta di consultazione, fornisce una consulenza per iscritto al titolare del trattamento dei dati, e ove applicabile al responsabile del trattamento. Questo periodo può essere prorogato di ulteriori sei settimane, tenendo conto della complessità del trattamento previsto. Qualora si applichi la proroga, il titolare del trattamento e, ove applicabile, il responsabile del trattamento ne sono informati, incluso dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

M1.19 Certificazioni

Gli artt. 42 e 43 del Regolamento danno ampio spazio alla certificazione ed agli organismi di certificazione. In particolare l'art. 42 prevede che gli Stati membri, le autorità di controllo, il Comitato europeo per la protezione dei dati e la Commissione incoraggiano, in particolare a livello di Unione, 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 al Regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Si tiene conto delle esigenze specifiche delle micro, piccole e medie imprese.

I meccanismi, i sigilli o i marchi approvati, oltre ad essere applicati dai titolari del trattamento e dai responsabili del trattamento soggetti al Regolamento, possono essere istituiti anche al fine di dimostrare la previsione di adeguate garanzie da parte dei titolari del trattamento o responsabili del trattamento non soggetti al Regolamento ai sensi dell'articolo 3, nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'articolo 46, paragrafo 2, lettera f).

La certificazione è rilasciata dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente in base ai criteri approvati da tale autorità di controllo competente ai sensi dell'articolo 58, paragrafo 3, o dal comitato, ai sensi dell'articolo 63. Ove i criteri siano approvati dal comitato, ciò può risultare in una certificazione comune, il sigillo europeo per la protezione dei dati.
Naturalmente il titolare del trattamento o il responsabile del trattamento che sottopone il trattamento effettuato al meccanismo di certificazione fornisce all'organismo di certificazione o, se del caso, all'autorità di controllo competente tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione.

La certificazione è rilasciata al titolare del trattamento o responsabile del trattamento per un periodo massimo di 3 anni e può essere rinnovata alle stesse condizioni purché continuino ad essere soddisfatti i requisiti pertinenti. È revocata, se del caso, dagli organismi di certificazione o dall'autorità di controllo competente, qualora non siano o non siano più soddisfatti i requisiti per la certificazione.

M1.20 Codici di condotta

I codici di condotta sono regole di condotta o pratiche uniformi elaborate da vari organismi internazionali o anche da singoli Stati, particolarmente diffuse nei rapporti economici internazionali. In genere contengono disposizioni non vincolanti anche se l'autorevolezza dell'organismo da cui promanano fanno si che siano di larga e diffusa applicazione.

Il regolamento europeo n. 679/2016 contiene un grosso incoraggiamento all'utilizzo dei codici di condotta, ma ovviamente in un'ottica comunitaria.
In effetti il GDPR all'art. 40 sancisce che gli Stati membri, le autorità di controllo, il Comitato europeo per la protezione dei dati e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del Regolamento, in funzione delle specificità settoriali e delle esigenze specifiche delle micro, piccole e medie imprese.

Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono, quindi, elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione delle disposizioni del Regolamento.

Si pensi:
a) il trattamento corretto e trasparente dei dati;
b) i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;
c) la raccolta dei dati personali;
d) la pseudonimizzazione dei dati personali;
e) l'informazione fornita al pubblico e agli interessati;
f) l'esercizio dei diritti degli interessati;
g) l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;
h) le misure e le procedure di cui agli articoli 24 e 25 del GDPR e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32;
i) la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato;
j) il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali;
k) le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli articoli 77 e 79 del GDPR.

Le associazioni e gli altri organismi previsti dal Regolamento che intendono elaborare un codice di condotta o modificare o prorogare un codice esistente sottopongono il progetto di codice all'autorità di controllo (cioé al nostro Garante). L'autorità di controllo esprime un parere sulla conformità al Regolamento del progetto di codice o del codice modificato o prorogato e lo approva, se ritiene che offra garanzie sufficientemente adeguate. In questo caso l'autorità di controllo registra e pubblica il codice.

Qualora il progetto di codice di condotta si riferisca alle attività di trattamento in vari Stati membri, prima di approvare il progetto, la modifica o la proroga, l'autorità di controllo che è competente ai sensi dell'articolo 55 del regolamento lo sottopone, tramite la procedura di coerenza, al comitato, il quale formula un parere sulla conformità al regolamento del progetto di codice, della modifica o della proroga o, nel caso di cui al paragrafo 3 dell'art. 40 del GDPR, sulla previsione di adeguate garanzie.

Qualora il parere confermi che il progetto di codice di condotta, la modifica o la proroga è conforme al regolamento o, nel caso di cui al paragrafo 3, fornisce adeguate garanzie, il comitato trasmette il suo parere alla Commissione. A questo punto la Commissione può decidere, mediante atti di esecuzione, che il codice di condotta, la modifica o la proroga approvati, che le sono stati sottoposti hanno validità generale all'interno dell'Unione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2 del regolamento.

La Commissione provvede a dare un'adeguata pubblicità dei codici approvati per i quali è stata decisa la validità generale ai sensi del paragrafo 9 dell'art. 40 del GDPR.
Il comitato raccoglie in un registro tutti i codici di condotta, le modifiche e le proroghe approvati e li rende pubblici mediante mezzi appropriati.

M1.21 Trasferimento dati all'estero
M1.22 Condizioni di adeguatezza per il trasferimento dei dati all'estero

La materia del trasferimento dei dati personali all'estero è sempre stata oggetto di grande attenzione in ambito europeo per i suoi inevitabili risvolti in materia di privacy per cui sia la Direttiva comunitaria 95/46/CE che l'attuale Regolamento Europeo n. 2016/679 hanno previsto particolari cautele in tale settore.

In particolare l'art. 44 del GDPR come principio generale sancisce che qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui capo V del Regolamento. Tutte le disposizioni sono applicate al fine di assicurare che il livello di tutela delle persone fisiche garantito dal Regolamento non sia pregiudicato.

Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso, innanzitutto, se la Commissione ha deciso che il paese terzo, o un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscano un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche (art. 45).

In mancanza di una valutazione di adeguatezza il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha offerto garanzie adeguate e a condizione che siano disponibili diritti azionabili degli interessati e mezzi di ricorso effettivi per gli interessati (art. 46).

Il trasferimento dei dati verso paesi terzi può anche avvenire quando vi siano norme vincolanti d'impresa (art. 47) che però devono essere approvate dall'Autorità di controllo purché:
a) siano giuridicamente vincolanti e si applichino a tutti i membri interessati del gruppo di imprese o gruppi di imprese che svolgono un'attività economica comune, compresi i loro dipendenti;
b) conferiscano espressamente agli interessati diritti azionabili in relazione al trattamento dei loro dati personali;
c) soddisfino tutta una serie di requisiti quali l'indicazione della struttura e delle coordinate di contatto del gruppo d'imprese in questione e di ciascuno dei suoi membri; l'indicazione dei trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione; l'applicazione dei principi generali di protezione dei dati, in particolare in relazione alla limitazione della finalità, alla minimizzazione dei dati, alla limitazione del periodo di conservazione, alla qualità dei dati, alla protezione fin dalla progettazione e alla protezione di default, ecc.

Appare quindi evidente che nella materia della tutela dei dati personali vi è da sempre la preoccupazione che, proprio al fine di eludere le protezioni offerte dalle legislazioni degli Stati, i dati personali vengono trasferiti all'estero, verso paesi con una minore, o con nessuna, legislazione sul punto della protezione degli individui rispetto al trattamento dei dati personali.

La stessa Autorità Garante ha sempre sostenuto che per superare gli ostacoli relativi al trasferimento di dati personali presso paesi terzi vengono predisposti su scala europea alcuni contratti-tipo che hanno permesso di regolare in modo uniforme, e tendenzialmente agevole, diversi flussi di dati verso Paesi terzi nei quali operino titolari del trattamento autonomi rispetto al soggetto esportatore, oppure strutture che agiscono in funzione strumentale quali "responsabili" del trattamento.

Il problema è che questo sistema non funziona al meglio per molti gruppi multinazionali in quanto nell'ambito degli stessi l'impiego di modelli contrattuali standardizzati viene avvertito, a volte, come farraginoso, poiché ciascuna società stabilita all'interno dello Spazio economico europeo e appartenente ad un medesimo gruppo multinazionale deve comunque includere le garanzie previste dai predetti schemi tipo in un suo contratto con le società del gruppo situate in Paesi terzi.

Al fine di risolvere tale problematica le autorità garanti d'Europa, riunite nel gruppo istituito ai sensi dell'art. 29 della direttiva 95/46/CE (c.d. Gruppo art. 29), hanno preso in considerazione ulteriori strumenti, rispetto a quello contrattuale, che possano assicurare anch'essi un livello adeguato di protezione per i diritti degli interessati, con particolare riguardo al trasferimento all'estero dei dati personali nell'ambito dei gruppi multinazionali.

Il Gruppo ha operato alcune prime valutazioni con riserva di eventuali situazioni specifiche connesse a singole realtà nazionali, ravvisando un'interessante prospettiva di lavoro nelle regole di comportamento che una società capogruppo può impartire, generalmente all'interno di appositi codici di condotta interni al gruppo multinazionale e resi vincolanti per tutte le società ad esso appartenenti.

Tali regole, ormai conosciute nella prassi applicativa come "*binding corporate rules*", sono state ritenute come uno strumento astrattamente idoneo ad assicurare un livello adeguato di protezione per i diritti degli interessati, compatibile con la disciplina contenuta nella direttiva 95/46/CE sempreché siano vincolanti sia all'interno che all'esterno del gruppo di società.

Esse si concretizzano in un documento contenente una serie di clausole (rules) che fissano i principi vincolanti (binding) al cui rispetto sono tenute tutte le società appartenenti ad uno stesso gruppo (corporate).

Le Bcr costituiscono un meccanismo in grado di semplificare gli oneri amministrativi a carico delle società di carattere multinazionale con riferimento ai flussi intra-gruppo di dati personali.

M1.23 Sanzioni

L'art. 83 del Regolamento disciplina la delicata materia delle sanzioni che risultano di gran lunga più pesanti rispetto alla precedente normativa.
Innanzitutto viene specificato che ogni autorità di controllo garantisce che le sanzioni amministrative pecuniarie irrogate in relazione alle violazioni del Regolamento siano in ogni singolo caso effettive, proporzionate e dissuasive.
Le sanzioni amministrative pecuniarie sono irrogate, in funzione delle circostanze di ogni singolo caso. Al momento di decidere se irrogare una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto di diversi elementi.

Tali elementi sono:
a) la natura, la gravità e la durata della violazione;
b) il carattere doloso o colposo della violazione;
c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento;
e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
g) le categorie di dati personali interessate dalla violazione;
h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
j) l'adesione ai codici di condotta;
k) eventuali altri fattori aggravanti o attenuanti.

L'art. 83 del Regolamento sancisce che la violazione di determinate disposizioni è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 EUR, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.
Tali disposizioni sono:
a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;
b) i diritti degli interessati a norma degli articoli da 12 a 22;
c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;
d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;
e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo.

La violazione di altre disposizioni è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 EUR, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Tali disposizioni sono:
a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;
b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;
c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4.

La mancata osservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

L'art. 84 attribuisce, comunque, in materia una certa discrezionalità agli stati membri nel momento in cui stabilisce che gli stessi determinano le sanzioni per le violazioni del Regolamento, in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e prendono tutti i provvedimenti necessari per assicurarne l'applicazione.

Si ricorda che il gruppo di lavoro ex art. 29 per la protezione dei dati ha adottato il 3 ottobre 2017 delle linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679.

Nuovi illeciti penali

Con il d.lgs. n. 101/2018 nel quadro delle sanzioni penali rinvenibili nel codice in materia di protezione dei dati personali il legislatore ha ritenuto opportuno proporre l'opzione volta a depenalizzare la fattispecie di cui all'art. 169 del Codice (Misure di sicurezza).

Difatti le radicali modifiche apportate alle "misure minime" di cui all'articolo 33 che hanno imposto di dequotare la corrispondente fattispecie sanzionatoria, applicando le sanzioni amministrative nei casi previsti dal Regolamento.

Quanto all'articolo 167, invece, occorre osservare che tale fattispecie, nell'esperienza giurisprudenziale formatasi, ha dimostrato una limitata operatività ed una scarsa aderenza a ipotesi di trattamento illecito realmente significative. Pertanto, in luogo di tale fattispecie ne è stata introdotta altra, ben differente, contraddistinta dall'intento di arrecare danno all'interessato ed alla quale se ne aggiungono ulteriori come l'art. **167-bis** in caso di **comunicazione o diffusione illecita di dati personali oggetto di trattamento su larga scala** e l'art. **167-ter** in caso di **acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala.**

L'art. 167-bis dispone che chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, è punito con la reclusione da uno a sei anni.
Inoltre anche chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.

L'art. 167-ter, invece, stabilisce che chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è punito con la reclusione da uno a quattro anni.

Rispetto alla fattispecie di cui all'articolo 168 (Falsità nelle dichiarazioni e notificazioni al Garante), si è ritenuto opportuno conservare l'opzione punitiva giacché tale fattispecie sanziona condotte caratterizzate da apprezzabile meritevolezza di pena e/o contrassegnate da significativo disvalore. Tale previsione, del resto, è esclusa dall'ambito di applicazione delle sanzioni amministrative, non ponendo problemi in punto di ne bis in idem.

In riferimento al reato previsto ex articolo 170 (Inosservanza di provvedimenti del Garante), si è ritenuto di mantenere l'illecito seppur inquadrato negli attuali ambiti normativi.

Al pari si è ritenuto di mantenere, anche, l'illecito di cui all'art.171, seppur diversamente rubricato (Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori) e con specifici riferimenti all'art. 4 dello Statuto dei Lavoratori.

M1.24 Tutele e danno risarcibile

L’art. 77 del Regolamento stabilisce come principio generale che fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento dei dati personali che lo riguardano non sia conforme al Regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure nel luogo della presunta violazione.

Si ritorna, quindi, a concepire un rimedio amministrativo dinanzi all’Autorità garante come alternativo rispetto agli altri rimedi giurisdizionali.

L’art. 80 del Regolamento chiarisce, inoltre, che l'interessato ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione, che siano debitamente costituiti secondo il diritto di uno Stato membro, che non abbiano scopo di lucro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della tutela dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti previsti dal Regolamento.

L'art. 78 del Regolamento sancisce che fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ogni persona fisica o giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda.
Nello specifico ciascun interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora l'autorità di controllo che sia competente ai sensi degli articoli 55 e 56 non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto ai sensi dell'articolo 77. Le azioni nei confronti dell'autorità di controllo sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita.

L'art. 79 del Regolamento, invece, sancisce che fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 77, ogni interessato ha il diritto di proporre un ricorso giurisdizionale nei confronti del titolare del trattamento o del responsabile del trattamento qualora ritenga che i diritti di cui gode a norma del presente regolamento siano stati violati a seguito di un trattamento.
Le azioni sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri.

Risarcimento del danno

Il Regolamento UE 2016/679 ribadisce i principi propri della Direttiva 95/46/CE in merito al risarcimento del danno a favore dell'interessato. Difatti l'art. 82 prevede che chiunque subisca un danno materiale o immateriale cagionato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento non conforme al Regolamento. Un responsabile del trattamento risponde per il danno cagionato dal trattamento solo se non ha adempiuto gli obblighi del Regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo esterno o contrario alle legittime istruzioni del titolare del trattamento.

Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, se dimostra che l'evento dannoso non gli è in alcun modo imputabile (probatio diabolica).

Qualora più titolari del trattamento o responsabili del trattamento oppure un titolare del trattamento e un responsabile del trattamento siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno cagionato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

Qualora, poi, un titolare del trattamento o un responsabile del trattamento abbia pagato, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno.

Le azioni legali relative al risarcimento del danno sono naturalmente promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto nazionale dello Stato membro.

Tipologia del danno

Naturalmente in questo campo rileva il danno alla persona in tutte le sue accezioni. Difatti il danno alla persona comprende tutti i danni, patrimoniali e non, che sono cagionati ad un essere umano.
Si tratta quindi di una macrocategoria, che racchiude al suo interno altre categorie: danno alla salute, danno biologico, danno esistenziale, danno morale, danno non patrimoniale, danno patrimoniale, danno all'onore, alla riservatezza, ecc. Qualsiasi danno che faccia capo ad un soggetto, di qualsiasi tipo o entità, è inquadrabile in questa categoria.

Tale figura ha subito nei decenni un progressivo cambiamento, partendo da un'ottica squisitamente patrimoniale, ove erano considerati eccezionali i risarcimenti per le voci di danno che non fossero calcolabili dal punto di vista economico, ad un ottica non patrimoniale, per cui qualsiasi tipo di lesione, qualunque sia la sua natura, deve essere risarcita.

In particolare il sistema del danno alla persona può quindi essere, oggi, schematizzabile in questo modo:
- danno patrimoniale (articolo 2043): risarcibile sempre;
- danno non patrimoniale (articolo 2059): risarcibile in sede civile nei casi previsti dalla legge (ordinaria, costituzionale, o comunitaria).
Tale sistema è detto "bipolare" perché anziché disarticolare il danno alla persona in una pluralità di voci di danno, si compone di due sole grandi voci (danno patrimoniale e non patrimoniale) al cui interno rientrano tutte le altre.

M1.25 Le Autorità di Controllo

L’art. 51 del Regolamento prevede che ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (l'«autorità di controllo»).

Ogni Autorità di controllo agisce in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri conformemente al GDPR.
Nell'adempimento dei rispettivi compiti e nell'esercizio dei rispettivi poteri previsti dal Regolamento, il membro o i membri di ogni autorità di controllo non subiscono pressioni esterne, né dirette, né indirette, e non sollecitano né accettano istruzioni da alcuno.

Ogni Stato membro provvede affinché ogni autorità di controllo sia dotata delle risorse umane, tecniche e finanziarie, dei locali e delle infrastrutture necessari per l'effettivo adempimento dei suoi compiti e l'esercizio dei propri poteri, compresi quelli nell'ambito dell'assistenza reciproca, della cooperazione e della partecipazione al comitato.
Ogni Stato membro provvede affinché ogni autorità di controllo selezioni e disponga di proprio personale, soggetto alla direzione esclusiva del membro o dei membri dell'autorità di controllo interessata.
Ogni Stato membro provvede affinché ogni autorità di controllo sia soggetta a un controllo finanziario che non ne pregiudichi l'indipendenza e disponga di bilanci annuali, separati e pubblici, che possono far parte del bilancio generale statale o nazionale.

Gli Stati membri dispongono che ciascun membro delle rispettive autorità di controllo sia nominato attraverso una procedura trasparente:
— dal rispettivo parlamento;
— dal rispettivo governo;
— dal rispettivo capo di Stato; oppure
— da un organismo indipendente incaricato della nomina a norma del diritto dello Stato membro.
Ogni membro possiede le qualifiche, l'esperienza e le competenze, in particolare nel settore della protezione dei dati personali, richieste per l'esercizio delle sue funzioni e dei suoi poteri.
Il mandato dei membri cessa alla scadenza del termine o in caso di dimissioni volontarie o di provvedimento d'ufficio, a norma del diritto dello Stato membro interessato (art. 53 GDPR).

M1.26 Compiti dell'Autorità di Controllo

a) sorveglia e assicura l'applicazione del presente regolamento;
b) promuove la consapevolezza e favorisce la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento.
c) fornisce consulenza, a norma del diritto degli Stati membri, al parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento;
d) promuove la consapevolezza dei titolari del trattamento e dei responsabili del trattamento riguardo agli obblighi imposti loro dal presente regolamento;
e) su richiesta, fornisce informazioni all'interessato in merito all'esercizio dei propri diritti derivanti dal presente regolamento e, se del caso, coopera a tal fine con le autorità di controllo di altri Stati membri;
f) tratta i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione ai sensi dell'articolo 80;

g) collabora, anche tramite scambi di informazioni, con le altre autorità di controllo e presta assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del presente regolamento;
h) svolge indagini sull'applicazione del presente regolamento, anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica;
i) sorveglia gli sviluppi che presentano un interesse, se e in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione e le prassi commerciali;
j) adotta le clausole contrattuali tipo di cui all'articolo 28, paragrafo 8, e all'articolo 46, paragrafo 2, lettera d);
k) redige e tiene un elenco in relazione al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35, paragrafo 4;
l) offre consulenza sui trattamenti di cui all'articolo 36, paragrafo 2;
m) incoraggia l'elaborazione di codici di condotta ai sensi dell'articolo 40, paragrafo 1;

n) incoraggia l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati a norma dell'articolo 42, paragrafo 1, e approva i criteri di certificazione a norma dell'articolo 42, paragrafo 5;
o) ove applicabile, effettua un riesame periodico delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7; 4.5.2016 L 119/68 Gazzetta ufficiale dell'Unione europea IT
p) definisce e pubblica i criteri per l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 41 e di un organismo di certificazione ai sensi dell'articolo 43;
q) effettua l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 41 e di un organismo di certificazione ai sensi dell'articolo 43;
r) approva le norme vincolanti d'impresa ai sensi dell'articolo 47;
s) contribuisce alle attività del comitato;
t) tiene registri interni delle violazioni del presente regolamento e delle misure adottate in conformità dell'articolo 58, paragrafo 2;
u) svolge qualsiasi altro compito legato alla protezione dei dati personali.

Poteri

Poteri di indagine

a) ingiungere al titolare del trattamento e al responsabile del trattamento e, ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento, di fornirle ogni informazione di cui necessiti per l'esecuzione dei suoi compiti;
b) condurre indagini sotto forma di attività di revisione sulla protezione dei dati;
c) effettuare un riesame delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7;
d) notificare al titolare del trattamento o al responsabile del trattamento le presunte violazioni del presente regolamento;
e) ottenere, dal titolare del trattamento o dal responsabile del trattamento, l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti;
f) ottenere accesso a tutti i locali del titolare del trattamento e del responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri.

Poteri correttivi

a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento;
b) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento;
c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento;
d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine;
e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;

g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19;
h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;
i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso;
j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

Poteri autorizzativi e consultivi

a) fornire consulenza al titolare del trattamento, secondo la procedura di consultazione preventiva di cui all'articolo 36;
b) rilasciare, di propria iniziativa o su richiesta, pareri destinati al parlamento nazionale, al governo dello Stato membro, oppure, conformemente al diritto degli Stati membri, ad altri organismi e istituzioni e al pubblico su questioni riguardanti la protezione dei dati personali;
c) autorizzare il trattamento di cui all'articolo 36, paragrafo 5, se il diritto dello Stato membro richiede una siffatta autorizzazione preliminare;
d) rilasciare un parere sui progetti di codici di condotta e approvarli, ai sensi dell'articolo 40, paragrafo 5;
e) accreditare gli organismi di certificazione a norma dell'articolo 43;
f) rilasciare certificazioni e approvare i criteri di certificazione conformemente all'articolo 42, paragrafo 5;
g) adottare le clausole tipo di protezione dei dati di cui all'articolo 28, paragrafo 8, e all'articolo 46, paragrafo 2, lettera d);
h) autorizzare le clausole contrattuali di cui all'articolo 46, paragrafo 3, lettera a);
i) autorizzare gli accordi amministrativi di cui all'articolo 46, paragrafo 3, lettera b);
j) approvare le norme vincolanti d'impresa ai sensi dell'articolo 47.

M1.27 One stop shop e cooperazione

Il nuovo Regolamento europeo per la protezione dei dati personali introduce il principio dello sportello unico (*one stop shop*).
Poiché l'obiettivo del regolamento europeo è quello di armonizzare le norme e l'applicazione di tali norme nel territorio dell'Unione, tale principio stabilisce che le imprese, e in genere i titolari del trattamento, avranno a che fare con una sola Autorità di controllo, cioè quella del paese dove hanno la sede principale, piuttosto che con le autorità di 28 Stati europei. Ciò che decide l'autorità di controllo nazionale (es. le norme vincolanti di impresa) trova applicazione anche negli altri paesi dell'Unione.

Questo principio, fortemente auspicato dalle imprese, porta alla semplificazione delle procedure e dovrebbe garantire una maggiore coerenza delle decisioni. Di contro consente all'azienda di scegliersi l'Autorità di vigilanza con la quale avrà a che fare, potendo ovviamente decidere dove stabilire la sede nell'ambito del territorio dell'Unione.

Tale principio si pone anche in contrapposizione con i principi alla base della normativa posta a tutela dei consumatori, che radica la competenza di un Giudice presso la residenza del consumatore medesimo. Tutto ciò finisce per alimentare l'idea di un'Europa burocratica e lontana dai cittadini.

Cooperazione

L’art. 60 del Regolamento prevede in determinati casi una particolare procedura definita di cooperazione tra l'autorità di controllo capofila e le altre autorità di controllo interessate al fine di raggiungere un consenso.
L'autorità di controllo capofila e le autorità di controllo interessate si scambiano tutte le informazioni utili e l'autorità di controllo capofila può chiedere in qualunque momento alle altre autorità di controllo interessate di fornire assistenza reciproca a norma dell'articolo 61 e può condurre operazioni congiunte a norma dell'articolo 62, in particolare per lo svolgimento di indagini o il controllo dell'attuazione di una misura riguardante un titolare del trattamento o responsabile del trattamento stabilito in un altro Stato membro.

Se una delle altre autorità di controllo interessate solleva un'obiezione pertinente e motivata al progetto di decisione entro un termine di quattro settimane dopo essere stata consultata, l'autorità di controllo capofila, ove non dia seguito all'obiezione pertinente e motivata o ritenga l'obiezione non pertinente o non motivata, sottopone la questione al meccanismo di coerenza di cui all'articolo 63.
In caso contrario se l'autorità di controllo capofila, intende dare seguito all'obiezione pertinente e motivata sollevata, trasmette un progetto di decisione riveduto alle altre autorità di controllo interessate per ottenere il loro parere.

Meccanismo di coerenza

L’art. 63 del Regolamento sancisce che al fine di contribuire all'applicazione coerente dello stesso Regolamento in tutta l'Unione, le autorità di controllo cooperano tra loro e, se del caso, con la Commissione mediante il meccanismo di coerenza.

In determinate circostanze l'Autorità di Controllo competente può comunicare un progetto di decisione al Comitato europeo che emette un parere.
In particolare l'Autorità di controllo si rivolge al Comitato quando la decisione:
-è finalizzata a stabilire un elenco di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35, paragrafo 4;
- riguarda una questione di cui all'articolo 40, paragrafo 7, relativa alla conformità al presente regolamento di un progetto di codice di condotta o una modifica o proroga di un codice di condotta;
- è finalizzata ad approvare i criteri per l'accreditamento di un organismo ai sensi dell'articolo 41, paragrafo 3, o di un organismo di certificazione ai sensi dell'articolo 43, paragrafo 3;
- è finalizzata a determinare clausole tipo di protezione dei dati;
- è finalizzata ad autorizzare clausole contrattuali di cui all'articolo 46, paragrafo *3, lettera a)* oppure è finalizzata ad approvare norme vincolanti d'impresa ai sensi dell'articolo 47.

Il parere è adottato dal Comitato entro un termine di otto settimane a maggioranza semplice dei membri. Tale termine può essere prorogato di sei settimane, tenendo conto della complessità della questione.
L'autorità di controllo tiene nella massima considerazione il parere del comitato e, entro due settimane dal ricevimento del parere, comunica per via elettronica, usando un modulo standard, al presidente del comitato se intende mantenere o modificare il progetto di decisione e, se del caso, il progetto di decisione modificato.
Se l'autorità di controllo interessata informa il presidente del comitato, fornendo le pertinenti motivazioni, che non intende conformarsi al parere del comitato, in tutto o in parte, quest'ultimo dovrà adottare una decisione vincolante di cui all'art. 65 del Regolamento.

Ai sensi dell'art. 65 del Regolamento il comitato adotta una decisione vincolante nei seguenti casi:

-se un'autorità di controllo interessata ha sollevato un'obiezione pertinente e motivata a un progetto di decisione dell'autorità capofila o l'autorità capofila ha rigettato tale obiezione in quanto non pertinente o non motivata.

- se vi sono opinioni contrastanti in merito alla competenza delle autorità di controllo interessate per lo stabilimento principale;

- se un'autorità di controllo competente non richiede il parere del comitato o non si conforma al parere del comitato emesso a norma dell'articolo 64.

La decisione è adottata entro un mese dal deferimento della questione da parte di una maggioranza di due terzi dei membri del comitato. Tale termine può essere prorogato di un mese, in considerazione della complessità della questione.

La decisione del comitato è motivata e trasmessa all'autorità di controllo capofila e a tutte le autorità di controllo interessate ed è per esse vincolante.

La decisione è pubblicata senza ritardo sul sito web del comitato dopo che l'autorità di controllo ha notificato la decisione definitiva.

M.1.28 EDPB
M1.29 Il Comitato europeo per la protezione dei dati
M1.30 Le Linee Guida/opinion del WP29
M1.31 Commissione Europea

L’art. 68 prevede il Comitato europeo per la protezione dei dati che è istituito come organismo dell'Unione ed è dotato di personalità giuridica. Il Comitato europeo per la protezione dei dati è rappresentato dal suo presidente.
Il Comitato europeo per la protezione dei dati è composto dal titolare di un'autorità di controllo di ciascuno Stato membro e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti.

Nell'adempimento dei suoi compiti o nell'esercizio dei suoi poteri, ai sensi degli articoli 70 e 71 del Regolamento, il Comitato europeo per la protezione dei dati opera con indipendenza.

I compiti

- sorveglia il Regolamento e ne assicura l'applicazione corretta;
- fornisce consulenza alla Commissione;
- pubblica linee guida, raccomandazioni e migliori prassi in materia di procedure per la cancellazione di link, copie o riproduzioni di dati personali; per specificare ulteriormente i criteri e le condizioni delle decisioni basate sulla profilazione; per accertare la violazione di dati personali; per specificare ulteriormente i criteri e i requisiti dei trasferimenti di dati personali; per stabilire procedure comuni per le segnalazioni da parte di persone fisiche di violazioni del regolamento;
- esamina, di propria iniziativa o su richiesta di uno dei suoi membri o della Commissione, qualsiasi questione relativa all'applicazione del regolamento;
- incoraggia l'elaborazione di codici di condotta e l'istituzione di meccanismi di certificazione della protezione dei dati;
- effettua l'accreditamento di organismi di certificazione e il suo riesame periodico a norma dell'articolo 43 e tiene un registro pubblico di organismi accreditati;
- fornisce alla Commissione un parere in merito ai requisiti di certificazione;

- fornisce alla Commissione un parere per valutare l'adeguatezza del livello di protezione in un paese terzo o in un'organizzazione internazionale;
- emette pareri sui progetti di decisione delle autorità di controllo conformemente al meccanismo di coerenza;
- promuove la cooperazione e l'effettivo scambio di informazioni e prassi tra le autorità di controllo a livello bilaterale e multilaterale;
- promuove programmi comuni di formazione e facilita lo scambio di personale tra le autorità di controllo e, se del caso, con le autorità di controllo di paesi terzi o di organizzazioni internazionali;
- promuove lo scambio di conoscenze e documentazione sulla legislazione e sulle prassi in materia di protezione dei dati tra autorità di controllo di tutto il mondo;
- emette pareri sui codici di condotta redatti a livello di Unione;
- tiene un registro elettronico, accessibile al pubblico, delle decisioni adottate dalle autorità di controllo e dalle autorità giurisdizionali su questioni trattate nell'ambito del meccanismo di coerenza.

M1.32 Il diritto privacy nazionale e rapporti con il GDPR

Dopo il regolamento europeo sulla protezione dei dati personali n. 2016/679 (GDPR), come noto è stato necessario emanare un decreto legislativo di adeguamento della normativa nazionale in materia di protezione dei dati personali e per la precisione il d.lgs. n. 101 del 10 agosto 2018 pubblicato il 4 settembre sulla G.U. n. 205.

Il d.lgs. n. 101/18 ha provveduto ad abrogare le disposizioni del d.lgs. n.196/2003 non più compatibili con il GDPR introducendone nuove, ma anche ad integrare e modificare le disposizioni che rimangono in vita. Ne è venuta fuori una versione del codice più ridotta ma anche più coerente con la normativa comunitaria.

Tale decreto è stato emanato nel rispetto di quanto sancito dall'art. 13 della legge n. 163/2017 che contiene una delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del GDPR.

La tecnica legislativa adottata dal legislatore è stata quella di evitare di duplicare alcune disposizioni, molto simili ma non coincidenti, presenti sia nel regolamento che nel codice, operando cosi una scelta chiara.
In effetti codice e regolamento sono informati a due filosofie diverse. Il regolamento, come è noto, è basato sulla cosiddetta accountability. Dunque il provvedimento comunitario non effettua la scelta in molti casi specifici, ma la rimette al titolare del trattamento che è chiamato ad effettuare una valutazione, ad assumere una decisione e a provare di avere adottato misure proporzionate ed efficaci.

Inoltre, si è voluto dare un segnale del cambiamento intervenuto: cioè del passaggio dalla direttiva 95/46/CE al regolamento (UE) 679/2016.
Dopo oltre 20 anni, la disciplina della protezione dei dati personali è stata oggetto di una riformulazione non formale ma sostanziale, essendo cambiato l'approccio stesso alla materia che oggi è dominata dal principio dell'accountability.

In particolare analizzando il testo legislativo si comprende come si sia scelto di garantire la continuità facendo salvi per un periodo transitorio i provvedimenti del Garante e le autorizzazioni, che saranno oggetto di successivo riesame, nonché i Codici deontologici vigenti. Essi restano fermi nell'attuale configurazione nelle materie di competenza degli Stati membri, mentre possono essere riassunti e modificati su iniziativa delle categorie interessate quali codici di settore.

Le disposizioni concernenti le comunicazioni elettroniche non sono state modificate, in attesa dell'emanando regolamento europeo in materia di e-privacy.
Inoltre molte disposizioni del previgente codice non sono state espressamente richiamate, perché assorbite dalle norme del regolamento europeo. Fra queste, a mero titolo esemplificativo, quelle che consentono di trattare i dati senza consenso per la finalità dell'esercizio del diritto di difesa. Il trattamento di questi dati, così come il trattamento dei dati provenienti da registri pubblici, o la comunicazione dei dati infragruppo, rientra certamente nei presupposti di legittimità del trattamento previsti dall'articolo 6 del regolamento e in particolare nell'esercizio del "legittimo interesse" cui il regolamento accorda ampio spazio.

Nel complesso il decreto è suddiviso in sei Capi e si compone di 27 articoli, dedicati a specifici aspetti della materia. Cerchiamo di analizzare i punti salienti.

INTERESSE PUBBLICO

E' inserito il richiamo alla legge e ai regolamenti come base giuridica e presupposto di liceità del trattamento svolto “per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri” .

LIMITAZIONE DEI DIRITTI

I diritti dell'interessato possono essere limitati in caso di pregiudizio per altri interessi normativamente tutelati (es: antiriciclaggio, sostegno alle vittime di estorsione, ragioni di giustizia ...)

CONSENSO DEL MINORE

Il minore che ha compiuto 14 anni può esprimere il consenso al trattamenti dei dati personali.

PERSONE DECEDUTE

I diritti della persona deceduta possono essere esercitati da chi abbia un interesse proprio o agisca a tutela dell'interessato o da un mandatario.

DATI BIOMETRICI, GENETICI E RELATIVI ALLA SALUTE

Per i dati genetici, biometrici e relativi alla salute il trattamento è subordinato al rispetto di misure di garanzia disposte dal Garante ogni due anni.

FIGURE INTERMEDIE

Alcuni compiti e funzioni in capo al titolare e al responsabile possono essere delegati a persone fisiche operanti sotto la loro autorità.

CONDANNE PENALI E REATI

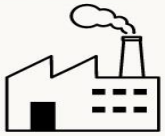
Il trattamento di dati concernenti condanne penali e reati è consentito nei limiti di quanto previsto da norme di legge o di regolamento.

INUTILIZZABILITA' DEI DATI

I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati, salvo quanto previsto dall’articolo 160-bis

PICCOLE E MEDIE IMPRESE

Il Garante, ha il potere di introdurre meccanismi di semplificazione per le micro, piccole e medie imprese.



REGIME TRANSITORIO SANZIONI

Per i primi 8 mesi il Garante tiene conto, per l'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con il GDPR, della fase di prima applicazione delle disposizioni sanzionatorie.

Base giuridica per l'esecuzione di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri

L’art. 2 del provvedimento introduce l'articolo 2-ter del codice privacy il quale specifica che per quanto riguarda i trattamenti effettuati per "l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri" la base giuridica per i trattamenti aventi ad oggetto dati personali "comuni" sia da rinvenirsi esclusivamente in una norma di legge o di regolamento.

L'articolo si presenta come una riformulazione del previgente articolo 19 del Codice, il cui ambito di applicazione soggettivo viene, però, esteso al fine di adeguarsi all'impostazione adottata dal Regolamento.

Nel Regolamento, infatti – come può leggersi nella relazione - scompare la distinzione basata sulla natura pubblica o privata dei soggetti che trattano i dati, rilevando unicamente la finalità del trattamento perseguita, vale a dire se la finalità concerne un interesse pubblico o privato.

Consenso del minore

Viene introdotto anche l'articolo 2-quinquies del codice in materia di protezione dei dati personali il quale stabilisce che in attuazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione.

Con riguardo a tali servizi, naturalmente il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale.

Individuazione degli interessi pubblici

In relazione al trattamento di particolari categorie di dati viene stabilito l'obbligo di previsione normativa ed è individuato un elenco di trattamenti che si considerano effettuati per "motivi di interesse pubblico rilevante" (art. 2-sexies in relazione all'art. 9 del Regolamento concernente i dati che il Codice previgente definiva "dati sensibili")

Il regime normativo per tali trattamenti è sostanzialmente rimasto inalterato rispetto a quello previsto dal Codice per i trattamenti effettuati da soggetti pubblici (art. 20) e, in particolare, l'elenco predetto è tratto dalle diverse disposizioni del Codice riferite ai trattamenti effettuati per finalità di rilevante interesse pubblico (ad es. artt. 64-73, che il decreto abroga).

- accesso a documenti amministrativi e accesso civico;
- tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia;
- tenuta di registri pubblici relativi a beni immobili o mobili;
- cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;
- elettorato attivo e passivo ed esercizio di altri diritti politici;
- esercizio del mandato degli organi rappresentativi;
- svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo;
- attività di controllo e ispettive;
- concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
- conferimento di onorificenze e ricompense;
- rapporti tra i soggetti pubblici e gli enti del terzo settore;
- obiezione di coscienza;
- attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;
- compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario;
- istruzione e formazione in ambito scolastico, professionale, superiore o universitario;
- instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo.

Misure di garanzia per i dati genetici, biometrici e relativi alla salute

Con riferimento ai dati genetici, biometrici e relativi alla salute, inoltre, oggetto di specifica "riserva" della normativa nazionale (cfr. art. 9, par. 4, Reg.), viene previsto che il relativo trattamento è subordinato anche al rispetto di misure di garanzia disposte dal Garante (art. 2-septies del codice) con provvedimento, soggetto a consultazione pubblica, adottato con cadenza almeno biennale.

In particolare, le misure di garanzia individuano le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonimizzazione, misure di minimizzazione, specifiche modalità di accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché eventuali altre misure necessarie a garantire i diritti degli interessati.

Trattamento dati concernenti condanne penali e reati

Anche il trattamento di dati concernenti condanne penali e reati (che trovano nei "dati giudiziari" del Codice il loro "antecedente") è consentito nei limiti di quanto previsto da norme di legge o di regolamento (art. 2-octies; cfr. già art. 21, d. lgs. n. 196/2003), salvo, ovviamente, quanto stabilito dal d.lgs . n. 51 del 18 maggio 2018 che ha recepito in Italia la direttiva UE 2016/680.

Salvaguardia dei codici di deontologia e buona condotta

Il d.lgs. n. 101/2018 introduce anche l'articolo 2-decies del codice che conferma l'inutilizzabilità dei dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali (cfr art. 12, comma 2, d. lgs. 196/2003), come pure nell'articolo 2-quater è fatta salva l'adozione di "regole deontologiche" negli ambiti in cui il Regolamento riserva la materia agli Stati membri:
a) trattamenti necessari per adempiere un obbligo legale;
b) trattamenti necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
c) trattamento di dati genetici, biometrici o relativi alla salute;
d) talune specifiche situazioni di trattamento di cui al Capo IX.

Tale disposizione trova la propria ratio nella scelta di conservare le regole stabilite nei "Codici di deontologia e di buona condotta", previsti all'articolo 12 del previgente Codice che sino ad oggi hanno costituito una rilevante fonte di riferimento per i settori a cui sono diretti; ciò, però, solo nelle materie oggetto di "riserva" normativa interna agli Stati membri (art. 6, par. 2, Reg.).

In effetti proprio recentemente il Garante ha verificato la conformità dei Codici di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici, statistici, scientifici e investigazioni difensive nonché del Codice deontologico dei giornalisti al Regolamento Ue 2016/679 sulla protezione dei dati personali.

Limitazione dei diritti degli interessati

Gli artt. 2-undecies e 2-duodecies del d.lgs. 196/2003 introdotti dal d.lgs. n. 101/2018 concernente i diritti garantiti all'interessato, sulla falsariga di quanto previsto dall'articolo 8 del Codice previgente, contiene ipotesi di limitazione degli stessi in caso di concreto pregiudizio per altri interessi normativamente tutelati (antiriciclaggio, sostegno delle vittime di atti estorsivi, attività delle commissioni parlamentari d'inchiesta, controllo dei mercati finanziari e monetari, esercizio di diritti in sede giudiziaria e per ragioni di giustizia, indipendenza della magistratura).

Trattamento dati di persone decedute

Alcuni aspetti innovativi presenta, invece, rispetto alla disposizione del Codice previgente (art. 9, comma 3), il nuovo articolo 2-terdecies, concernente il trattamento relativo ai dati di persone decedute, che attribuisce l'esercizio dei diritti dell'interessato a chi abbia un interesse proprio o agisca a tutela dell'interessato o per particolari ragioni familiari, ma anche al mandatario.

Previsione di figure intermedie operanti sotto l'autorità del titolare o responsabile

Molto importante è l'art. 2-quaterdecies del codice introdotto sempre dall'art. 2 del d.lgs. n. 101/2018 che reca una serie di disposizioni volte a precisare taluni poteri e obblighi in capo al titolare e al responsabile, tra cui la possibilità di delegare compiti e funzioni a persone fisiche operanti sotto la loro autorità e responsabilità.

Tale disposizione assume una particolare rilevanza in quanto risolve in parte le diverse problematiche sorte a seguito di quanto stabilito dall'art. 28 del GDPR che concepisce il solo responsabile esterno del trattamento.
Viene poi precisato che ogni qualvolta il titolare intende effettuare un trattamento connesso all'esecuzione di un compito di pubblico interesse che presenta rischi particolarmente elevati, deve obbligatoriamente chiedere la previa autorizzazione del Garante (cfr. art. 36, comma 5, Reg).

Consenso degli interessati in materia sanitaria

Di particolare rilevanza è quanto sancito in materia sanitaria dove ormai anche a seguito della nuova formulazione dell'art. 75 del d.lgs. n. 196/2003 è chiarito che non occorre più il consenso per il trattamento dei dati per finalità di diagnosi e cura (art. 2-septies del Codice Privacy emendato) anche se occorrerà sempre rispettare le misure di garanzie stabilite dal Garante con cadenza biennale.

L'obbligo di informativa al paziente continua ad essere reso in area sanitaria con modalità semplificate (art. 78 e 79 del Codice Privacy emendato).

Lo stesso consenso dell'interessato, nella nuova formulazione dell'art. 110 del codice per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando, tra l'altro, la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del GDPR.

Caratteristiche del reclamo

Avuto poi riferimento alle forme di tutela dinanzi al Garante il d.lgs. n. 101/2018 dedica una particolare attenzione alla disciplina del reclamo che presenta molte affinità con il ricorso del codice previgente. In realtà viene precisato nell'art. 142 rinnovellato che il procedimento relativo all'esame dei reclami sarà disciplinato dal garante con un proprio regolamento, anche se le tempistiche sono sicuramente più lunghe visto che il nuovo art. 143 del codice precisa, al 3° comma, che il Garante decide il reclamo entro nove mesi dalla presentazione.

Autorizzazioni generali

L'art. 21 del d.lgs. n. 101/2018 cerca di salvaguardare le autorizzazioni generali del Garante per la protezione dei dati personali prevedendo però che la stessa Autorità con provvedimento di carattere generale da porre in consultazione pubblica entro novanta giorni dalla data di entrata in vigore del decreto, individui le prescrizioni contenute nelle autorizzazioni generali già adottate, relative alle situazioni di trattamento di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 2, lettera b) e 4, nonché al Capo IX del regolamento (UE) 2016/679, che risultano compatibili con le disposizioni del medesimo regolamento e del presente decreto e, ove occorra, provvede al loro aggiornamento. Il provvedimento deve essere adottato entro sessanta giorni dall'esito del procedimento di consultazione pubblica.

In effetti proprio recentemente con provvedimento n. 497 del 13 dicembre 2018 l'Autorità ha proceduto alla revisione delle nove autorizzazioni generali al trattamento dei dati precedentemente esistenti secondo i criteri stabiliti dal decreto n. 101/2018.
In base all'analisi effettuata, quattro autorizzazioni hanno cessato completamente i loro effetti, in particolare: Autorizzazione generale n. 2/2016 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale; Autorizzazione generale n. 4/2016 al trattamento dei dati sensibili da parte dei liberi professionisti; Autorizzazione generale n. 5/2016 al trattamento dei dati sensibili da parte di diverse categorie di titolari; Autorizzazione generale n. 7/2016 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici.
Sono state invece individuate cinque autorizzazioni che contengono specifiche prescrizioni compatibili con il nuovo assetto normativo: Autorizzazione generale n. 1/2016 al trattamento dei dati sensibili nei rapporti di lavoro; Autorizzazione generale n. 3/2016 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni; Autorizzazione generale n. 6/2016 al trattamento dei dati sensibili da parte degli investigatori privati; Autorizzazione generale n. 8/2016 al trattamento dei dati genetici; Autorizzazione generale n. 9/2016 al trattamento dei dati personali effettuato per scopi di ricerca scientifica.

Disciplina semplificata per piccole e medie imprese

Il Garante ha il potere di introdurre meccanismi di semplificazione per le micro, piccole e medie imprese, con riferimento agli obblighi del titolare del trattamento.
In particolare l'art. 154-bis comma 4 del Codice Privacy emendato sancisce che in considerazione delle esigenze di semplificazione delle micro, piccole e medie imprese, come definite dalla raccomandazione 2003/361/CE, il Garante per la protezione dei dati personali, nel rispetto delle disposizioni del Regolamento e del Codice, promuove, nelle linee guida adottate a norma del comma 1, lettera a), modalità semplificate di adempimento degli obblighi del titolare del trattamento.

Particolare riguardo per i primi 8 mesi dalla data di entrata in vigore del decreto nell'applicazione delle sanzioni

L'applicazione delle sanzioni dovrà tenere conto, per i primi otto mesi dalla data di entrata in vigore del decreto, della fase di prima applicazione delle sanzioni stesse (art. 22, comma 13, del Decreto di adeguamento). Quindi le ispezioni ci saranno, ma terranno conto di tutti gli strumenti che gli ispettori hanno a loro disposizione e non solo delle sanzioni.