filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

# Il regolamento UE 2016/679 sul trattamento e la circolazione dei dati personali: una sintetica ricognizione

19 Settembre 2017
Alessandra Sarlo

**Premessa**

Scopo di questo scritto è di evidenziare, con un taglio ricognitivo e di sintesi, gli aspetti di maggiore rilievo del Regolamento 2016/679, in direzione sia dei soggetti protetti che di coloro, tra questi con particolare evidenza le p.a., cui vengono assegnati gli obblighi necessari a realizzare la protezione.

Il provvedimento, in vigore dal 24 maggio 2016 ed applicabile dal 25 maggio 2018, assicura effettività e concretezza al diritto di protezione dei dati personali, riconosciuto ad ogni persona fisica dalla Carta dei diritti fondamentali dell'UE e dal trattato sul funzionamento dell'UE.

Il legislatore europeo prende atto del considerevole aumento dei flussi transfrontalieri di tali dati, tanto più agevolato dalla globalizzazione e dalla rapidità dell'evoluzione tecnologica.

Si preoccupa quindi di adottare tutte le misure necessarie per assicurare agli individui il controllo delle informazioni che li riguardano e far sì che il loro trattamento sia "*al servizio dell'uomo*".

Riconosce tuttavia che **il diritto alla protezione ha una funzione sociale, sicché non ha portata assoluta e deve essere contemperato con altri diritti fondamentali in un'ottica di proporzionalità**.

Osserva anche che la regolamentazione precedente ha portato ad un'eccessiva frammentazione dei livelli di protezione dei dati personali il che rende necessario il rafforzamento e una disciplina più dettagliata dei diritti dei titolari dei dati personali e dei correlati obblighi di coloro che determinano ed effettuano il trattamento.

La prospettive e le finalità dell'atto legislativo europeo rendono quanto mai evidente la sua importanza e l'ampiezza delle conseguenze che produrrà negli ordinamenti giuridici degli Stati eurounitari.

È dunque innegabile ed oggettivo l'interesse dei pratici e degli studiosi ad un'analisi puntuale del Regolamento 679 e di ciascuna delle sue linee direttrici.

**L'ambito applicativo**

Il Regolamento ha ad oggetto il trattamento e la circolazione dei dati personali contenuti in un archivio o destinati a confluirvi.

L'atto, nella parte iniziale, definisce opportunamente e con accuratezza i concetti essenziali ai fini della sua esatta comprensione e applicazione.

Il legislatore europeo adotta anzitutto una definizione amplissima di **dati personali**, considerando come tali (art. 3.1) tutte le informazioni riguardanti persone fisiche identificate o identificabili.

Il **trattamento** (art. 3.2) è inteso come "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*

”.

La **profilazione** (art. 3.4) è “*qualsiasi forma di trattamento automatizzato di dati personali consistente nell’utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l’affidabilità, il comportamento, l’ubicazione o gli spostamenti di detta persona fisica*”.

La **pseudonimizzazione** (art. 3.5) è il “*trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l’utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*”.

L’**archivio** (art. 3.6) è “*qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico*”.

Il **titolare del trattamento** (art. 3.7) è “*la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*”.

Il **responsabile del trattamento** (art. 3.8) è “*la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*”.

Il **destinatario** (art. 3.9) è “*la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che riceve comunicazioni di dati personali, che si tratti o meno di terzi”*.

Il **terzo** (art. 3.10) è “*la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che non sia l’interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l’autorità diretta del titolare o del responsabile*”.

**Il decalogo dei principi (art. 5)**

Il legislatore europeo compila una sorta di decalogo dei principi cui deve attenersi ogni attività di trattamento di dati.

Prescrive dunque che il trattamento debba avvenire in modo lecito, corretto e trasparente, che la raccolta dei dati avvenga esclusivamente per finalità determinate, esplicite e legittime e abbia ad oggetto soltanto i dati adeguati, pertinenti e limitati per la realizzazione di tali finalità, che i dati raccolti siano esatti e tempestivamente aggiornati, che siano conservati in una forma che consenta l’identificazione degli interessati per un lasso di tempo non superiore a quello necessario, che i dati siano trattati in modo da garantirne la sicurezza e la protezione da trattamenti illeciti o non autorizzati e da evitarne la perdita, la distruzione e la sottoposizione a danni accidentali.

**Quando è lecito il trattamento (art. 6)**

Il trattamento dei dati personali è lecito se è esplicitamente consentito dal titolare oppure quando sia necessario per l’adempimento di obblighi contrattuali, la cura di interessi vitali del titolare o di terzi, l’assicurazione di obblighi di legge del titolare, per ragioni di interesse pubblico, per un interesse legittimo prevalente del titolare o di terzi.

**In particolare: il consenso (artt. 8 e 9)**

Spetta al titolare del trattamento l'onere di dimostrare l'avvenuta prestazione del consenso che deve essere libero, specifico, informato ed inequivocabile.

Se è contenuto in una dichiarazione scritta ad oggetto multiplo, il consenso è efficace solo se sia stato richiesto "*in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro*".

Il titolare può revocare il consenso in qualsiasi momento e deve essere preventivamente informato di tale suo diritto.

**I minori ultrasedicenni possono esprimere personalmente il consenso. È invece necessario il consenso dei genitori per gli infrasedicenni**.

**Quali diritti per il titolare dei dati (artt. 12 e ss.)**

Il regolamento 2016/679 dedica un'ampia sezione ai diritti del titolare dei dati.

È di particolare ampiezza, anzitutto, il **diritto, correlato ad un obbligo del titolare del trattamento, ad essere informato adeguatamente al momento della comunicazione dei dati**.

L'informativa deve comprendere l'identità e i dati di contatto del titolare del trattamento e, se presente, del responsabile della protezione dei dati.

Deve poi chiarire le finalità del trattamento e la sua base giuridica e identificare i legittimi interessi perseguiti dal titolare del trattamento o da terzi e gli eventuali destinatari o categorie di destinatari dei dati personali.

Il titolare del trattamento è tenuto inoltre ad indicare all'interessato **il periodo di conservazione dei dati**, il suo diritto a chiedere l'accesso ai dati, la loro rettifica o la cancellazione, la limitazione del loro trattamento, l'opposizione al trattamento e il diritto di portabilità degli stessi, il diritto di proporre reclamo a un'autorità di controllo, l'esistenza di processi decisionali automatizzati (compresa la profilazione).

Diritti e informative analoghe sono previsti (art. 14) quando i dati personali non siano stati ottenuti dall'interessato.

Una speciale rilevanza è riconosciuta al **diritto di accesso dell'interessato** (art. 15).

Esso comprende il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati e, in caso positivo, di accedere ai medesimi e di conoscere le finalità del trattamento, i destinatari, il periodo, il diritto di reclamo ed altro ancora.

Di pari importanza è il **diritto alla cancellazione, altrimenti definito diritto all'oblio** (art. 17).

L'interessato può chiedere e ottenere la cancellazione dei dati personali che lo riguardano quando ricorra almeno uno dei seguenti casi: venir meno della necessità del trattamento rispetto alle finalità originarie; revoca del consenso; opposizione al trattamento; illiceità del trattamento.

Il **diritto di limitazione del trattamento** (art. 18), a sua volta, è attribuito al titolare dei dati personali allorchè questi abbia contestato l'esattezza dei dati e fino a che il titolare del trattamento abbia completato le opportune verifiche, se il trattamento è stato illecito, se il titolare non ha più bisogno dei dati ma questi servono all'interessato in sede giudiziaria.

Il **diritto alla portabilità dei dati** (art. 20) consente all'interessato di ricevere in formato strutturato, di uso comune e leggibile da un dispositivo automatico, i dati personali che lo riguardano e che siano stati forniti al titolare del trattamento.

Spetta inoltre all'interessato la trasmissione di tali dati ad un altro titolare di trattamenti senza che il precedente titolare possa frapporre alcun impedimento.

È bene chiarire che il diritto in questione è limitato ai dati chiaramente riferibili all'interessato (sono quindi

esclusi, a titolo di esempio, i dati anonimi), trattati sulla base di un consenso preventivo, forniti consapevolmente e attivamente dall'interessato.
Di notevole interesse è il **diritto dell'interessato a non essere sottoposto a decisioni fondate unicamente sul trattamento automatizzato, ivi compresa la profilazione, che producano effetti giuridici che lo riguardano o che comunque incidano significativamente sulla sua persona** (art.22).
È facile intravedere in questa norma la concreta realizzazione del quarto "considerando" del Regolamento e del suo richiamo all'umanesimo che dovrebbe caratterizzare le attività di trattamento dei dati.
Al tempo stesso, il diritto pone un freno alla progressiva tendenza, agevolata dalla formazione di gigantesche banche digitali (i cosiddetti **big data**) nelle mani dei provider più radicati sul mercato, di utilizzare la profilazione digitale come base per la creazione di identità digitali imposte, cioè costruite senza alcun concorso di colui al quale sono applicate.

**I titolari e i responsabili del trattamento e i responsabili della protezione dei dati (artt. 24 e ss.)**
Quest'ampia sezione del Regolamento disciplina principalmente i doveri delle persone fisiche o giuridiche che determinano e controllano le attività di trattamento dati.
In via generale (art. 25), il **titolare del trattamento** è tenuto ad adottare le misure tecniche e organizzative adeguate a garantire e dimostrare che il trattamento è svolto in piena conformità al Regolamento e che ha ad oggetto solo i dati personali necessari per le sue finalità.
Una notevole importanza è attribuita al **responsabile del trattamento** (art. 28).
Si prevede che costui debba garantire sufficientemente la sua adeguatezza a realizzare i compiti indicati nell'art. 25.
Il suo ruolo e le sue funzioni devono essere disciplinati da un accordo giuridico in forma scritta che indichi con chiarezza gli obblighi assunti, soprattutto per ciò che concerne la coerenza del trattamento al Regolamento e la sua riservatezza e le modalità da rispettare nel caso di delega di funzioni ad altro responsabile.
L'art. 30 istituisce i **registri delle attività di trattamento**.
Essi devono contenere tutte le informazioni essenziali per l'identificazione del trattamento, del suo oggetto, delle misure tecniche e organizzative assunte per la sua salvaguardia e di chi ne ha avuto la responsabilità.
**L'obbligo dei registri non è applicabile alle imprese e organizzazioni che abbiano meno di 250 dipendenti**, fatta eccezione per i casi in cui il trattamento possa comportare rischi per i diritti e le libertà dell'interessato, non sia occasionale oppure includa categorie particolari di dati, ivi compresi quelli su condanne penali e reati.
Il titolare del trattamento, il responsabile e gli eventuali incaricati sono tenuti a collaborare con l'autorità di controllo (art. 31).
Il titolare e il responsabile del trattamento sono tenuti a predisporre le misure tecniche e organizzative idonee a garantire un adeguato livello di sicurezza contro i rischi per i diritti e le libertà delle persone fisiche (art. 32).
Deve essere prioritaria l'attenzione ai rischi connessi alla distruzione, perdita, modifica, diffusione non autorizzata e accesso accidentale o illegale ai dati personali trasmessi, conservati o comunque trattati.
Fanno parte di tali misure la pseudonimizzazione e la cifrature dei dati personali, l'assicurazione permanente della riservatezza, integrità, disponibilità e resilienza dei sistemi e servizi di trattamento, il ripristino tempestivo della disponibilità e dell'accesso dei dati personali a seguito di incidenti fisici o tecnici, le procedure per testare, verificare e valutare con regolarità l'efficacia delle misure tecniche e

organizzative.
Ove si sia verificata una violazione dei dati personali (art. 33), il titolare del trattamento è tenuto a notificarla tempestivamente all'autorità di controllo, fornendo tutte le informazioni utili per determinarne la natura e le conseguenze e chiarire le misure adottate per porre rimedio.
La violazione va inoltre comunicata all'interessato (art. 34) se ricorra un rischio elevato per i suoi diritti e le sue libertà.
L'art. 35 disciplina l'innovativo istituto della **valutazione di impatto sulla protezione dei dati**.
In forza di questa disposizione, il titolare del trattamento è tenuto a compiere una valutazione preventiva dell'impatto di un trattamento sulla protezione dei dati personali ogni qualvolta esso richieda l'uso di nuove tecnologie che comportino un rischio elevato per i diritti e le libertà delle persone fisiche.
Questo presupposto è considerato sempre esistente quando sia prevista una valutazione sistematica e globale (compresa la profilazione) di aspetti personali relativi a persone fisiche da cui dipendono decisioni che producono effetti giuridici o comunque incidono significativamente sulle persone medesime.
Lo stesso vale per trattamenti su larga scala di categorie particolari di dati personali compresi tra quelli elencati nell'art. 9 paragrafo 1 o relativi a condanne penali e reati e per sorveglianze sistematiche su larga scala di zone accessibili al pubblico.
Spetta comunque all'autorità di controllo redigere e rendere pubblici gli elenchi di tipologie di trattamenti sottoposti alla valutazione di impatto.
Gli artt. 37/39 disciplinano il ruolo e le funzioni del **responsabile della protezione dei dati**.
La sua designazione è obbligatoria (art. 37) per i trattamenti svolti da autorità e organismi pubblici (fatta eccezione per le autorità giurisdizionali nell'esercizio delle loro funzioni tipiche), per i trattamenti che richiedono monitoraggi regolari e sistematici degli interessati su larga scala, per i trattamenti dei dati personali particolari elencati dall'art. 9 paragrafo 1 o dei dati attinenti a condanne penali e reati.
**Il responsabile della protezione dei dati deve possedere adeguate qualità professionali, una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e la capacità di assolvere i compiti che gli spettano.**
Egli deve essere tempestivamente e adeguatamente informato e coinvolto in tutte le questioni che riguardano la protezione dei dati e deve disporre delle risorse necessarie per far fronte alle sue responsabilità, la cui dettagliata elencazione è contenuta nell'art. 39.
L'art. 40 incoraggia l'adozione di **codici di condotta** "*destinati a contribuire alla corretta applicazione del presente regolamento, in funzione della specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese*".
L'art. 42 a sua volta auspica l'istituzione di **meccanismi di certificazione della protezione dei dati** allo scopo di dimostrare la coerenza dei trattamenti alla normativa regolamentare, precisando comunque che **la certificazione è volontaria, non riduce la responsabilità del titolare e del responsabile del trattamento per eventuali violazioni, lascia impregiudicati i compiti e i poteri dell'autorità di controllo.**
Gli artt. 51 e ss. disciplinano le **autorità di controllo** cui spetta la sorveglianza sull'applicazione del regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei loro dati personali.

Di notevole interesse è il **diritto dell'interessato a non essere sottoposto a decisioni fondate unicamente sul trattamento automatizzato, ivi compresa la profilazione, che producano effetti giuridici che lo riguardano o che comunque incidano significativamente sulla sua persona** (art.22).
È facile intravedere in questa norma la concreta realizzazione del quarto "considerando" del Regolamento e del suo richiamo all'umanesimo che dovrebbe caratterizzare le attività di trattamento dei dati.
Al tempo stesso, il diritto pone un freno alla progressiva tendenza, agevolata dalla formazione di gigantesche banche digitali (i cosiddetti **big data**) nelle mani dei provider più radicati sul mercato, di utilizzare la profilazione digitale come base per la creazione di identità digitali imposte, cioè costruite senza alcun concorso di colui al quale sono applicate.

**I titolari e i responsabili del trattamento e i responsabili della protezione dei dati (artt. 24 e ss.)**
Quest'ampia sezione del Regolamento disciplina principalmente i doveri delle persone fisiche o giuridiche che determinano e controllano le attività di trattamento dati.
In via generale (art. 25), il **titolare del trattamento** è tenuto ad adottare le misure tecniche e organizzative adeguate a garantire e dimostrare che il trattamento è svolto in piena conformità al Regolamento e che ha ad oggetto solo i dati personali necessari per le sue finalità.
Una notevole importanza è attribuita al **responsabile del trattamento** (art. 28).
Si prevede che costui debba garantire sufficientemente la sua adeguatezza a realizzare i compiti indicati nell'art. 25.
Il suo ruolo e le sue funzioni devono essere disciplinati da un accordo giuridico in forma scritta che indichi con chiarezza gli obblighi assunti, soprattutto per ciò che concerne la coerenza del trattamento al Regolamento e la sua riservatezza e le modalità da rispettare nel caso di delega di funzioni ad altro responsabile.
L'art. 30 istituisce i **registri delle attività di trattamento**.
Essi devono contenere tutte le informazioni essenziali per l'identificazione del trattamento, del suo oggetto, delle misure tecniche e organizzative assunte per la sua salvaguardia e di chi ne ha avuto la responsabilità.
**L'obbligo dei registri non è applicabile alle imprese e organizzazioni che abbiano meno di 250 dipendenti**, fatta eccezione per i casi in cui il trattamento possa comportare rischi per i diritti e le libertà dell'interessato, non sia occasionale oppure includa categorie particolari di dati, ivi compresi quelli su condanne penali e reati.
Il titolare del trattamento, il responsabile e gli eventuali incaricati sono tenuti a collaborare con l'autorità di controllo (art. 31).
Il titolare e il responsabile del trattamento sono tenuti a predisporre le misure tecniche e organizzative idonee a garantire un adeguato livello di sicurezza contro i rischi per i diritti e le libertà delle persone fisiche (art. 32).
Deve essere prioritaria l'attenzione ai rischi connessi alla distruzione, perdita, modifica, diffusione non autorizzata e accesso accidentale o illegale ai dati personali trasmessi, conservati o comunque trattati.
Fanno parte di tali misure la pseudonimizzazione e la cifrature dei dati personali, l'assicurazione permanente della riservatezza, integrità, disponibilità e resilienza dei sistemi e servizi di trattamento, il ripristino tempestivo della disponibilità e dell'accesso dei dati personali a seguito di incidenti fisici o tecnici, le procedure per testare, verificare e valutare con regolarità l'efficacia delle misure tecniche e organizzative.
Ove si sia verificata una violazione dei dati personali (art. 33), il titolare del trattamento è tenuto a

notificarla tempestivamente all'autorità di controllo, fornendo tutte le informazioni utili per determinarne la natura e le conseguenze e chiarire le misure adottate per porre rimedio.
La violazione va inoltre comunicata all'interessato (art. 34) se ricorra un rischio elevato per i suoi diritti e le sue libertà.
L'art. 35 disciplina l'innovativo istituto della **valutazione di impatto sulla protezione dei dati**.
In forza di questa disposizione, il titolare del trattamento è tenuto a compiere una valutazione preventiva dell'impatto di un trattamento sulla protezione dei dati personali ogni qualvolta esso richieda l'uso di nuove tecnologie che comportino un rischio elevato per i diritti e le libertà delle persone fisiche.
Questo presupposto è considerato sempre esistente quando sia prevista una valutazione sistematica e globale (compresa la profilazione) di aspetti personali relativi a persone fisiche da cui dipendono decisioni che producono effetti giuridici o comunque incidono significativamente sulle persone medesime.
Lo stesso vale per trattamenti su larga scala di categorie particolari di dati personali compresi tra quelli elencati nell'art. 9 paragrafo 1 o relativi a condanne penali e reati e per sorveglianze sistematiche su larga scala di zone accessibili al pubblico.
Spetta comunque all'autorità di controllo redigere e rendere pubblici gli elenchi di tipologie di trattamenti sottoposti alla valutazione di impatto.
Gli artt. 37/39 disciplinano il ruolo e le funzioni del **responsabile della protezione dei dati**.
La sua designazione è obbligatoria (art. 37) per i trattamenti svolti da autorità e organismi pubblici (fatta eccezione per le autorità giurisdizionali nell'esercizio delle loro funzioni tipiche), per i trattamenti che richiedono monitoraggi regolari e sistematici degli interessati su larga scala, per i trattamenti dei dati personali particolari elencati dall'art. 9 paragrafo 1 o dei dati attinenti a condanne penali e reati.
**Il responsabile della protezione dei dati deve possedere adeguate qualità professionali, una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e la capacità di assolvere i compiti che gli spettano.**
Egli deve essere tempestivamente e adeguatamente informato e coinvolto in tutte le questioni che riguardano la protezione dei dati e deve disporre delle risorse necessarie per far fronte alle sue responsabilità, la cui dettagliata elencazione è contenuta nell'art. 39.
L'art. 40 incoraggia l'adozione di **codici di condotta** "*destinati a contribuire alla corretta applicazione del presente regolamento, in funzione della specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese*".
L'art. 42 a sua volta auspica l'istituzione di **meccanismi di certificazione della protezione dei dati** allo scopo di dimostrare la coerenza dei trattamenti alla normativa regolamentare, precisando comunque che **la certificazione è volontaria, non riduce la responsabilità del titolare e del responsabile del trattamento per eventuali violazioni, lascia impregiudicati i compiti e i poteri dell'autorità di controllo.**
Gli artt. 51 e ss. disciplinano le **autorità di controllo** cui spetta la sorveglianza sull'applicazione del regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei loro dati personali.
Si prescrive che ogni Stato UE deve prevedere una o più di tali autorità (in caso di pluralità, deve essere indicata l'autorità designata a far parte del Comitato europeo per la protezione dei dati).
Ad esse viene riconosciuta piena autonomia e gli si assicura la disponibilità di risorse umane, tecniche e finanziarie adeguate allo svolgimento dei compiti assegnatigli.
Si prevede che i loro componenti, da nominarsi attraverso procedure trasparenti, debbano possedere

un’adeguata specializzazione professionale.
Ciascuna autorità di controllo è competente ad eseguire i compiti e esercitare i poteri previsti dal Regolamento nel territorio dello Stato membro di appartenenza.
Più nel dettaglio, alle autorità di controllo (art. 57) sono attribuiti compiti di sorveglianza, sensibilizzazione pubblica, consulenza alle istituzioni nazionali, decisione dei reclami degli interessati, collaborazione con le analoghe autorità degli altri Stati UE, istruttorie ed altro ancora.
L’art. 58 elenca i poteri delle autorità distinguendo i poteri istruttori, correttivi, autorizzativi e consultivi.
Si prevede inoltre (art. 59) che le autorità elaborino relazioni annuali sulla loro attività da trasmettere alle autorità statali.
L’art. 68 istituisce il **Comitato europeo per la protezione dei dati** cui vengono attribuiti lo status di organismo dell’UE e la personalità giuridica.
Gli articoli seguenti ne disciplinano la composizione, i compiti, le procedure di funzionamento e ad essi si rimanda per le relative elencazioni.
La parte finale del Regolamento (artt. 77 e ss.) disciplina i diritti di reclamo e ricorso degli interessati avverso violazioni in loro danno della normativa regolamentare, le correlative responsabilità e gli obblighi risarcitori conseguenti all’accertamento di un’effettiva violazione, le sanzioni amministrative irrogabili e talune deroghe o esenzioni agli obblighi regolamentari giustificate da esigenze particolari.

**Conclusione**

Il Regolamento 679 ha composto un quadro organico ed avanzato di norme che hanno lo scopo di individuare il migliore equilibrio possibile tra diritti essenziali degli esseri umani quali l’identità e la riservatezza e l’inarrestabile espansione di sempre nuove possibilità tecnologiche che soddisfano, ma talvolta addirittura creano, esigenze informative e comunicative di impressionante ampiezza.
Questa disciplina rappresenta al tempo stesso un’opportunità e una sfida.
Offre precisi punti di riferimento in un contesto magmatico e in perenne cambiamento, plasma livelli di tutela piuttosto efficaci, tiene adeguatamente in conto gli interessi e i bisogni delle aziende e del mercato.
Al tempo stesso il Regolamento chiama a raccolta numerose categorie di soggetti, e tra questi le istituzioni pubbliche in posizione di primo piano, e impone attenzione, responsabilità, professionalità, specializzazione.
È indubbio poi che la normativa europea sui dati personali richiederà l’apporto di vari ceti professionali, particolarmente quelli dotati di competenze giuridiche, informatiche, gestionali, formative, certificative di standard di qualità.
Un’opportunità e una sfida alle quali è già ora di prepararsi, a pena di rimanere esclusi dalla grande corsa.

***TAG:*** *dati personali, Guida Regolamento UE Privacy, privacy, Regolamento privacy, GDPR, Diritto dell'Unione Europea, Diritto della privacy, Diritto delle nuove tecnologie e delle comunicazioni*

---

---