

PRIVACY

NUOVO REGOLAMENTO UE

1. Privacy - Nuovo Regolamento Ue
2. Novità introdotte dal Regolamento Ue
3. Informativa sulla privacy e consenso
4. Sicurezza dei dati
5. Impianto sanzionatorio

Studio Associato Trombetta Teruggia

Con l'obiettivo di armonizzare in tutti i Paesi membri della Ue le disposizioni in tema di privacy è stato emanato un nuovo regolamento che entrerà in vigore fra poco meno di un anno.

Il Garante della Privacy individuerà le disposizioni - contenute nel D.Lgs. 30.6.2003, n. 196 - che dovranno essere modificate.

Vengono introdotte nuove figure, i cui compiti in relazione al trattamento dei dati personali va attentamente valutato per tempo dalle aziende.

1. Privacy - Nuovo Regolamento Ue

Il 4.5.2016 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il nuovo Regolamento Ue 679/2016 in materia di protezione dei dati personali (Privacy).

Ancorché l'entrata in vigore sia fissata al 25.5.2016, è stato previsto che i Paesi membri dell'Unione europea avranno 2 anni di tempo (25.5.2018) per darne applicazione interna adeguandosi alle nuove norme.

Il Regolamento ha come obiettivo l'armonizzazione della disciplina della protezione dei dati personali, che a livello comunitario scaturiva dalla Direttiva 95/46/Ce, che è stata diversamente recepita nei diversi Stati membri dell'Unione.

Dal momento che la Ue ha emanato un Regolamento, esso sarà immediatamente applicabile in tutti gli Stati membri, senza alcuna necessità, per i singoli Stati, di introdurre una norma interna di recepimento.

La struttura del Regolamento Ue 679/2016 è indicata nella Tabella n. 1.

Tabella n. 1 – Struttura del Regolamento Ue 679/2016		
	Capitolo	Articoli
1	Disposizioni generali	1-4
2	Principi	5-11
3	Diritti dell'interessato	12-23
4	Titolare del trattamento e responsabile del trattamento	24-43
5	Trasferimenti di dati personali verso Paesi terzi o organizzazioni internazionali	44-50
6	Autorità di controllo indipendenti	51-59
7	Cooperazione e coerenza	60-76
8	Mezzi di ricorso, responsabilità e sanzioni	77-84
9	Disposizioni relative a specifiche situazioni di trattamento	85-91
10	Atti delegati e atti di esecuzione	92-93
11	Disposizioni finali	94-99

Inoltre, il Regolamento è preceduto da 173 «considerando», che hanno solo un valore interpretativo, mentre va escluso un loro carattere normativo (art. 10 dell'Accordo interistituzionale sulle linee direttrici comuni relative alla qualità redazionale della legislazione comunitaria del 22.12.1998). La Corte di Giustizia ha avuto modo di spiegare che, se il corpo del testo non fosse chiaro o fosse impreciso, l'interprete può fare riferimento ai considerando, fermo restando la loro cedevolezza rispetto al testo dell'articolato, laddove difforme.

Studio Associato Trombetta Teruggia

Per quanto riguarda il nostro Paese, dal momento della sua entrata in vigore il nuovo Regolamento Ue 679/2016 andrà a sostituire il Codice Privacy in vigore dal 2004, contenuto nel D.Lgs. 30.6.2003, n. 196, ma la sostituzione non sarà integrale; infatti, il Garante della Privacy avrà il compito di verificare quali articoli della precedente normativa dovranno essere cambiati.

Come si evince dalla lettura del considerando n. 9 del Regolamento europeo in tema di protezione dei dati personali, i principi e gli obiettivi della Direttiva 95/46/Ce rimangono validi e la Tabella n. 2 mostra la profonda similitudine con l'art. 11 del Codice della Privacy.

Tabella n. 2 – Confronto tra la disciplina italiana (Codice Privacy) e Regolamento Ue 679/2016	
Codice Privacy (D.Lgs. 196/2003)	Regolamento Ue 679/2016
Art. 11	Art. 5
1. I dati personali oggetto di trattamento sono:	1. I dati personali sono:
a) trattati in modo lecito e secondo correttezza;	a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti e registrati per scopi determinati, espliciti e legittimi, e utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;	b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, par. 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
(vedi punto d)	c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
c) esatti e, se necessario, aggiornati;	d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;	(vedi punto c)
e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.	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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89, par. 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e della libertà dell'interessato («limitazione della conservazione»);
	f) trattati in maniera 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»).
2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.	2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di provarlo («responsabilizzazione»).

2. Novità introdotte dal Regolamento Ue

Nel prosieguo di questa breve trattazione saranno evidenziate esclusivamente le novità introdotte dal Regolamento Ue 679/2016.

Studio Associato Trombetta Teruggia

Le figure soggettive privacy previste dal Codice della Privacy erano il titolare, il responsabile e l'incaricato: sostanzialmente la loro nomina e i loro compiti sono rimasti invariati e schematicamente si possono riassumere nella Tabella n. 3.

Tabella n. 3 – Privacy: nomina e compiti del titolare, del responsabile e dell'incaricato	
Interessato	La persona fisica cui si riferiscono i dati personali (art. 4, co. 1, lett. i), Codice Privacy)
Titolare	La persona fisica, la persona giuridica, la pubblica Amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza (art. 4, co. 1, p.to 7, Reg. Ue 679/2016)
Responsabile	La persona fisica, la persona giuridica, la pubblica Amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali (art. 4, co. 1, p.to 8, Reg. Ue 679/2016)
Incaricati	Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile (art. 4, co. 1, lett. h), Codice Privacy)
Amministratore di sistema	Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile (Garante della Privacy, prot. 27.11.2008 – doc. web n. 1577499)

Una nuova figura è il D.P.O., Data Protection Officer, non obbligatoria in ogni realtà ma solo nei casi previsti dalla normativa e più precisamente:

- se il trattamento venga svolto da un'autorità (con esclusione di quelle giurisdizionali) o da un organismo pubblico;
- se si riferisca a trattamenti che necessitano il monitoraggio regolare e sistematico degli interessati ad ampio raggio;
- se il trattamento riguardi, ad ampio raggio, informazioni e dati sensibili, ma anche quelli sanitari e personali in generale (come dati sulla vita o sull'orientamento sessuale, biometrici o sulla fedina penale).

Potrà essere nominato come Data Protection Officer un dipendente del titolare del trattamento o un consulente esterno appositamente nominato con idoneo contratto per l'attività da compiere. Nella lettera di nomina per il dipendente o nel contratto del consulente esterno dovranno essere specificamente indicati i compiti che il DPO dovrà svolgere e gli strumenti che il titolare del trattamento metterà a disposizione dello stesso, strumenti intesi sia in termini tecnici che in termini economici; dovrà quindi trattarsi di una persona che godrà di requisiti di qualità professionali e specializzazioni in materia di normativa sulla privacy.

La nuova figura del DPO assumerà nel nuovo Regolamento un ruolo importante e centrale ma soprattutto, indipendentemente dalla circostanza che il soggetto sia una persona dipendente (quindi con vincolo di subordinazione) o meno, il DPO dovrà svolgere il proprio lavoro in modo autonomo e dovrà essere coinvolto in ogni questione inerente alla protezione dei dati personali.

Accentuando l'importanza e la trasparenza verso gli interessati, i riferimenti del DPO dovranno essere comunicati al Garante della Privacy e dovranno essere pubblici, evidenziandoli anche nell'informativa.

Studio Associato Trombetta Teruggia

Il Regolamento europeo, all'art. 30, ha introdotto in capo al titolare e al responsabile, ove nominato, l'obbligo di redazione e detenzione del Registro generale delle attività di trattamento svolte e l'esibizione dello stesso su richiesta del Garante della Privacy.

L'obbligo, in sé, consiste nell'attività di conservazione dei documenti di tutti i trattamenti dei dati realizzati di cui si è titolari o responsabili. I dati da conservare riguardano:

- l'indicazione delle informazioni relative al titolare del trattamento;
- lo scopo del trattamento dei dati;
- la tipologia di soggetti interessati e di dati personali;
- l'indicazione dei soggetti destinatari delle informazioni raccolte;
- i trasferimenti delle informazioni personali verso un paese terzo o un'organizzazione internazionale con evidenza delle garanzie necessarie;
- l'indicazione dei termini entro i quali si prevede l'eliminazione dei dati;
- l'indicazione delle misure di sicurezza tecniche e organizzative.

L'obbligo del Registro è previsto anche per le imprese aventi meno di 250 dipendenti qualora il trattamento:

- presenti un rischio per i diritti e le libertà del diretto interessato;
- non sia occasionale e includa dati personali sensibili, sanitari, sulla vita, sulla storia giudiziaria passata, sull'orientamento sessuale, su dati biometrici o genetici (definiti all'art. 4, co. 1, p.to 14, Regolamento Ue 679/2016 come «i dati personali ottenuti da un trattamento tecnico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici»).

Un altro elemento di novità del nuovo Regolamento europeo è il principio del *privacy impact assessment* (P.I.A.). Il P.I.A. è fondamentale nei casi di utilizzo di nuove tecnologie o, comunque, in tutti i casi in cui vi sia un rischio elevato per i diritti e le libertà delle singole persone.

Nel caso di redazione del P.I.A., il titolare del trattamento deve, prima di procedere e confrontandosi, qualora vi sia, con il Data Protection Officer, effettuare una valutazione preventiva dell'impatto che può avere il trattamento sulla protezione dei dati personali.

La valutazione avrà ad oggetto:

- la descrizione dei trattamenti che si prevede saranno svolti;
- le finalità del trattamento;
- l'interesse legittimo per il quale il titolare effettua i trattamenti;
- la valutazione della necessità e della proporzionalità del rischio per i diritti e libertà dei soggetti interessati;
- le misure di sicurezza e le garanzie da adottare.

Nel caso in cui dalla valutazione preventiva si evinca un rilevante rischio conseguente al trattamento e si sia in assenza di misure volte a contrastarlo, il titolare interessato è tenuto a chiedere consulto al Garante prima di dare inizio al trattamento stesso.

3. Informativa sulla privacy e consenso

L'informativa Privacy prevista in sostituzione dell'attuale art. 13 del Codice della Privacy viene integrata e rafforzata, in quanto sono state aggiunte molteplici informazioni affinché gli interessati possano ricevere le informazioni obbligatorie in modo conciso, trasparente, intellegibile e di facile comprensione (artt. 13 e 14, Regolamento Ue 679/2016).

Studio Associato Trombetta Teruggia

Come nel Codice della Privacy, l'informazione deve essere fornita per iscritto; su richiesta del diretto interessato può essere fornita in via orale, ma deve essere verificata l'identità dell'interessato stesso.

Le informazioni che si vanno ad aggiungere a quanto già previsto dal vecchio codice sono:

- i dati di contatto, qualora ne sia prevista la presenza, del Data Protection Officer;
- la struttura giuridica del trattamento da eseguire che si aggiunga all'indicazione dello scopo del trattamento medesimo;
- l'indicazione puntuale dei legittimi interessi cui mira il titolare del trattamento o dei terzi (qualora l'obiettivo sia il perseguimento di un legittimo interesse);
- l'ambito di trasferimento dei dati ad un'organizzazione internazionale o all'estero fuori dall'Ue;
- l'indicazione del quantitativo di tempo durante il quale i dati verranno conservati e, qualora non sia conosciuto, l'indicazione delle modalità per determinarlo;
- la precisazione della possibilità di esercitare il diritto alla portabilità dei dati;
- la precisazione della possibilità di revocare il consenso al trattamento in ogni momento;
- l'indicazione del diritto di proporre reclamo al Garante della Privacy;
- in caso sia presente un processo decisionale automatizzato, ne va dichiarata l'esistenza con indicazione delle possibili conseguenze che dal trattamento possono derivare;
- la precisazione della fonte dalla quale hanno origine i dati oggetto di trattamento con l'obbligo, qualora i dati non siano reperiti dal diretto interessato, di indicare la possibilità che i dati giungano da fonti raggiungibili dal pubblico;
- la precisazione delle categorie di dati assoggettati al trattamento. L'obbligo non sussiste qualora i dati siano reperiti presso l'interessato.

Il consenso di cui agli artt. 7 e 8, Regolamento Ue 679/2016, deve essere prestato dal diretto interessato e deve sempre essere antecedente rispetto al trattamento dei dati personali, e viene ulteriormente definito e dettagliato come evidenziato nella Tabella n. 4.

Tabella n. 4 – Consenso al trattamento dei dati	
Direttiva 95/45/Ce	Regolamento Ue 679/2016
Art. 2, co. 1, lett. h)	Art. 4, co. 1, punto 11
Qualsiasi manifestazione di volontà, libera, specifica e informata	Qualsiasi manifestazione di volontà, libera, specifica e informata e
	inequivocabile dell'interessato
con la quale la persona interessata	con la quale lo stesso
accetta	manifesta il proprio assenso mediante dichiarazione o azione positiva inequivocabile
che i dati personali che la riguardano siano oggetto di un trattamento	che i dati personali che lo riguardano siano oggetto di trattamento

La centralità della prestazione del consenso fa sì che questo debba essere sempre posto in risalto, soprattutto nei casi in cui non sia la sola e unica questione sottoposta all'attenzione del soggetto interessato, pena l'invalidità del consenso stesso.

Come precedentemente osservato, il consenso può essere revocato liberamente dall'interessato in ogni momento e le modalità di revoca debbono essere agili e semplici come nel caso in cui il consenso viene espresso.

In ambito di fornitura a minorenni di servizi sociali o di informazione-media, è previsto un consenso preventivo. Il titolare del trattamento dei dati ha l'obbligo (nei limiti della ragionevolezza e con i mezzi tecnologici a disposizione) di effettuare una verifica dell'età dell'interessato, nei casi in cui l'età del minorenne sia inferiore a 16 anni (in alcuni paesi dell'Ue è previsto un limite più basso che, però, non

Studio Associato Trombetta Teruggia

deve scendere al di sotto del tredicesimo anno di età), della presenza del consenso e che questo sia stato manifestato o autorizzato da chi ne esercita la potestà genitoriale.

Il nuovo Regolamento ha introdotto il diritto alla portabilità dei dati personali, prevedendo che l'interessato ha la facoltà di trasferire i dati ad un altro titolare del trattamento senza che ciò possa essere impedito dal titolare originario, sempre che l'operazione che sia tecnicamente fattibile.

4. Sicurezza dei dati

Il Regolamento in commento ha enfatizzato le misure di sicurezza; infatti nel testo normativo si fa riferimento ad un'adeguata sicurezza dei dati, in relazione, anche, alla protezione degli stessi, che deve essere prestata con misure tecniche e organizzative altrettanto adeguate. Tutto ciò è finalizzato ad evitare trattamenti non autorizzati o illeciti e, anche, proteggere dalla perdita, dalla distruzione o da danni accidentali in pieno rispetto del cd. principio della «integrità e riservatezza».

Un possibile elenco delle misure di sicurezza ritenute adeguate è il seguente:

- la pseudonimizzazione dei dati personali;
- la cifratura dei dati personali;
- la costante sicurezza in tema di riservatezza, integrità, disponibilità e resilienza dei sistemi e servizi di trattamento;
- qualora vi sia un danno fisico o un incidente tecnico, deve esservi la capacità di tempestivo ripristino dell'accesso e della disponibilità dei dati;
- la presenza di una procedura apposita per effettuare test, verifiche e valutazioni circa l'efficacia delle misure di sicurezza applicate.

Nel Codice della Privacy l'obbligo di notificare al Garante l'avvenuta violazione dei dati personali era imposto solo ai fornitori di servizi di comunicazione elettronica accessibili al pubblico, mentre con il nuovo Regolamento tale obbligo viene esteso a tutti i titolari del trattamento. Questo cambio di rotta è stato dettato dalla necessità di sostituire la «vecchia» notifica con l'obbligo per il titolare del trattamento di conservare la documentazione sui trattamenti, a seguito di un'attenta valutazione dell'impatto del trattamento sulla protezione dei dati, attraverso la supervisione specialistica del Data Protection Officer.

Quindi il Regolamento europeo supera la logica della notificazione e prevede nuovi strumenti:

- l'introduzione di una nuova figura, ossia il cosiddetto Data Protection Officer;
- la valutazione dell'impatto della privacy, ovvero il *privacy impact assessment*;
- la notificazione delle violazioni, cioè il cosiddetto *Data Breach* (artt. 33 e 34, Reg. Ue 679/2016).

La notifica dell'avvenuta violazione dei dati personali deve avvenire in breve tempo e se possibile entro 72 ore da quando se ne ha avuta cognizione e comunque senza giustificato ritardo. Superate le 72 ore, il titolare del trattamento dei dati dovrà redigere, oltre alla notifica, anche le motivazioni che ne hanno determinato il ritardo.

Nella notifica dovranno essere evidenziati i seguenti argomenti:

- l'origine della violazione con l'indicazione di quali dati o categorie di dati siano stati colpiti;
- la comunicazione del nominativo e dei riferimenti del responsabile della protezione dei dati dal quale reperire le informazioni e gli approfondimenti;
- le possibili conseguenze che la violazione può comportare;
- le misure applicate o applicabili da parte del titolare del trattamento al fine di rimediare alla violazione o ridurre le conseguenze negative.

Studio Associato Trombetta Teruggia

Nel caso in cui la violazione colpisca anche diritti e libertà delle persone fisiche, il danneggiato deve essere informato in modo che possa comprendere il fatto in maniera semplice e chiara.

Per quanto concerne poi il trasferimento dei dati in un Paese extra Ue, il Regolamento non evidenzia particolari novità in merito: infatti il titolare e il responsabile del trattamento, ove nominato, devono rispettare le seguenti condizioni:

- il trasferimento deve essere effettuato a seguito di una decisione di adeguatezza nel senso che la Commissione Ue deve valutare che nel paese (od organizzazione internazionale) destinatario esista un adeguato grado di protezione, perché se così fosse non vi sono altre particolari autorizzazioni da richiedere;
- il trasferimento deve avere garanzie adeguate quali, ad esempio, specifici previsioni contrattuali, previsione di un sistema di certificazione, esistenza di regole vincolanti d'impresa, ecc.

Nel caso in cui le condizioni di cui sopra non fossero verificate o applicabili, dovranno essere presenti almeno una di queste condizioni:

- il consenso informato dell'interessato;
- la necessità del trasferimento al fine di dare esecuzione ad un contratto o a misure precontrattuali da adottare su richiesta dell'interessato;
- la necessità del trasferimento dei dati per motivi di interesse pubblico o per la difesa o l'esercizio di un diritto per via giudiziaria;
- il trasferimento dei dati è fondamentale ai fini della salvaguardia di interessi vitali del diretto interessato o altre persone e l'interessato stesso si trovi nell'impossibilità fisica o giuridica di provvedere alla prestazione del consenso;
- il trasferimento dei dati è legato da un registro pubblico.

Il trattamento di profilazione rappresenta una novità introdotta dal nuovo Regolamento. Quest'ultimo si riferisce a *«qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi ad una certa 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»*.

Dal nuovo testo entrato in vigore, emerge un generale divieto alla profilazione, fatta eccezione per casi particolari quali, ad esempio, l'aver ottenuto il consenso informato del diretto interessato.

La materia della profilazione è uno degli ambiti direttamente interessati dall'obbligo di valutazione preventiva di impatto sulla protezione dei dati.

5. Impianto sanzionatorio

Infine, per quanto concerne l'aspetto sanzionatorio del nuovo Regolamento europeo, permane la responsabilità al risarcimento, da parte del titolare o del responsabile, del «danno da trattamento» e vengono determinati i sistemi di suddivisione della responsabilità risarcitoria tra il titolare e il responsabile del trattamento, tra i contitolari, e le possibilità di esonero da responsabilità.

In tema di sanzioni amministrative pecuniarie irrogate dal Garante, il successivo art. 83 del Regolamento Ue 679/2016 si occupa di stabilire le condizioni per la determinazione delle sanzioni e fissa importi specifici distinguendo tra:

- sanzioni amministrative pecuniarie fino a euro 10.000 (o, per le aziende, fino al 2% del fatturato mondiale totale annuo dell'anno antecedente), per la violazione di specifici obblighi imposti dal nuovo Regolamento;

Studio Associato Trombetta Teruggia

- sanzioni amministrative pecuniarie fino a euro 20.000 (o, per le aziende, fino al 4% del fatturato mondiale totale annuo **dell'anno antecedente**), per la violazione di più rigidi obblighi imposti dal nuovo Regolamento o per il mancato rispetto degli ordini dettati dal Garante.

In ambito penale **vige la competenza del singolo Stato, data l'impossibilità di una previsione del diritto dell'Unione europea. Perciò, entro il 25.5.2018, i singoli Stati membri dovranno stabilire la disciplina da applicare in materia di sanzioni, differenti da quelle amministrative pecuniarie, da irrogare in caso di violazione del nuovo Regolamento, oltre a fornire tutta una serie di chiarimenti in merito alle questioni ancora da dettagliare.**