



PrivacyControl è una società specializzata nell'analisi di conformità del trattamento e della gestione dei Dati Personali, nel rispetto di tutti i requisiti e delle misure previste dalla vigente normativa.

PrivacyControl effettua **servizi** consistenti in: verifiche preliminari (audit) per valutare la conformità alla normativa, una Valutazione d'Impatto sulla protezione dei dati personali, corsi di formazione dedicati, informative e consenso sul trattamento dei dati, privacy e cookie policies, redazioni documentali richieste per legge e l'obbligatoria nomina del Responsabile per la Protezione dei Dati personali.

Il "*Sistema Integrato Gestione Privacy*" consente il raggiungimento ed il mantenimento degli standard previsti dal legislatore in ambito privacy.

# Privacy & PA

## Regolamento UE n. 679/2016

**Dott. Massimo Zampetti**

Data Protection Officer di PrivacyControl, *brand di Privacyncert Lombardia S.r.l.*  
*info @privacycontrol.it – lombardia @privacyncert.it*

## Introduzione al Reg. Europeo n. 679/2016

Il Parlamento Europeo, in data 14 Aprile u.s., ha **APPROVATO** definitivamente il c.d. “**pacchetto protezione dati**”, che si compone di due diversi strumenti:

- un nuovo **Regolamento** concernente la “*tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati*”;
- una nuova **Direttiva** indirizzata alla “*regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all’esecuzione delle sanzioni penali*”.

**La pubblicazione** del Nuovo Regolamento sulla Gazzetta UE è avvenuta in data **4 maggio 2016**.

A partire dal ventesimo giorno dalla pubblicazione ( 24 maggio p.v.), gli **Stati membri** avranno **due anni** di tempo per allineare la normativa nazionale alle nuove prescrizioni introdotte dal Nuovo Regolamento, che diventerà definitivamente applicabile in tutto il territorio UE a partire dal **25 maggio 2018**.

Il regolamento sarà direttamente applicabile senza necessità di recepimento.

Per quanto riguarda l'Italia:

- Il regolamento sostituisce (non integralmente) il D.lgs. n. 196/2003, *Codice in materia di Protezione dei Dati Personali* (c.d. Codice Privacy) in vigore dall'1 gennaio 2004;
- Il D.lgs. n. 196/2003 è stato integrato dal D.lgs n. 101/2018, pubblicato in data 4 settembre 2018 ed entrato in vigore in data 19 settembre 2018. Il nuovo Codice abroga tutte le disposizioni in contrasto con il Regolamento Europeo n. 679/2016, e rimanda per quasi la totalità degli Articoli ai Considerando e/o Articoli del Regolamento Europeo in materia di Privacy;
- Il Garante Privacy ha in corso una ricognizione normativa per verificare quali provvedimenti generali del garante sopravvivranno alla riforma.

# AMBITO DI APPLICABILITÀ MATERIALE

- ▶ Si applica solo al trattamento dei dati di persone fisiche.
- ▶ Riguarda trattamenti interamente o parzialmente automatizzati o non automatizzati, se i dati sono contenuti in un archivio o sono destinati a confluirci.
- ▶ Il regolamento non si applica ai trattamenti di dati personali effettuati:
  - Da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
  - Da un'Autorità di pubblica sicurezza;
  - Per attività che non rientrano nell'ambito di applicazione del diritto UE.

# AMBITO DI APPLICABILITÀ TERRITORIALE

Il Regolamento si applica:

- al trattamento di dati personali effettuato da un **Titolare o Responsabile stabilito nella UE**, indipendentemente dal fatto che il trattamento sia effettuato o meno nella UE;
- al trattamento di dati personali effettuato da **Titolari o Responsabili non Stabiliti nell'UE**, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione, se il **trattamento ha ad oggetto dati personali di interessati che si trovano nella UE** e riguarda **l'offerta di beni o servizi** (anche non a pagamento) ai suddetti interessati oppure il **monitoraggio** del loro comportamento nel territorio della UE;
- al trattamento effettuato da un Titolare stabilito in uno **Stato extra UE** **soggetto al diritto di uno Stato UE** in virtù del diritto internazionale pubblico.

## I principali 8 impatti del Regolamento

1. **NUOVE INFORMAZIONI** da gestire;
2. **DIMOSTRAZIONE** della «*compliance*» (o in inglese, c.d. Principio dell'Accountability);
3. **VALUTAZIONE d'Impatto** della gestione dei dati personali;
4. Nomina di un **R.P.D.** (o in inglese, c.d. Data Protection Officer);
5. Segnalazione di una **VIOLAZIONE di Dati** (o in inglese c.d. Data Breach);
6. Nuovi requisiti per i **fornitori**;
7. Accresciuti obblighi **di trasparenza** ;
8. **SANZIONI** più rigide rispetto al Codice della Privacy n. 196/2003.

## 1.0 Nuove informazioni per gli interessati

- ❖ I nuovi **Obblighi** e i nuovi **Diritti** per l'Interessato:
  - Obbligo di informare gli interessati anche in merito a:
    - Tempi di conservazione dei dati
    - Origine dei dati
    - Diritto alla portabilità dei dati e restrizioni
    - Diritto ad adire l'Autorità di controllo competente.
  - Nuovi diritti:
    - Diritto all'oblio
    - Diritto alla limitazione del trattamento
    - Diritto alla portabilità dei dati (a certe condizioni)
    - Diritto di opporsi a processi di trattamento automatizzati.

## 2.0 La responsabilizzazione del Titolare del Trattamento ex Art. 24 (Reg. UE n. 679/2016)

Il Regolamento introduce **degli obblighi organizzativi nuovi** con riferimento ai loro ruoli e funzioni, come ad esempio i seguenti:

- Il Titolare deve attuare **misure tecniche ed organizzative adeguate per garantire e dimostrare che il trattamento è effettuato conformemente al Regolamento**. Le misure devono essere riesaminate periodicamente e aggiornate ove necessario. L'adesione a Codici di condotta o a meccanismi di certificazione, può essere utilizzata come elemento per dimostrare il rispetto degli obblighi imposti al Titolare del trattamento.
- In caso di **contitolarità del trattamento**: i Contitolari devono stipulare tra loro **uno specifico accordo interno** che disciplini in modo trasparente le rispettive responsabilità e rifletta adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo va messo a disposizione dell'interessato.

- 
- Obbligatoria per il Titolare la nomina del Responsabile del Trattamento, va documentata con un “*contratto o altro atto giuridico*”, stipulato in forma scritta anche su supporto elettronico, che regoli 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. Ammessa la designazione di Sub-Responsabili previa autorizzazione scritta, specifica o generale del Titolare del trattamento;
  - **Incaricati del trattamento:** categoria di soggetti, identificata con le “*persone autorizzate al trattamento*” non è definita formalmente, ma disciplinata indirettamente. Viene previsto per il Titolare l’obbligo di indicare le persone autorizzate all’interno della sua struttura;

## 3.0 La nuova figura del Responsabile della Protezione dei Dati personali (R.P.D.)

### 4.1 Nomina ex artt. 37 – 39 Reg. UE

#### ✓ Obbligatorietà

Il R.P.D. (in lingua inglese, *Data Protection Officer, D.P.O.*) dovrà essere **obbligatoriamente** nominato da **tutte le Autorità Pubbliche** od assimilate.

#### ✓ Requisiti

I requisiti del R.P.D. consistono nella **conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati**. Può essere un libero professionista o una società, e può essere nominato un singolo R.P.D. anche da più Enti.

#### ✓ Indipendenza

Il R.P.D. dovrà riferire direttamente al **Titolare del Trattamento** o comunque ai vertici gerarchici, senza intermediazioni, con grande **autonomia e indipendenza** rispetto agli altri dirigenti interessati.

## 3.2 Quali sono i principali compiti del R.P.D.?

**Compiti Generali** ai sensi dell'Art. 39 del Regolamento Europeo:

- **Informare, consigliare e FORMARE** il titolare o il responsabile del trattamento, i dipendenti e i quadri, in merito agli obblighi derivanti dal Regolamento (Art. 39 Reg UE);
- **Verificare** l'attuazione e l'applicazione della normativa;
- **Fornire** pareri e consulenza in merito alla valutazione d'impatto (Art. 35) sulla protezione dei dati;
- **Fungere da punto di contatto** per gli "interessati", in merito a qualunque problematica connessa al trattamento dei loro dati;
- **Fungere da punto di contatto** per il **Garante** per la Protezione dei Dati Personali.

### 3.3 Compiti Specifici ai sensi del Reg. UE n. 679/2016:

1. **Aiutare** a condurre la **Valutazione d’Impatto** (c.d. in inglese, *Data Protection Impact Assessment, DPIA*)
2. **Registro delle attività dei trattamenti**: In merito al registro delle attività dei trattamenti, la sua tenuta è un obbligo che ricade sul titolare e sul responsabile, e non sul **DPO**. La sua obbligatorietà viene scaturita dalla presenza di un numero di 250 dipendenti o maggiore, e alla presenza di un «*rischio elevato*» di Tutela di dati personali.
3. **Data breach**: In merito al «*data breach*», il **DPO** svolge un ruolo chiave nella notifica e comunicazione delle **violazioni di dati personali**.

*Niente vieta al titolare o al responsabile del trattamento di affidare al DPO il **compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile stesso.***

*Inoltre, si osservi che l’art. 33, par. 3, lettera b) **GDPR**, ove sono indicate le informazioni da fornire all’Autorità di controllo, prevede che **tali informazioni comprendano anche il nominativo** (e non solo le informazioni di contatto) **del DPO.***

## 3.5 Responsabilità del DPO

- ❖ **Domanda:** Il **DPO** è personalmente responsabile in caso di inosservanza degli obblighi in materia di protezione dei dati?

**No, il DPO non è responsabile personalmente in caso di inosservanza degli obblighi in materia di protezione dei dati.** Spetta al titolare o al responsabile del trattamento garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al regolamento. La responsabilità di garantire l'osservanza della normativa in materia di protezione dei dati ricade sul titolare / sul responsabile del trattamento.

## 4.0 La Valutazione d'Impatto sulla protezione dei dati (Art. 35 Reg .UE)

Qualora un tipo di trattamento presenti un «**rischio** elevato» per i diritti e le libertà delle persone fisiche, il **titolare** deve effettuare:

- una **Valutazione dell'Impatto del Trattamento** (*o analisi del rischio*) sulla protezione dei dati personali.

La **Valutazione d'Impatto** sulla protezione dei dati è **richiesta** specialmente nei seguenti casi:

- **Trattamento automatizzato**, su cui si basano decisioni che hanno **effetti giuridici** o che incidono in modo analogo su persone fisiche;
- **Trattamenti**, su larga scala, di **categorie particolari** di dati personali;
- **Sorveglianza** sistematica, su larga scala, di una **zona accessibile al pubblico**.

## 4.1 Cosa deve contenere la Valutazione d'Impatto ai sensi dell'Art. 35 del Regolamento Europeo?

La **VALUTAZIONE D'IMPATTO** deve almeno contenere:

- **Descrizione e finalità** dei trattamenti previsti;
- Valutazione di **necessità** e **proporzionalità** dei trattamenti;
- Valutazione dei **rischi** per i **diritti e le libertà** degli interessati;
- Le **misure** previste per affrontare eventuali rischi.

## 5.0 Violazione dei dati - Data breach (artt. 33 e 34)

Attualmente il Regolamento UE prevede per l'Autorità Pubblica l'**obbligo** di comunicare l'**avvenuta violazione** di dati personali:

- al **Garante** per la protezione dei dati personali;
- in determinati casi, anche al contraente/cliente.

Il Nuovo Regolamento estende tale **OBBLIGO** di comunicazione a **TUTTI i Titolari e Responsabili**.

## 5.1 Nello specifico, quali sono i compiti e i doveri del Titolare e del Responsabile del Trattamento?

- ▶ il **Responsabile** deve informare il Titolare senza ingiustificato ritardo della violazione;
  - ▶ Il **Titolare** deve notificare «*la violazione*», a sua volta senza ingiustificato ritardo, all'autorità di controllo (i.e., al Garante) e, ove possibile, **entro 72 ore** dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la suesposta violazione presenti un rischio per i diritti e le libertà delle persone.
- ❖ **Domanda:** Quali Sanzioni comporta la mancata segnalazione della violazione?
- ▶ **Sanzioni amministrative** fino a **10 milioni di Euro** o fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore

## 6.0 Nuovi requisiti per i fornitori

**Obblighi diretti** tra cui:

- **Obblighi di documentazione:** *Policy* sul trattamento dei dati, *Policy* di sicurezza, procedure atte a dimostrare la compliance con il Regolamento;
- Tenuta di un **registro delle attività di trattamento** per ciascun cliente/titolare (Art.30.2);
- **Innalzamento requisiti di sicurezza** sui dati adottando misure specifiche parametrare ai **rischi**, tra cui, pseudonimizzazione, crittografia, ecc.(Art.32);
- **Obbligo di segnalazione** al titolare dei *Data breach* (Art.33.2).

**Che tipi di Responsabilità sono previsti per gli Interessati e il Titolare?**

- **diretta** verso gli interessati per i danni subiti (se l'inadempimento dei propri obblighi è diretto o prevede la violazione delle istruzioni legittime del titolare);
- **solidale** con il titolare (Art.82).

## 6.1 Contratti con i fornitori

**Clausole obbligatorie** da inserire nei contratti/atti di nomina del responsabile:

- **Descrizione dettagliata** dei trattamenti: *oggetto, durata, natura e finalità dei trattamenti, tipologia di dati registrati, categorie di interessati, obblighi e diritti del titolare.*

**Obbligazioni del Responsabile**, tra cui:

- Elenco delle **misure tecniche e organizzative**;
- Trattamento dei dati SOLO su **istruzioni documentate** per iscritto del Titolare, **incluse eventuali previsioni sul trasferimento dei dati fuori dalla Unione Europea**;
- Obbligo nel gestire i **diritti** degli interessati: *accesso, correzione, cancellazione, limitazione, opposizione, portabilità*;
- Restituzione o **cancellazione** dei dati a discrezione del Titolare alla cessazione del contratto;
- **Obblighi di cooperazione con il Titolare nel notificare i «Data Breach»** e implementare le valutazioni d'impatto.

## 7. Accresciuti obblighi di trasparenza (artt. 5 e 12 Reg. UE)

Il Legislatore europeo dedica una sezione del Nuovo Regolamento alla “**Trasparenza**” (Sezione 1 del Capo III) e **richiede** che le informazioni all’interessato:

- siano rese con un **linguaggio semplice** e chiaro, soprattutto nel caso di minori;
- abbiano sempre **forma scritta**;
- **prevedano**:
  - il **periodo di conservazione** dei dati personali;
  - il diritto di **proporre reclamo** ad un’autorità di controllo;
  - l’**intenzione** del titolare di **trasferire** dati personali a un paese terzo.

## 7.1 L'informativa

Con l'informativa il responsabile del trattamento deve fornire all'interessato tutte le informazioni e le comunicazioni relative al trattamento dei dati personali in **forma intelligibile**, utilizzando un **linguaggio semplice, chiaro e adeguato** con riferimento alla condizione dell'interessato, con la particolare attenzione se le informazioni sono destinate ai minori.

Nell'informativa **si deve INDICARE specificamente il diritto di proporre reclamo all'Autorità di controllo**, fornendo le coordinate di contatto della predetta Autorità.

**Si dovrà inoltre FORNIRE** ogni eventuale informazione ritenuta necessaria al fine di garantire un trattamento equo nei confronti dell'interessato, in relazione alle peculiari circostanze in cui viene effettuata la raccolta dei dati personali.

**Domanda:** Sono previste Sanzioni in caso di omessa o inidonea informativa all'Interessato?

Omessa o inidonea informativa all'interessato:

- **Fino a 20.000.000,00 euro** (rispetto alle condizioni economiche del contravventore).

## 7.2 Il consenso

- ❖ **Domanda:** Quali sono le novità introdotte dal Nuovo Regolamento Europeo?
- Criterio principale di liceità rimane il consenso dell'interessato.
- Il consenso, inteso (art. 4, n. 11) come qualsiasi manifestazione di assenso dell'interessato, **deve** essere **libero, specifico, informato e inequivocabile**, cioè espresso mediante dichiarazione o azione positiva inequivocabile (non può mai essere desunto dal silenzio o da un comportamento inattivo: v. considerando 32).
- Il consenso non dovrebbe costituire il presupposto per un valido trattamento qualora vi sia un "*evidente squilibrio tra interessato e titolare del trattamento*", **soprattutto nei casi in cui quest'ultima sia un'autorità pubblica** o comunque si possa presumere che il consenso non si sia liberamente formato (Considerando 43).
- Il consenso è liberamente revocabile (art. 7, par. 3).

## 7.3 La prova del consenso

- È innovativa la previsione introdotta dall'art. 7, par. 1: *“qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali”*;
- si pone in capo al **titolare** un vero e proprio **onere della prova** sulla raccolta del consenso;
- per converso non è necessario che il consenso sia documentato per iscritto (v. invece art. 23, co. 3 cod. privacy).

## 8. SANZIONI

Il Regolamento Europeo ha inasprito l'ammontare delle **sanzioni**:

- **Sanzioni amministrative** fino a **10 milioni di Euro** o fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore;

*(Es. Violazione obblighi in materia di consenso dei minori, misure di sicurezza; Violazione obblighi impartiti dal Titolare; Violazione obblighi di comunicazione per Data Breach);*

- **Sanzioni amministrative** fino a **20 milioni di Euro** o fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

*(Es. Violazioni concernenti i diritti degli interessati, i principi cardine del trattamento (es. consenso; trasferimenti dei dati; Violazioni di ordini o misure imposte dall'Autorità).*

Le sanzioni amministrative pecuniarie sono inflitte **in aggiunta o in luogo alle sanzioni di cui all'art. 58, par. 2, lett. da a) a h) e j) del Regolamento** (avvertimenti, ammonimenti, ingiunzioni, limitazioni ai trattamenti, ordine di cancellazione, rettifica o limitazioni del trattamento, revoca della certificazione o ingiunzione all'Organismo certificatore di ritirare o non emettere la certificazione, ordine di sospensione dei flussi di dati verso un destinatario)

SANZIONE AMMINISTRATIVA PECUNIARIA	DISPOSIZIONE VIOLATA	OBBLIGO VIOLATO (in sintesi)
<p>Fino a <b>10.000.000 EUR</b> o, per le imprese, fino al <b>2%</b> del fatturato mondiale totale Annuo dell'esercizio precedente, se superiore.</p>	Art. 8	Verifica che il consenso al trattamento sia prestato o autorizzato dal titolare della responsabilità genitoriale nel caso di offerta diretta di servizi della società dell'informazione a minori di età inferiore a 16 anni.
	Art. 11	Obbligo di non conservazione, acquisizione o trattamento di informazioni per identificare l'interessato se le finalità del trattamento non richiedono più l'identificazione dell'interessato non richiedono o non richiedono più l'identificazione dell'interessato.
	Art. 25	Adozione di misure tecniche e organizzative atte ad attuare i principi di protezione dei dati, la tutela dei diritti degli interessati e la garanzia che siano trattati, per impostazione predefinita, solo i dati necessari per ogni specifica finalità di trattamento (c.d. <i>privacy by design e by default</i> ).
	Art. 28	Designazione del Responsabile del trattamento e rispetto degli obblighi e compiti posti a carico del Responsabile.
	Art. 30	Tenuta dei Registri delle attività di trattamento.
	Art. 32	Adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.
	Art. 33	Notifica di una violazione dei dati personali all'autorità di controllo.
	Artt. 35 e 36	Svolgimento di una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali e conseguente consultazione preventiva dell'Autorità di controllo.
	Artt. 37 e 39	Prescrizioni in tema di designazione del Responsabile della protezione dei dati (Data Protection Officer).

SANZIONE AMMINISTRATIVA PECUNIARIA	DISPOSIZIONE VIOLATA	OBBLIGO VIOLATO (in sintesi)
<p>Fino a <b>20.000.000 EUR</b> o, per le imprese, fino al <b>4%</b> del fatturato mondiale totale Annuo dell'esercizio precedente, se superiore.</p>	Art. 5	Rispetto dei principi applicabili al trattamento trasparenza; liceità, correttezza e limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
	Art. 6	Rispetto delle condizioni di liceità del trattamento.
	Art. 7	Dimostrazione della prestazione del consenso e del rispetto delle condizioni per il consenso. Tutela del dritto dell'interessato di revoca del consenso.
	Art. 9	Rispetto delle condizioni di liceità del trattamento di categorie particolari di dati personali.
	Artt. da 12 a 22	Obblighi informativi nei confronti dell'interessato. Tutela dei diritti dell'interessato (diritto d'accesso; di rettifica; all'oblio; di limitazione del trattamento; di notifica in caso di rettifica o cancellazione dei dati o limitazione del trattamento; alla portabilità dei dati; di opposizione; alla profilazione consenziente)
	Artt. da 44 a 49	Obblighi connessi al trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali.
	Capo IX	Qualsiasi obbligo previsto dalle legislazioni degli Stati membri per specifiche situazioni di trattamento a norma del Capo IX del Regolamento.
	Art. 58	Rispetto di un ordine, di una limitazione di trattamento o di un ordine di sospensione di flussi di dati dell'Autorità di controllo o di un negato accesso ai sensi dell'art. 58, par. I

## Prepararsi al Regolamento: 7 punti chiave

- **Consapevolezza del cambiamento:** analizzare e anticipare gli impatti del Regolamento (analisi dei rischi).
- **Individuazione dei trattamenti:** documentare tutti i trattamenti di dati personali effettuati dall'azienda, precisando per ciascuno di essi l'origine e la natura dei dati, le categorie di interessati, le modalità e le finalità di trattamento, i tempi di conservazione, nonché eventuali comunicazioni a soggetti terzi o diffusioni.
- **Revisione della documentazione privacy:** identificare e aggiornare le informative agli interessati, i moduli di consenso, le nomine a responsabile del trattamento e le clausole “Dati Personali” nei contratti con i fornitori o dipendenti e pianificarne l'adozione.

- **Responsabilizzazione del Titolare - Principio di Accountability:** definire un piano di compliance, che comprenda le valutazioni di impatto, la revisione dei piani di audit, delle procedure e delle policy nonché piani di formazione.
- **Data Protection Impact Assessment** (c.d. Valutazione d'Impatto): iniziare a familiarizzare con questi concetti e capire quando e come implementarli.
- Nomina di un **DPO**.
- **Data Breach:** definire le procedure per la rilevazione, segnalazione e indagine di violazioni di sicurezza (entro 72 ore dalla conoscenza dell'evento).



# Grazie per l'attenzione!

**Dott. Massimo Zampetti**

Data Protection Officer

[info@privacycontrol.it](mailto:info@privacycontrol.it)

*© 2018 Privacycert Lombardia S.r.l. – Tutti i diritti riservati. Ferme restando le utilizzazioni libere consentite dalle leggi vigenti, in mancanza di un'espressa autorizzazione scritta di Privacycert Lombardia S.r.l. è vietata qualunque riproduzione, utilizzazione o qualunque altra forma di messa a disposizione di terzi del presente documento o di una parte di essi.*

[www.privacycontrol.it](http://www.privacycontrol.it)