

Privacy & P.A. Regolamento UE n. 679/2016

NUOVI ADEMPIMENTI PRIVACY & CYBERSECURITY

Avv. Manlio Filippo Zampetti
Senior Legal Advisor – Formatore

Mail: *info@privacycontrol.it*

Introduzione al Reg. Europeo n. 679/2016

- **Pubblicazione** sulla Gazzetta Ufficiale dell'Unione Europea:
4 maggio 2016.
- Entrata in vigore: **24 maggio 2016.**
- Efficacia / Applicabilità in **tutti** i paesi dell'UE: **25 maggio 2018.**

Tutti i soggetti interessati (STATI MEMBRI DELL'UNIONE EUROPEA) hanno avuto **DUE ANNI** di tempo per adeguarsi alla nuova normativa tramite la modifica/implementazione delle proprie politiche Nazionali di trattamento dei dati.

Il Regolamento Europeo, per sua natura, è 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 **D.lgs n. 101/2018** ha reinserito le **sanzioni penali** non previste dal Regolamento UE (vedi slides nel Capitolo «Sanzioni»)
- 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**;
 - 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** per gli interessati (Artt. 12 al 22);
2. **DIMOSTRAZIONE** della «conformità al GDPR n. 679/16» (o in inglese, c.d. «*Principio dell'Accountability*»);
3. Nomina di un **R.P.D.** (o in inglese, c.d. Data Protection Officer);
4. **VALUTAZIONE d'Impatto** della **GESTIONE** dei dati personali;
5. **OBBLIGO** di Segnalazione di una **VIOLAZIONE in materia di Dati Personali** (o in inglese c.d. «*Data Breach*»);
6. Nuovi requisiti per i **fornitori** (Art. 28 del GDPR);
7. Accresciuti obblighi di trasparenza ;
8. **SANZIONI** più rigide rispetto al «Codice Privacy» (art. 83 e 84).

1.0 Nuove informazioni per gli interessati

- ❖ I nuovi **Obblighi** nell'informare gli interessati e i nuovi **Diritti** per l'Interessato:
 - I nuovi **Obblighi** :
 - Tempi di conservazione dei dati
 - Origine dei dati
 - Diritto alla portabilità dei dati e restrizioni
 - Diritto ad adire l'Autorità di controllo competente (Garante).
 - I 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.

1.1 Organigramma – I SOGGETTI (ART. 4)

Il Titolare del trattamento:

- La persona fisica o giuridica che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento di dati personali.

Il Responsabile del trattamento:

- La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta, archivia e conserva **dati personali** per conto del titolare del trattamento:
 - ✓ responsabile interno, solo per le Imprese con settori amministrativi distaccati;
 - ✓ qualsiasi **outsourcers** a cui sono trasferiti i dati (es. Segreteria digitale, Registro elettronico, Amministratore di sistema, Mensa, Agenzia di Viaggi).

Gli Incaricati del trattamento:

- Tutti coloro che hanno accesso ai dati (es. impiegati ufficio del personale).

II DATA PROTECTION OFFICER, o Responsabile per la Protezione dei Dati:

- Il DPO (Data Protection Officer) è colui che, in una posizione di indipendenza dal Titolare e dal Responsabile del trattamento, sorveglia il rispetto del Regolamento.
- Potrebbe essere nominato un unico DPO anche da un gruppo di Enti.
- La nomina del DPO deve essere comunicata all'Autorità di controllo (Garante).

Gli Interessati:

- Coloro i cui dati vengono trattati dal titolare e dai responsabili del trattamento.

N.B.: la nuova figura del «**Responsabile per la Protezione dei Dati**» personali (ndr. *Data Protection Officer*, in inglese) è approfondita nel Cap. 3, dalla pag. 16.

1.3 Principali Definizioni Modificate

- **Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- **Trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati, come la *raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.*

1.4 LA PROFILAZIONE

Introdotta per la prima volta **una definizione e una regolamentazione del particolare trattamento rappresentato dalla profilazione dell'interessato**, giuridicamente definita come “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”.

In linea generale è **vietata**.

L'interessato ha il diritto di NON essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, a meno che non vi siano circostanze specifiche, tra le quali il **chiaro consenso informato dell'interessato**.

2. La Responsabilizzazione del Titolare del Trattamento – NUOVI OBBLIGHI – Art. 24 e ss.

Il Regolamento introduce degli **OBBLIGHI** organizzativi nuovi con riferimento ai loro ruoli e funzioni, in particolare per il **Titolare del trattamento**, il quale:

- ▶ deve attuare **misure TECNICHE ED ORGANIZZATIVE** (Art. 32 e ss. del GDPR) **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.

MISURE TECNICHE

- a. autenticazione/tracciabilità
- b. autorizzazione univoca/profilazione
- c. cifratura dei dati (es. *sito web e allegati Mail*)
- d. separazione dei dati personali
- e. firewall/controllo degli accessi/black list/anti spam
- f. antivirus
- g. sicurezza dei dati cartacei
- h. disaster recovery
- i. intrusion detection
- j. vulnerability assessment/penetration test/monitoraggio delle attività di rete
- k. pseudonimizzazione/anonimizzazione dei dati (es. *Password*)
- l. backup ridondante
- m. politica di archiviazione sostitutiva

MISURE ORGANIZZATIVE

- a. nomina per iscritto degli incaricati del trattamento/personale
- b. istruzioni/disciplinare tecnico/politiche per il trattamento dei dati personali a tutto il personale
- c. accesso controllato
- d. armadi chiusi
- e. procedura modifica credenziali
- f. documentazione/Policy aggiornate
- g. formazione di tutto il personale
- h. nomina per iscritto dei responsabili esterni
- i. gestione delle postazioni da lavoro

MISURE SPECIFICHE

- 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 (Art. 28 del GDPR);
- 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.
- **Incaricati del trattamento**: categoria di soggetti, identificata dal Titolare del Trattamento 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 (Art. 29 del GDPR);

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

3.1 Nomina ex artt. 37 – 39 del Reg. UE 679/16

✓ 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» e mancanza di «Conflitti di Interesse»

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 CARATTERISTICHE PRINCIPALI DEL DPO

Il DPO deve essere **AUTONOMO** ed **INDIPENDENTE**:

- **NON** deve ricevere dal Titolare o dal Responsabile alcuna istruzione per quanto riguarda l'esecuzione dei compiti affidati **né è soggetto a potere disciplinare o sanzionatorio** per l'adempimento dei propri compiti.
- deve avere le risorse necessarie e il **potere di spesa** per assolvere ai compiti assegnati - accedere ai dati personali e ai trattamenti - mantenere le proprie conoscenze specialistiche (es. aggiornamento professionale).
- Deve fungere da punto di contatto con il **Garante** italiano per la protezione dei dati personali e con gli **interessati**.

3.3 Quali sono i principali compiti del R.P.D.?

Compiti Generali ai sensi dell'Art. 39 del Regolamento UE n. 679/16:

- **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 e in generale;
- **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.

4. 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. 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 Consenso Del Minore

Se un trattamento di dati nell'ambito **della fornitura ad un minore di un servizio della società dell'informazione** (es. l'accesso a Internet, l'iscrizione a un social network, etc.) prevede l'acquisizione del consenso preventivo, la **raccolta del consenso e il trattamento dei dati del minore sono leciti se egli abbia compiuto almeno 16 anni** (salvo il diritto degli Stati membri di stabilire anche un'età inferiore a tali fini, purché non inferiore ai 13 anni).

Il Titolare deve adottare **misure ragionevoli per verificare che il consenso sia prestato** o autorizzato dal titolare della potestà genitoriale sul minore.

7.4 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. IL NUOVO APPARATO SANZIONATORIO

8.1 La tutela dell'interessato e le sanzioni Penali

Art. 167 - Trattamento illecito dei dati personali:

- 「 ... 」 Chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato 「 ... 」 è punito con la **reclusione da sei mesi a tre anni**

Art. 167 bis - Comunicazione e diffusione illecita di dati oggetto di trattamento su larga scala

- 「 ... 」 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 「 ... 」 è punito con la **reclusione da uno a sei anni**

Art. 167-ter. Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala

- 「 ... 」 Chiunque 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**.

Art. 168 - Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio di poteri del Garante

- 「 ... 」 Chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, 「 ... 」 è punito con la **reclusione da sei mesi a tre anni**.

Art. 170 - Inosservanza dei provvedimenti del Garante

- 「 ... 」 Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante 「 ... 」 è punito con la **reclusione da tre mesi a due anni**.

8.2 RESPONSABILITÀ CIVILE

Dal punto di vista **civilistico**, confermata la responsabilità risarcitoria per il c.d. “*danno da trattamento*”.

L’art. 82 prescrive difatti che “Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento”.

Chiariti i **meccanismi di ripartizione della responsabilità risarcitoria** tra Titolare e Responsabile del trattamento, e tra contitolari del trattamento (con la previsione specifica di azioni di regresso reciproche), così come i meccanismi di esonero.

8.3 SANZIONI AMMINISTRATIVE

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 10.000.000 EUR o, per le imprese, fino al 2% 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 20.000.000 EUR o, per le imprese, fino al 4% 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: 6 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 dal personale.
- **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.
- 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!

Avv. Manlio Filippo Zampetti

Senior Legal Advisor

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 esso.

www.privacycontrol.it