CDT LEGAL

CASUCCI DI TARDO

& ASSOCIATI

REGOLAMENTO UE 679/2016

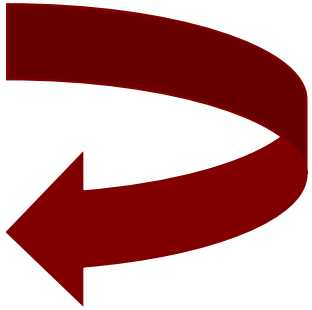
principali modifiche e novità

Titolare del trattamento

- ✓ Introduzione di un nuovo concetto di «**responsabilizzazione**» del Titolare del trattamento che attribuisce *in toto* a questa figura la regia dell'intera *compliance* aziendale.
- ✓ Previsione del nuovo «principio di rendicontazione» o di «***accountability***» ovvero l'obbligo di adozione di comportamenti proattivi tali da dimostrare la concreta adozione di misure atte ad assicurare l'applicazione del Regolamento. Al Titolare spetta il compito **AUTONOMO** di decidere modalità, garanzie e limiti dei trattamenti nel rispetto delle previsioni di legge.
- ✓ Per l'effetto dei punti che precedono, introduzione dell'obbligo agli adempimenti che seguono:

=>Privacy by default and by design (*segue slide*)

=>Valutazione del rischio inerente il trattamento (*segue slide*)



Privacy by design & **Privacy by default**

Obbligo del Titolare di adottare e attuare misure tecniche ed organizzative che tutelino i principi di protezione del trattamento, già in un **momento precedente** allo stesso (sin dalla sua progettazione).

Obbligo del Titolare di eseguire il trattamento con modalità e tecniche che, **per impostazione predefinita**, garantiscano l'utilizzo **dei soli dati personali necessari** per ciascuna specifica finalità del trattamento.

Gli obblighi suddetti devono essere assolti **in via preventiva** al trattamento e devono sostanziarsi in una serie di **attività specifiche e dimostrabili.**

Valutazione d'impatto sulla protezione dei dati personali

Qualora un determinato trattamento possa avere un impatto negativo sulla libertà o sui diritti degli interessati, il Titolare ha un obbligo di effettuare, preventivamente al trattamento, una specifica valutazione di impatto.

Solo all'esito di detta analisi che dovrà tenere conto dei rischi noti, delle misure tecniche ed organizzative e delle misure di sicurezza che il titolare ritiene di dover adottare, potrà essere svolto il trattamento.

In ogni caso la valutazione è obbligatoria nei casi tassativi di cui all'art. 35 del Regolamento.

Valutazione d'impatto sulla protezione dei dati personali

… *Segue*

La valutazione deve contenere:

- ✓ una descrizione dei trattamenti previsti e delle finalità del trattamento;
- ✓ una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- ✓ una valutazione per i rischi per i diritti e le libertà degli interessati e le misure previste per affrontarli.

L'intervento dell'Autorità di Controllo non sarà più preventivo, ma "*ex post*" ciò ulteriormente gravando la figura del Titolare della responsabilità in termini di accountability.

Co-Titolare

Nei casi di co-titolarità di un trattamento, il Regolamento impone a ciascun Titolare la definizione specifica, con **apposito atto giuridicamente vincolante**,

- ✓ Del rispettivo ambito di responsabilità;
- ✓ Dei rispettivi compiti con specifico riferimento ai **diritti degli interessati.**

Responsabile del trattamento

Il Titolare del trattamento può nominare un Responsabile attraverso la sottoscrizione di uno **specifico contratto** avente almeno i contenuti tassativi di cui all'art. 28, comma III del Regolamento.

Il Responsabile, previa autorizzazione scritta del Titolare, può nominare, a sua volta, **sub-responsabili** con sottoscrizione di **specifico contratto**. In ogni caso, resta ferma la responsabilità del Responsabile per le violazioni effettuate dai sub-responsabili.

Responsabile del trattamento

…Segue:

Principali nuove e tassative funzioni del Responsabile:

✓ Adotta tutte le misure di sicurezza adeguate a contenere il rischio del trattamento dei dati personali specificamente individuato dal Titolare e/o dal Responsabile in funzione alla tipologia e alle finalità del trattamento stesso;

✓ Assiste il Titolare del trattamento al fine di soddisfare gli obblighi di richiesta di esercizio dei diritti da parte degli interessati;

✓ Assiste il Titolare nel garantire il rispetto degli obblighi circa la notifica della violazione dei dati personali e la valutazione d'impatto sulla protezione dei dati personali;

✓ Cancella o restituisce tutti i dati personali oggetto del trattamento e le eventuali copie esistenti al Titolare alla scadenza del contratto.

Obblighi di trasparenza

L'informativa è stata **maggiormente dettagliata**, prevedendo una serie di contenuti aggiuntivi ed obbligatori. Nello specifico la stessa deve essere:

- ✓ chiara, semplice, concisa;
- ✓ in forma scritta (preferibilmente in formato elettronico); è possibile l'utilizzo di icone "in combinazione" con l'informativa estesa;
- ✓ trasparente, intelligibile, facilmente accessibile.

Deve altresì prevedere necessariamente:

- ✓ il periodo di conservazione dei dati personali trattati o, se non è possibile, i criteri utilizzati per definire tale periodo;
- ✓ il diritto di proporre reclamo ad un'autorità di controllo;
- ✓ l'intenzione del Titolare di trasferire i dati personali ad un paese terzo.

Informativa all'interessato

Il Titolare deve sempre specificare:

- ✓ i dati di contatto del Responsabile della protezione dei dati personali o, dove esistente, del Data Protection Officer;
- ✓ la base giuridica del trattamento;
- ✓ le informazioni previste nel rispetto degli obblighi di trasparenza;
- ✓ se il trattamento comporta processi decisionali automatizzati (anche la profilazione), indicando anche la logica di tali processi e le conseguenze per l'interessato.

Nel caso di dati personali non raccolti direttamente presso l'interessato, l'informativa deve essere fornita entro 1 mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati personali (a terzi o all'interessato).

Consenso dell'interessato

Deve necessariamente essere "esplicito":

✓ per i dati personali "sensibili";

✓ per i trattamenti automatizzati (compresa la profilazione).

Non deve essere necessariamente "documentato per iscritto", anche se la "forma scritta" è modalità idonea a configurare l'inequivocabilità del consenso e la prova dello stesso.

In tutti i casi in cui il trattamento è basato sul consenso il Titolare deve dare prova dell'intervenuta acquisizione dello stesso.

=> Il consenso dei minori è valido a partire dai 16 anni; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Registri delle attività di trattamento

Obbligo per il Responsabile e il Titolare di tenuta di un registro delle attività di trattamento dei dati personali in forma scritta (anche in formato elettronico), contenente tutte le attività, regolarmente aggiornate, svolte per soddisfare i requisiti di conformità al Regolamento.

L'obbligo di tenuta dei suddetti registri non si applica a soggetti giuridici aventi meno di 250 dipendenti (con limitate eccezioni). Tuttavia, il Garante, organo deputato al controllo della tenuta obbligatoria degli stessi, invita tutti i Titolari del trattamento e i Responsabili, a prescindere dalle dimensioni delle imprese, a dotarsi di tale registro poiché "*non costituisce un adempimento formale bensì* ***parte integrante di un sistema di corretta gestione dei dati personali***".

DPO
Responsabile della Protezione dei Dati

Il Regolamento introduce una nuova figura professionale: il DPO (Data Protection Officer), la cui nomina risulta obbligatoria in alcuni casi, ed avente lo specifico compito di facilitare l'attuazione del Regolamento da parte del Titolare e/o del Responsabile.

Compiti tassativi del DPO:

- ✓ sensibilizzazione e formazione del personale;
- ✓ sorveglianza sullo svolgimento della valutazione di impatto;
- ✓ assistenza al Titolare/Responsabile in merito agli obblighi derivanti dalla normativa;
- ✓ cooperazione con l'autorità di controllo.

DPO
Responsabile della Protezione dei Dati

… *Segue*

Requisiti soggettivi del DPO:

- indipendenza;
- autorevolezza;
- competenze manageriali;
- conoscenza specialistica della normativa e della prassi in materia di protezione dei dati personali;
- competenze informatiche e conoscenza dell'architettura IT del Titolare.

Diritti dell'interessato

Il Regolamento introduce una maggiore articolazione dei diritti dell'interessato ed in particolare:

✓ Il **diritto di accesso**, possibilità di verifica e ricezione di una copia dei dati personali oggetto di trattamento.

✓ Il **diritto alla portabilità dei dati**, possibilità di:

- ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali forniti al Titolare;
- trasmettere i propri dati personali da un Titolare ad un altro Titolare, senza impedimenti da parte di colui al quale sono stati forniti in precedenza. Non si applica ai trattamenti non automatizzati e sono previste specifiche condizioni per il suo esercizio (sono portabili solo i dati personali trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato e solo i dati personali che siano stati "forniti" dall'interessato al Titolare).

Diritti dell'interessato

…*Segue*

✓ Il **diritto all'oblio**, cancellazione dei dati personali in forma rafforzata: obbligo per i Titolari (se hanno "reso pubblici" i dati personali dell'interessato) di informare della richiesta di cancellazione tutti gli altri Titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione".

✓ Il **diritto di limitazione del trattamento**, in caso di:

- violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati personali stessi);
- rettifica dei dati personali (in attesa di tale rettifica da parte del Titolare);
- opposizione al trattamento (in attesa della valutazione da parte del Titolare).

Modalità di esercizio dei diritti dell'interessato

Il termine per rispondere alla richiesta dell'interessato di esercizio di un diritto è di 1 mese, estendibile fino a 3, in casi di particolare complessità.

Il Titolare deve:

- ✓ dare sempre (anche in caso di diniego) riscontro scritto all'interessato entro 1 mese dalla richiesta. La forma orale è consentita solo se preferita dall'interessato;
- ✓ valutare la complessità del riscontro e stabilire, solo in caso di richieste manifestamente infondate o eccessive, l'ammontare dell'eventuale contributo da chiedere all'interessato;
- ✓ rispondere in modo semplice, chiaro, "intelligibile", conciso, trasparente e facilmente accessibile.

Misure di sicurezza

Devono essere adeguate al rischio del trattamento dei dati personali specificamente individuato dal Titolare e/o dal Responsabile in funzione alla tipologia e alle finalità del trattamento stesso.

Il regolamento prevede una lista di misure (art. 32) che non possono, in ogni caso, essere considerate come «minime», ma mera indicazione aperta e non esaustiva: si ricorda infatti che il tema è rimesso interamente al Titolare e al Responsabile che dovranno valutare discrezionalmente e fattivamente le misure più adeguate al singolo caso.

Il Garante promuove l'adozione di specifici **codici di condotta o schemi di certificazione** per attestare, in caso di verifica da parte dell'Autorità di Controllo, l'adeguatezza delle misure di sicurezza adottate al rischio specifico del trattamento dei dati personali individuato dal Titolare e/o dal Responsabile.

Notifica Data Breach

Tutti i Titolari – non solo i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all'Autorità di Controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.

Se la probabilità di tale rischio è elevata, i Titolari dovranno informare delle violazioni anche gli interessati, salvo nei casi espressamente previsti, sempre "senza ingiustificato ritardo".

Termini

- **Entro il termine del 25 maggio 2018** tutti i Titolari del Trattamento dovranno adeguarsi alla nuova legge sulla privacy.

- I Regolamenti UE **sono immediatamente esecutivi,** pertanto non richiedendo la necessità di recepimento da parte degli Stati membri. A decorrere dal suddetto termine, quindi, la nuova normativa risulterà immediatamente applicabile ed obbligatoria per tutti gli **Stati membri UE** con conseguente uniformazione dell'intera disciplina.

Nuove Sanzioni

SANZIONE AMMINISTRATIVA PECUNIARIA	MODIFICHE/NOVITA'	DISPOSIZIONE VIOLATA
FINO A 10.000.000,00 € PER LE IMPRESE, O FINO AL 2% DEL FATTURATO MONDIALE TOTALE ANNUO DELL'ESERCIZIO PRECEDENTE SE SUPERIORE	Per i servizi diretti a minori di età < ai 16 anni, il consenso al trattamento deve essere prestato o autorizzato dal titolare della responsabilità genitoriale	ART. 8
	Obbligo di non conservazione, acquisizione o trattamento di informazioni per identificare l'interessato se le finalità del trattamento non lo richiedono (o non lo richiedono più)	ART. 11
	Adozione di misure tecniche e organizzative per 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. privacy by design e privacy by default)	ART. 25
	Designazione del Responsabile del trattamento e rispetto degli obblighi e compiti posti a suo carico mediante contratto	ART. 28
	Tenuta dei Registri delle attività di trattamento	ART. 30
	Adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza corrispondente al rischio	ART. 32
	Notifica di una violazione dei dati personali all'autorità di controllo (c.d. data breach)	ART. 33
	Svolgimento di una valutazione preventiva dell'impatto dei trattamenti previsti sulla protezione dei dati personali e conseguente consultazione dell'Autorità di controllo	ART. 35 E 36
	Designazione del Responsabile della protezione dei dati (c.d. DPO)	ART. 37 - 39

Nuove Sanzioni

SANZIONE AMMINISTRATIVA PECUNIARIA	MODIFICHE/NOVITA'	DISPOSIZIONE VIOLATA
FINO A 20.000.000,00 € PER LE IMPRESE, O FINO AL 4% DEL FATTURATO MONDIALE TOTALE ANNUO DELL'ESERCIZIO PRECEDENTE SE SUPERIORE	Dimostrazione della prestazione del **consenso** e del rispetto delle condizioni per il consenso. Tutela del diritto dell'interessato alla revoca del consenso	ART. 7
	Obblighi **informativi** nei confronti dell'interessato. Tutela dei diritti dell'interessato (diritto di 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)	ART. 12 - 22
	Obblighi connessi al trasferimento di dati personali verso **paesi terzi** o organizzazioni internazionali	ART. 44 – 49

Nuove Sanzioni

SANZIONE AMMINISTRATIVA PECUNIARIA	DISPOSIZIONI PREESISTENTI	DISPOSIZIONE VIOLATA
FINO A 20.000.000,00 € PER LE IMPRESE, O FINO AL 4% DEL FATTURATO MONDIALE TOTALE ANNUO DELL'ESERCIZIO PRECEDENTE SE SUPERIORE	Rispetto dei **principi** applicabili al trattamento: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza	ART. 5
	Rispetto delle **condizioni** di liceità del trattamento	ART. 6
	Rispetto delle condizioni di liceità del trattamento di **categorie particolari** di dati personali	ART. 9
	Qualsiasi obbligo previsto dalle legislazioni degli Stati membri per **specifiche situazioni** di trattamento	CAPO IX
	Rispetto di un ordine, di una limitazione di trattamento dell'**Autorità di controllo** o di un negato accesso ai dati	ART. 58

Sanzioni Penali*

DISPOSIZIONE VIOLATA	SANZIONE PENALE
Trattamento illecito dei dati	Reclusione da 6 a 18 mesi
Trattamento illecito dei dati con comunicazione e diffusione	Reclusione da 6 mesi a 2 anni
Trattamento illecito dei dati per i fatti sensibili o particolari	Reclusione da 1 a 3 anni
Falsità nelle dichiarazioni e notificazioni	Reclusione da 6 mesi a 3 anni
Omessa adozione delle misure di sicurezza	Arresto sino a 2 anni o ammenda pari ad ¼ della sanzione massima per la violazione amministrativa **
Inosservanza provvedimenti Autorità di controllo (Garante per la privacy)	Reclusione da 3 mesi a 2 anni

* Così come previste dal D.Lgs.196/2003 ed in attesa delle nuove disposizioni del legislatore italiano a cui è demandata dal Regolamento UE la previsione di specifiche e nuove sanzioni penali

** Art. 162, comma 2-bis TU 196/2003*: «In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'articolo 154, comma 1, lettere c) e d), è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da trentamila euro a centottantamila euro».*

CDT

LEGAL

Rome
Via Romagnosi n. 1/B ,
00196 Roma

Florence
Via Cantagalli 2 (Viale del Poggio Imperiale)
50125 Firenze

Milan
Via dell'Annunciata, 23/4
20121 Milano

Ref.: Avv. Elena Baudo
info@cdt.legal
Tel.:+39.055.22.98.222

Member of

MARCALLIANCE
THE BRIDGE TO YOUR GLOBAL LAWYER