Tonucci & Partners

IL NUOVO REGOLAMENTO GENERALE UE SULLA PROTEZIONE DEI DATI PERSONALI N. 679/2016.

Analisi pratica del quadro generale di insieme e dei nuovi adempimenti privacy.

1. Entrata in vigore

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679 ENTRATA IN VIGORE

Pubblicazione nella Gazzetta Ufficiale dell'Unione Europea n. 119/2016: **4 Maggio 2016**.

Entrata in vigore: **25 Maggio 2016**.

Applicabilità in tutti i Paesi della UE: **25 Maggio 2018**.

Tutti i soggetti interessati hanno **due anni di tempo** per adeguare alle nuove norme le politiche del trattamento dei dati.

Il Regolamento sarà **immediatamente applicabile** senza necessità di recepimento.

Per quanto riguarda l'Italia, il Regolamento sostituirebbe (non integralmente) il Codice Privacy in vigore dal 1° Gennaio 2004 ma sarà **necessario comunque un coordinamento normativo** (Il Garante privacy ha in corso una ricognizione normativa per verificare quali parti del Codice privacy e quali provvedimenti generali del Garante sopravvivranno alla riforma).

2. L’ambito di applicabilità soggettiva e territoriale del Regolamento privacy UE.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
AMBITO DI APPLICABILITÀ

Il Regolamento si applica solo al **trattamento dei dati personali di persone fisiche.**

Il Regolamento si applica inoltre:

1) al trattamento di dati personali effettuato da un **titolare stabilito nella UE**;

ma anche

2) al trattamento di dati personali effettuato da **titolari non stabiliti nell'Unione Europea** se il **trattamento ha ad oggetto dati personali di interessati che si trovano nella UE** e riguarda (1) **l'offerta di beni o servizi** (anche non a pagamento) ai suddetti interessati (2) il **monitoraggio** del loro comportamento nel territorio dell'Unione Europea.

Ricorrendo tali presupposti **qualsiasi ente/azienda mondiale**, anche non avente sede nella UE sarà soggetta al Regolamento.

3. Le nuove definizioni giuridiche dei concetti privacy.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
ALCUNE DEFINIZIONI

1) **«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;

2) **«trattamento»:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
ALCUNE DEFINIZIONI

3) **«titolare del trattamento»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

4) **«responsabile del trattamento»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

5) **«consenso dell'interessato»:** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
DEFINIZIONI

Non esiste più una specifica definizione di dati personali "*sensibili*" o di dati personali "*giudiziari*", ancorchè la definizione sia ricavabile dagli articoli generali dedicati a queste categorie di informazioni.

L'articolo 9, difatti, individua in generale le **"*categorie particolari di dati personali*"** nelle informazioni "*che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona fisica*".

Il Regolamento introduce comunque **una nuova definizione limitata ai "*dati relativi alla salute*"** intesi quali i "*dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*".

L'articolo 10 del Regolamento disciplina poi il trattamento dei "***dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza*".**

4. Le figure soggettive privacy: Titolare del trattamento. Responsabile del trattamento. Persone autorizzate al trattamento. Rappresentante designato del titolare trattamento.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
NUOVI OBBLIGHI NEI RAPPORTI TRA SOGGETTI PRIVACY

Le figure soggettive privacy tipiche restano sostanzialmente invariate, ma **il Regolamento introduce degli obblighi organizzativi nuovi con riferimento ai loro ruoli e funzioni**, come ad esempio i seguenti:

1. **nel caso di contitolarità del trattamento**, cioè allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, **va redatto uno specifico accordo interno** tra i contitolari 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;

2. con riferimento al **Responsabile del trattamento**, figura facoltativa nel Codice della privacy, **la sua nomina diventa obbligatoria e va documentata con un "*contratto o altro atto giuridico*"**- stipulato in forma scritta o anche in formato 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.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
NUOVI OBBLIGHI NEI RAPPORTI TRA SOGGETTI PRIVACY

3. Il Responsabile del trattamento **può a sua volta designare altri responsabili del trattamento** ma previa autorizzazione scritta – specifica o generale – del titolare del trattamento;
4. gli **incaricati del trattamento** (che il Codice della privacy obbliga a designare per iscritto) non sono menzionati nel Regolamento, che però prevede la figura delle "***persone autorizzate al trattamento***", cioè i soggetti che operano sotto la diretta responsabilità del titolare o del responsabile con apposite istruzioni (sembrerebbero restare in vigore le obbligatorie istruzioni agli incaricati, anche se il Regolamento non prevede nulla riguardo alla forma scritta);
5. Il "***rappresentante del titolare del trattamento***" stabilito nella UE va designato per iscritto in caso di trattamenti effettuati da titolari non stabiliti nell'Unione Europea se il trattamento ha ad oggetto dati personali di interessati che si trovano nella UE e riguarda (1) l'offerta di beni o servizi (anche non a pagamento) ai suddetti interessati (2) il monitoraggio del loro comportamento nel territorio dell'Unione Europea.

5. La nuova figura del *Data Protection Officer*.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
IL DATA PROTECTION OFFICER

Del tutto nuova è la figura del ***Responsabile della protezione dei dati*** (*Data Protection Officer*) introdotta dall'art. 37 del Regolamento.

L'**obbligo di designazione** del *Responsabile della protezione dei dati* (da parte del titolare o del responsabile del trattamento) **non è generale ma si applica solo se**:

1.il trattamento **è effettuato da un'autorità pubblica o da un organismo pubblico**, eccettuate le autorità giurisdizionali;

2.le attività **principali** del titolare del trattamento o del responsabile del trattamento consistono in **trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala**;

3.le attività **principali** del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, **su larga scala**, di dati personali sensibili, sanitari, sulla vita o sull'orientamento sessuale, genetici, biometrici, o di dati relativi a condanne penali e a reati.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
IL DATA PROTECTION OFFICER: CARATTERISTICHE E MODALITA' DI NOMINA

Un **gruppo** imprenditoriale **può nominare un unico** Data Protection Officer.

Il Data Protection Officer **può essere un dipendente** del titolare del trattamento o del responsabile del trattamento oppure **un consulente esterno** che assolve i suoi compiti in base a un **contratto di servizi**.

Il Data Protection Officer va designato in funzione delle **elevate qualità professionali e della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati**.

I **dati di contatto** del Data Protection Officer vanno **comunicati al Garante e resi pubblici**.

Il Data Protection Officer **è una figura apicale**, assolutamente diversa quanto a ruolo e funzioni dal "semplice" responsabile del trattamento (con il quale **non va confuso**). Va coinvolto in tutte le questioni riguardanti la protezione dei dati personali e deve avere le risorse necessarie e il **potere di spesa** per assolvere ai compiti assegnati.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
IL DATA PROTECTION OFFICER: CARATTERISTICHE E MODALITA' DI NOMINA

Il Data Protection Officer **non deve ricevere dal titolare o dal responsabile alcuna istruzione per quanto riguarda l'esecuzione dei compiti affidati** (è figura del tutto autonoma) **né è soggetto a potere disciplinare o sanzionatorio** per l'adempimento dei propri compiti (ad esempio in ciò – tra l'altro - risiedono i caratteri distintivi tra *Data Protection Officer* e responsabile del trattamento, che al contrario deve ricevere istruzioni scritte ed è soggetto al controllo e all'autorità del titolare del trattamento, ivi compresi i profili sanzionatori).

L'articolo 39 del Regolamento individua il **nucleo minimo** (che dunque può essere anche esteso) dei compiti assegnati al Responsabile della protezione dei dati.

6. Il nuovo obbligo di redazione e detenzione del Registro generale delle attività di trattamento svolte.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
IL REGISTRO DELLE ATTIVITA' DI TRATTAMENTO SVOLTE

Il Regolamento introduce - **per le imprese o organizzazioni con più di 250 dipendenti** - un **duplice obbligo documentale nuovo**: quello del **Registro delle attività di trattamento** che – secondo le rispettive responsabilità e competenze - deve essere redatto (anche in formato elettronico) sia dal titolare che dal responsabile del trattamento e **va esibito** su richiesta al Garante.

Il Registro delle attività di trattamento è la parte più importante dell'obbligo di elaborare un sistema documentale di gestione della privacy contenente tutti gli atti, regolarmente aggiornati, elaborati per soddisfare i requisiti di conformità al Regolamento. Tale **obbligo di rendicontazione (o di "*accountability*")** impone a ciascun titolare del trattamento di conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità, indicando obbligatoriamente - per ognuno di essi – le seguenti informazioni.

L'obbligo di tenuta del **Registro delle attività di trattamento** si applica **anche** ad imprese **con meno di 250 dipendenti**, se il trattamento: (a) presenta un rischio per i diritti e le libertà dell'interessato; (b) non è occasionale e include dati personali sensibili, sanitari, sulla vita o sull'orientamento sessuale, genetici, biometrici, relativi a condanne penali e a reati.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
IL REGISTRO DELLE ATTIVITA' DI TRATTAMENTO SVOLTE

a)il nome e i **dati di contatto** del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b)le **finalità** del trattamento;
c)una **descrizione** delle categorie di interessati e delle categorie di dati personali;
d)le **categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e)ove applicabile, i **trasferimenti di dati personali verso un paese terzo** o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;
f)ove possibile, i **termini ultimi previsti per la cancellazione** delle diverse categorie di dati;
g)ove possibile, una **descrizione generale delle misure di sicurezza tecniche e organizzative.**

7. Il nuovo obbligo di valutazione preventiva d'impatto sulla protezione dei dati.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
IL PRIVACY IMPACT ASSESSMENT (PIA)

Tra i nuovi **e più rilevanti oneri** posti a carico del titolare del trattamento vi è quello della valutazione preventiva d'impatto sulla protezione dei dati (c.d. principio della ***privacy impact assessment***).

Quando un **trattamento prevede in particolare l'uso di nuove tecnologie** oppure considerati la natura, l'oggetto, il contesto e le finalità del trattamento può presentare un **rischio elevato per i diritti e le libertà delle persone fisiche** (es: trattamenti automatizzati di profilazione sistematica degli interessati, sorveglianza sistematica su larga scala di una zona accessibile al pubblico, trattamenti di dati personali sensibili, sanitari, sulla vita o sull'orientamento sessuale, genetici, biometrici, relativi a condanne penali e a reati) il titolare del trattamento, **prima di procedere** (e consultandosi con il *Data Protection Officer*, ove nominato, e - se del caso – raccogliendo anche le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto) **deve preventivamente effettuare una valutazione dell'impatto del trattamento previsto sulla protezione dei dati personali** (una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi).

.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
IL PRIVACY IMPACT ASSESSMENT (PIA)

Il **Garante redigerà un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati** (e anche – al contrario - un elenco delle tipologie di trattamenti per le quali **non è richiesta** una valutazione d'impatto sulla protezione dei dati, come nei casi di trattamento necessario per adempiere un obbligo legale o a un contratto.

La valutazione – **soggetta a riesame periodico** - contiene almeno una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, dell'interesse legittimo perseguito dal titolare del trattamento, la valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità, la valutazione dei rischi per i diritti e le libertà degli interessati e le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati.
Se la valutazione preventiva indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate per attenuare il rischio, il titolare, prima di procedere al trattamento, **è tenuto a consultare il Garante** (con una procedura analoga all'attuale interpello previsto dall'art. 17 del Codice della privacy).

8. I nuovi obblighi c.d. di *privacy by design* e *privacy by default*.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
PRIVACY BY DESIGN

L'articolo 25 del Regolamento ("*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*") **impone vincoli che impattano sulle stesse fasi produttive e di operatività di apparati e/o servizi** che implicano il trattamento di dati personali.

Con riferimento al principio cosiddetto della ***privacy by design***, il Regolamento prescrive che il titolare del trattamento - tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento - debba **applicare misure tecniche e organizzative adeguate** (es: anonimizzazione) volte ad attuare in modo efficace i principi di protezione dei dati e a **integrare nel trattamento le necessarie** garanzie per tutelare i diritti degli interessati. E tale adempimento va effettuato sia al momento di determinare i mezzi del trattamento (es: progettazione di *device*) sia all'atto del trattamento stesso.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
PRIVACY BY DEFAULT

Con riferimento al principio cosiddetto della ***privacy by default*, il Regolamento stabilisce che il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate **per garantire che siano trattati, per impostazione predefinita** (cioè *by default*), **solo i dati personali necessari per ogni specifica finalità del trattamento**.

Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure devono garantire che, per impostazione predefinita, **non siano resi accessibili dati personali** a un numero indefinito di persone fisiche senza l'intervento della persona fisica (che ad esempio consapevolmente disponga il settaggio dell'apparato o del servizio scegliendo di condividere con i terzi i dati personali oggetto di trattamento nell'ambito della operatività dell'apparato o del servizio).

Il titolare può ottenere una **certificazione *ad hoc*,** prevista dal Regolamento in base ad una specifica procedura, per dimostrare la **conformità ai principi di privacy by design e by default.**

9. La nuova Informativa privacy rafforzata.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
LA NUOVA INFORMATIVA PRIVACY

Il Regolamento sancisce a carico dei titolari del trattamento **obblighi di informativa rafforzati** rispetto a quanto avviene ora con l'art. 13 del Codice della privacy, prevedendosi **numerose informazioni aggiuntive** da fornire agli interessati **in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro**.

L'Informativa **va resa per iscritto o con altri mezzi, anche elettronici**. Se richiesto dall'interessato, le informazioni possono essere fornite **oralmente**, purché sia comprovata con altri mezzi l'identità dell'interessato.

Rispetto agli elementi obbligatori da indicare nell'informativa privacy che già siamo abituati a conoscere in applicazione dell'art. 13 del Codice della privacy italiano (**e che ovviamente non vengono meno**), i titolari del trattamento dovranno inserire obbligatoriamente anche le seguenti informazioni aggiuntive sul trattamento:

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
LA NUOVA INFORMATIVA PRIVACY

1. i **dati di contatto** della nuova figura del *Data Protection Officer* (Responsabile della protezione dei dati personali) ove prevista;
2. la **base giuridica del trattamento** a corredo della illustrazione delle finalità del trattamento;
3. qualora il trattamento si basi sulla necessità di perseguire un legittimo interesse del titolare del trattamento o di terzi, **la specificazione di quali siano i legittimi interessi** perseguiti dal titolare del trattamento o da terzi;
4. **l'ambito del trasferimento all'estero** (ovviamente extra UE) o a un'organizzazione internazionale dei dati personali;
5. il **periodo di conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
6. la **specifica esistenza del diritto alla portabilità dei dati**;
7. l'esistenza del **diritto di revocare il consenso in qualsiasi momento** senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
8. il diritto di **proporre reclamo** al Garante privacy;

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
LA NUOVA INFORMATIVA PRIVACY

9. la **eventuale esistenza di un processo decisionale automatizzato**, compresa la **profilazione** e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato;
10. **la fonte da cui hanno origine i dati personali** e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico (tale informazione è obbligatoria solo ove i dati non siano raccolti presso l'interessato);
11. le **categorie di dati personali oggetto del trattamento** (tale informazione è obbligatoria solo ove i dati non siano raccolti presso l'interessato).

Le informazioni da rendere agli interessati possono essere fornite anche in combinazione con **icone standardizzate** per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un **quadro d'insieme del trattamento previsto**. Se presentate elettronicamente, le icone devono essere leggibili da qualsiasi dispositivo.

10. Il consenso al trattamento dei dati personali.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
IL CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Il Regolamento fonda sul ***«consenso dell'interessato»*** la principale precondizione (salve le deroghe) di liceità del trattamento.

Il titolare del trattamento deve poter dimostrare che l'interessato ha prestato il consenso al trattamento dei propri dati personali. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve **essere presentata in modo chiaramente distinguibile dalle altre materie**, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro, **pena l'invalidità del consenso prestato.**

L'interessato ha poi il **diritto di revocare il proprio consenso** (e tale informazione è uno dei nuovi elementi obbligatori dell'informativa privacy) in qualsiasi momento (anche se la revoca non pregiudica la liceità del trattamento fino a quel momento effettuato), con modalità di esecuzione della revoca del consenso facili come la sua prestazione originaria.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
IL CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

E' **specificatamente vietato** che l'esecuzione di un contratto o la prestazione di un servizio siano condizionati alla prestazione del consenso al trattamento di dati personali **non necessario** all'esecuzione del contratto o servizio.

Alla **specifica manifestazione del consenso è poi subordinata**:

1. la liceità del trattamento (**altrimenti vietato**, a meno che non si applichino gli altri presupposti alternativi al consenso di cui all'art. 9 del Regolamento) dei dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dei dati genetici, dei dati biometrici, dei dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

2. la possibilità – **altrimenti vietata** – di procedere alla **profilazione dell'interessato**;

3. la possibilità di **trasferire i dati personali dell'interessato verso un paese terzo extra UE** o verso un'organizzazione internazionale.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
IL CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Se un trattamento di dati nell'ambito **della fornitura ad un minore di un servizio della società dell'informazione** (ad esempio l'accesso a Internet, l'iscrizione a un social network, l' apertura di un account email, o il download di un'applicazione, 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 del trattamento è obbligato – sia pur con il criterio della "*ragionevolezza*" e tenendo presenti comunque le "*tecnologie disponibili*" - **a verificare** nei casi di minore infrasedicenne che il consenso sia prestato o autorizzato dal titolare della potestà genitoriale sul minore.

11. Il nuovo diritto alla portabilità dei dati.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
LA PORTABILITA' DEI DATI PERSONALI

Il nuovo "**diritto alla portabilità dei dati personali**" consiste nel diritto dell'interessato di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti.

Tale diritto è esercitabile quando il trattamento: (1) è effettuato con mezzi automatizzati; (2) si basa sul consenso precedentemente prestato dall'interessato o (3) si basa su un contratto o su trattative precontrattuali.

In questi specifici casi l'interessato – fermo restando comunque il suo diritto alla cancellazione dei dati - ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, "*se tecnicamente fattibile*".

12. Le misure di sicurezza nel trattamento dei dati personali.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
LE MISURE DI SICUREZZA

La **sicurezza nel trattamento dei dati è uno dei principi fondamentali del trattamento** in base al nuovo articolo 5 del Regolamento (“*i dati devono essere 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 – principio della «integrità e riservatezza»”).*

L’articolo 32 del Regolamento precisa le misure stabilendo che - tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche - il titolare del trattamento e il responsabile del trattamento debbano mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre:

1. la **pseudonimizzazione** e la **cifratura** dei dati personali;
2. la capacità di **assicurare su base permanente** la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
3. la capacità di **ripristinare tempestivamente la disponibilità e l'accesso** dei dati personali in caso di incidente fisico o tecnico;
4. una **procedura per testare, verificare e valutare regolarmente l'efficacia delle misure** tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Circa gli **obblighi di documentazione delle misure di sicurezza** (analoghi al vecchio e abrogato DPS previsto dalla normativa italiana), il Regolamento prescrive "*ove possibile*" di **inserire nel nuovo *Registro delle attività di trattamento svolte "una descrizione generale delle misure di sicurezza tecniche e organizzative".*** Inoltre, nella documentazione della *valutazione preventiva di impatto sulla protezione dei dati*, il titolare deve descrivere anche – tra l'altro - le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone.

13. La notifica della violazione dei dati personali (“*Data Breach*”).

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
LA NOTIFICAZIONE DELLE VIOLAZIONI DI DATI PERSONALI

La principale novità in materia di **data breach** è rappresentata dal fatto che l'obbligo di notifica al Garante di una avvenuta violazione di dati personali (definita formalmente quale "*violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*";) - ora applicabile ai soli fornitori di servizi di comunicazione elettronica accessibili al pubblico - **diventa obbligo generale per tutti i titolari del trattamento**, indipendentemente dal fatto che siano o meno fornitori di servizi di comunicazione elettronica.

In caso di violazione dei dati personali, il **titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore** dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

La notifica deve almeno:

1. descrivere **la natura della violazione** dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

2. **comunicare il nome e i dati di contatto del responsabile** della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

3. descrivere le **probabili conseguenze della violazione** dei dati personali;

4. descrivere **le misure adottate o di cui si propone l'adozione** da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il **titolare del trattamento comunica la violazione anche all'interessato**, senza ingiustificato ritardo, descrivendola con un linguaggio semplice e chiaro, salve circostanze al verificarsi delle quali non è richiesta la comunicazione all'interessato.

14. Trasferimento dei dati fuori dell’Unione Europea.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
TRASFERIMENTO DEI DATI PERSONALI AL DI FUORI DELLA UE

Non vi sono particolari novità rispetto all'attuale quadro in materia di trasferimento dei dati personali al di fuori della UE. Qualunque trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale può avere luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni esplicitate dal Regolamento:

1. **trasferimento sulla base di una decisione di adeguatezza** (ove la Commissione UE abbia deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato; in tal caso il trasferimento non necessita di autorizzazioni specifiche);

2. **trasferimento soggetto a garanzie adeguate** (il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate, come ad esempio le norme vincolanti d'impresa, le clausole contrattuali standard, l'esistenza di un codice di condotta, l'esistenza di un meccanismo di certificazione, specifiche clausole contrattuali);

Se non è applicabile nessuna delle condizioni sopra illustrate il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale sono ammessi soltanto se si verifica una delle seguenti condizioni:

a) il consenso informato dell’interessato;

b) il trasferimento è necessario all'esecuzione di un contratto ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;

c) il trasferimento sia necessario per importanti motivi di interesse pubblico o per accertare, esercitare o difendere un diritto in sede giudiziaria;

d) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

c) il trasferimento sia effettuato a partire da un registro pubblico.

15. La disciplina del c.d. diritto all’oblio.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
IL DIRITTO ALL'OBLIO

Il **Regolamento codifica compiutamente il diritto all'oblio** (quale specifico esercizio del diritto alla cancellazione dei dati personali). L'interessato esercita il «diritto all'oblio» chiedendo al titolare del trattamento che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al Regolamento.

Tuttavia, rimane lecita l'ulteriore conservazione dei dati personali in caso di diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale o un compito di interesse pubblico, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, per accertare, esercitare o difendere un diritto in sede giudiziaria.
Il titolare del trattamento che **ha pubblicato on line dati personali deve informare altri titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link** verso tali dati personali o copia o riproduzione di detti dati personali.

16. La disciplina dei trattamenti di profilazione.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
LA PROFILAZIONE

Il Regolamento **introduce 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 **la profilazione appare sostanzialmente vietata** ("*L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*") a meno che non vi siano circostanze specifiche, tra le quali il **chiaro consenso informato dell'interessato**.

I trattamenti di profilazione rappresentano poi uno dei presupposti che **rendono obbligatoria la valutazione preventiva** di impatto sulla protezione dei dati.

17. Il nuovo apparato sanzionatorio.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
LE NUOVE SANZIONI

Dal punto di **vista civilistico**, viene confermata la responsabilità risarcitoria per il c.d. "*danno da trattamento*", che viene più precisamente codificato (rispetto, ad esempio, all'art. 15 del Codice della privacy): 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*". Sono inoltre meglio 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.

Per quanto riguarda l'applicazione delle **sanzioni amministrative pecuniarie** da parte delle autorità di controllo (il Garante), l'art. 83 del Regolamento, oltre e regolare le condizioni di determinazione delle sanzioni, fissa i seguenti importi:

1. sanzioni amministrative pecuniarie fino a **10.000.000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore, nel caso di violazione di determinati obblighi posti dal Regolamento;

2. sanzioni amministrative pecuniarie fino a **20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore, nel caso di violazione degli obblighi più stringenti posti dal Regolamento (anche nel semplice caso di inosservanza degli ordini del Garante).

Con riferimento alle **sanzioni penali**, come è noto il Diritto dell'Unione Europea non può prevederne, essendo la materia penale di stretta competenza nazionale. Occorrerà verificare – in sede di abrogazione del Codice della privacy – come sarà trattata la attuale disciplina di cui all'art. 167 che prevede il reato di trattamento illecito di dati personali. In ogni caso il Regolamento prevede che è competenza degli Stati membri stabilire (e notificare alla Commissione entro il 25 Maggio 2018) le norme relative alle altre sanzioni per le violazioni del Regolamento (in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie) e adottare tutti i provvedimenti necessari per assicurare l'applicazione di sanzioni effettive, proporzionate e dissuasive.

www.tonucci.com

Thank you