Euroconference NEWS
L'INFORMAZIONE QUOTIDIANA DA PROFESSIONISTA A PROFESSIONISTA
Direttori: Sergio Pellegrino e Giovanni Valcarenghi

Edizione di martedì 24 aprile 2018

ADEMPIMENTI

Le nuove regole privacy – V° parte

di **Lucia Recchioni**

Come già anticipato nei precedenti contributi, il **Regolamento europeo**, introducendo il nuovo **principio di "responsabilizzazione"** (o "***accountability***"), richiede la concreta adozione, da parte del titolare e dei responsabili, di **misure di sicurezza** appropriate per il rispetto del regolamento stesso.

I **titolari**, pertanto, devono svolgere una serie di specifiche **attività preventive (dimostrabili)**, tenendo conto del **rischio inerente al trattamento** (ovvero il **rischio di impatti negativi** sulle libertà e i diritti degli interessati).

Il **rischio inerente al trattamento** deve quindi essere preventivamente **valutato**, individuando le misure tecniche e organizzative idonee a **mitigare tali rischi**: più precisamente, l'articolo 35 Regolamento UE 2016/679 impone una "**valutazione dell'impatto dei trattamenti**" (o "***Data Protection Impact Assessment***" – **DPIA**), la quale **non** è tuttavia **obbligatoria** in ogni caso.

Le Linee guida "***Data Protection Impact Assessment***" propongono pertanto alcuni criteri utili per l'individuazione delle attività soggette alla **DPIA**.

In generale "*fatti salvi i casi in cui un trattamento rientra nel campo di applicazione di un'eccezione, **è necessario realizzare una valutazione d'impatto sulla protezione dei dati qualora un trattamento "possa presentare un rischio elevato"***".

Sul punto giova tra l'altro precisare che l'articolo 35 del Regolamento fornisce alcuni **esempi** di casi nei quali un trattamento "***possa presentare rischi elevati***":

"a) una ***valutazione sistematica e globale di aspetti personali*** *relativi a persone fisiche, basata su un **trattamento automatizzato**, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*

*b) il **trattamento**, su larga scala, di **categorie particolari di dati personali** di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;*

*o c) la **sorveglianza sistematica su larga scala di una zona accessibile al pubblico***".

Nel caso in cui sia obbligatoria una **valutazione d'impatto sulla protezione dei dati**, quest'ultima, ai sensi dell'**articolo 36, dovrà contenere almeno**:

1. una **descrizione** sistematica dei **trattamenti** previsti e delle **finalità del trattamento**, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
2. una valutazione della **necessità** e **proporzionalità** dei **trattamenti** in relazione alle **finalità**;
3. una **valutazione dei rischi** per i diritti e le libertà degli interessati;
4. 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 in questione.

Solo se le **misure** adottate sono idonee a **mitigare il rischio** potrà avvenire il **trattamento dei dati**; alternativamente sarà necessario consultare l'**autorità di controllo** competente per ottenere indicazioni su **come gestire il rischio residuale**.

L'Autorità, pur **non** avendo il potere di "**autorizzare**" il trattamento, potrà indicare le **misure ulteriori** che il titolare può implementare.

Come può desumersi, pertanto, il nuovo **principio di responsabilizzazione** prevede un intervento dell'**Autorità** solo ***ex-post***; non è invece prevista come in passato, la notifica preventiva dei trattamenti all'autorità di controllo.

I registri delle attività di trattamento

Un ulteriore adempimento imposto dalla nuova disciplina privacy è rappresentato dall'obbligo di **tenuta dei registri delle attività di trattamento**, di cui all'articolo 30 Regolamento**.**

È in primo luogo necessario premettere che i **Registri dei trattamenti** non devono essere tenuti dagli **organismi con meno di 250 dipendenti**, **a meno che il trattamento da effettuare**:

- presenti un **rischio per i diritti e le libertà dell'interessato**,
- **non sia occasionale**, oppure
- includa il trattamento di **categorie particolari di dati** di cui all'articolo 9 (dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) o i **dati personali relativi a condanne penali e a reati** di cui all'articolo 10.

Il primo registro (**registro delle attività di trattamento**) deve essere tenuto da ogni **titolare** o dal suo **rappresentante** e deve contenere tutte le seguenti **informazioni**:

1. 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;

2. le **finalità del trattamento**;
3. una descrizione delle **categorie di interessati** e delle **categorie di dati personali**;
4. le **categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
5. 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, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
6. ove possibile, i **termini** ultimi **previsti** per la **cancellazione** delle diverse categorie di dati;
7. ove possibile, una **descrizione generale delle misure di sicurezza tecniche e organizzative** di cui all'articolo 32, paragrafo 1.

Come detto, la compilazione dell'appena richiamato registro è demandata al titolare del trattamento; il Regolamento prevede poi un **ulteriore registro** la cui **compilazione** è richiesta al **responsabile del trattamento**, il quale, appunto, deve tenere un **registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento**, contenente:

1. il **nome e i dati di contatto del responsabile** o dei responsabili del trattamento, di ogni **titolare** del trattamento per conto del quale agisce il responsabile del trattamento, del **rappresentante del titolare** del trattamento o del responsabile del trattamento e, ove applicabile, del **responsabile della protezione dei dati**;
2. le **categorie dei trattamenti effettuati** per conto di ogni titolare del trattamento;
3. 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, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
4. ove possibile, una descrizione generale delle **misure di sicurezza tecniche e organizzative** di cui all'articolo 32 Regolamento.

Entrambi i registri devono essere **tenuti in forma scritta**, anche in formato elettronico, e devono essere **esibiti su richiesta al Garante**.

Il Garante, nelle sue recenti linee guida ha inoltre precisato che il **registro dei trattamenti** non costituisce un mero adempimento formale, ma "***parte integrante di un sistema di corretta gestione dei dati personali***. *Per tale motivo, si invitano* ***tutti i titolari di trattamento e i responsabili****, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per* ***dotarsi di tale registro*** *e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta*".

Le misure di sicurezza

Il **D.Lgs. 196/2003** prevedeva "**misure minime**" e "**misure idonee**" al fine di garantire la **sicurezza** dei dati personali.

Il nuovo **Regolamento privacy** abbandona questa previsione, soprattutto in considerazione della circostanza che la rapida evoluzione delle tecnologie **non** consente di individuare **preventivamente** le misure necessarie per garantire la **protezione dei dati**.

Ecco il motivo per il quale, in ossequio al più generale **principio di responsabilizzazione**, non sono state previste **misure minime di sicurezza**, preferendo invece attribuire ai **titolari** e ai **responsabili** del trattamento l'onere di individuare le **misure di sicurezza più idonee**.

L'articolo 32, pertanto, propone un semplice **elenco** di **misure di sicurezza adottabili**, lasciando tuttavia spazio anche a **soluzioni alternative** più adeguate in considerazione del **rischio nel trattamento dei dati**.

Tra gli esempi proposti di "**misure tecniche e organizzative adeguate**" assume particolare rilevanza la c.d. "**pseudonimizzazione**", ovvero il "***trattamento dei dati personali*** *in modo tale che i dati personali* ***non possano più essere attribuiti a un interessato specifico*** *senza l'utilizzo di* ***informazioni aggiuntive****, a condizione che tali informazioni aggiuntive siano* ***conservate separatamente*** *e soggette a* ***misure tecniche e organizzative*** *intese a garantire che tali dati personali non siano attribuiti a una* ***persona fisica identificata o identificabile***".

Per approfondire questioni attinenti all'articolo vi raccomandiamo il seguente corso: