La Comunicazione - Note, Recensioni e Notizie n. 65
Anno 2022

GDPR e analisi dei rischi: una doppia prospettiva

GDPR and risk analysis: a dual perspective

Giancarlo Butti♦, Alberto Piamonte□

♦ ISACA - Milano

□ ISACA – Roma

Sommario

L'articolo analizza due diverse prospettive con cui effettuare l'analisi dei rischi legata al rispetto del GDPR:

- quella richiesta dalla normativa, legata ai rischi per i diritti e libertà delle persone fisiche
- quella che valuta i rischi (in particolare sanzionatorio e risarcitorio) che il trattamento dei dati personali comporta per Titolari e Responsabili

e i vantaggi derivanti da un approccio basato su questa doppia prospettiva ai fini della valutazione costi/benefici delle contromisure adottate.

Abstract

The article analyzes two different perspectives used to conduct the risk analysis related to GDPR compliance:

- the one required by the legislation, related to the risks for the rights and freedoms of individuals
- the one that assesses the risks (in particular sanctions and compensation) that the processing of personal data entails for controllers and processors

and the advantages deriving from an approach based on this dual perspective for the purposes of assessing the costs/benefits of the countermeasures adopted.

Keyword

GDPR, Risk analysis and treatment, compliance

1 - Introduzione

L'analisi dei rischi nell'ambito del GDPR è una delle attività che la normativa prescrive come obbligatoria.

In realtà la valutazione sui rischi per i diritti e le libertà delle persone fisiche è ripresa in ben tre diversi articoli nel GDPR (artt. 24, 25 e 32) e non riguarda solo gli aspetti di sicurezza.

Accanto a queste valutazioni di natura obbligatoria, un Titolare o Responsabile di trattamento potrebbero valutare anche quale sia il proprio rischio, (ad esempio in termini sanzionatori o risarcitori) derivanti dal trattamento dei dati personali.

Le due prospettive possono essere svolte contemporaneamente.

2 - L'oggetto di tutela del GDPR

Il primo punto da chiarire per una corretta valutazione dei rischi nell'ambito del GDPR è comprendere esattamente quale sia l'oggetto di tutela del GDPR.

Al riguardo è l'articolo 1 che lo identifica correttamente:

Articolo 1 - Oggetto e finalità (C1-14, C170, C172)

1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare, il diritto alla protezione dei dati personali.

Quindi in sintesi:

- *protezione delle persone fisiche con riguardo al trattamento dei dati personali (art. 1.1)*
- *i diritti e le libertà fondamentali delle persone fisiche (art. 1.2)*

Di fatto gli articoli 24, 25 e 32 recitano in merito all'analisi dei rischi rispettivamente:

Articolo 24 - Responsabilità del titolare del trattamento (C74-C78)

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche…

Articolo 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (C75-C78)

1. 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…

Articolo 32 - Sicurezza del trattamento (C83)

1. 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…

Appaiono quindi evidenti alcuni aspetti, solitamente trascurati, che differenziano l'attuale normativa dalla precedente (in cui tali temi erano presenti, ma non così enfatizzati).

L'oggetto principale di tutela non sono strettamente e solamente i dati personali, ma le persone fisiche, o meglio i diritti e libertà delle persone fisiche.

Al riguardo è importante evidenziare che il testo di legge fa sempre riferimento alle persone fisiche (natural person) quando parla di analisi dei rischi e non agli interessati (data subject), ma su questo tema ritorneremo a breve.

Per quanto riguarda il concetto di diritti e libertà fondamentali (l'oggetto quindi di tutela del GDPR), il testo di legge non ne dà una definizione precisa, ma si limita a citarne qualche esempio nel considerando 75:

(75) I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Tali definizioni hanno origine dalla **Carta dei diritti fondamentali dell'Unione europea** che al riguardo cita come diritti fondamentali:

- dignità
- libertà
- uguaglianza
- solidarietà
- cittadinanza
- giustizia.

Le definizioni vengono quindi successivamente riprese dallo stesso WP29 (oggi EDPB) nel suo **Parere 218/14:**

> *…Risks, which are related to potential negative impact on the data subject's rights, freedoms and interests, should be determined taking into consideration specific objective criteria (…).*
> *In the context referred to above, the scope of "the rights and freedoms" of the data subjects primarily concerns the right to privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion*

3 – Chi sono le persone fisiche?

Parlando di GDPR si ritiene solitamente che i soggetti tutelati siano gli interessati, cioè i soggetti di cui vengono trattati i dati.

In realtà, come si è visto in precedenza, il GDPR estende la sua tutela anche alle persone fisiche di cui non si trattano i dati.

L'esempio che segue spiega il concetto meglio di molte altre parole essendo un fatto realmente accaduto.

La violazione di un sito per incontri fra persone sposate ha portato alla successiva diffusione dei dati relativi agli iscritti al sito (gli interessati).

Tali soggetti hanno subito un danno (divorzio, suicidio…) in conseguenza della pubblicazione del loro nominativo, in quanto pubblicamente riconosciuti come infedeli.

Tuttavia, la diffusione di tali dati, non ha avuto impatti solo sugli interessati, ma ovviamente anche sui loro familiari (coniugi, figli) ed eventuali altri soggetti.

I familiari sono ovviamente delle persone fisiche che hanno subito un danno e come tali sono tutelati dal GDPR e possono, ad esempio, richiedere un risarcimento dei danni ai sensi dell'art. 82.

4 - L'analisi dei rischi dal punto di vista delle persone fisiche

4.1 – Le difficoltà nell'analisi del rischio nel GDPR

Per svolgere un'analisi del rischio sui diritti e libertà delle persone fisiche è necessario ricorrere a metodologie specifiche.

Le tradizionali metodologie di analisi del rischio hanno infatti come finalità una valutazione dei rischi per l'azienda, ad esempio in seguito a eventi che interessano asset aziendali (le informazioni sono ad esempio l'asset preso in considerazione della ISO 27001).

In questo caso la valutazione dei rischi riguarda soggetti terzi (le persone fisiche) e presenta alcune particolarità.

Si dà per acquisito cha la valutazione del rischio è una combinazione da un lato:

- della probabilità di accadimento di un evento avverso e della probabilità che tale evento abbia effettivamente delle conseguenze negative

e dall'altro:

- dall'impatto di tale evento, espresso secondo le metriche quali/quantitative definite dalla metodologia di analisi del rischio utilizzata.

Per la valutazione delle PROBABILITÀ di accadimento di un evento avverso solitamente si considerano i seguenti criteri:

- nel caso di azione volontaria
    - appetibilità del bene
    - vulnerabilità rispetto alle varie minacce
    - determinazione dell'attaccante
- nel caso di azione involontaria, come un evento naturale, dalle vulnerabilità intrinseche di un asset rispetto alle varie minacce.

Tuttavia, nel caso di diritti e libertà fondamentali delle persone fisiche, è molto probabile che queste non siano il reale obiettivo di un attacco, ma che siano solo indirettamente coinvolte nello stesso. Diventa quindi difficile valutare effettivamente una probabilità di accadimento per i diversi scenari di rischio.

Per quanto riguarda la valutazione dell'IMPATTO il Titolare non ha una reale visibilità di tutti i soggetti coinvolti (le persone fisiche) in quanto di norma la sua visibilità è limitata agli interessati di cui tratta i dati.

Risulta anche molto difficile dare un valore, ad esempio economico, ai possibili impatti sulle persone fisiche di un determinato evento.

Per tale motivo per svolgere tale analisi dei rischi è opportuno utilizzare metodologie specifiche.

4.2 – Metodologie e strumenti

Esistono alcune metodologie "ufficiali" per la valutazione del rischio GDPR (essenzialmente tutte si riferiscono solo ai rischi in ambito sicurezza ai sensi dell'art. 32).

Con il termine "ufficiale" si intende che tali metodologie sono emesse da DPA o da altri enti governativi.

Al riguardo ENISA[1] ha proposto una metodologia illustrata nelle pubblicazioni:

- **Handbook on Security of Personal Data Processing di ENISA**
- **Guidelines for SMEs on the security of personal data processing di ENISA**

Anche l'Autorità Garante italiana ha dato il proprio contributo sul tema ed è disponibile una breve presentazione che illustra i concetti sopra esposti:

https://www.garanteprivacy.it/garante/document?ID=8581408

Le altre metodologie disponibili sono quelle proposte dall'**AEPD** (Autorità Garante Spagnola) e dal **CNIL** (Autorità Garante Francese).

È tuttavia consigliabile utilizzare la metodologia di ENISA in quanto semplifica enormemente la valutazione delle probabilità, mentre la valutazione degli impatti è essenzialmente qualitativa e basata su solo 4 valori.

[1] https://www.enisa.europa.eu/

Nell'ambito del GDPR, come evidenziato in precedenza, è molto difficile effettuare una valutazione di natura quantitativa, motivo per cui una metodologia qualitativa è più che sufficiente.

Inoltre, la metodologia di ENISA presenta numerosi vantaggi:

- è relativamente semplice
- è pensata specificatamente per il GDPR; l'oggetto di tutela sono i diritti e le libertà delle persone fisiche
- il livello di granularità dell'analisi è quello della singola finalità di trattamento
- non necessità di mappature ulteriori rispetto a quanto il Titolare ha già fatto per la compilazione dei Registri delle attività di trattamento.

Inoltre, tale metodologia propone delle contromisure organizzate per livello di rischio.

Questo è un ulteriore vantaggio che dovrebbe orientare all'uso di tale metodologia.

Infatti, l'analisi del rischio è un'attività propedeutica alla definizione di idonee misure di sicurezza.

È evidente che il concetto di idoneità potrebbe essere molto aleatorio e la disponibilità di una metodologia ufficiale che sia in grado non soltanto di effettuare una valutazione del rischio, ma anche di proporre delle misure di sicurezza in funzione del livello di rischio agevola notevolmente chi deve rispettare la normativa.

4.3 – Il trattamento del rischio

Anche il trattamento del rischio nell'ambito del GDPR segue un iter diverso dal convenzionale.

Solitamente il trattamento del rischio comporta alcune possibili soluzioni, quali:

- la riduzione del rischio (contromisure)
  - riduzione dell'impatto
  - riduzione della probabilità
- l'eliminazione del rischio
- il trasferimento del rischio
  - assicurativo
  - non assicurativo
- l'accettazione del rischio.

La diversa modalità di gestione è determinata dal fatto che il rischio GDPR non è un rischio del Titolare, ma un rischio di soggetti terzi, le persone fisiche.

Quindi il Titolare non può accettare o trasferire il rischio, ma potrà solo ridurlo al minimo.

In effetti il Titolare deve seguire un percorso obbligato per gestire il rischio; nel caso in cui il rischio sia basso o comunque non elevato deve definire le misure di sicurezza idonee a ridurlo il più possibile.

Se invece il rischio è elevato deve effettuare una valutazione di impatto ai sensi dell'articolo 35 e definire idonee contromisure.

Nel caso in cui anche in presenza delle contromisure previste il rischio permanga elevato è necessario rivolgersi all'Autorità Garante o rinunciare al trattamento.

5 - L'analisi dei rischi dal punto di vista del Titolare e del Responsabile

La valutazione dei rischi dal punto di vista del Titolare e del Responsabile avviene da due ottiche:

- rischi primari direttamente collegabili al GDPR
- rischi secondari collegati indirettamente al GDPR.

5.1 - Rischi primari

Per la violazione dei seguenti articoli il GDPR prevede, in caso di responsabilità del Titolare o del Responsabile, risarcimenti e sanzioni pecuniarie:

Articolo 82 Diritto al risarcimento e responsabilità

1. *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.*
2. *Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.*

…

Articolo 83 Condizioni generali per infliggere sanzioni amministrative pecuniarie

…

2. Le sanzioni amministrative pecuniarie sono inflitte …

Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

b) il carattere doloso o colposo della violazione;

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

…

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR,

… :

a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;

Per ridurre la probabilità ed entità di tali rischi dovranno essere adottate tecniche che consentano di affrontare in modo sistematico e documentato al rispetto dei suddetti articoli, come quelle riportate nel nuovo standard ISO/IEC 27701 che è stato sviluppato a questo preciso scopo e costituisce un punto di riferimento ufficialmente riconosciuto.

5.2 - Rischi secondari

Si tratta di Rischi indotti come conseguenza di incidenti o di sanzioni che abbiano riguardato il trattamento, in senso lato, di dati personali.

Un'analisi del rischio relativa a tali possibili eventi dovrà, ad esempio, esaminare la probabilità e l'entità del danno potenziale subito per:

- **perdita di produttività**: interruzione, alterazione o limitazione nella produzione od erogazione di servizi a causa del blocco di un trattamento di dati personali
- **gestione di una violazione / incidente che coinvolga dati personali (data breach)**
  - costi di gestione dell'incidente
  - spese legali
  - costi di notifica agli interessati
- **danni reputazionali**
  - danni all'immagine
  - perdita di clientela
  - perdite in borsa.

Definire regole per una stima qualitativa o quantitativa di questo tipo di rischi è molto difficile ed essi, quindi, dovranno essere valutati caso per caso tenendo conto del tipo e dimensione dell'azienda in esame, del mercato in cui opera e di aspetti specifici difficilmente generalizzabili.

6 – Conclusioni

Sebbene il GDPR richieda espressamente l'esecuzione di analisi del rischio esclusivamente per la valutazione dei rischi dei diritti e libertà delle persone fisiche, nondimeno una valutazione dei rischi dal punto di vista del Titolare e dal Responsabile è non solo opportuna, ma anche auspicabile, in quanto solo in questo modo sarà possibile effettuare una corretta valutazione dei costi benefici derivanti dall'adozione di adeguate contromisure.

Il GDPR prevede infatti che il Titolare o il Responsabile adottino adeguate misure di sicurezza essenzialmente per la tutela dei diritti e libertà delle persone fisiche e non anche per la tutela del Titolare.

Considerando la difficoltà nell'esprimere una valutazione sui rischi delle persone fisiche la disponibilità di un'analisi dei rischi svolta anche dal punto di vista del Titolare o del Responsabile consente di avere delle stime che consentono una più facile valutazione dei costi/benefici legati all'uso di specifiche contromisure.