Gestione del rischio: quale processo adottare per la protezione dei dati personali

Author : Ivano Pattelli

Date : 4 Aprile 2019

La gestione del rischio ed il concetto di accountability sono due principi fondamentali del Regolamento (UE) 2016/679 (di seguito Regolamento) e fra le principali innovazioni da questi introdotte. Infatti, la gestione del rischio diventa lo strumento atto a dimostrare l'adeguatezza delle misure implementate a tutela dei dati trattati. Soprattutto per le aziende italiane, questa è una grande novità in termini di approccio, in quanto, abituate a leggi prescrittive predeterminate, hanno basato in passato la loro azione sulla rigorosa valutazione ed applicazione delle misure indicate, c.d. *checklist*, come, ad esempio, l'Allegato B (Misure Minime di Sicurezza) del Decreto Legislativo 30 Giugno 2003, n. 196. Il Regolamento, invece, non prescrive misure tecniche ed organizzative puntuali per proteggere i dati, ma chiede al titolare di essere in grado di dimostrare di averle protette in modo adeguato, rispetto ai rischi che presentano i trattamenti ed alla natura dei dati personali da proteggere.

Diventa a questo punto molto utile, se non indispensabile, al fine di dimostrare il rispetto del principio di accountability, seguire e documentare un percorso logico in grado di individuare e valutare il rischio inerente al trattamento e, quindi, ponderare e mettere in atto misure adeguate a limitare la portata di tale rischio sui diritti e le libertà degli interessati. Con tale valutazione, quindi, si determina il grado di responsabilità del titolare o del responsabile del trattamento nella gestione del rischio inerente al trattamento, attraverso la valutazione delle misure messe in atto per prevenire eventuali limitazioni dei diritti e libertà degli Interessati, per consentire a questi di mantenere un controllo sui dati che li riguardano, nonché per garantire un livello di protezione adeguato dei dati da minacce che possono pregiudicare la loro riservatezza, integrità e disponibilità ed essere la causa di un danno, materiale o immateriale, per le persone fisiche.

Definizione del rischio per la protezione dei dati

Il primo punto da chiarire per poter attuare un processo di gestione del rischio coerente e conforme ai requisiti del Regolamento, è la definizione stessa di rischio. Al riguardo, l'Autorità di Controllo nazionale (di seguito Garante), ai sensi dell'Art. 2-bis del Decreto Legislativo 30 Giugno 2003, n. 196 e *s.m.i.*, fornisce nella guida "La Valutazione di Impatto - Individuazione e

gestione del Rischio" una definizione del rischio, quale: *"scenario che descrive un evento e le sue conseguenze, stimati in termini di gravità e probabilità".*

A sua volta, il Considerando 83 del Regolamento precisa:

"[…] *Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati"*.

Tale definizione di rischi può essere assimilabile anche alla definizione di "eventi temuti" (in inglese *feared event*) fornita dalle Linee Guida "Privacy Impact Assessment (PIA)" del CNIL, oppure "privacy risk" come indicati dalla standard internazionale ISO/IEC 29134. In entrambi i casi, i rischi che può presentare il trattamento possono essere riassunti in: accesso illegittimo, modifica indesiderata e perdita dei dati.

L'evento e le relative conseguenze, comunque, sono esplicitamente riferiti dal Regolamento per l'interessato o la persona a cui i dati personali fanno riferimento. La valutazione del rischio deve, quindi, focalizzarsi sui risvolti in termini di possibile violazione della protezione dei dati che riguardano gli interessati, escludendo altri aspetti riferibili al titolare o al responsabile del trattamento.

Nell'ambito dell'applicazione del Regolamento, il rischio per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, sono da intendersi, quindi, come eventi che possono generare effetti negativi, o impatti, sugli Interessati, come un danno fisico, materiale o immateriale. Il Considerando 75 del Regolamento ci aiuta ad individuare le tipologie di rischi che possono derivare dal trattamento o dalla natura dei dati trattati, e che possono a loro volta essere classificati come:

- **Rischi per la sicurezza del trattamento e per i dati trattati**, in termini di riservatezza, integrità e disponibilità (di seguito RID), che possono comportare per gli Interessati, ad esempio, discriminazione, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, ecc. Dove la violazione delle dimensioni di sicurezza dei dati (RID) e degli strumenti utilizzati (ad esempio sistemi informatici o mezzi cartacei) possono essere la causa degli effetti negativi sugli interessati, è necessario identificare le minacce che potrebbero causare l'evento dannoso e portare ad accessi illegittimi, modifiche indesiderate e perdita dei dati (Allegato 2 - Linee Guida per la DPIA del Working Party article 29, n. wp248 rev1.0). Tali rischi possono essere ricondotti, pertanto, alla definizione più generale di "violazione dei dati personali", c.d. *data breach*, che, se non affrontata in modo adeguato e tempestivo, può provocare danni fisici, materiali o immateriali alle persone fisiche (Considerando 85).
- **Rischi che possono derivare da un trattamento non conforme ai principi generali del Regolamento e limitare i diritti e le libertà degli interessati,** come ad esempio:
    - un trattamento di dati effettuato per finalità diverse rispetto a quelle dichiarate e legittime (principio di "limitazioni delle finalità");
    - un trattamento dei dati effettuato in assenza di una base giuridica legittima,

come il consenso espresso dall’Interessato (principio di “liceità del trattamento”);
    - un trattamento di dati eccedente rispetto alle finalità perseguite (principio di “minimizzazione dei dati”);
    - un trattamento di dati non esatti o aggiornati (principio di “esattezza”);
    - una conservazione dei dati, o anche non cancellazione, per un periodo superiore a quello consentito per il conseguimento delle finalità legittime (principio di “limitazione della conservazione”).
- **Rischi che possono impedire agli Interessati l’esercizio dei loro diritti ed il controllo sui dati personali** che li riguardano, come ad esempio:
    - informazioni fornite agli Interessati non complete o chiare circa i termini del trattamento di dati personali che li riguardano (articoli 12, 13 e 14 del Regolamento)
    - Modalità e meccanismi non in grado di consentire l’accesso e la portabilità dei dati in base ad una richiesta effettuata dall’Interessato (articoli 15 e 20 del Regolamento);
    - Modalità e meccanismi non in grado di consentire la rettifica, la cancellazione, l’opposizione e la limitazione del trattamento da parte dell’Interessato (articoli da 16 a 19 e 21 del Regolamento);
    - Impossibilità per l’Interessato di esprimere la propria opinione o contestare 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 (articoli da 22 del Regolamento).

Requisiti normativi per la valutazione del rischio

Il principio di accountability rappresenta uno dei pilastri su cui si fonda l’impianto normativo del Regolamento e, anche se nella traduzione del termine anglosassone viene tradotto impropriamente in “responsabilità”, la sua traduzione più corretta, anche se poco pratica, potrebbe essere quella di “rendicontazione”. Infatti, l’articolo 24 del Regolamento dispone:

“*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, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*”.

Inoltre, se ciò è proporzionato rispetto alle attività di trattamento, le predette misure includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

L’accountability è oggi considerata come un approccio pratico al trattamento dei dati personali, avendo l’obiettivo di individuare le attività e sviluppare gli strumenti che possano consentire alle organizzazioni di valutare ed individuare le misure in grado di raggiungere la conformità al Regolamento e renderne conto alle Autorità di Controllo competenti. Fondamentale tra le tali attività da prevedere per rispondere al principio di accountability è, quindi, la gestione del rischio

per la protezione dei dati personali. Quest'ultimo è da intendersi come rischio che può generare impatti negativi sulle libertà e i diritti degli interessati (Considerando 75 e 77), che devono essere analizzati attraverso un apposito processo di valutazione (Articoli 32 e 35), tenuto conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative, anche di sicurezza, che il titolare ritiene di dover adottare per mitigarli. E' da sottolineare che il processo di valutazione del rischio può essere sviluppato in momenti differenti: prima di iniziare le operazioni di trattamento dei dati personali e all'atto del trattamento stesso, prevedendo un riesame e aggiornamento periodico tenuto conto dei possibili cambiamenti che possono avvenire in riferimento ai termini del trattamento (ad esempio, finalità, destinatari, trasferimenti dei dati, ecc.), alle responsabilità organizzative, all'introduzione di nuove tecnologie ed, in particolar modo, all'evoluzione delle minacce informatiche che possono incombere sulla protezione dei dati.

Il Regolamento richiede alle organizzazioni, in particolare, di effettuare una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato "inerente" per i diritti e le libertà delle persone fisiche, in relazione alla loro natura, ambito di applicazione, contesto e finalità. È utile però precisare che vi sono due tipologie di valutazione del rischio previste dal Regolamento, distinte e complementari.

La prima, denominata Data Protection Impact Assessment (DPIA), prevede ai sensi dell'articolo 35 una valutazione degli impatti per la protezione dei dati prima di procedere con un nuovo trattamento, quando questi possa presentare un rischio elevato intrinseco, come ad esempio:

- "*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.*
- *di sorveglianza di zone accessibili al pubblico su larga scala"*.

Il Working Party article 29 (di seguito WP29) prima con le Linee Guida per la DPIA, n. wp248 rev1.0, e successivamente il Garante con l'Allegato 1 al Provvedimento n. 467 dell'11 Ottobre 2018 [doc. web n. 905897], hanno indicato le tipologie di trattamenti che presentano un rischio elevato intrinseco e devono essere oggetto di una DPIA.

Per comprendere se i trattamenti effettuati dal titolare del trattamento presentino un rischio elevato intrinseco, è necessario che l'Organizzazione definisca una procedura che valuti la necessità di effettuare la DPIA nella fase di progettazione o, comunque, prima di procedere alla realizzazione di un nuovo servizio, processo o applicazione che comporti il trattamento di dati

personali. Comunque, vista la sua utilità per facilitare il processo decisionale relativo al trattamento, il WP29 suggerisce di valutarne l'impiego per tutti i trattamenti, e non solo nei casi in cui il Regolamento o l'Autorità di Controllo la prescrive come obbligatoria.

La DPIA è un onere posto direttamente a carico del titolare del trattamento e rappresenta uno strumento importante in termini di accountability, in quanto, è in grado di attestare l'adozione di misure adeguate a garantire il rispetto delle prescrizioni del Regolamento. Il suo obiettivo è quello di determinare, in particolare, l'origine, la natura, la particolarità e la gravità dei rischi sulla protezione dei dati personali per quei trattamenti che presentano intrinsecamente un rischio elevato per i diritti e le libertà delle persone fisiche, al fine di adottare tutte le opportune misure per dimostrare che il trattamento dei dati personali rispetta le disposizioni del Regolamento (Considerando 84). È da sottolineare che l'esecuzione della DPIA nella fase di progettazione di un nuovo trattamento rappresenta uno strumento efficace per rispondere anche ai principi di "*data protection by default and by design*" (articolo 25 del Regolamento), ossia alla necessità di configurare il trattamento prevedendo fin dall´inizio le garanzie indispensabili "in grado di soddisfare i requisiti" del Regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

La DPIA è forse uno degli argomenti più complessi del Regolamento e pone molti dubbi che la sola lettura dell'articolo 35 non riesce a dipanare. Infatti, il Regolamento non impone una metodologia o specifica le operazioni da effettuare per la valutazione del rischio per la protezione dei dati e indubbiamente le Linee Guida n. wp248 rev1.0 del WP29 hanno portato un importante contributo nel fare chiarezza e fornire indicazioni utili di lavoro. A tal riguardo, l'Allegato 2 - "Criteri per una DPIA adeguata" delle Linee Guida n. wp248 rev1.0 del WP29 fornisco i criteri che i titolari possono utilizzare per valutare se il modello di DPIA utilizzato è sufficientemente completo per conformarsi alle prescrizioni del Regolamento, prevedendo:

1. una descrizione sistematica del trattamento (articolo 35, comma 7, lett. a)), al fine di individuare e determinare:
    - la natura, la portata, il contesto e le finalità del trattamento (Considerando 90);
    - i dati personali trattati e il loro periodo di conservazione;
    - i destinatari a cui possono essere comunicati i dati;
    - una descrizione funzionale del trattamento, che comprenda, ad esempio, il servizio o il processo per cui vengono raccolti ed elaborati i dati;
    - le risorse utilizzate per il trattamento dei dati personali (hardware, software, reti di comunicazione elettronica, persone, mezzi cartacei);
2. una valutazione di necessità e proporzionalità del trattamento (articolo 35, comma 7, lett. b)), tenuto conto delle:
    - misure che contribuiscono al rispetto dei principi generali del trattamento, la cui mancanza o inefficacia possono comportare un rischio per i diritti e delle libertà degli Interessati riguardo ai dati trattati che li riguardano:
        - determinazione e documentazione di finalità specifiche, esplicite e legittime (articolo 5, comma 1, lett. b));
        - determinazione e documentazione della/e condizioni di liceità del trattamento (articolo 6);

        - meccanismi e procedure per garantire l’adeguatezza, la pertinenza e limitazione dei dati a quanto necessario (articolo 5, comma 1, lett. c));
        - meccanismi e procedure per garantire la limitazione della durata di conservazione dei dati (articolo 5, comma 1, lett. e));
    - misure che contribuiscono all’esercizio dei diritti delle persone interessate, la cui mancanza o inefficacia possono comportare un rischio per il controllo sui dati:
        - mezzi e completezza delle informazioni fornite alle persone interessate riguardo il trattamento di dati personali che li riguardano (articoli 12, 13 e 14);
        - meccanismi e procedure per garantire l’accesso e la portabilità dei dati (articoli 15 e 20);
        - meccanismi e procedure per garantire la rettifica e la cancellazione dei dati, oppure l’opposizione e limitazione del trattamento (articolo da 16 a 19 e 21);
        - completezza delle informazioni fornite sui destinatari a cui possono essere comunicati i dati;
        - informazioni fornite sui responsabili, che eseguono per conto del titolare operazioni di trattamento di dati personali, ad esempio, nell’ambito di contratti di fornitura (articolo 28);
        - misure di tutela adottate in caso di trasferimento dei dati a soggetti stabili al di fuori dell’Unione Europea (Capitolo V).

3. una gestione dei rischi per i diritti e le libertà delle persone (articolo 35, comma 7 lett. c), che possono derivare da un accesso illegittimo, modifica indesiderata e perdita dei dati e causare un danno fisico, materiale o immateriale, agli interessati, attraverso:
    - l’analisi dell’origine, della natura, della probabilità e gravità dei rischi per la protezione dei dati (Considerando 84), tenendo conto di:
        - fonti o origine di rischio (considerando 90);
        - minacce che potrebbero portare all’accesso illegittimo, alla modifica indesiderata e alla perdita dei dati;
        - impatti, o danni, potenziali per i diritti e le libertà delle persone in caso di accesso illegittimo, modifica indesiderata e perdita dei dati;
        - probabilità e la gravità di ciascun rischio individuato (Considerando 90);
        - misure previste per il trattamento di tali rischi (articolo 35 comma 7, lett. d), e il considerando 90).

Quest’ultimo punto rappresenta la seconda tipologia di valutazione del rischio, riconducibile principalmente all’articolo 32 del Regolamento, che ha lo scopo di valutare il livello di sicurezza del trattamento e dei dati trattati, in funzione dei rischi che possono derivare, in particolar modo, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati (articolo 32, comma 2 del Regolamento). Questa seconda analisi è parte complementare della DPIA, ma è dovuta in generale per tutti i trattamenti effettuati sia dal titolare che dal responsabile del trattamento. Si tratta di uno dei criteri principali previsti dal Regolamento, che prevede appunto l'obbligo di effettuare una valutazione del rischio del trattamento, al fine di adottare le misure di sicurezza tecniche od organizzative “adeguate” a garantire un livello di

sicurezza adeguato al rischio a cui può essere esposto il trattamento e i dati personali trattati.

Partendo dalle indicazioni fornite dalle Linee Guida n. wp248 rev1.0 del WP29, è possibile strutturare il processo generale di valutazione del rischio di sicurezza come segue:

1. Identificare le fonti di rischio
    - Chi e cosa potrebbe essere la causa degli eventi che potrebbero creare un danno ai dati personali?

Esempio:

- Amministratori di Sistema
- Utenti o esterni all'organizzazione
- Attacchi informatici
- Virus e Malware
- Competitor
- Eventi climatici
- Acqua, fuoco ed esplosioni

2. Identificare le potenziali minacce
    - Quali possono essere le minacce agli strumenti informatici e non (ad esempio, applicazioni, hardware, networking, hard disk esterni, archivi cartacei, ecc.) utilizzati per il trattamento e che possono avere conseguenze per la protezione dei dati personali da questi elaborati o archiviati?

Esempio:

- Errori utente: utilizzo in modo inappropriato degli asset, mancato rispetto delle politiche e procedure di sicurezza
- Denial of service: Attacchi di rete di tipo DDoS, attacchi di tipo SQL injection, saturazione della capacità elaborativa delle componenti del sistema informativo.
- Abuso di privilegi: escalation illecita dei privilegi di accesso ai programmi informatici per la lettura e modifica illecita dei dati, accesso a programmi di posta elettronica per l'invio di posta indesiderata o non autorizzato.
- Malware: perdita di riservatezza o disponibilità dei dati in seguito all'installazione accidentale di codice malevolo, virus e software vulnerabile.
- Furto: furto di dispositivi in cui sono archiviati, come computer portatili, smartphone, unità di memorizzazione elettronica.
- Spionaggio: analisi del traffico di rete, acquisizione di dati attraverso strumenti di geolocalizzazione di hardware.
- Sovraccarico: attacchi DDOS o overload dei supporti di memorizzazione

3. Individuare i potenziali effetti sui diritti e le libertà delle persone interessate:
    - Quali conseguenze per i dati personali degli Interessati nel caso che una o più minacce si concretizzino?

Esempio:

- Accesso non autorizzato ai dati personali: discriminazione, problemi di natura psicologica, ricezione di comunicazioni indesiderate.
- Modifica indesiderata dei dati: negazione dell'accesso a servizi, pagamenti imprevisti, perdita di tempo per la ripetizione di formalità.
- Indisponibilità temporanea o definitiva dei dati: perdita finanziaria, mancanza di cure adeguate, perdita di opportunità uniche e non ricorrenti.

4. Valutare alla probabilità e la gravità dei rischi:
    - Quali possibilità esistono che una minaccia possa concretizzarsi ed eventualmente che livello di danno può produrre sugli strumenti utilizzati (informatici e cartacei) e, quindi, sui dati personali trattati?
        - Probabilità: stima della possibilità di accadimento di una minaccia rispetto agli strumenti utilizzati per il trattamento.
        - Gravità: stima del livello di compromissione, o anche di danno, che una minaccia può causare sugli strumenti utilizzati e sui dati stessi.

5. Identificare ed implementare le misure di sicurezza:
    - quali misure di sicurezza è necessario adottare per proteggere gli strumenti utilizzati e i dati trattati, in modo da limitare la probabilità di accadimento e gli effettivi negativi che possono essere generati dal concretizzarsi di una o più minacce?

Esempio:

- Controllo degli accessi a sistemi e ai dati.
- Analisi degli eventi di sistema.
- Backup e Disaster Recovery.
- Crittografia, anonimizzazione e pseudonimizzazione.

In conclusione, la valutazione degli impatti (DPIA) e quella per la sicurezza del trattamento e protezione dei dati pare evidente siano differenti e complementari, dove, in caso contrario, avremmo avuto esplicite indicazioni della DPIA anche negli articoli 24, 25 e 32 del Regolamento. È da considerare che le normative e gli standard non sempre presentano una coerenza interna, in quanto, l’elaborazione del testo può essere il prodotto di più gruppi di lavoro o il frutto di compromessi, come l’aggiunta di alcuni passaggi in momenti diversi. Data la premessa, è ragionevole pensare che gli articoli relativi alla DPIA siano stati introdotti non considerando appieno le relazioni con gli articoli relativi alla sicurezza del trattamento e dei dati (articolo 32). Infatti, non è possibile immaginare di valutare gli impatti per la protezione dei dati in relazione al rischio elevato inerente al trattamento per i diritti e le libertà delle persone fisiche, senza effettuare una valutazione del rischio per la sicurezza del trattamento e dei dati da proteggere. Al contempo, non è possibile valutare soltanto il rischio per la sicurezza del trattamento, trascurando i rischi inerenti che possono derivare da un trattamento non conforme ai principi generali del Regolamento o che possono impedire l’esercizio dei diritti degli agli Interessati (vedi anche principio di “necessità e proporzionalità del trattamento” dell’Allegato 2

alle Linee Guida n. wp248 rev.1.0 del WP29). In questo caso, il Regolamento non richiede di effettuare una valutazione “necessità e proporzionalità” se il trattamento non presenti un rischio elevato o, comunque, non rappresenti un nuovo trattamento, ma è sottinteso che il titolare abbia adottato e sappia dimostrare l’adeguatezza delle misure necessarie perché il trattamento sia conforme ai principi generali (Capo II del Regolamento) e sia consentito l’esercizio dei diritti degli Interessati (Capo III del Regolamento).

Definizione del processo di gestione del rischio

I rischi per la protezione dei dati personali non possono essere decontestualizzati dal più ampio processo della "Gestione dei rischi aziendali", c.d. *Enterprise Risk Management* (ERM), in una visione aziendale generale che dovrebbe essere basata sul rischio. Il processo di gestione del rischio per la protezione dei dati personali, pertanto, dovrebbe anch’esso considerare preliminarmente il settore in cui opera l’organizzazione, i suoi particolari obiettivi di business, le principali attività svolte in termini di servizi e prodotti offerti, la sua struttura, i processi organizzativi adottati, i sistemi informatici utilizzati, le sedi, i relativi portatori d'interesse (utenti, dipendenti, clienti, pazienti, ecc.) e la diversità dei criteri di identificazione e valutazione del rischio. Tutti elementi che contribuiscono a rivelare e valutare la natura e la complessità dei rischi specifici connessi al trattamento dei dati personali.

Il processo di gestione del rischio per la protezione dei dati personali, essendo applicabile a tutti i settori economici, dovrebbe fa riferimento in generale alla norma di ISO 31000 che ha, tra i suoi scopi, anche quello di armonizzare i processi della gestione del rischio di una organizzazione alle norme attuali e future. Al riguardo, diverse norme, che definiscono i criteri e le linee guida per i sistemi di gestione aziendale basati sul rischio, fanno riferimento alla ISO 31000, al fine di determinare i criteri per lo sviluppo di un processo di gestione del rischio adeguato agli obiettivi dell’organizzazione.

La definizione generale che può essere fornita per il processo di gestione del rischio (o anche Risk Management) è relativa allo sviluppo di un processo complessivo di identificazione, analisi e ponderazione e trattamento del rischio, dove quest’ultimo rappresenta l’adozione delle misure necessarie a mitigare i rischi residui. In altre parole, la gestione del rischio è un insieme di attività volte ad identificare i rischi, calcolarne il livello di gravità, decidere se sono accettabili o da ridurre e, se del caso, agire in modo da prevenirne o limitarne gli effetti. Pertanto, il processo di valutazione del rischio risulta essere parte del processo generale di gestione del rischio, come rappresentato nella figura seguente:

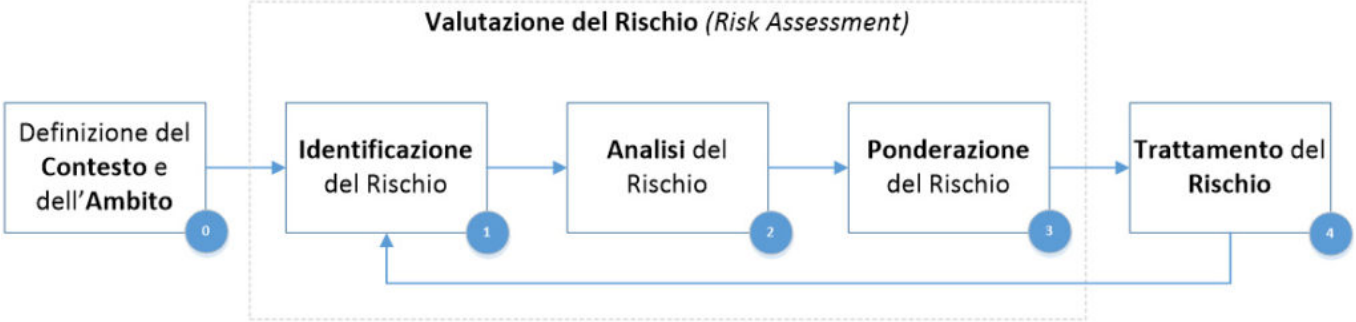

Figura 1: processo di Gestione del Rischio

Le fasi che costituiscono il processo possono essere descritte come segue:

1. **Identificazione del Rischio**: il processo di valutazione del rischio del trattamento deve prevedere una prima valutazione che stabilisca quali siano i rischi per i diritti e le libertà delle persone fisiche a cui l'organizzazione è potenzialmente esposta. L'obiettivo di tale fase è quello di generare un elenco completo dei rischi, basato sull'individuazione di quegli eventi che possono generare un accesso illegittimo, una modifica indesiderata o una perdita dei dati, coerenti con il contesto, con i termini del trattamento e gli strumenti utilizzati. L'identificazione globale è un'attività critica, poiché un rischio non identificato in questa fase non viene considerato nelle fasi successive. Oltre ad identificare i rischi per i diritti e le libertà degli Interessati, è necessario considerare gli effetti negativi che possono essere generati (valutazione degli impatti) come, ad esempio, un danno per la reputazione, discriminazione, furto d'identità, perdite finanziarie, danni fisici o psicologici, perdita di controllo dei dati, ecc. Al riguardo, l'Organizzazione dovrebbe applicare metodologie e strumenti per l'identificazione dei rischi adatti per la natura, l'ambito di applicazione, il contesto e le finalità del trattamento. Nella fase d'identificazione dei rischi è importante avere disponibili informazioni pertinenti ed aggiornate, come check-list e appropriate informazioni derivanti dal riesame dei dati storici (IEC 31010 par. 5.2 Risk identification). L'elemento principale in cui consiste il processo di identificazione dei rischi è la mappatura dei rischi al trattamento, anche se le metodologie di mappatura possono variare in base al contesto e ai principi generali applicati nella gestione dei rischi derivanti dal trattamento dei dati. L'identificazione dei rischi e la conseguente mappatura è preliminare alla fase successiva di analisi dei rischi del trattamento di dati personali e andrebbe effettuata su più livelli, tenendo conto che un rischio può incombere su uno o più trattamenti o su parti di esso.
2. **Analisi del rischio**: questa fase implica lo sviluppo di una conoscenza specifica degli stessi, fornisce i dati per effettuare la ponderazione dei rischi e per prendere decisioni sulla necessità di gestione o meno di ogni singolo rischio identificato, risultando oltremodo di supporto alle strategie ed ai metodi di trattamento dei rischi (par. 5.4.3 UNI ISO 31000). L'analisi del rischio richiede una valutazione sull'origine, la natura, la gravità per la protezione dei dati personali, la loro probabilità di accadimento e l'impatto sui diritti e le libertà degli interessati. Il rischio è analizzato mediante la determinazione della gravità per la protezione dei dati e la probabilità che tale rischio si concretizzi. L'analisi del rischio può essere intrapresa con vari livelli di dettaglio, in funzione del rischio, dello scopo dell'analisi e delle informazioni, dei dati e delle risorse disponibili, ma è importante che sia coerente con la metodologia e la relativa procedura definita dall'Organizzazione. L'elemento importante che deriva dal Considerando 76 del Regolamento è la differenziazione tra "rischio" e "rischio elevato", dove quest'ultimo dovesse presentare un rischio elevato per i diritti e le libertà delle persone fisiche, si dovrebbe applicare, prima di procedere, una valutazione dell'impatto per la protezione dei dati personali (DPIA). Come visto in precedenza, la DPIA deve valutare, oltre i rischi per la sicurezza del trattamento (ai sensi dell'art.32), la necessità e proporzionalità del

trattamento.

3. **Ponderazione del Rischio**: l’obiettivo di questa fase è di agevolare, sulla base degli esiti dell’analisi del rischio, i processi decisionali riguardo quali rischi necessitano un trattamento e le relative priorità di attuazione, considerando gli obiettivi dell’organizzazione ed il contesto in cui la stessa organizzazione opera, nonché l’equilibrio tra costi e benefici nel trattare i rischi stessi. La ponderazione del rischio implica il confronto tra il livello di rischio identificato durante il processo di analisi ed i criteri di rischio stabiliti per la rappresentazione della sua significatività (ad esempio, Alto, Medio, Basso). La necessità di trattamento, o anche di adottare misure tecniche ed organizzative adeguate a ridurre il livello di rischio determinato, può essere considerata sulla base di questo confronto. Con la ponderazione del rischio si perviene alla conclusione della fase di "Valutazione del rischio" producendo risultati tesi a massimizzare l'efficacia e l'efficienza delle misure di trattamento dei rischi assunti; ma si perviene, soprattutto, ad effettuare misurazioni nel continuo dei rischi, al fine di verificare l'emergere di rischi prima ritenuti poco significativi per l'organizzazione.
4. **Trattamento del Rischio**: Il trattamento del rischio implica la selezione di una o più opzioni per modificare il livello dei rischi individuati e l’attuazione di tali opzioni. Le opzioni di trattamento del rischio non sono necessariamente incompatibili tra loro o adatte a tutte le circostanze e possono comprendere:
   a) evitare il rischio decidendo di non avviare o continuare l’attività che comporta l’insorgere del rischio;
   b) assumere o aumentare il rischio al fine di perseguire una opportunità;
   c) rimuovere l'origine del rischio;
   d) modificare la probabilità;
   e) modificare la gravità per la protezione dei dati;
   f) condividere il rischio con altra parte o parti (ad esempio forme assicurative, contratti di fornitura, ecc.); e
   g) ritenere il rischio con una decisione informata.

La scelta dell’opzione di trattamento del rischio più appropriata implica l'individuazione delle misure tecniche ed organizzative adeguate a gestire il livello di rischio identificato, tenendo conto del bilanciamento dei costi e degli sforzi di attuazione a fronte dei benefici derivanti, dei requisiti cogenti e dei diritti e delle libertà degli Interessati. È da notare che il rispetto delle disposizioni del Regolamento dovrebbero imporre all’Organizzazione una propensione a ridurre sempre il livello di rischio identificato, adottando misure tecniche ed organizzative adeguate definite dal piano di trattamento.

Il piano di trattamento dovrebbe identificare chiaramente l’ordine di priorità in cui i singoli trattamenti del rischio dovrebbero essere attuati. Poiché, il trattamento stesso del rischio può introdurre rischi come, ad esempio, il fallimento o l’inefficacia delle misure di trattamento individuate, è necessario che il monitoraggio sia una parte integrante del piano in modo da assicurare che le misure siano e rimangano efficaci. Le informazioni fornite nei piani di trattamento dovrebbero comprendere:

- le motivazioni per la scelta delle opzioni di trattamento, compresi i benefici attesi;
- i soggetti che devono rendere conto dell’approvazione del piano e quelli responsabili

della loro attuazione;
- le misure tecniche ed organizzative proposte;
- le risorse necessarie per l'attuazione delle misure tecniche ed organizzative proposte;
- la tempistica e la programmazione.

I piani di trattamento dovrebbero essere integrati con il processo di gestione del trattamento e discussi con i responsabili delle strutture organizzative deputate all'attuazione della politica per la protezione dei dati personali.

Questa definizione generale del processo può essere applicata alla protezione dei dati personali, come anche all'analisi dei rischi strategici di un'organizzazione, di quelli finanziari, di quelli sulla sicurezza dei lavoratori, ecc.

Per poter sviluppare un processo coerente e adeguato, è possibile riferirsi ad alcuni standard e linee guida che utilizzano un approccio basato sul rischio per l'implementazione del relativo sistema di gestione aziendale (ad esempio, ISO 9001, ISO 27001, UNI/PdR 43.1:2018, ecc.), oppure che definiscono in particolare il processo di gestione del rischio per la protezione dei dati personali.

Il primo standard internazionale che è opportuno considerare è la ISO/IEC 29134, dal titolo "Guidelines for privacy impact assessment", che integra le norme della famiglia ISO per la gestione dei dati personali (ISO 29100, ISO 29151, ISO 27018) e specifica il processo e le linee guida per effettuare una privacy impact assessment (PIA), la cui denominazione è possibile considerarla sinonimo della DPIA del Regolamento. Lo standard non concentra la sua attenzione sui trattamenti, anche se sarebbe possibile interpretarlo in quest'ottica, ma sugli elementi, o asset, che concorrono all'elaborazione ed archiviazione dei dati (principalmente programmi, sistemi informatici, processi, ecc.). Di particolare interesse, oltre a definire i criteri per una gestione del rischio adeguata, risulta essere l'Allegato B, dove viene fornito un catalogo di minacce generiche per la protezione dei dati, tenendo conto della tipologia di asset a cui si applicano (hardware, software, reti di comunicazione elettronica, persone e documenti cartacei) e delle possibili azioni che possono essere condotte dalle minacce (ad esempio, attacchi informatici, virus e malware, errori utente, eventi climatici, ecc.). Il processo di valutazione del rischio presenta, quindi, un livello di dettaglio più ampio se riferito al trattamento di dati personali nel suo insieme, andando ad analizzare le vulnerabilità delle sue componenti che possono essere sfruttate dalle minacce. A titolo esemplificativo, possiamo riferirci alle vulnerabilità del software che possono essere sfruttate da hacker per portare i loro attacchi al sistema informativo dell'organizzazione; oppure, carenze da parte di quest'ultima per le attività di formazione e sensibilizzazione del personale riguardo la sicurezza dei sistemi informatici utilizzati, che possono causare un'involontaria installazione sui computer in dotazione di codice malevolo.

La ISO/IEC 29134 per diversi aspetti ricorda molto la metodologia e le linee guida pubblicate dal CNIL (*Commission nationale de l'informatique et des libertés*), l'Autorità di Controllo francese per la protezione dei dati personali. Creata nel 1978, il CNIL è un'autorità amministrativa indipendente che esercita le sue funzioni in conformità con il French Data Protection Act del 6 Gennaio 1978, modificata dalla legge del 20 giugno 2018 in accordo con le

disposizioni del Regolamento (UE) 2016/679. L'ordinamento nazionale francese prevedeva, già prima dell'entrata in vigore del Regolamento nel maggio del 2016, lo strumento della valutazione di impatto per la protezione dei dati, denominato anch'esso Privacy Impact Assessment (PIA). Nel corso degli anni ha sviluppato ed aggiornato la metodologia e gli strumenti per poterla effettuare conformemente al Regolamento, arrivando a pubblicare nel febbraio del 2018 l'ultima versione, recependo i criteri contenuti nell'Allegato 2 delle Linee Guida n. wp248 rev1.0 del WP29 e dichiarando la sua compatibilità con gli standard internazionali sulla gestione del rischio ([ISO 31000).

L'approccio sviluppato dal CNIL per l'esecuzione di una PIA conforme al Regolamento, riprende i punti evidenziati nell'Allegato 2 delle Linee Guida n. wp248 rev1.0 del WP29 e possono essere riassunti in:

1. definizione e descrizione del contesto del trattamento dei dati personali in esame;
2. analisi dei controlli che garantiscono il rispetto dei principi fondamentali del Regolamento: la proporzionalità e la necessità del trattamento (articolo 5) e la protezione dei diritti delle persone interessate (Capo III);
3. valutazione dei rischi per la privacy associati alla sicurezza dei dati e garantire che siano trattati correttamente;
4. documentazione ed accettazione formale della PIA.

Per quanto riguarda la valutazione dei rischi di sicurezza dei dati, riprende quanto già indicato nella ISO 29134, fornendo la definizione di rischio come: "*uno scenario ipotetico che descrive un evento temuto e tutte le minacce che permetterebbero che ciò accadesse*", indicando più specificamente:

- le fonti di rischio (ad esempio, un dipendente corrotto da un concorrente)
- le vulnerabilità delle risorse di supporto che potrebbero essere sfruttate (ad esempio, il sistema di gestione dei file che consente la manipolazione dei dati)
- il contesto di minacce (ad esempio, un uso improprio di e-mail)
- gli eventi temuti che potrebbero verificarsi (ad es. un accesso illegittimo ai dati personali)
- la natura dei dati personali soggetti al rischio (ad esempio: file cliente)
- gli impatti sulla privacy degli interessati (ad esempio, sollecitazioni indesiderate, sentimenti di violazione della privacy, problemi personali o professionali).

Al documento che descrive la metodologia, il CNIL ha accompagnato anche un modello "tipo" di PIA e, soprattutto, un documento (denominato Knowledge base) che descrive in dettaglio gli elementi e i criteri del processo PIA da considerare. Per comprendere al meglio il processo di valutazione dei rischi per la sicurezza dei dati, risulta molto utile l'elenco degli esempi di minacce che possono incombere sulle categorie di asset che concorrono ai trattamenti, suddivisi per le possibili conseguenze che potrebbero ricadere sulla loro protezione (accesso illegittimo, modifiche indesiderate e perdita). Pur considerando punto centrale il trattamento per valutare tramite la PIA la conformità alla disposizione del Regolamento, il CNIL non prescinde dalla valutazione del rischio per i diritti e le libertà degli Interessati dall'analisi degli asset utilizzati per il trattamento (hardware, software, reti, persone, mezzi cartacei) e delle potenziali minacce a cui possono essere esposti, come già visto nella ISO29134.

Il CNIL ha, inoltro, pubblicato un software per la conduzione di una PIA, che rappresenta in realtà un modello di documento che indica quali argomenti trattare in ciascun capitolo del rapporto di PIA, seguendo la metodologia e le linee guida di cui sopra.

Un'altra metodologia interessante per la gestione del rischio è quella pubblicata dall'ENISA (Agenzia europea per la sicurezza delle reti e delle informazioni), per aiutare le PMI ad effettuare la valutazione dei rischi per la sicurezza dei trattamenti ed adottare conseguentemente le contromisure necessarie per la protezione dei dati personali. Su questa base e come parte del suo continuo supporto sull'implementazione delle politiche di sicurezza della UE, ENISA ha pubblicato nel 2016 una serie di linee guida per le PMI che agiscono come Titolare o come Responsabile del trattamento. Nel corso del 2017 l'Agenzia ha continuato la sua attività e si è concentrata sulla fornitura di ulteriori indicazioni circa l'applicazione delle sopradescritte linee guida, attraverso lo sviluppo di casi di utilizzo specifici e criteri interpretativi, in stretta collaborazione con gli esperti delle autorità nazionali per la protezione dei dati, rendendo tali linee guida utili in tutti i casi in cui è prevista la valutazione del rischio ai sensi del Regolamento (vedi DPIA e sicurezza del trattamento). E' da sottolineare che la norma UNI/PdR 43.1:2018 ritiene la pubblicazione dell'ENISA una *best practice* di mercato riconosciuta ed affidabile anche per organizzazioni diverse dal settore PMI, in grado di assicurare l'esaustività delle misure di sicurezza da valutare ed adottare nel processo di gestione del rischio, rendendo disponibile un elenco di controlli divisi in funzione del livello di rischio a cui è esposto il trattamento e sulla base dei controlli di sicurezza previsti dalle norme internazionali ISO/IEC 27001 e ISO/IEC 27002.

Il documento non nomina quasi mai la PIA, ma presenta un metodo molto semplice e pragmatico per la valutazione del rischio dei trattamenti, mantenendo il punto di vista del trattamento piuttosto degli asset che vengono utilizzati per l'elaborazione ed archiviazione dei dati, come già visto nella ISO 29134 e nelle Linee Guida del CNIL.

La pubblicazione dell'ENISA, in particolare, si fonda su un processo semplificato di valutazione del rischio, suddiviso in 4 fasi:

1. **Definizione dell'operazione di trattamento e del relativo contesto**: questa fase è da considerarsi come il punto di partenza della valutazione del rischio e risulta fondamentale per definire i termini del trattamento dei dati oggetto di valutazione (ad esempio, finalità perseguite, natura dei dati trattati, strumenti utilizzati, destinatari dei dati, ecc.).
2. **Comprensione e valutazione dell'impatto per i diritti e le libertà degli interessati**: questa fase ha l'obiettivo di valutare l'impatto sui diritti e sulle libertà degli Interessati, derivanti dall'eventuale perdita di sicurezza dei dati, utilizzando metodologie qualitative e una scala di valori (Basso/Medio/Alto/Molto Alto). Per supportare la fase di valutazione, vengono proposte una serie di domande volte ad identificare il livello di impatto in termini di perdita di riservatezza, integrità e disponibilità dei dati, come ad esempio:
   a) Quale potrebbe essere l'impatto per l'Interessato in caso di divulgazione non autorizzata (perdita di riservatezza) dei dati che lo riguardano?
   b) Quale potrebbe essere l'impatto per l'Interessato in caso di un'alterazione non

autorizzata (perdita di integrità) dei dati che lo riguardano?
c) Quale potrebbe essere l'impatto per l'Interessato in caso di distruzione o perdita non autorizzata (perdita di disponibilità) dei dati che lo riguardano?

Per ciascun valore considerato valore di impatto considerato (Basso/Medio/Alto/Molto Alto), vengono forniti degli esempi di danni materiali o immateriali in cui le persone fisiche possono incorrere, in modo da agevolare la selezione del livello di rischio inerente al trattamento, avendo il punto di vista degli Interessati.

3. **Definizione delle possibili minacce e la valutazione della loro probabilità**: questa fase ha lo scopo di comprendere le minacce correlate al contesto complessivo del trattamento dei dati personali (esterno o interno) e valutare la loro probabilità (probabilità di accadimento della minaccia). Per semplificare il processo, è stato realizzato un questionario di 20 domande, suddiviso in 4 aree rilevanti, che mira a sensibilizzare l'organizzazione sugli elementi del trattamento e su quei fattori che possono consentire alle minacce di violare la sicurezza dei dati personali. In tale prospettiva, le domande sono relative a quattro diverse aree di valutazione che interessano gli ambienti di elaborazione e trattamento dei dati, vale a dire:
   a) Risorse di rete e tecniche (hardware e software);
   b) Processi/procedure relativi all'operazione di trattamento dei dati;
   c) Parti/persone coinvolte nel trattamento di dati personali;
   d) Settore di operatività e scala del trattamento.

Ciascuna domanda rappresenta una minaccia inerente del trattamento a cui viene richiesto all'Organizzazione di valutare il livello probabilità di occorrenza, utilizzando una scala di valori (Basso/Medio/Alto).

4. **Valutazione del rischio, combinando la probabilità di accadimento della minaccia e il relativo impatto**: questa fase ha l'obiettivo di effettuare la valutazione finale del rischio, dopo aver valutato l'impatto dell'operazione di trattamento dei dati personali e la probabilità di accadimento della minaccia rilavante, utilizzando una griglia di valori 3x3, al fine di ottenere la stima del livello di rischio in una scala Basso/Medio/Alto.

Al termine della valutazione, l'Organizzazione è in grado di procedere con la selezione delle misure di sicurezza appropriate al livello di rischio calcolato per la protezione dei dati personali. Le misure sono, peraltro, perfettamente coerenti con quelle proposte dalla norma ISO 27001:2013 (norma cardine sulla sicurezza delle informazioni).

Conclusioni

In conclusione, alle norme e linee guida sopra citate, è possibile aggiungere numerosi altri documenti pubblicati per fornire un aiuto nelle realizzazione di un processo di gestione del rischio per la protezione dei dati, ma ciascuna della metodologia o del processo utilizzato dall'Organizzazione dovrà prevedere alcune fasi preliminari per dimostrare il rispetto del principio di accountability e altre fasi successive essenziali per gestire correttamente le risultanze, in modo da rendere l'intero processo adattabile e aggiornabile al mutare delle

condizioni e delle esigenze organizzative. A tal fine, è possibile riassumere le macro-fasi del processo di gestione del rischio nell'ambito dei trattamenti effettuati dall'Organizzazione:

1. Mappatura dei processi e dei servizi che sottintendono gli scopi per cui vengono trattati i dati personali, tenendo conto delle finalità perseguite, della natura dei dati, delle categorie di interessati, di eventuali destinatari o trasferimenti dati a un paese terzo, nonché degli strumenti, o asset, utilizzati per la loro raccolta ed elaborazione;
2. Esecuzione della DPIA, qualora il trattamento presenti un rischio elevato intrinseco per i diritti e le libertà degli interessati, ovvero ricada nelle fattispecie indicate, dall'articolo 35, comma 3 del Regolamento, dal Garante o dal WP29.
3. Valutazione del rischio per la sicurezza del trattamento e dei dati trattati, sia nel caso sia parte integrante della DPIA, sia per tutti i tutti i trattamenti in essere e che devo rispondere all'obbligo di cui all'articolo 32 del Regolamento;
4. Ponderazione del rischio valutato in funzione dei criteri di accettazione stabiliti dall'Organizzazione, in modo da individuare le opzioni di trattamento del rischio coerenti (evitare, modificare, condividere, ecc.) e le relative misure tecniche ed organizzative da adottare, che costituiscono i Piani di trattamento del rischio.
5. Richiesta di consultazione preventiva all'autorità di controllo, prima di procedere al trattamento, qualora la DPIA indichi che il trattamento presenta un rischio elevato in assenza di misure o di misure sufficientemente efficaci che l'Organizzazione può adottare per mitigare tale rischio.
6. Costituzione ed aggiornamento del Registro dei rischi per la protezione dei dati, al fine di mantenere un elenco aggiornato e periodicamente adattabile delle valutazioni effettuate, incluse le DPIA.

Il Regolamento, come precedentemente trattato, non specifica una metodologia specifica da seguire per effettuare la valutazione del rischio per i diritti e le libertà degli Interessati, salvo fornire alcune indicazioni nei Considerando 83 e 85, che chiariscono quanto disposto all'articolo 32 del Regolamento. Pertanto, anche se il processo complessivo di gestione del rischio che può adottare l'Organizzazione può essere diverso ed ispirato a standard e linee guida differenti, è utile far riferimento alla norma ISO 31000, in quanto, in grado di porre ogni organizzazione nelle condizioni di individuare, analizzare e gestire tutti i rischi incombenti nell'ambito della propria attività, attraverso un approccio strutturato.

Per quanto riguarda, invece, le modalità e le operazioni da seguire per la valutazione del rischio, è da registrare che le norme prese in esame propongono un livello di dettaglio differente, in funzione che l'oggetto dell'analisi sia il trattamento nel suo insieme, oppure siano considerati gli asset che lo costituiscono. Pertanto, il livello di dettaglio prodotto dalla valutazione del rischio sarà sicuramente diverso in funzione che l'oggetto sia il trattamento, piuttosto che gli asset che lo costituiscono. Per definire e realizzare un corretto processo di valutazione del rischio è necessario avere chiare gli obiettivi e la disponibilità delle informazioni necessarie, in modo da individuare i metodi più adeguati.

Al riguardo, è possibile utilizzare la piramide di Robert Anthony per comprendere quale approccio adottare per il processo di valutazione del rischio, in funzione degli obiettivi gestionali o operativi di diversa lunghezza temporale che si vuole. Rappresenta, in particolare, un modello

gerarchico di comportamento organizzativo, articolato su tre livelli di decrescente importanza e che può essere mutuato, pertanto, anche per definire l'approccio del processo di valutazione del rischio:

1. **A livello strategico** sono richiesti dati stimati e approssimati, utili per dare indirizzi con prospettive a lungo termine (qualche anno) e per individuare i rischi principali, in modo da definire un programma di implementazione di misure tecniche ed organizzative adeguato, che possono essere comuni anche a più trattamenti. Questo può essere il caso, ad esempio, di un'Organizzazione che deve predisporre il Registro dei trattamenti ed effettuare la valutazione del rischio *ex novo* per tutti i trattamenti censiti, richiedendo un approccio semplificato e rapido per rispondere nei tempi agli obbiettivi prefissati. Di conseguenza, la valutazione del rischio potrà avere come oggetto il trattamento, piuttosto, che i singoli asset che lo compongono, in modo da ottenere più velocemente informazioni utili su eventuali impatti che possono derivare dal trattamento sui diritti e le libertà degli Interessati e adottare, conseguentemente, le misure di sicurezza che possono conseguire efficaci risultati di protezione dei dati a lungo termine (ad esempio, pseudonimizzazione e cifratura dei dati personali, politiche di sicurezza, back up dei dati e dei sistemi, controllo degli accessi ai dati e ai sistemi, ecc.), definendo, al contempo, le basi per lo sviluppo di un sistema di gestione della protezione dei dati adeguato.
2. **A livello tattico** sono richiesti dati consuntivi, arrotondati e abbastanza tempestivi, utili per avere indicazioni sull'andamento delle attività operative e prendere decisioni con prospettive a medio termine (qualche mese). Questo tipo di approccio del processo di valutazione del rischio può essere indicato, ad esempio, successivamente alla prima ricognizione, soprattutto per ottenere un dettaglio maggiore dei rischi specifici di ciascun trattamento censito dall'Organizzazione. Tale approccio richiede, quindi, l'individuazione dell'origine, natura, gravità, probabilità ed impatto sui diritti e le libertà degli interessati, tenuto conto degli strumenti utilizzati (hardware, software, reti di comunicazione elettronica, persone, mezzi cartacei) e di un modello di controlli esaustivo per valutare le vulnerabilità del sistema di protezione dei dati ed adottare misure di sicurezza adeguate al rischio (ad esempio, ISO 27002, ISO 29151, ecc.). Tale approccio è particolarmente indicato per verificare periodicamente l'efficacia delle misure di sicurezza tecniche e organizzative adottate, anche in funzione dei possibili cambiamenti che possono avvenire in riferimento ai termini del trattamento, alle responsabilità organizzative, all'introduzione di nuove tecnologie e, in special modo, all'evoluzione delle minacce informatiche.
3. **A livello operativo** i dati devono essere esatti e in tempo reale, poiché servono ad effettuare e tenere sotto controllo le attività in corso. Il processo di valutazione del rischio in questo caso deve essere supportato da adeguati strumenti e risorse, in grado di individuare e contrastare le minacce per la protezione dei dati in tempo reale (ad esempio, Intrusion Prevention System) o di determinare tempestivamente se è avvenuta una violazione dei dati personali (ad esempio, SIEM), al fine di ottemperare agli obblighi di notifica previsti dal Regolamento.

Concludendo, qualsiasi metodologia utilizzata, punto di vista adottato o processo definito, la valutazione del rischio per la sicurezza del trattamento e dei dati trattati non può prescindere da considerare la sua "*origine, natura, gravità, probabilità e impatto sui diritti e le libertà degli*

interessati” (cfr. Garante per la protezione dei dati).

Articolo a cura di **Ivano Pattelli**