GDPR – General Data Protection Regulation

La direttiva GDPR e la sua attuazione nel Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile

19 Giugno 2018

Il Regolamento generale per la protezione dei dati personali n. 2016/679 e la sua attuazione

Prof. Ing. Fabio Garzia, PhD

Ingegneria della Sicurezza - DICMA, SAPIENZA – Università di Roma
Wessex Institute of Technology (Inghilterra)
European Academy of Sciences and Arts (Austria)

www.fabiogarzia.name

Il Regolamento Generale sulla Protezione dei Dati dell'Unione Europea (GDPR - General Data Protection Regulation), entrato in vigore il 25 maggio 2018 in tutti i Paesi dell'Unione Europea (e quindi anche in Italia) è un insieme di regole su come le organizzazioni debbano trattare i dati personali degli interessati.

Il GDPR definisce le responsabilità delle organizzazioni per garantire la privacy e la protezione dei dati personali, fornisce agli interessati determinati diritti e assegna poteri ai regolatori per chiedere dimostrazioni di responsabilità o persino per imporre sanzioni nei casi in cui un'organizzazione non rispetti i requisiti del GDPR.

In caso di infrazione, non conformità o non rispetto dei requisiti richiesti dal GDPR sono previste sanzioni fino a 20 milioni di euro o al 4% del fatturato.

Il Regolamento UE 2016/679 è applicabile direttamente in tutti i Paesi Membri dal 25 Maggio 2018.

Esso abroga la direttiva 95/46/CE che è stata recepita in Italia dal D.Lgs. 196/2003.

Esso è volto a:

1) fronteggiare le sfide che l'evoluzione tecnologica e lo sviluppo dell'economia digitale presentano nei confronti della protezione dei dati personali;

2) garantire la tutela dei Diritti delle persone fisiche in tutti I Paesi Membri;

3) garantire la libera circolazione dei dati personali all'interno della Comunità Europea.

La Privacy rappresenta un tema conosciuto da tempo. In realtà il nuovo GDPR amplia il «concetto» di dati personali, estendendo il campo d'azione sia nella gestione dei dati da parte delle organizzazioni a più livelli sia nel diritto alla privacy dei privati nel controllo delle informazioni personali, soprattutto in rete.

Trasparenza nel trattamento dei dati personali e diritto alla privacy che presuppongono anche un'attenta analisi dei rischi ed una serie di altre attività di tipo multidisciplinare integrato che possono generare un impatto importante sull'intera organizzazione.

Il GDPR contiene, dunque, i requisiti per la messa in opera di un vero e proprio sistema di gestione della protezione dei dati in senso ampio e completo.

Il Regolamento Generale per la Protezione dei Dati Personali si compone di 11 Capi suddivisi in 99 Articoli.

Nel Capo I si disciplinano le DISPOSIZIONI GENERALI in 4 Articoli:

1. Oggetto e finalità
2. Ambito di applicazione materiale
3. Ambito di applicazione territoriale
4. Definizioni

Nel Capo II si disciplinano i PRINCIPI in 11 Articoli:

5. Principi applicabili al Trattamento di dati personali
6. Liceità del Trattamento
7. Condizioni per il consenso
8. Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione
9. Trattamento di categorie particolari di dati personali
10. Trattamento dei dati personali relativi a condanne penali e reati
11. Trattamento che non richiede l'identificazione

Nel Capo III si disciplinano i DIRITTI DELL'INTERESSATO in 5 Sezioni e 12 Articoli:
Sezione 1 - Trasparenza e modalità
Sezione 2 - Informazione e accesso ai dati personali
Sezione 3 - Rettifica e cancellazione
Sezione 4 - Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche
Sezione 5 – Limitazioni

Nel Capo IV si disciplinano il Titolare del Trattamento e responsabile del trattamento in 5 Sezioni e 20 Articoli:
Sezione 1 – Obblighi generali
Sezione 2 – Sicurezza dei dati personali
Sezione 3 – Valutazione di impatto sulla protezione dei dati e consultazione preventiva
Sezione 4 – Responsabile della protezione dei dati
Sezione 5 – Codici di condotta e certificazione

Nel Capo V si disciplinano i Trasferimenti di dati verso paesi terzi o organizzazioni internazionali in 7 Articoli:

44. Principio generale per il trasferimento
45. Trasferimento sulla base di una decisione di adeguatezza
46. Trasferimento soggetto a garanzie adeguate
47. Norme vincolanti d'impresa
48. Trasferimento o comunicazione non autorizzati dal diritto dell'Unione
49. Deroghe in specifiche situazioni
50. Cooperazione internazionale per la protezione dei dati personali

Nel Capo VI si disciplinano le Autorità di controllo indipendenti in 2 Sezioni e 9 Articoli:

Sezione 1 – Indipendenza
Sezione 2 – Competenza, compiti e poteri

Nel Capo VII si disciplinano la Cooperazione e la Coerenza in 3 Sezioni e 26 Articoli:
Sezione 1 – Cooperazione
Sezione 2 – Coerenza
Sezione 3 – Comitato europeo per la protezione dei dati

Nel Capo VIII si disciplinano i Mezzi di ricorso, le responsabilità e le sanzioni in 8 Articoli:
77. Diritto di proporre reclamo all'autorità di controllo
78. Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo
79. Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del Trattamento o del responsabile del Trattamento
80. Rappresentanza degli interessati
81. Sospensione delle azioni
82. Diritto al risarcimento e responsabilità
83. Condizioni generali per infliggere sanzioni amministrative pecuniarie
84. Sanzioni

Nel Capo IX si disciplinano le Disposizioni relative a specifiche situazioni di Trattamento in 7 Articoli:

85. Trattamento e libertà d'espressione e di informazione
86. Trattamento e accesso del pubblico ai documenti ufficiali
87. Trattamento del numero di identificazione nazionale
88. Trattamento dei dati nell'ambito dei rapporti di lavoro
89. Garanzie e deroghe relative al Trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici
90. Obblighi di segretezza
91. Norme di protezione dei dati vigenti presso chiese e associazioni religiose

Nel Capo X si disciplinano gli Atti delegati e gli Atti di esecuzione in 2 Articoli:
92. Esercizio della delega
93. Procedura di comitato

Nel Capo XI si riportano le Disposizioni Finali in 6 Articoli:
94. Abrogazione della direttiva 95/46/CE
95. Rapporto con la direttiva 2002/58/CE
96. Rapporto con accordi precedentemente conclusi
97. Relazioni della Commissione
98. Riesame di altri atti legislativi dell'Unione in materia di protezione dei dati
99. Entrata in vigore e applicazione

Nuovi principi
Accountability, trasparenza, privacy by design, privacy by default, ecc.

Nuovi diritti
Diritto di accesso ai dati e rettifica dei medesimi, limitazione o opposizione al trattamento, diritto all'oblio, diritto dalla portabilità dei dati, diritto al risarcimento, ecc.

Nuove figure
Data Protection Officer (DPO), ecc.

L'ambito di applicazione materiale del GDPR è rappresentato dai trattamenti interamente o parzialmente automatizzati dei dati personali o dai trattamenti non automatizzati dei dati personali contenuti in un archivio o comunque destinati a figurarvi.

Restano esclusi:

1) i trattamenti effettuati da persone fisiche per lo svolgimento di attività a carattere esclusivamente personale o domestico;

2) i trattamenti effettuati dalle autorità competenti nel perseguimenti di reati.

L'ambito di applicazione territoriale del GDPR è rappresentato da:

1) trattamenti effettuati nell'ambito di uno stabilimento da parte di un Titolare o di un responsabile stabilito nel UE, a prescindere dal fatto che i trattamenti siano effettuati all'interno del UE;

2) trattamenti di dati personali di interessati che si trovano all'interno del UE da parte di un titolare o di un responsabile che non si trova all'interno del UE, se tali attività riguardano:

    a) offerta di beni o servizi a interessati che si trovano all'interno del UE;

    b) monitoraggio di comportamento di interessati che abbiano luogo all'interno del UE.

I punti chiave del GDPR sono rappresentati da:

1) trattamento lecito, equo e trasparente;

2) limitazione di scopo, dati e archiviazione;

3) diritti degli interessati;

4) consenso;

5) violazioni dei dati personali.

Trattamento lecito, equo e trasparente

Alle organizzazioni che trattano dati personali viene richiesto di trattare i dati personali in modo lecito (tutti i trattamenti devono essere basati su uno scopo legittimo), equo (le organizzazioni si assumono la responsabilità e non trattano i dati per scopi diversi da quelli legittimi) e trasparente (le organizzazioni devono informare gli interessati delle attività di trattamento dei loro dati personali).

Limitazione di scopo, dati e archiviazione

Ci si aspetta che le organizzazioni limitino il trattamento, raccolgano solo i dati necessari e non conservino i dati personali una volta completato lo scopo del trattamento. Ciò comporta il soddisfacimento dei seguenti requisiti:

1) vietare il trattamento di dati personali al di fuori degli scopi legittimi per i quali tali dati personali sono stati raccolti;

2) imporre che non vengano richiesti dati personali diversi da quelli necessari;

3) chiedere che i dati personali siano cancellati una volta raggiunto lo scopo legittimo per il quale sono stati raccolti.

I Diritti degli interessati

Agli interessati è stato dato il diritto di chiedere alle organizzazioni quali informazioni queste abbiano su di loro e cosa facciano con tali informazioni. Inoltre, l'interessato ha il diritto di chiederne la rettifica, opporsi al trattamento, presentare un reclamo o anche chiedere la cancellazione o il trasferimento dei propri dati personali.

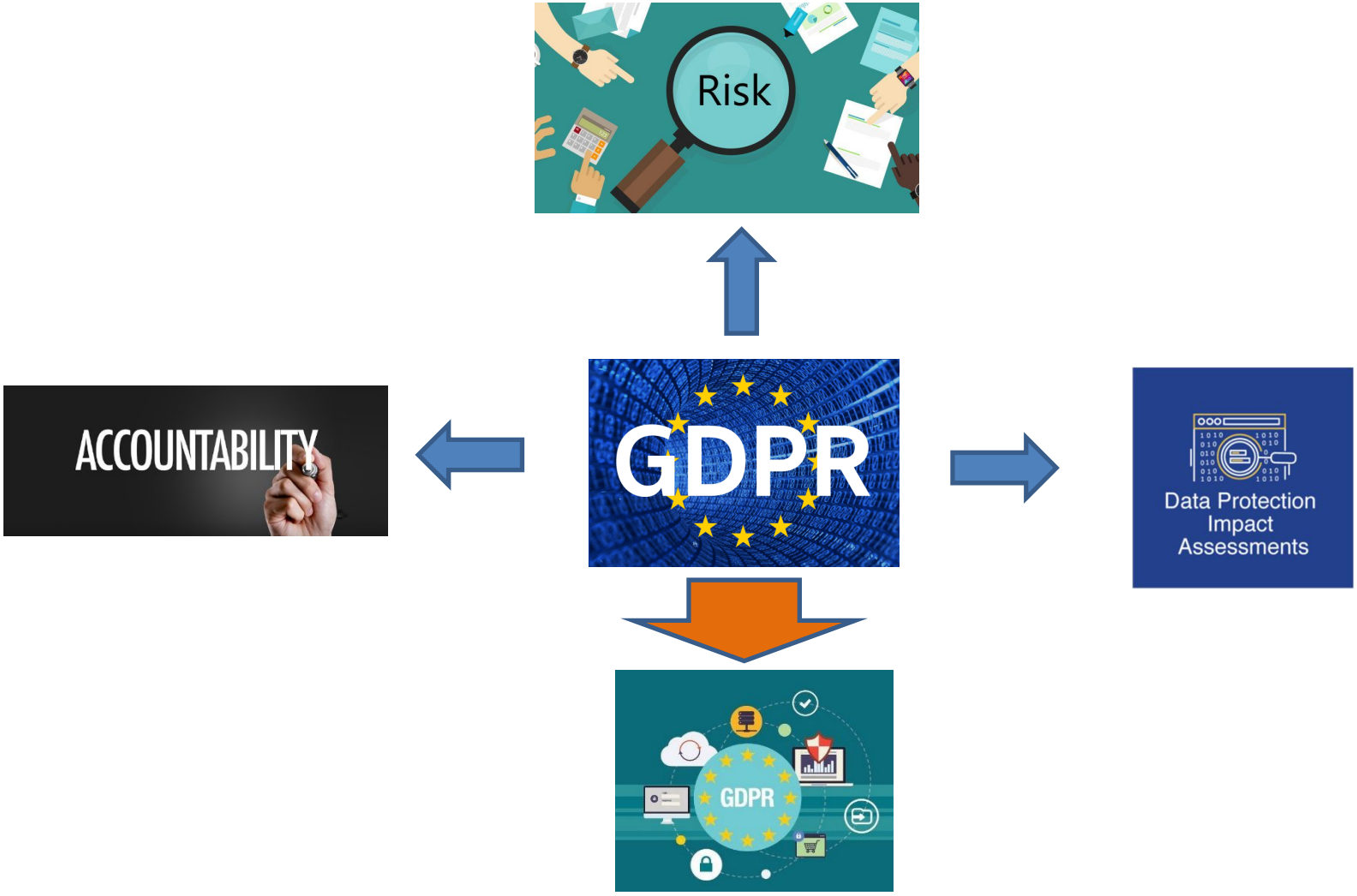
Il Consenso

Se e quando l'organizzazione intende trattare i dati personali oltre allo scopo legittimo per cui sono stati raccolti tali dati, è necessario che sia richiesto un consenso chiaro ed esplicito all'interessato. Una volta raccolto, questo consenso deve essere documentato e l'interessato è autorizzato a ritirare il proprio consenso in qualsiasi momento. Inoltre, per il trattamento dei dati dei minori, il GDPR richiede il consenso esplicito dei genitori (o tutori) se l'età del minore è inferiore ai 16 anni.

Violazioni dei dati personali

*L*e organizzazioni devono mantenere un Registro delle Violazioni dei Dati Personali e, in base alla gravità, il regolatore e l'interessato devono essere informati entro 72 ore dall'identificazione della violazione (data breach, che verrà illustrata più dettagliatamente nel seguito).

Gli elementi fondamentali del GDPR sono rappresentati da: accountability; valutazione di impatto e valutazione del rischio che comportano la creazione o la revisione del processo di gestione dei dati e delle informazioni.



Creazione o revisione del processo di gestione dei dati e delle informazioni.

Il GDPR prescrive la responsabilizzazione (accountability) di quello che viene denominato il Titolare del trattamento il quale viene obbligato a dimostrare la conformità (compliance) alle prescrizioni del GDPR attraverso:

1) misure tecnologiche, rappresentate da sicurezza fisica e logica dei dati e delle informazioni;

2) organizzative, rappresentate da politiche e procedure interne, formazione del personale, verifiche o audit, ecc.;

3) sistema documentale;

4) adesione a codici di condotta o sistemi di autenticazione;

5) ecc.

Il Titolare del trattamento (o data controller) che è colui che *«da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali»* e che decide quali categorie di dati personali devono essere registrate, o anche, *«la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza»*.

Il Titolare del trattamento non è, quindi, chi gestisce i dati, ma chi decide il motivo e le modalità del trattamento, ed è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa, sia nazionale che internazionale, in materia di protezione dei dati personali, compreso l'obbligo di notifica al Garante nei casi previsti.

Tra questi obblighi è importante ricordare che il titolare del trattamento deve porre in essere misure tecniche e organizzative adeguate per garantire, sin dalla fase della progettazione, la tutela dei diritti dell'interessato (privacy by design).

Nel settore privato il titolare del trattamento può essere una persona fisica oppure una persona giuridica. Nel settore pubblico in genere il titolare del trattamento è l'autorità, cioè una persona giuridica.

ACCOUNTABILITY: IL RESPONSABILE DEL TRATTAMENTO (DATA PROCESSOR)

Il Responsabile del trattamento (data processor) è *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che* tratta dati personali per conto del titolare del trattamento.

Si tratta di un soggetto, distinto dal Titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.

Il responsabile del trattamento dovrà avere innanzitutto una competenza qualificata (ad esempio, frequentazione di corsi di aggiornamento e, in tal senso, si può fare riferimento alle norme UNI 11697:2017), dovendo garantire una conoscenza specialistica della materia e l'attuazione delle misure tecniche e organizzative in grado di soddisfare i requisiti stabiliti dal Regolamento Europeo.

Inoltre dovrà garantire una particolare affidabilità, un requisito fondato su aspetti etici e deontologici (ad esempio, l'assenza di condanne penali).

Ovviamente dovrà disporre delle risorse tecniche adeguate per l'attuazione degli obblighi derivanti dal contratto di designazione e dalle norme in materia. Se è soggetto interno, le risorse saranno a carico del Titolare.

ACCOUNTABILITY: IL RESPONSABILE DEL TRATTAMENTO (DATA PROCESSOR)

Il responsabile ha obblighi di trasparenza. In tal senso occorre contrattualizzare il rapporto tra titolare e responsabile, specificando gli obblighi e i limiti del trattamento dati. Il responsabile riceverà, tramite l'atto giuridico (cioè per iscritto), tutte le istruzioni in merito ai trattamenti operati per conto del titolare, alle quali dovrà attenersi.

Inoltre, il responsabile del trattamento dovrà mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che gli impone l'articolo 28 del Regolamento e dovrà tenere il registro dei trattamenti svolti.

Il responsabile ha anche obblighi di garantire la sicurezza dei dati. Egli deve adottare tutte le misure di sicurezza adeguate al rischio (art. 32 regolamento), tra le quali anche le misure di attuazione dei principi di privacy by design e by default. Egli dovrà inoltre garantire la riservatezza dei dati, vincolando i dipendenti, dovrà informare il titolare delle violazioni avvenute e dovrà occuparsi della cancellazione dei dati alla fine del trattamento.

Sia il Titolare del trattamento che il responsabile, sono tenuti ad attuare le misure tecniche ed organizzative tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, 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.

Si tratta di specifici requisiti previsti dal GDPR che indica alcune misure di sicurezza utili per ridurre i rischi del trattamento, quali:

1) la pseudonimizzazione e la cifratura dei dati personali;

2) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;

3) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;

4) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Inoltre, il responsabile ha l'obbligo di avvisare, assistere e consigliare il Titolare. Dovrà, quindi, consentire e contribuire alle attività di revisione, comprese le ispezioni (o audit), realizzate dal Titolare del trattamento, dovrà avvisare il Titolare se ritiene che un'istruzione ricevuta viola qualche norma in materia, dovrà prestare assistenza al Titolare per l'evasione delle richieste degli interessati, dovrà avvisare il Titolare in caso di violazioni dei dati, e assisterlo nella conduzione di una valutazione di impatto (DPIA).

Il Responsabile della protezione dei dati (DPO o Data Protection Officer) rappresenta una persona fisica, una sorta di figura ibrida fra il ruolo di vigilanza dei processi interni alla struttura (del Titolare e del responsabile, che lo devono nominare, obbligatoriamente in taluni casi previsti per legge) ed il ruolo di consulenza.

Egli funge inoltre da “ponte di contatto” e *super partes* con l’Autorità Garante Nazionale.

La figura del DPO verrà illustrata più dettagliatamente nel seguito.

L’analisi dei rischi deve tener conto di:

1) eventuale distruzione accidentale o illegale, perdita, modifica, rivelazione o accesso non autorizzati a dati personali trasmessi, conservati o elaborati;

2) eventuali pregiudizi derivati;

3) danni fisici, materiali o immateriali;

4) valore del rischio.

Il rischio va valutato in base alla sussistenza, frequenza e gravità.

Diventa a questo punto molto utile, se non indispensabile, al fine di dimostrare *accountability* richiesta dal Regolamento (artt. 5, 24), seguire un percorso logico che dimostri come si sono protette le informazioni gestite e quali rischi corrono gli interessati che autorizzano a trattare i loro dati.

In tutte le organizzazioni dove il Sistema di gestione della sicurezza delle informazioni ha raggiunto un livello minimo di maturità, è presente un documento di analisi dei rischi che viene applicato a processi, applicazioni, classi di informazioni e/o altri asset.

Questi documenti elencano le minacce da cui l'organizzazione intende tutelarsi e come lo fa.

Per raggiungere questo scopo viene innanzitutto definito il *risk appetite*, vale a dire quanto l'organizzazione è disposta ad esporsi all'impatto del realizzarsi di una minaccia.

Definito il *risk appetite,* viene attribuito ad ogni rischio il suo grado di probabilità di verificarsi e quale è di conseguenza l'impatto che tale rischio avrebbe sull'organizzazione, in termini di riservatezza, integrità e disponibilità.

Verificate quali misure sono state adottate per proteggere l'asset oggetto di valutazione, il rischio viene riclassificato, per verificare se l'impatto residuo è accettabile, secondo quanto definito dal *risk appetite*.

Nel caso in cui l'impatto non sia accettabile, va pianificata una strategia tesa a mitigare il rischio, fino a renderlo accettabile.

Anche se l'approccio all'analisi del rischio sopra descritto è in linea con i più diffusi standard e *best practice* internazionali (es. ISO/IEC 27001:2013, ISO 31000:2009, etc.), il GDPR chiede di fare un passo in più che consiste nello svolgere l'analisi non nell'ottica del Titolare del trattamento, ma in quella dell'Interessato.

Innanzitutto è indispensabile creare il Registro dei trattamenti (art. 30). In questo documento si trova almeno l'elenco dei trattamenti svolti dal Titolare, i processi a cui afferiscono e gli asset coinvolti nel trattamento oltre a quanto prescritto dal comma 1 dell'art. 30.

A partire da queste informazioni è possibile integrare le analisi del rischio esistenti o crearne una ad-hoc per la *Data Protection*.

Integrandolo con le analisi del rischio precedentemente svolte, è possibile utilizzare per gli stessi asset, le stesse minacce, le stesse probabilità ed aggiungere quindi gli impatti specifici, quelli nell'ottica dell'interessato.

Integrare la documentazione esistente e progettare un sistema di gestione integrato rappresenta sempre il metodo più efficace ed efficiente per garantire la maggior accuratezza ed il minor onere di gestione, non solo in fase di realizzazione, ma soprattutto in fase di mantenimento.

Progettare in modo lungimirante il sistema di analisi del rischio privacy permette di tener conto di tutte le altre aree di applicazione del GDPR: i risultati dell'analisi del rischio diventano indispensabili come dati di ingresso per la Data Protection Impact Analysis, DPIA (art. 35) e per garantire la Privacy by Design (art. 25).

Diventa quindi chiaro il ruolo chiave rappresentato dalla valutazione del rischio in quanto essa può arrivare a richiedere eventuali consultazioni preventive al Garante (art. 36), influenzando la DPIA.

Particolarmente illuminante il contenuto dell'art. 25 che sottolinea che le misure a tutela del trattamento da attuare dipendono dal trattamento ma anche dalle caratteristiche del Titolare.

Una multinazionale probabilmente avrà una capacità di spesa che la metterà in grado di accedere a soluzioni di mercato (stato dell'arte) diverse da quelle di una PMI (Piccola-Media Impresa). Per questa ragione misure adottate da una PMI a tutela dei trattamenti potrebbero essere giudicate insufficienti per una multinazionale.

Un errore da evitare con attenzione è il considerare l'analisi dei rischi in oggetto una attività di esclusiva competenza dei Sistemi Informativi / Dipartimenti IT.

L'analisi del rischio, infatti, deve tener conto di tutti i processi ed asset coinvolti nel trattamento, anche quelli non informatici.

E' infatti necessario proteggere non solo i database elettronici (security logica) ma anche i faldoni ed i locali in cui essi sono conservati (security fisica).

La valutazione di impatto o DPIA (Data Protection Impact Assessment) è richiesta dal GDPR quando un trattamento può essere caratterizzato da un rischio elevato per i diritti e le libertà delle persone fisiche, in maniera specifica se esso prevede l'utilizzo di nuove tecnologie.

Essa rappresenta uno strumento per garantire il rispetto del principio di *accountability* in quanto va giustificata in maniera scritta e documentata la relativa non necessità.

Il GDPR individua, in particolare, 9 casi specifici in cui è necessario eseguire la valutazione di impatto o DPIA (Data Protection Impact Assessment).

Essi sono rappresentati da:
1) trattamento valutativi o di *scoring*, compresa la profilazione;
2) decisioni automatizzate che producono significativi effetti giuridici (assunzioni, concessioni di prestiti, stipula di assicurazioni, ecc.);
3) monitoraggio sistematico (videosorveglianza);
4) trattamento di dati sensibili, giudiziari o di natura estremamente personale (come, ad esempio, le opinioni politiche);
5) trattamento dati personali su larga scala;
6) trattamento di Big Data;
7) trattamento di dati di soggetti vulnerabili (anziani, minori, richiedenti asilo);
8) trattamento di dati con l'utilizzo di nuove tecnologie (riconoscimento biometrico, dispositivi IoT, ecc.);
9) trattamento che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (*screening* dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

È sufficiente che sussistano due delle nove condizioni per rendere obbligatoria la DPIA.

I punti chiave per gestire la violazione dei dati (data breach) secondo il GDPR sono rappresentati da:

1) privacy by design;

2) valutazione dell'impatto sulla protezione dei dati;

3) trattamento e/o trasferimenti di dati;

4) responsabile della protezione dei dati;

5) consapevolezza e formazione.

Privacy by design

Le organizzazioni devono incorporare meccanismi organizzativi e tecnici per proteggere i dati personali nella progettazione di nuovi sistemi e processi; cioè, gli aspetti relativi alla privacy e alla protezione dei dati devono essere garantiti per default. In ogni modo, si deve intervenire nei sistemi già esistenti per perseguire la finalità della protezione dei dati.

Valutazione dell'Impatto sulla Protezione dei Dati

Per valutare l'impatto della situazione esistente, di cambiamenti, di azioni nuove e di avvio di un nuovo progetto, è necessario condurre una Valutazione dell'Impatto sulla Protezione dei Dati. La Valutazione dell'Impatto sulla Protezione dei Dati è una procedura che deve essere sempre eseguita quando viene introdotta una modifica significativa nel trattamento dei dati personali. Questa modifica potrebbe essere rappresentata da un nuovo processo o una modifica a un processo esistente che altera il modo in cui i dati personali vengono trattati.

Trattamento e/o trasferimenti di dati

Il Titolare del trattamento o controllore (data controller) dei dati personali ha la responsabilità di garantire che i dati personali siano protetti e che i requisiti GDPR siano rispettati, anche se il trattamento viene eseguito da una terza parte. Ciò significa che i controllori hanno l'obbligo di garantire la protezione e la riservatezza dei dati personali anche quando tali dati vengono trasferiti all'esterno dell'organizzazione, a una terza parte e/o un'altra funzione all'interno della stessa organizzazione.

Responsabile della Protezione dei Dati

In caso di trattamento significativo di dati personali all'interno di un'organizzazione, l'organizzazione deve nominare un Responsabile della Protezione dei Dati (Data Protection Officer o DPO). Una volta nominato, il Responsabile della Protezione dei Dati ha la responsabilità di consultare l'organizzazione sulla conformità ai requisiti del GDPR del UE.

Consapevolezza e formazione: le organizzazioni devono creare consapevolezza tra i dipendenti sui principali requisiti del GDPR e condurre corsi di formazione regolari per garantire che i dipendenti rimangano consapevoli delle proprie responsabilità in merito alla protezione dei dati personali e all'identificazione delle violazioni dei dati personali nel più breve tempo possibile.

Il DPO deve:

1) informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

2) verificare l'attuazione e l'applicazione del Regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;

3) fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;

4) fungere da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;

5) fungere da punto di contatto per il Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa.

In sintesi, il DPO effettua sia un'attività interna alla struttura del preponente, sia un'attività esterna, in quanto punto di contatto fra la struttura e l'Autorità Garante.

Da un lato le sue competenze sembrerebbero molto ampie (effettuare una valutazione dei rischi; trovare soluzioni giuridiche al problema; conoscere sia il diritto nazionale sia quello comunitario; svolgere verifiche, coordinare i lavori in caso di incidenti/violazioni informatiche, etc.). Dall'altro, invece, non è ben chiara la definizione, anzi, il collocamento, del suo ruolo.

Ecco allora che, visti i dubbi e le incertezze capillarmente diffusi a livello europeo sulle caratteristiche ed i compiti del DPO, il Gruppo dei Garanti Europei (*WP 29*) ha emanato, lo scorso dicembre, delle Linee Guida in cui viene data un'interpretazione puntuale di quanto elencato negli articoli 37, 38 e 39 del GDPR: in particolare, chiariscono quali dovranno essere i requisiti soggettivi e oggettivi di questa nuova figura professionale.

Il Responsabile della protezione dei dati (DPO), nominato dal Titolare o dal responsabile del trattamento, deve:

1. possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;

2. adempiere alle sue funzioni in piena indipendenza ed in assenza di conflitti di interesse;

3. operare alle dipendenze del Titolare o del responsabile oppure sulla base di un contratto di servizio.

Il Titolare o il responsabile dovranno mettere a disposizione del DPO le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

In base al Regolamento, il DPO dovrebbe essere nominato quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico: il WP29 dà un'interpretazione estensiva di organismo pubblico e raccomanda, come una buona pratica, la nomina del DPO anche da parte delle organizzazioni private che svolgono funzioni pubbliche o che esercitano pubblici poteri.

La sua attività dovrebbe coprire tutte le operazioni di trattamento, comprese quelle che non sono legate alla esecuzione di un compito pubblico o esercizio del dovere ufficiale (ad esempio la gestione di un database dei dipendenti).

Ancora, la nomina dovrebbe essere obbligatoria quando le attività principali (*core business*) del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati.

Per «attività *core*» si intende un'operazione necessaria per raggiungere lo scopo, appunto, del Titolare o responsabile.

Infine, terzo ed ultimo punto di designazione obbligatoria del DPO: nel caso di trattamento, su larga scala, di speciali categorie di dati personali o di dati relativi a reati e condanne penali.

Il concetto di “larga scala” dev’essere valutato sulla base di alcuni specifici criteri quali, ad esempio, il numero di interessati coinvolti nel trattamento, la durata del trattamento e la sua estensione geografica.

Tra i trattamenti effettuati su larga scala, in particolare, rientrano:
1) la geo-localizzazione, per finalità statistiche, dei clienti di una certa attività, ad esempio catene di ristoranti;
2) il trattamento dei dati bancari dei propri clienti da parte di una compagnia assicurativa;
3) il trattamento, da parte di un motore di ricerca, dei dati personali degli utenti per l’invio di pubblicità mirata.

Tra i trattamenti non su larga scala, invece, sono ricompresi: il trattamento dei dati di un proprio paziente da parte del medico di famiglia ed il trattamento dei dati personali di natura penale da parte di un avvocato.

Il DPO, in sostanza, è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa in materia di protezione dei dati e può essere tanto un dipendente del Titolare del trattamento o del responsabile del trattamento quanto un libero professionista che opera in forza di un contratto di servizi.

Tuttavia, in merito a questo punto, il Regolamento sottolinea che i suoi compiti e le sue funzioni non devono dar adito a possibili conflitti di interessi.

L'assenza del conflitto di interessi è strettamente legata alla necessità di agire in modo indipendente: ciò comporta, in particolare, che il DPO non può mantenere una posizione all'interno dell'organizzazione che lo portino a determinare le finalità e gli strumenti del trattamento dei dati personali. Appare evidente, scrive il WP29, che, a causa della specifica struttura organizzativa in ogni realtà, questo deve essere considerato caso per caso.

Anche se l'art. 37 del Regolamento non specifica le qualità professionali che dovrebbero essere considerate quando si designa un DPO, è chiaro che, come affermato in precedenza, il responsabile della protezione dei dati dovrebbe avere esperienza sulla legislazione relativa alla protezione dei dati personali sia nazionale che europea. Per il WP29 risulta utile che le autorità di controllo promuovano una formazione adeguata e regolare per il DPO. Il riferimento per la formazione, in Italia, è rappresentato dalla norma UNI 11697:2017.

Indubbiamente è utile anche che il DPO abbia la conoscenza del settore di *business* delle imprese e dell'organizzazione del titolare e, nel caso di un ente pubblico, dovrebbe anche avere una buona conoscenza delle regole e delle procedure dell'organizzazione amministrativa.

INFORMATIVA

Deve essere concisa, trasparente (conservazione dei dati, nuovi diritti per gli interessati, ecc.) e facilmente accessibile.

Deve essere disponibile all'ottenimento dei dati personali e comunque entro 1 mese, possibilmente in formato elettronico.

I contenuti devono riportare:

1) i dati di contatto del Titolare;
2) i dati di contatto del DPO;
3) le finalità e la base giuridica del trattamento;
4) i legittimi interessi perseguiti;
5) gli eventuali destinatari dei dati personali;
6) gli eventuali trasferimenti a Paesi terzi.

CONSENSO

Deve essere:

1) libero;
2) esplicito;
3) espresso mediante dichiarazione o azione inequivocabile;
4) dimostrabile;
5) chiaramente distinguibile;
6) revocabile;
7) non condizionabile.

I minori di 16 anni devono avere il consenso dei genitori.

LEGITTIMO INTERESSE

Base giuridica del trattamento dei dati, anche senza consenso, purché siano bilanciati i diritti del titolare e i diritti dell'interessato. La relativa valutazione è a carico del Titolare.

REGISTRI DEL TRATTAMENTO

Sono obbligatori per organizzazioni o imprese con più di 250 dipendenti. Il Garante ne raccomanda comunque la dotazione a tutti i Titolari.

Le contromisure tecniche adeguate per la sicurezza del trattamento devono essere in grado di contrastare:

1) distruzione;

2) perdita;

3) modifica;

4) divulgazione non autorizzata;

5) accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

1) Per il contrasto di virus informatici di vario tipo: antivirus e antispam; email gateway; firewal specifici e/o avanzati;
2) per la sicurezza nel ripristino dei dati: adozione di specifiche politiche e procedure di backup (periodico su di un unico supporto; giornaliero + settimanale + mensile su supporti differenti, includendo eventualmente anche la delocalizzazione e il cloud);
3) per il contrasto di intrusioni non desiderate: firewall tradizionale, sistemi firewall con funzionalità avanzate e di controllo della navigazione sul web;
4) ecc.

Altre contromisure tecniche possono essere rappresentate da:

1) utilizzo di connessioni VPN (Virtual Private network) interno/esterno e viceversa;
2) utilizzo di una corretta politica e di corrette procedure di gestione delle password (complessità, frequenza di variazione, ecc.);
3) sistemi di autenticazione a due o tre fattori (autenticazione forte);
4) disattivazione immediata degli account non più utilizzati;
5) utilizzo di misure tecniche adeguate in funzione dei tempi di ripristino auspicati (disaster recovery, business continuity, ecc.)
6) ecc.

Le contromisure tecniche adeguate, che possono essere obbligatori o consigliate, sono rappresentate da:

1) formazione obbligatoria degli addetti al trattamento dei dati;

2) regolamentazione dell'utilizzo dei sistemi informatici/telematici;

3) adozione di procedure per la verifica dell'adeguatezza delle misure tecniche adottate;

4) adesione a codici di condotta o certificazioni specifiche (ad esempio ISO 27001, ecc.)

5) ecc.


Act
Plan
GDPR
Check
Do

IMPLEMENTAZIONE DEL GDPR MEDIANTE 9 PASSAGGI CHIAVE