NOVEMBER
2017

CPS GUIDE TO GDPR COMPLIANCE

By Gabriele Falasca - Raffaello Leti Messina

IL GDPR E L'IMPATTO PER AZIENDE E ISTITUZIONI

Il Regolamento UE 2016/679, integrante le direttive 2016/680 e 2016/681, in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, altrimenti noto come General Data Protection Regulation (in breve GDPR), indica principi e obblighi generali afferenti il tema del trattamento dei dati personali.

Prima di iniziare questa breve discussione sulla specifica disciplina e sulla sua portata sulle attività di aziende ed istituzioni, si ritiene utile introdurre le due definizioni giuridiche cardine della norma così come riportate nel regolamento stesso:

- Dato Personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

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

Rimandando al paragrafo successivo per una breve sintesi dei punti chiave del Regolamento e alla norma stessa per una più dettagliata trattazione degli stessi, il GDPR stabilisce che ciascun soggetto, azienda o organizzazione, interessato al trattamento di dati personali, quali anche semplicemente: nominativi, indirizzi, numeri telefonici e altri dati atti ad identificare e qualificare persone, dovendosi ovviamente includere in tale fattispecie le immagini e le copie di documenti in forme fisiche o digitali, è tenuto ad uniformarsi a nuovi e più stringenti obblighi a garanzia della riservatezza di tali dati a pena di pesanti conseguenze in termini di sanzioni civili e penali. Pertanto i soggetti interessati al trattamento di dati personali, in pratica la totalità delle aziende, che debbono almeno trattare i dati personali dei propri dipendenti, e la quasi totalità delle istituzioni, che normalmente trattano i dati dei propri utenti, dovranno, a partire dalla data prevista di applicazione del Regolamento fissata al 25 maggio 2018, aver adottato tutte le misure necessarie a minimizzare i rischi che potrebbero determinare ciò che è identificato dalla norma come limitazione o pregiudizio delle libertà e dei diritti dell'interessato.

NOVEMBER
2017

CPS GUIDE TO GDPR COMPLIANCE

By Gabriele Falasca - Raffaello Leti Messina

IN BREVE

La nuova normativa reca importanti novità e chiarimenti in merito alla natura dei dati interessati dalla stessa, definisce specifici obblighi organizzativi e procedurali atti a garantire il rispetto delle prescrizioni in essa contenute identificando altresì specifiche responsabilità in capo a nuove figure interne e/o esterne alle organizzazioni che realizzano i trattamenti oggetto del regolamento, introduce specifici obblighi di comunicazione verso l'Autorità di Controllo (Garante per la Protezione dei dati Personali).

ALCUNI PUNTI CHIAVE DELLA NORMATIVA

Di seguito vengono riportate alcune novità fondamentali rispetto al Decreto Legislativo n. 196/2003 denominato "Codice in materia di protezione dei dati personali" destinato ad essere superato dalla normativa di cui trattasi.

OGGETTO E FINALITA'

Oggetto e finalità del nuovo regolamento europeo, come si può evincere dall'articolo 1 dello stesso, sono rappresentati dalla protezione delle persone fisiche con riguardo al trattamento dei dati personali, corroborando i diritti dell'interessato ed introducendo, con l'ausilio di nuovi obblighi e doveri, il principio di responsabilizzazione a carico del Titolare del trattamento.
L'interessato al trattamento sì trova, così, ad essere protagonista di un progetto ambizioso che mira a garantire, la massima circolazione dei dati personali di un soggetto unitamente al più alto grado di sicurezza raggiungibile.

DIRITTO ALL'OBLIO

Il diritto all'oblio inteso come particolare forma di garanzia, prevede la non diffusione, senza particolari motivi, di precedenti pregiudizievoli dell'onorabilità della persona e rappresenta la maggiore novità in ambito privacy trovando la sua prima regolamentazione nell'articolo 17 del Regolamento UE 2016/679.
L'origine del diritto all'oblio può essere ricondotto alla sentenza Google Spain del 13 maggio 2014 nella quale venne accolto il ricorso di un cittadino spagnolo che chiedeva la cancellazione e la deindicizzazione delle pagine web che lo riguardavano a discapito del famoso motore di ricerca.
L'odierno articolo 17 definisce il diritto all'oblio come "il diritto che ha l'interessato di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo". Tale diritto viene meno solamente quando la diffusione o conservazione di determinate informazioni sia necessaria per l'esercizio del diritto alla libertà di espressione e di informazione, per l'adempimento di un obbligo legale cui è soggetto il Titolare del trattamento, per motivi di interesse pubblico nel settore della sanità o per motivi di archiviazione nel pubblico interesse, di ricerca scientifica o storica o per fini statistici.

DIRITTO ALLA PORTABILITA' DEL DATO

Il diritto alla portabilità del dato è un diritto innovativo regolamentato dall'articolo 20 del Regolamento UE 2016/679 che consente all'interessato di ricevere i dati personali forniti a un Titolare del trattamento in un formato strutturato, di uso comune e leggibile da dispositivo automatico e di trasmetterli ad un altro Titolare del trattamento senza impedimenti. Tale diritto oltre a facilitare il passaggio di dati da un fornitore di servizi all'altro, offrirà la possibilità di "riequilibrare" i rapporti tra l'interessato al trattamento e il Titolare del trattamento rafforzando il diritto di controllo dei propri dati personali. Affinché i dati possano essere "portabili" dovranno essere: riferibili in modo chiaro

all'interessato e trattati sulla base del consenso preventivo utilizzando metodi automatizzati. Tale diritto non si applica ai così detti diritti inferenziali e ai diritti derivati.
L'esercizio di tali diritti non pregiudica minimamente il diritto di continuare a fruire del servizio e di esercitare il diritto di cancellazione.

PRIVACY BY DESIGN

Il concetto di *privacy by design* risale al 2010, già presente negli Usa e Canada venne poi adottato nel corso della 32ma Conferenza mondiale dei Garanti privacy. L'art. 25 del nuovo regolamento impone al Titolare del trattamento l'utilizzo di misure tecniche e organizzative adeguate, al fine di tutelare i dati da trattamenti illeciti.
L'obbligo di *privacy by design* prevede, quindi, che qualsiasi progetto che implichi il trattamento di dati sia strutturato considerando, sin dalla progettazione, la riservatezza e la protezione degli stessi. Tale obbligo, inoltre, si basa sulla valutazione di rischio con il quale si determina la misura di responsabilità del Titolare e/o del Responsabile del trattamento.

PRIVACY BY DEFAULT

Lo stesso articolo 25 regola il concetto di *privacy by default*. Adeguarsi a tale concetto significa che ogni volta che un soggetto cede dati personali ad un terzo deve, a monte, esistere una procedura interna che preveda e disciplini le modalità di acquisizione, trattamento, protezione e diffusione. Il concetto di *privacy by default* sottolinea la necessità della tutela della vita privata dei cittadini come impostazione predefinita.

RUOLI

Dal punto di vista organizzativo, il nuovo Regolamento prevede l'adozione delle seguenti figure:

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

- Responsabile del trattamento: la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;

- "Responsabile della Protezione dei Dati" o "Data Protection Owner": è la figura prevista dall'articolo 37 del Regolamento UE 2016/679 la cui responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento dei dati personali all'interno dell'azienda. La figura del DPO è designata dal Titolare del trattamento: ogniqualvolta il trattamento sia effettuato da un'Autorità pubblica o da un organismo pubblico; quando le attività principali consistono nel trattamento, su larga scala, di categorie particolari di soggetti di cui all'articolo 9 o di dati relativi a condanne penali ed infine quando le attività principali, concernenti il raccoglimento dei dati personali, richiedano un monitoraggio regolare e sistematico.

NOVEMBER
2017

CPS GUIDE TO GDPR COMPLIANCE

By Gabriele Falasca - Raffaello Leti Messina

ACCOUNTABILITY

Il Regolamento UE 2016/679 introduce il concetto di *accountability* (responsabilità). Tale definizione sottolinea appunto la "responsabilità" in capo al Titolare del trattamento e al Responsabile del trattamento in relazione alla tutela dei diritti garantiti dalla normativa. L'obiettivo perseguito è chiaramente quello di identificare, nell'ambito dell'organizzazione che realizza i trattamenti di cui trattasi, chiare responsabilità in modo che i soggetti che determinano le finalità e i mezzi del trattamento siano spinti a porre in essere qualsiasi misura necessaria al fine di garantire il rispetto dei principi e delle prescrizioni introdotti dalla nuova disciplina in materia di protezione dei dati personali. Di seguito viene riportato un parere del gruppo di lavoro Articolo 29 a riguardo, estratto da un documento chiamato "*Opinion 3/2010 on the principle of accountability*": "il Titolare del trattamento dei dati deve essere in grado di dimostrare di avere adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi egli deve altresì dimostrare in modo positivo e proattivo che i trattamenti di dati effettuati sono adeguati e conformi al regolamento europeo in materia di privacy."

OBBLIGO DI NOTIFICA DELLE VIOLAZIONI

Importante novità in materia di "diritti dell'interessato" è costituita dall'obbligo di notificazione, in capo al Titolare del trattamento, di una violazione dei dati personali dell'interessato. Tale obbligo è previsto dall'articolo 33 e deve essere adempiuto senza ingiustificato ritardo e, possibilmente, entro 72 ore dal momento in cui il Titolare ne è venuto a conoscenza a meno che sia improbabile che tale violazione costituisca un rischio per i diritti e le libertà fondamentali delle persone fisiche. Alla notificazione deve seguire una comunicazione nella quale deve essere descritto con linguaggio chiaro e semplice la natura della violazione e le possibili conseguenze che ne derivano.

LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

Uno degli elementi di maggiore importanza del nuovo quadro normativo è rappresentato dall'introduzione di una valutazione d'impatto sul trattamento dei dati personali qualora lo stesso possa comportare un rischio elevato per i diritti e le libertà fondamentali delle persone interessate. La valutazione d'impatto è espressamente regolamentata nell'articolo 35 che definisce l'ambito di applicazione e nell'articolo 36 dove sono riportati i casi in cui tale valutazione d'impatto debba essere svolta preliminarmente rispetto all'inizio del trattamento.

CONSULTAZIONE PREVENTIVA

Qualora la valutazione d'impatto ai sensi dell'articolo 35 indichi la presenza di un rischio elevato in assenza di misure adeguate alla mitigazione dello stesso, l'articolo 36 prevede la necessità di rivolgersi all'Autorità di controllo per una consultazione preventiva. L'Autorità di controllo fornisce, entro sei settimane dalla richiesta di consultazione, un parere scritto avvalendosi, se necessario, dei poteri autorizzativi e consultivi di cui all'articolo 58. Tale periodo può essere prorogato di ulteriori sei settimane qualora il trattamento di dati personali presenti particolari complessità.

NOVEMBER
2017

CPS GUIDE TO GDPR COMPLIANCE

By Gabriele Falasca - Raffaello Leti Messina

L'ADEGUAMENTO NORMATIVO COME OPPORTUNITA' DI TRASFORMAZIONE

Stante la necessità di far fronte a tutti gli impegni necessari a raggiungere la conformità entro la data di piena operatività del Regolamento, le organizzazioni che si trovano convolte nelle attività di adeguamento possono considerare gli interventi da realizzare come l'ennesimo adempimento normativo rispetto al quale si è tenuti ad allinearsi oppure accogliere gli stessi come un'opportunità per riesaminare e migliorare i propri processi di business o addirittura come acceleratore verso l'innovazione tecnologica.
Basti pensare all'esigenza di definire una solida *governance* per la gestione dei dati personali che a vario titolo vengono trattati dall'organizzazione, alle necessità di ottimizzare le operazioni di trattamento al fine di rispondere ai requisiti di "minimizzazione" espressi dal Regolamento, all'introduzione di radicali trasformazioni come la dematerializzazione, che riduce i rischi correlati alle violazioni dei dati trattati su supporti cartacei, o la migrazione verso il modello IaaS (Infrastructure as a Service) che riduce, o per lo meno distribuisce temporalmente, sia i costi di implementazione delle misure orientate alla sicurezza informatica da violazioni esterne e interne sia i costi di mantenimento, inclusi quelli connessi all'obsolescenza tecnologica, delle risorse ICT.

In tale ottica, si ritiene che l'approccio ad un *audit* condotto dal punto di vista dei processi possa costituire un fattore abilitante sia per le azioni di miglioramento e trasformazione precedentemente esemplificate sia per le ulteriori opportunità di efficientamento e innovazione che potrebbero emergere in fase di disegno delle misure di adeguamento.

C'è inoltre da considerare il fatto che la violazione di archivi di clienti e dipendenti può tradursi in danni diretti per l'azienda a vantaggio di competitor.

IN BREVE

La metodologia proposta si basa sull'approccio per processi al fine di strutturare un *audit* che verifichi la *compliance* al Regolamento analizzandola dal punto di vista delle necessità di trattamento derivanti dai processi aziendali, quindi del "business" dell'organizzazione. Il rispetto dei criteri di minimizzazione del trattamento e della durata dello stesso verrebbe verificato sia per gli step di processo gestiti mediante strumenti tecnologici sia per quelli che prevedono l'utilizzo di media fisici (documenti cartacei e relativi archivi).

LA METODOLOGIA PROPOSTA

Nel predisporsi all'attività di verifica potrebbe sembrare inevitabile cominciare con quanto già implementato da parte dell'organizzazione sia per supportare i precedenti adempimenti, si vedano le informative ai sensi dell'art. 13 del D.Lgs 196/03 o le misure di carattere tecnologico (log accessi degli amministratori di sistema, password policy, ecc.), sia per anticipare quanto previsto dalla normativa, come ad esempio un Registro delle attività di trattamento già redatto. Benché il lavoro già svolto possa costituire un validissimo punto di partenza, specie quando questo è ben strutturato e adeguato alle prescrizioni del GDPR, si rischierebbe che siano i documenti e i registri a guidare la fase di *audit*, riducendo quindi la "soglia di attenzione" con cui verificare in maniera efficace la *compliance* relativamente alla nuova normativa.
Anche l'analisi dal punto di vista dei flussi delle informazioni potrebbe rappresentare un buon punto di partenza, poiché una descrizione degli stessi e del loro utilizzo potrebbe dare l'idea di avere un quadro completo dei dati gestiti da parte

dell'azienda o dell'istituzione e di come questi vengono trattati. Anche in questo caso il rischio è quello di partire da una visione parziale dei trattamenti e di influenzare l'accuratezza dell'*audit*.

È importante ricordare che la normativa si fonda anche sul concetto di minimizzazione del rischio inerente il trattamento e un Registro correttamente approntato e manutenuto, così come una esaustiva mappatura dei flussi dati gestiti in azienda, potrebbe non evidenziare attività di carattere meramente operativo che porrebbero un serio rischio di violazione dei dati personali, con potenziale pregiudizio dei diritti e delle libertà degli interessati. Si pensi alla stampa di schede anagrafiche dei contatti censiti nel proprio sistema CRM, raccolte, fascicolate, utilizzate e poi cestinate senza averle rese illeggibili tramite un distruggi documenti…
La GDPR non si riferisce ai soli rischi derivanti dall'utilizzo di tecnologie o di strumenti informatici.

Certamente le organizzazioni che abbiano adottato un sistema di gestione ISO/IEC 27001 si troveranno in una posizione di particolare vantaggio poiché l'implementazione di un Information Security Management System (ISMS) conforme a tale normativa presenta diversi punti di contatto il GDPR e implica necessariamente che l'organizzazione stessa abbia maturato la necessaria consapevolezza sulle tematiche inerenti la sicurezza delle informazioni e abbia avuto modo di confrontarsi e dare risposte – ad esempio – rispetto a problematiche di Risk Assessment, classificazione delle informazioni, *compliance*, mantenimento e aggiornamento della documentazione e delle registrazioni di riferimento potendo altresì contare sulla solidità di un *assessment* condotto da soggetti terzi ed indipendenti. Ciononostante, la conformità alla ISO 27001 non garantisce la piena conformità al Regolamento UE 2016/679 e soltanto un *audit* mirato consente l'individuazione degli eventuali gap e l'implementazione delle necessarie misure di adeguamento.

Appare quindi preferibile adottare un approccio orientato ai processi che consenta di verificare la conformità alle prescrizioni normative analizzando per primo il trattamento dei dati personali dal punto di vista delle reali necessità dei processi aziendali (principali e di supporto) e successivamente verificare la conformità rispetto alle altre misure previste dalla normativa. L'analisi a livello dei singoli step di processo (attività ed eventi) porterebbe alla luce quali attività di trattamento, fisiche o digitali, dei dati personali vengono condotte all'interno dell'azienda o dell'istituzione e quali potrebbero essere le eventuali *failure* del processo. La rimozione delle failure – ove possibile – eliminerebbe quindi i rischi a queste correlati, lasciando "sotto osservazione" e prevedendo l'eventuale gestione dei soli rischi residui.

Lo stesso approccio dovrebbe informare la garanzia di conformità al paradigma di "privacy by design" nel caso in cui le attività di trattamento siano inerenti il disegno di un nuovo processo o la reingegnerizzazione di un processo esistente. In questo caso la verifica verrebbe condotta "a monte", rimuovendo le *failure* prima di implementare il nuovo trattamento e focalizzando le attività sulla mitigazione dei rischi residui.

Segue una breve descrizione delle fasi della metodologia proposta.

ATTIVITÀ PRELIMINARI

Rientrano in questa fase tutte le attività propedeutiche all'avvio dell'attività di *audit*. Esse non riguardano esclusivamente la raccolta delle informazioni preliminari ma includono anche

l'individuazione di tutte le figure, interne o esterne, coinvolte nella fase di *audit* e la gestione delle comunicazioni.

IDENTIFICAZIONE DEI RUOLI CHIAVE

È determinante individuare tutti gli attori coinvolti a vario titolo nella fase di *audit*. Oltre alle figure previste dalla normativa – Titolare, Responsabili del trattamento, DPO – è necessario identificare i rappresentanti delle funzioni aziendali o delle aree organizzative che verranno interessate dall'attività di *audit*. Queste dovranno designare dei referenti di area o, nelle realtà con maggiore complessità operativa e/o organizzativa, dei referenti di processo che potranno supportare la fase di *discovery* dei processi aziendali e la successiva verifica di conformità.

CONDIVISIONE DEGLI OBIETTIVI E DELLE FINALITA' DELL'AUDIT

L'indagine in merito alla *compliance* al GDPR rappresenta un momento di verifica che coinvolge interamente l'azienda o l'istituzione e, il principio di *accountability* di Titolari e Responsabili, implica un forte impegno da parte di tutti i ruoli chiave presenti nell'organizzazione affinché questi ultimi collaborino fattivamente durante l'*assessment* e, ove possibile, contribuiscano in maniera proattiva alla successiva fase di disegno delle misure.

PREDISPOSIZIONE DEL COMMUNICATION PLAN

Per portata e caratteristiche intrinseche della stessa, l'attività di *audit* può essere considerata a tutti gli effetti un progetto vero e proprio. L'articolazione delle attività, le necessità di allineamento continuo, il numero potenziale di soggetti coinvolti e la natura degli interventi sottostanti rendono imprescindibile la predisposizione di un Piano di Comunicazione. Questo dovrà individuare chiaramente le tipologie di comunicazione che verranno scambiate durante le attività successive, le tempistiche, i canali e i gruppi di destinatari interessati. Poiché dall'attività di *audit* deriverà quasi certamente la necessità di adottare delle misure che in alcuni casi posso incidere in maniera sensibile anche sulle dinamiche interne dell'azienda o dell'istituzione, un efficace comunicazione contribuisce a garantire il costante coinvolgimento e allineamento di tutti gli *stakeholders* e a ridurre le fisiologiche resistenze al cambiamento che adeguamenti di carattere operativo e organizzativo possono sovente ingenerare.

CENSIMENTO E RACCOLTA DELLA DOCUMENTAZIONE

Nonostante le premesse che giustificano un approccio all'*audit* a partire dai processi, è opportuno raccogliere prima delle verifiche tutta la documentazione o le registrazioni già predisposte la cui finalità sia quella di supportare il corretto trattamento dei dati personali e la conformità alle prescrizioni normative di riferimento. Fanno parte di questa documentazione, a titolo indicativo e non esaustivo, le Informative, il Registro delle attività di trattamento, i contratti di servizio relativi alle nomine interne (Titolare, Responsabile, DPO), codici di condotta di dipendenti, collaboratori e fornitori, i documenti e le registrazioni implementate nell'ambito del proprio Information Security Management System conforme alla ISO 27001 (ove presente), ecc. Questo materiale dovrà essere interamente e continuativamente disponibile durante la fase di *auditing* per verificarne l'efficacia e l'adeguatezza.

CPS GUIDE TO GDPR COMPLIANCE

By Gabriele Falasca - Raffaello Leti Messina

COMPLIANCE DEI TRATTAMENTI GIÀ IMPLEMENTATI

In questa fase si procede alla vera e propria attività di verifica, analisi e classificazione dei rischi che consentirà di disegnare le misure necessarie a mitigare i rischi correlati al trattamento dei dati personali, in conformità con le prescrizioni del Regolamento UE 2016/679.

DATA PROTECTION COMPLIANCE AUDIT

La verifica sui trattamenti già implementati, che potremmo chiamare *Data Protection Compliance Audit*, costituisce, in ottica ISO 31000, la fase di *Risk Assessment* e richiede, al fine di essere condotta in maniera veramente efficace, la disponibilità e la collaborazione di almeno un referente di area e, ove necessario, un referente per ciascun processo esaminato.
Il primo step è rappresentato dall'individuazione di tutti i processi aziendali per i quali è previsto il trattamento di dati personali, siano questi processi primari riferiti al *core business* dell'azienda (gestione clienti, richieste di assistenza, ecc.) che processi di supporto come quelli legati all'area Risorse Umane.

Successivamente dovranno essere identificati i singoli step di processo (eventi e/o attività anche automatizzati, inclusa la profilazione) basati sul trattamento di dati personali e che potremmo definire *Data Touch Points*. In questa fase è necessario individuare chiaramente la tipologia dei dati interessati al trattamento nello specifico step di processo nonché i soggetti e/o le categorie di soggetti coinvolti nel trattamento: interessati (inclusi minori), personale aziendale e/o terzi (es: operatori dedicati al *customer care*, funzionari HR, responsabili e titolari del trattamento, consulenti esterni, ecc.) inclusi i destinatari a cui i dati vengono o saranno comunicati (nazionali, UE, extra UE).

Il passo seguente è la verifica di *compliance* con la normativa per ciascun *Data Touch Point*, logico o fisico, dal punto di vista dei requisiti legali, dell'integrità, della riservatezza, della sicurezza, ecc. Gli aspetti da considerare sono molteplici:

- Finalità
- Liceità (rif. Art. 6)
- Rispetto del principio di "minimizzazione dei dati" (art. 5 lett. C)
- Assoggettabilità a DPIA e/o a Consultazione preventiva
- Durata della conservazione
- Sicurezza dei canali di comunicazione, trasmissione e movimentazione (fisici e logici, anche nel caso di flussi massivi digitali)
- Sicurezza dei dispositivi tecnologici utilizzati
- Sicurezza degli strumenti informatici (sistemi) utilizzati
- Sicurezza degli archivi e dei luoghi di conservazione
- Gestione degli accessi (fisici e logici)
- Autorizzazione al trattamento e perimetro di visibilità del personale che partecipa ai trattamenti (anche derivante da funzionalità applicative che consentono visualizzazione, modifica, ecc.)
- Livello di formazione del personale che partecipa ai trattamenti (con accesso permanente o regolare ai dati personali)
- Segregazione e disponibilità fisica/temporale delle copie di servizio

- Logiche di profilazione automatica (ove presenti)
- Idoneità alla portabilità
- Adeguatezza delle garanzie di sicurezza applicate per dati assoggettabili al trasferimento verso paesi terzi o organizzazioni internazionali (rif. Capo V)

In questa fase è necessario individuare e classificare i cosiddetti *point of failure* negli step di processo e i *Data Protection Risks* a questi correlati (*Failure & Risk Identification Step 1*). Al termine di questa attività è anche possibile costruire delle *Information Flow Maps* che costituiscono un *deliverable* utile a inquadrare l'intero "andamento" dei dati personali all'interno dell'azienda o dell'istituzione così come alla costruzione o verifica del Registro delle attività di trattamento, se presente.

Il passaggio successivo è costituito dalla verifica circa il rispetto delle altre misure previste dalla normativa. Tali misure riguardano sia veri e propri adempimenti sia prescrizioni con impatti più o meno diretti su aspetti organizzativi e di processo. Tra gli aspetti da considerare è opportuno citare a titolo indicativo:

- Nomine (Titolare, Responsabili del trattamento, Responsabili della protezione dei dati – DPO) e vincoli contrattuali
- Vincoli di contitolarità del trattamento
- Disponibilità e adeguatezza del Registro delle attività di trattamento, ove previsto (contenuti minimi)
- Valutazioni di impatto sul trattamento dei dati, ove necessario
- Adeguatezza delle Informative e Consenso al trattamento
- Gestione delle Richieste provenienti dagli interessati (adeguatezza di procedure e strumenti necessari all'esercizio dei diritti dell'interessato: consultazione, accesso, modifica, cancellazione, ecc.)
- Obblighi di notifica verso i destinatari (es.: gestione del processo di violazione dei dati personali dell'interessato inclusa la segnalazione all'Autorità di controllo)
- Gestione dei processi di cancellazione/distruzione del dato (non legata a diritti dell'interessato)

Anche in questa fase è necessario individuare e classificare i *point of failure* negli step di processo e i *Data Protection Risks* ad essi correlati (Failure & Risk Identification Step 2).

Al termine della fase di *Failure & Risk Identification* è opportuno procedere alla fase denominata *Data Protection Risks Identification*. Nell'ambito della stessa si ritiene molto efficace mutuare le *best practices* della tecnica FMEA (*Failure Mode and Effect Analysis*). Essa viene impiegata per analizzare le c.d. modalità di fallimento (*failure mode*) o difetto per un prodotto un processo o un sistema, stabilendone cause ed effetti e successivamente individuando gli elementi critici rispetto ai quali indirizzare specifiche azioni di miglioramento. Per ciascuna delle "configurazioni di fallimento" o debolezza del processo individuate è necessario valutare:

- Probabilità di accadimento
- Livello di gravità, incluso quello previsto dalla normativa, che tiene conto dei seguenti aspetti:
    - Frequenza di esposizione
    - Quantità di dati esposti

    - Livello di sicurezza applicato al trattamento
- Capacità di rilevazione

Dalla valutazione dei fattori precedentemente indicati discende l'attribuzione dell'Indice di Priorità di Rischio (o *Risk Priority Number* – RPN) consente di determinare i *failure mode* più critici e, conseguentemente, di priorizzare gli interventi successivi.

La matrice di valutazione dei *failure mode* confluirà nel *Data Protection Audit Report* che costituisce il *deliverable* di riferimento della fase di *audit*. Al termine di questa fase è anche possibile, ove necessario, predisporre il Registro dei trattamenti o adeguare quello già implementato.

REMEDIATION

La fase di *Remediation, Risk Response* in chiave ISO 31000, prevede come primo step il disegno delle misure che saranno orientate all'eliminazione delle *failure* e alla minimizzazione dei rischi residui per quelle non completamente eliminabili. È importante evidenziare che le misure potrebbero riguardare adeguamenti organizzativi, ai processi (ottimizzazione/ridisegno), a policy e procedure o tecnologici (infrastrutture, sistemi e strumenti di supporto). Per ciascuna delle misure individuate è necessario stimare i relativi costi di implementazione. Tale valutazione assume maggior rilevanza nel caso in cui siano presenti scenari alternativi per la mitigazione dei rischi o l'eliminazione delle *failure*. Normalmente infatti, non esiste un solo modo per conformarsi alle prescrizioni normative, potendosi valutare differenti alternative ciascuna implicante una diversa struttura dei costi. Le stesse dovranno essere valutate in ragione del RPN proprio di ciascuna configurazione per accertare che questo rientri nei margini di tollerabilità stabiliti dal Titolare del trattamento e che non necessiti di ulteriori interventi di mitigazione.

L'analisi precedentemente condotta consente di rappresentare al management l'impatto in termini economici e organizzativi delle misure proposte al fine di consentirne la valutazione e successiva approvazione.

Le misure adottate confluiranno nel *Remediation Plan* che illustra la pianificazione degli interventi a breve e a medio/lungo termine. Il *Remediation Plan* indica inoltre, le eventuali necessità di adeguamento della documentazione aziendale (manuale della qualità, procedure operative, linee guida, integrazione al codice di condotta aziendale e dei fornitori, ecc.) nonché le necessità di formazione dei soggetti coinvolti in maniera diretta o indiretta nelle attività di trattamento dei dati personali.

MONITORING

Il piano, o programma, di *Remediation* richiede necessariamente un costante allineamento tra gli attori coinvolti nell'implementazione delle misure, il management e il Titolare del trattamento. Poiché la necessità di tale controllo si estende a tutte le azioni previste nel piano, è auspicabile – anche in funzione della natura degli interventi – affidare il monitoraggio in merito all'implementazione delle attività ad un *Implementation Manager*. Tale figura ha inoltre il compito di coadiuvare il Titolare, i Responsabili e il DPO nel mantenere un costante aggiornamento dei documenti e delle registrazioni di supporto, come il Registro delle attività di trattamento o le Valutazioni di Impatto sulla protezione dei dati (c.d. DPIA, ove applicabile), che forniranno evidenza dell'effettivo adempimento da parte del Titolare del trattamento agli obblighi prescritti in tema di *accountability*.

Il coinvolgimento di un *Implementation Manager* consentirà altresì di supportare il Top Management e il Titolare del trattamento durante le fasi di transizione o cambiamento derivanti dall'adozione di quelle misure previste nel *Remediation Plan* che implicano rilevanti impatti dal punto di vista organizzativo o operativo. Solitamente, infatti, si assiste ad una generale resistenza al cambiamento da parte dei soggetti destinatari degli adeguamenti, i quali potrebbero subire sia variazioni nelle proprie modalità di lavoro quotidiano sia limitazioni o estensioni di poteri ed obblighi associati alle loro mansioni funzionali all'allineamento con il Regolamento.

DISEGNO E REINGEGNERIZZAZIONE DEI PROCESSI AZIENDALI

Nel caso del disegno di un nuovo processo o reingegnerizzazione di un processo esistente, l'organizzazione si troverà in una posizione diversa rispetto alla necessità di condurre un *audit* a posteriori. La caratteristica di questo scenario è quella di offrire l'opportunità per rispettare il paradigma della "*privacy by design*" espresso nel Regolamento 2016/679. È questo infatti il caso in cui la conformità del trattamento può essere verificata nelle attività di disegno o reingegnerizzazione del processo nell'ambito del quale il trattamento si rende necessario, consentendo la risoluzione delle *failure* a "*design time*" e focalizzando quindi gli interventi sulla mitigazione dei rischi residui.

PRELIMINARY ASSESSMENT

Analogamente a quanto previsto in fase di *Data Protection Compliance Audit* – in aggiunta alle figure individuate dalla normativa quali Titolare, Responsabili del trattamento, DPO – è necessario identificare i rappresentanti delle funzioni aziendali o delle aree organizzative coinvolte nel disegno del nuovo processo o reingegnerizzazione del processo esistente. Anche in questo caso la predisposizione di un efficace *Communication Plan* garantirà l'ordinato procedere delle attività.

Oltre all'individuazione di soggetti (inclusi eventuali contitolari) e processi aziendali interessati, dovranno essere definite, o verificate se già esistenti, le finalità di trattamento, la durata, il contesto, la tipologia e la quantità dei dati personali oggetto dei trattamenti nonché le tecnologie/infrastrutture utilizzate. Tali elementi consentiranno una prima individuazione dei livelli di rischio connessi al trattamento anche al fine di determinare la necessità di procedere con una Valutazione di Impatto sulla Protezione dei Dati. A tale riguardo si rappresenta l'utilità delle "Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento 'possa presentare un rischio elevato' ai sensi del regolamento 2016/679" predisposte dal Gruppo di Lavoro ex art. 29 (WP29).

DATA PROCESSING ANALYSIS

Anche nella verifica in fase di disegno l'analisi viene condotta individuando gli step di processo basati sul trattamento dei dati personali (precedentemente definiti come *Data Touch Points*) e verificando la *compliance* con le prescrizioni del Regolamento. Vengono quindi identificati i *Data Protection Risks* e predisposte le *Information Flow Maps* utili a integrare poi il Registro delle attività di trattamento.
In seguito si procede alla valutazione dei rischi e alla priorizzazione degli stessi secondo quanto descritto nel paragrafo relativo al *Data Protection Compliance Audit*. Il risultato delle attività di identificazione e priorizzazione dei rischi confluirà nel *Data Processing Analysis Report*.

DESIGN CONSTRAINTS – INTEGRAZIONE DELLE MISURE NEL PROGETTO DEL NUOVO TRATTAMENTO

L'analisi consente di individuare i *constraints* di processo necessari a rispettare le prescrizioni normative previste dal Regolamento. Detti *constraints* potrebbero riguardare adeguamenti organizzativi, operativi, tecnologici, di processo e che per ciascuno di questi è opportuno stimare i relativi costi di implementazione, inclusi quelli di eventuali scenari alternativi.
Questo permette di rappresentare al management l'impatto in termini economici e organizzativi degli stessi *constraints* e al Titolare del trattamento di valutare le configurazioni, il rispetto dei margini di tollerabilità accettabili e l'eventuale necessità – in funzione del livello di gravità dei rischi residui – di procedere con una Valutazione di Impatto sulla Protezione dei Dati.
Gestire la minimizzazione del rischio direttamente nella fase di disegno del nuovo processo o di reingegnerizzazione di un processo esistente permette di garantire che il trattamento dei dati personali implementato sia coerente con le finalità dello stesso e supportato da sufficienti misure tese a minimizzare il rischio di violazione delle informazioni, quindi l'impatto che queste avrebbero sui diritti e sulle libertà degli interessati.

Sia i *constraints* integrati nel processo che l'eventuale riscontro proveniente dalla Valutazione di impatto forniranno gli elementi necessari ad aggiornare il Registro delle attività di trattamento, che deve riportare i contenuti minimi previsti dalla normativa e ogni altra informazione necessaria a supportare eventuali future attività di verifica o *audit*. Affinché la conformità alle prescrizioni del Regolamento sia garantita nel tempo, tenendo in considerazione che nel ciclo di vita di un progetto è sempre rilevabile una componente fisiologica di cambiamento, è necessario accertare che le future modifiche al progetto non pregiudichino la conformità del trattamento alle prescrizioni del GDPR. Pertanto è opportuno non solo monitorare continuativamente la corretta implementazione dei *constraints* e delle risultanze della DPIA ma anche includere come prassi, tra le attività inerenti la gestione del cambiamento, la verifica di adeguatezza dei *constraints* e della stessa DPIA al fine di attivare – ove necessario – specifici interventi di allineamento o revisione.

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI E CONSULTAZIONE PREVENTIVA

Vale la pena aggiungere poche precisazioni sulla Valutazione di Impatto e sullo strumento della Consultazione Preventiva, rimandando alla normativa di riferimento e alle linee guida per gli eventuali dettagli e approfondimenti. Secondo il Regolamento UE 2016/679, la Valutazione di Impatto sulla Protezione dei Dati (DPIA) è un'attività prevista in tutti i casi in cui i diritti e le libertà degli interessati possano trovarsi esposti ad un rischio elevato. Nello specifico, il Titolare del trattamento è tenuto ad effettuare tale valutazione per tutti i trattamenti individuati – benché in maniera non esaustiva – dalla normativa, incluse le tipologie pubblicate negli elenchi resi disponibili dall'Autorità di controllo secondo quanto stabilito nell'art. 35 del Regolamento.

Lo stesso articolo 35 del Regolamento specifica i contenuti minimi della Valutazione di impatto, che deve includere il disegno delle misure previste (*constraints*) per mitigare i rischi e rendere il trattamento conforme al GDPR. Qualora le misure previste presentino dei rischi residui elevati, o come espresso nel Considerando 94 al GDPR, nel caso in cui il Titolare ritenga "che il rischio non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e costi di attuazione", è necessario procedere alla Consultazione Preventiva dell'Autorità di controllo prima di procedere al trattamento, come disciplinato dall'art. 36 del Regolamento. Tale Consultazione deve includere, tra gli elementi obbligatori, proprio la Valutazione di Impatto prevista dall'art. 35.

Si ricorda che la DPIA è obbligatoria, in base ai presupposti precedentemente citati, per tutti i nuovi trattamenti – che rispondono ai criteri individuati nell'art. 35 – a partire dal 25 maggio 2018. Ciononostante, le Linee Guida predisposte dal WP29 raccomandano, anche in virtù della "dinamicità" che si attribuisce al processo di valutazione, di adottare le Valutazioni di impatto – ove necessario – anche prima di tale data.

CONCLUSIONI

La scadenza del 25 maggio 2018 pone aziende e istituzioni davanti alla necessità di mettere in campo tutte le azioni – di carattere operativo, organizzativo, tecnologico – necessarie ad assicurare la conformità del trattamento dei dati personali operata nell'ambito dei propri processi con le prescrizioni normative presenti nel Regolamento UE 2016/679.

La metodologia proposta permette alle organizzazioni di approcciare le attività di *audit* o di implementazione di un nuovo trattamento dal punto di vista dei processi – abilitati da strumenti tecnologici e/o elementi di natura fisica – e quindi di rispondere alle indicazioni della norma tenendo in debita considerazione le necessità operative e di business che rendono indispensabile l'utilizzo dei dati personali da parte dell'organizzazione stessa.

Accostarsi alla verifica di conformità secondo tale orientamento rappresenta inoltre un momento di riesame degli stessi processi interni e dei relativi sistemi di supporto dal quale possono emergere le opportunità per promuovere interventi di innovazione tecnologica e di trasformazione interna.

Appare inoltre evidente che la *compliance* normativa potrà essere accertata in maniera efficace solo facendo ricorso ad un team interdisciplinare che integri particolari competenze nei seguenti campi: consulenza strategica, ambito legale e normativa di riferimento in merito alla privacy e al trattamento dei dati, analisi di processo, Gestione del Fabbisogno (*Demand Management*), disegno di soluzioni tecnologiche e architetture ICT, Sicurezza Informatica, *Program/Project Management*.

CREDITS

Ha collaborato alla stesura del presente documento e alla relativa ricerca normativa: Gabriele Molteni

Per quesiti o commenti è possibile contattare gli autori via email all'indirizzo papers@cpsweb.it