IL GDPR / **GENERAL DATA PROTECTION REGULATION**

in 10 passi

Che cos'è il GDPR UE 2016/679

Come oramai molti sanno il 24 maggio 2016 è entrato in vigore a livello di Comunità Europea il nuovo Regolamento Europeo sulla Privacy.

Le norme saranno applicabili dal 25 maggio 2018 ed il tempo a disposizione per capire la strategia migliore da applicare e metterla in atto non è molto.

Il regolamento porterà una serie di innovazioni non solo per il singolo cittadino ma anche per aziende, enti pubblici, liberi professioni ed associazioni.

In primis il legislatore ha voluto introdurre regole più chiare in merito all'informativa ed al consenso stabilendo precisi limiti al trattamento automatizzato dei dati, alla relativa violazione ed all'interscambio degli stessi al di fuori della Comunità Europea.

Si è voluto rendere la norma più trasparente, con un'unica visione in tutta l'Unione Europea, rendendo molto chiara e semplice la gestione del proprio dato per ogni cittadino mediante consensi e revoche evidenti.

La definizione presente nell'articolo 4 stabilisce l'oggetto del regolamento: «**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;

e la gestione stessa come: «**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;

Il consenso ad un certo trattamento che fino ad oggi poteva anche essere tacito diventa obbligatoriamente esplicito ed il cittadino potrà verificare in ogni istante come questo viene applicato ed eventualmente revocarlo in modo semplice.

Cambia quindi la visione data oggi ai processi di marketing diretto, ma cambiano anche le modalità di registrazione e fruizione dei molti servizi internet; così varia anche la visione relativa alla profilazione dell'utente che non sarà più sufficiente, nel caso di questioni che hanno effetti giuridici, a deciderne una soluzione.

Riportiamo la definizione data dal Regolamento:

«**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per

analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Nel caso di marketing diretto l'interessato avrà sempre diritto di opporsi alle attività di profilazione.

Inoltre è stato introdotto in modo chiaro il diritto all'oblio, cioè la cancellazione dei propri dati personali da parte di un titolare del trattamento qualora ad esempio cessino i motivi per cui si era dato il consenso.

Se ne pongono dei limiti di applicazione e si obbliga il titolare del trattamento ad agire tempestivamente perché l'informazione sia rimossa ovunque venga trattata.

In un mondo sempre più digitale si è dato particolare risalto alla portabilità dei dati personali. In particolare diventerà molto più semplice trasferire i propri dati da un gestore ad un altro per i contratti come la telefonia, e quelli urbani (acqua, luce e gas) in quanto sarà fatto obbligo al gestore attuale il trasferimento autorizzato delle informazioni verso terzi.

Anche dati più strutturati, come la messaggistica elettronica o i file nel cloud, dovranno essere trattati secondo questa nuova visione.

Ovviamente la normativa non si spinge a definire le caratteristiche tecniche per l'interscambio dei dati né a livello europeo né nazionale.

Saranno presumibilmente i vari enti nazionali, da noi il Garante per la Privacy, a concepire le opportune interfacce informatiche per i vari temi. Una particolare attenzione viene data al trasferimento dei dati al di fuori dell'Unione Europea dove dovrà essere accuratamente valutata l'adeguatezza rispetto alla tutela dei dati della controparte e in caso di insufficienza si potranno richiedere opportune garanzie ed il cittadino dovrà esplicitamente dare il proprio consenso ad ogni forma di trasferimento.

La violazione dei dati personali (Data breach) non potrà essere una problematica solamente aziendale ma richiederà maggiore informazione verso l'interessato e una comunicazione tempestiva ed obbligatoria verso l'autorità nazionale per la protezione dati.

Per le aziende, di qualsiasi ordine e grado, cambia radicalmente la visione generale che passa da un censimento dei trattamenti effettuati relativi alla privacy ad un vero e proprio Sistema Rischi dove, con le medesime metodologie messe in campo per il trattamento, ad esempio dei rischi finanziari od operativi, si riportano gli elementi della privacy ad elementi di rischio per il quale si devono fare attente misurazioni, mettere in atto politiche di riduzione del rischio, pianificare i costi che vanno ad impattare sul conto economico dell'impresa.

I legislatori europei hanno voluto dichiarare in modo evidente l'importanza del provvedimento stabilendo forti sanzioni pecuniarie nel caso di non rispetto della norma (articolo 84, sanzioni). Parimenti le imprese che saranno particolarmente virtuose, in cui il titolare potrà in ogni momento certificare i propri trattamenti e nelle quali si applicano in modo serio codici di condotta sottoposta all'approvazione dell'autorità nazionale tramite associazioni di categoria o altri soggetti, avranno diritto a valutazioni meno stringenti nel caso si manifestassero problematiche nei processi privacy.

Nelle sezioni che seguiranno verranno approfondite alcune delle problematiche citate dando enfasi alle azioni che le imprese dovranno attuare per adempiere al Regolamento.

1 - Il nuovo regolamento cambia visione: Risk Management per i dati personali

Il modello che permette di trattare correttamente la gestione delle problematiche privacy nasce da modelli già esistenti e normati. In particolare ci si rifà in primis alla normativa UNI EN ISO 9001 che definisce per un'organizzazione i requisiti di un sistema di gestione per la qualità ed in particolare la creazione, all'interno dell'azienda, di un sistema organizzativo i cui requisiti rispettino tale norma.

Le metodologie e i requisiti previsti devono essere applicati a tutti i processi aziendali, dalla Produzione all'Area commerciale, dagli Acquisti alla Direzione Generale.

Ogni processo deve essere censito attraverso apposita documentazione (il manuale di qualità, l'elenco delle procedure, le istruzioni operative, la registrazione delle attività di qualità).

Il Sistema Qualità monitora tutto ciò che è previsto dalle procedure relative riportando le non conformità del processo dopo opportuna misurazione dei vari fenomeni. Quindi viene prevista una metodologia che contempla la riduzione delle Non Conformità in un ciclo continuo di miglioramento.

Un'azienda che si è dotata di un Sistema Qualità in conformità alla normativa UNI EN ISO 9001 è favorita nell'affrontare le metodologie per definire il proprio Sistema Privacy in quanto si parte da una medesima metodologia.

Un ulteriore modello normativo sul quale i legislatori hanno basato la visione del GDPR è la ISO 31000.

Questo standard internazionale tratta in modo preciso il concetto di Rischio, che può essere definito come la potenzialità che un'azione o un'attività scelta (includendo la scelta di non agire) porti a una perdita o ad un evento indesiderabile.

La nozione implica che una scelta influenzi il risultato. Le stesse perdite potenziali possono anche essere chiamate "rischi". Sebbene ogni comportamento umano sia rischioso alcuni hanno una percentuale di rischio maggiore.

Per "rischio" possiamo indicare anche la distribuzione dei possibili scostamenti dai risultati attesi per effetto di eventi di incerta manifestazione, interni o esterni ad un sistema.

In questa definizione, il rischio non ha solo un'accezione negativa (downside risk), ma anche una positiva (upside risk).

Esso è definito dal prodotto della frequenza di accadimento e della gravità delle conseguenze (magnitudo). (Wikipedia – Rischio) Le politiche di prevenzione e mitigazione del Rischio vengono normalmente applicate a macro-fenomeni precisi, rischi economici legati a costi e ricavi, rischi finanziari legati ai flussi monetari in entrata e uscita, rischi patrimoniali, rischi penali e rischi operativi derivanti dall'inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi.

Ora si è fortemente voluto che anche il trattamento delle attività legate alla Privacy ricadesse fra gli eventi di Rischio e pertanto risulta compatibile con procedure, metodi, sistemi di controllo derivanti dall'applicazione della ISO 31000.

Ogni elemento di Privacy deve essere quindi misurato dal punto di vista della probabilità di accadimento dei rischi connessi partendo comunque dal principio che, trattandosi di un rischio possibile, non si potranno mai realizzare processi atti ad eliminarlo completamente ma solamente a renderne minima la probabilità di accadimento.

Quindi si parlerà spesso di Non Conformità quando non vengono prese opportune decisioni in merito al trattamento del Rischio e tutto il sistema dovrà essere incentrato sulle politiche di mitigazione del Rischio.

Dal momento che una buona parte degli strumenti utilizzati per il trattamento del dato personale sono di carattere tecnologico/informatico risulta che un altro standard europeo diventa un'importante base per l'approccio al Sistema Privacy. Si tratta della ISO/IEC 27001:2005 (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti) che definisce i requisiti per impostare e gestire un Sistema di Gestione della Sicurezza delle Informazioni includendo aspetti relativi alla sicurezza logica, fisica ed organizzativa. Gli standard citati sono la base sulla quale ci si deve avventurare per affrontare la gestione della Privacy.

Non più una visione a sé stante ma un sistema Rischio che si cala su di un sistema Qualità.

Ne consegue che le aziende che già hanno affrontato in modo sistematico queste problematiche si trovino avvantaggiate nel mettere in atto ciò che viene richiesto dal GDPR.

2 - Un piano di implementazione per la "protezione dei Dati Personali"

Che cosa bisogna fare quindi per implementare Sistema Privacy nella propria azienda?

Seguendo i dettami dei Sistemi Qualità si dovranno definire formalmente i responsabili Privacy (come da articolo 4 del GDPR):

il «**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;

il «**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;

Poi dovrà essere mappata l'azienda dando una rilevanza all'organigramma in modo da poter attribuire funzionalmente ogni risorsa ad una unità operativa, includendo non solo il personale dipendente ma tutti coloro che hanno una qualche attività con l'impresa stessa (ogni persona che può essere coinvolta in un processo di trattamento privacy).

Quindi, a partire dal censimento dei dati personali presenti e dei relativi trattamenti, si dovrà riportare alle singole risorse l'incarico di trattare quel particolare dato.

Si dovrà prevedere per ogni risorsa una lettera di incarico che evidenzi compiti e responsabilità di trattamento e un piano formativo idoneo a preparare ad una corretta gestione.

La conservazione ed il trattamento del dato creano, come evidenziato in precedenza, eventi di rischio (accesso indesiderato, perdita, utilizzo non permesso, trattamento non conforme, ecc.).

Risulta un passo inevitabile attuare un PIA preventivo (Privacy Impact Assessment = censimento degli impatti privacy) in cui per ogni fenomeno si valuta rischiosità complessiva, azioni intraprese e rischiosità residua in modo da realizzare il primo documento che fotografa la situazione corrente.

Dalla valutazione del PIA nasce un piano interno in cui viene stabilito in quale modo verrà mitigato il singolo rischio, coloro che sono incaricati di operare in tal senso e il costo previsto per l'attività.

Questo planning operativo deve essere costantemente monitorato e avrà impatto sul Privacy Impact Assessment successivo (uno/due all'anno potrebbero essere sufficienti) in cui si andranno ad evidenziare i miglioramenti ottenuti e le eventuali ulteriori rischiosità subentrate.

Per le aziende diventa allora fondamentale dotarsi di un sistema informatico atto a censire, valutare, monitorare lo stato di rischio e implementare automaticamente il reporting necessario e le comunicazioni operative per le varie risorse

3 - PIA (Privacy Impact Assessment): lo strumento base per censire i rischi privacy

Approfondiamo ora la valutazione d'impatto sulla protezione dei dati prevista dal Regolamento UE 2016/679. È possibile operare utilizzando risorse competenti interne all'azienda oppure avvalersi di professionisti esterni esperti nelle problematiche privacy.

Normalmente, almeno per il primo assessment, è consigliato avvalersi di risorse esterne esperte in modo da inquadrare velocemente i metodi e le azioni da intraprendersi e pervenire in breve tempo ad una base dati completa.

Ricordiamoci che l'assessment rappresenta di solito uno strumento preventivo gestito dall'azienda stessa che decide di monitorare un determinato fenomeno.

I metodi sono i medesimi dell'audit che rappresenta uno strumento più ufficiale e certificante e che viene sempre attuato da esterni all'azienda (società di audit specializzate o autorità) per valutare l'idoneità del sistema a determinate norme.

Un PIA è disegnato per raggiungere normalmente tre obiettivi:

- Garantire la conformità con le normative, e requisiti di politica legali applicabili per la privacy;
- Determinare i rischi e gli effetti che ne conseguono;
- Valutare le protezioni e eventuali processi alternativi per mitigare i potenziali rischi per la privacy.

Non rappresenta quindi un mero strumento atto a censire, ma diventa l'elemento più importante per affermare di essere conformi alle prescrizioni del Regolamento.

Dalla valutazione di un PIA e dell'analogo Audit ufficiale nasce per le aziende la possibilità di raggiungere le certificazioni che sono previste dal Regolamento e che rendono virtuosa l'impresa stessa.

Un buon PIA comporta i seguenti vantaggi:

• Crea un sistema di preallarme, un modo per rilevare problemi di privacy costruendo garanzie in anticipo ed evitando problemi di investimento successivi;

• Evita errori costosi o imbarazzanti sulla privacy;

• Fornisce la prova che l'organizzazione ha tentato di evitare rischi per la privacy (ridurre la responsabilità, pubblicità negativa, danni alla reputazione);

• Migliora il processo decisionale;

• Aumenta la fiducia del pubblico e della clientela;

• Dimostra a dipendenti, collaboratori, clienti, cittadini che l'organizzazione prende sul serio la privacy. Le valutazioni d'impatto sulla privacy possono essere riassunte in un processo in quattro fasi:

• Inizializzazione del progetto: in questo passaggio si definisce il campo di applicazione del processo PIA (differente per ogni organizzazione).

È possibile fare un PIA preliminare se il progetto è all'inizio e non si hanno ancora informazioni dettagliate e successivamente realizzare un PIA completo;

• Analisi del flusso dati: in questa fase si mappano i processi di business per quanto riguarda il dato personale e si crea un diagramma di come il dato viene trattato attraverso l'organizzazione;

• Analisi della privacy: in questa fase viene richiesto al personale coinvolto con il trattamento delle informazioni di compilare i relativi questionari che vengono valutati nell'ottica rischio;

• Relazione sulla valutazione di impatto Privacy: in questo passaggio si richiede all'organizzazione di creare una valutazione documentata dei rischi per la privacy e le potenziali implicazioni di tali rischi e l'individuazione delle attività necessarie per mitigare o porre rimedio ai rischi.

Facendoci aiutare da quello che dice la **ISO/IEC 27001:2005** per la protezione informatica evidenziamo le funzioni che devono essere generalmente implementate:

Individuazione: mappare le possibili situazioni di rischio dal punto di vista del tipo di violazione, delle risorse e delle unità organizzative coinvolte, della probabilità dell'evento e della gravità delle conseguenze;

Protezione: adottare in modo preventivo misure atte ad evitare trattamenti non necessari, ridurre la possibilità di accadimento, ridurre le eventuali conseguenze negative;

Rilevazione: istituire, secondo processi di qualità, un sistema di monitoraggio continuo in grado di segnalare tempestivamente eventi legati al rischio privacy;

Risposta: predisporre misure correttive adatte in caso di incidente informando gli interessati e l'autorità competente; Ripristino: predisporre piani di ripristino della normale operatività.

4 - Il Consenso dell'interessato

Un deciso cambiamento si ha nei riguardi dell'autorizzazione che il soggetto, a cui fanno capo i dati personali, deve dare per un determinato trattamento.

L’attuale Codice della Privacy permette, in taluni situazioni, formule per cui la mancanza di opposizione ad un trattamento diventa implicitamente un assenso. Ciò che definiamo silenzio assenso.

Il regolamento europeo si esprime definendo

«consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Quindi, in ogni caso, l’interessato dovrà esprimersi in merito a trattamento fornendo un consenso effettivo ed inequivocabile, ad esempio, con dichiarazione scritta o attraverso mezzi elettronici o verbale (con registrazione).

Ci troviamo così in una situazione in cui molte attività di marketing, dove si utilizzano elenchi di destinatari di varia provenienza, diventano non più possibili, addirittura sanzionabili.

Ogni operazione di comunicazione dovrà quindi far capo ad un preciso consenso formalizzato per ogni controparte presentabile nel caso l’interessato ne facesse richiesta.

L’interessato ha il diritto di revocare qualsiasi consenso abbia dato e deve essere informato di questo dal titolare del trattamento. Restano leciti tutti i trattamenti compiuti prima della revoca stessa.

5 - Strumenti operativi innovativi

Qual è la vostra visione dello strumento che vi può aiutare a raggiungere nel modo migliore gli obiettivi previsti dal GDPR?

Sicuramente non avete in mente un sistema tradizionale fatto di moduli di censimento, di liste di responsabili o di questionari.

E non vi parlo solo di supporti cartacei ma anche dei documenti prodotti con gli applicativi tradizionali di Office Automation.

Non è più tempo di lavorare manualmente su dati disconnessi e non correlati ma diventa fondamentale avvalersi dei vantaggi che le nuove piattaforme informatiche ci mettono a disposizione.

Si deve poter disporre dell’organigramma aziendale aggiornato che fa da fulcro per tutte le operazioni di trattamento, per gli incarichi relativi, per le comunicazioni dirette e la formazione.

Deve essere un software in grado di essere utilizzato su ogni postazione aziendale (i trattamenti sono ovunque!) e deve fornire strumenti correlati con la funzione della risorsa che lo va ad utilizzare.

Il database centrale su cui si basa l’applicativo deve contenere tutte le informazioni necessarie al Sistema Privacy e deve permetterne la storicizzazione periodica in modo da creare sistemi di reportistica andamentale comparata.

Sono gradite le funzionalità di document management che permettono di archiviare, ad esempio, le lettere di incarico legate ai singoli trattamenti, o i report periodici o il materiale documentativo legato agli aspetti privacy.

Le funzionalità di comunicazione centralizzata sono fondamentali per distribuire i documenti e per rammentare in modo opportuno le scadenze che ognuno ha rispetto, ad esempio, all'ultimo piano di interventi previsti per mitigare i vari rischi.

Per ciò che riguarda le funzioni business l'applicativo deve ovviamente permettere di gestire un PIA nella sua interezza, di storicizzarlo, di generare un piano di interventi con i relativi costi da portare al vaglio della Direzione aziendale.

Deve essere possibile capire che nulla si è trascurato nella pianificazione e nella gestione delle problematiche privacy in modo da essere sempre pronti ad eventuali controlli in merito.

6 - La protezione fin dalla progettazione (Privacy by Design e by Default)

Il regolamento europeo 2016/679 prevede ulteriori elementi innovativi.

A fronte dell'obiettivo di proteggere il dato personale e al cambiamento di scenario tecnologico che ha visto sempre più la distribuzione del dato mediante strumenti informatici privati e pubblici, si è dovuto provvedere a mettere in piedi sistemi atti a garantirne la protezione.

Fin dagli anni '90 sono stati prodotte le prime tecnologie in ambito ICT utili ad accrescere la protezione dei dati personali (PET = Privacy Enhancing Technologies).

L'attuale codice italiano sulla privacy (D.L 196/2003) nell'articolo 3 (Principio di necessità nel trattamento dei dati) fa riferimento a tali tecnologie:

I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Il nuovo regolamento compie un altro passo in avanti introducendo la Privacy by Design che con un innovativo approccio concettuale pone le basi della privacy del futuro.

L'articolo 25 (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita) si esprime in tal senso:

1 Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Ovvero la nascita del sistema di protezione avviene contemporaneamente con l'evento di rischio di cui si deve fare trattamento e quindi non si fa trattamento fintantoché l'intero sistema non è stato definito.

È certamente una visione innovativa del problema che obbliga tutti coloro che introducono nuove rischiosità privacy sul mercato ad introdurre e certificare anche gli opportuni sistemi di sicurezza e di mitigazione del rischio.

Potete certamente pensarlo per nuovi apparati, ma anche per la creazione di nuovi servizi web o prodotti tecnologici che dovranno essere progettati tenendo conto sempre di questa norma.

Nella progettazione delle basi dati si dovrà tener sempre conto di rendere minimo il dato personale utilizzato concentrandolo in chiaro in componenti limitate e protette applicando nel resto del progetto la pseudonimizzazione dell'informazione, definita come:

«pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

Attenzione quindi ai nuovi progetti software atti a realizzare strumenti per il trattamento del dato personale.

Il medesimo articolo 25 dice anche che:

2 Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Qui viene rappresentato il concetto di Privacy by Default dove si chiede di utilizzare il numero di informazioni necessario e sufficiente al trattamento in atto per limitare già in fase di progettazione il rischio privacy.

7 - I registri dei trattamenti

Fra gli altri compiti, il titolare e il responsabile del trattamento devono redigere i registri delle attività e dei trattamenti effettuati.

Formalmente la tenuta del registro rappresenta il sostituto della comunicazione diretta delle medesime informazioni al Garante della Privacy. È presumibile pensare che nel prossimo futuro, come già avvenuto per i dati forniti all'Agenzia delle Entrate per via telematica, anche per tali informazioni avverrà un processo analogo.

In realtà i registri da conservare e mantenere sono due:

- Il **registro del titolare** del trattamento, che contiene:

  Anagrafica del titolare stesso, di un contitolare se presente, del rappresentante e del titolare alla protezione dati;

Le finalità del trattamento;

Le categorie degli interessati a cui fa capo il dato;

Eventuali termini per la cancellazione automatica del dato;

Un'eventuale descrizione generale delle misure di sicurezza tecnico-organizzative.

- Il **registro del responsabile** del trattamento, in cui sono presenti:

L'anagrafica dei responsabili del trattamento;

La descrizione delle categorie di trattamento effettuati;

Opzionalmente la descrizione delle misure di sicurezza intraprese.

La conservazione può avvenire in forma cartacea ma anche in forma elettronica rendendo sempre disponibile il dato ad eventuali ispezioni dell'autorità garante.

È bene che il software aziendale adottato per gestire il progetto Privacy integri la gestione dei registri derivandoli direttamente dalla normale operatività.

8 - Aspetti economici e sinergie

Ricordatevi che ogni attività che dovrete intraprendere per organizzare, monitorare e controllare gli aspetti legati al trattamento dei dati personali ha un preciso costo.

Un costo che cresce quanto più si trascurano gli aspetti preventivi legati alla mitigazione del rischio.

Una buona organizzazione vi consentirà di preventivare con buona approssimazione l'impianto di un sistema di gestione privacy efficiente che ridurrà gli imprevisti evitando di dover far fronte a situazioni dannose.

Ancor più quando, per trascuratezza, si rischiano pesanti sanzioni da parte del Garante Privacy (In Italia) e delle controparti nelle altre nazione dell'Unione Europea se si opera sul territorio della Comunità.

Gli articoli 83 (Condizioni generali per infliggere sanzioni amministrative pecuniarie) e 84 (Sanzioni) specificano i criteri da adottarsi per sanzionare l'attore inadempiente.

Sanzioni amministrative pecuniarie che possono arrivare fino a 20 milioni di euro e, per le imprese, fino al 4% del fatturato annuo mondiale precedente.

Sono numeri che non possono essere trascurati e che diventano elevati solo se non si è in grado di aver creato, mantenuto e gestito un Sistema Privacy di qualità.

Come in ogni sistema di qualità, diventano importanti le sinergie che si devono instaurare fra gli attori del processo privacy miranti ad un miglioramento continuo di ogni fase, ad una migliore distribuzione dell'informazione e della formazione.

9 - Data Breach: che cosa fare in caso di violazione dei dati

La nostra attenzione si concentra ora sulla

«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

Ovviamente questo rappresenta uno dei temi più cari al Garante della Privacy il quale, con attenzione anche per il nuovo GDPR, ha pubblicato gli adempimenti previsti.

In particolare vengono prese in considerazione le azioni da intraprendersi nel caso di perdita, distruzione, diffusione indebita di dati personali conservati, trasmessi o comunque trattati a causa di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi e altre calamità.

I casi finora analizzati riguardano:

- Le società telefoniche e gli internet provider;
- La biometria;
- Il dossier sanitario elettronico;
- Le amministrazioni pubbliche.

In particolare il testo del nuovo regolamento prevede l'obbligo di notifica all'autorità di controllo e la comunicazione della violazione al diretto interessato.

L'articolo 33 dice infatti:

Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:

   a. descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

   b. comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

   c. descrivere le probabili conseguenze della violazione dei dati personali;

d. descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

ed il 34:

Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

   a. il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

   b. il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

   c. detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

10 - Il ruolo del Data Protection Officer: che cosa prevede la normativa

Gli articoli 37, 38 e 39 (sezione 4) del GDPR trattano della figura del DPO (Data Protection Officer) in particolare della designazione, della posizione e dei compiti.

L’articolo 37 ci spiega che la figura del Data Protection Manager (DPO) non sempre è necessaria:

Designazione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

   a. il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

   b. le attività principali 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 su larga scala; oppure

   c. le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.

3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.

5. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.

6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Inoltre l’articolo seguente specifica che il DPO deve essere dotato di totale autonomia nella gestione delle problematiche affidate e devono essergli fornite risorse necessarie all’assolvimento dei compiti.

Viene peraltro visto come consulente interno per i temi privacy.

Posizione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile.

4. Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.

6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

Si conclude con l'articolo che ne definisce l'attività:

Compiti del responsabile della protezione dei dati

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

a. informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b. sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d. cooperare con l'autorità di controllo; e

e. fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

La figura del DPO è già presente sullo scenario internazionale da molti anni come un consulente interno o esterno esperto delle normative e delle problematiche privacy.

Sarà probabile che molte aziende, pur non obbligate ad avere un DPO, si doteranno di una figura con tale incarico destinata a diventare il controller interno del Sistema Privacy.

Per ovvie ragioni è bene evitare di nominare DPO figure come il CIO (responsabile informatico dell'azienda) in quanto si andrebbe normalmente in conflitto di interesse.

Conclusioni

Abbiamo toccato in questo documento i temi principali legati all'adozione da parte di aziende e privati del nuovo regolamento europeo privacy.

Le evidenze riportate ne sottolineano le criticità ed introducono i percorsi che devono essere intrapresi per raggiungere l'obiettivo.

Siamo riusciti a capire come fare per mettersi in regola? Possiamo fare tutto da soli o avvalerci di società di consulenza specializzate in grado di impostare il nostro Sistema.

Inoltre è indispensabile investire in un software di qualità, capace di gestire tutti gli aspetti del rischio privacy, dotato di una interfaccia semplice da utilizzare e che permetta la condivisione del dato, disponendo di un sistema documentale integrato, di comunicazione automatica e di alerting e di un completo ambiente di reportistica ad ogni livello.