OGGETTO: Circolare 13.2018 **Seregno, 2 maggio 2018**

NUOVO REGOLAMENTO PRIVACY – GDPR

Il **GDPR** (General Data Protection Regulation) è il nuovo regolamento n. 2016/679 con cui si opera l'armonizzazione della regolamentazione in materia di protezione dei dati personali nella Ue. **Le disposizioni entrano in vigore il 25 maggio 2018.**

Il Regolamento crea una regola unica europea. È un atto direttamente applicabile, quindi di per sé non necessita di recepimento dal nostro ordinamento. È lacunoso in alcune parti e in altre lascia un certo margine agli Stati membri nella definizione di talune regole. Rimangono ancora in vigore quelle parti del codice della privacy D.Lgs 196 2003 ed altre se non superate dalle norme del Regolamento.

Abbiamo realizzato una sintesi della nuova normativa sulla Privacy, ricordando che la stessa dovrà essere ancora integrata dal legislatore nazionale in forza della legge delega n. 163 del 25 ottobre 2017 che non ha ancora avuto riscontro normativo.

Si sottolinea come le imprese si avvicinano a questo importante passaggio senza chiarezza normativa e purtroppo – da quanto filtra dalla stampa specializzata - senza lasciare spazio a proroghe o a una sospensione temporanea delle sanzioni.

Cosa cambia nella nuova privacy

Una delle principali modifiche che si reputa sottolineare è la scelta di sostituire gli adempimenti formali previsti dal "codice sulla tutela dei dati personali" (D. Lgs. n. 196/2003) con quelli ben più rilevanti, mirati ad introdurre una forma di **responsabilizzazione** (accountability) preventiva a chiunque si occupi del trattamento dei dati personali.

Cioè, viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative e alla luce di alcuni **criteri** specifici indicati nel regolamento. Viene chiesta l'adozione di comportamenti tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.

Sensibilmente accresciute risultano poi le garanzie relative all'informativa e al consenso.

I nuovi "criteri" del regolamento Privacy

Privacy by design e by default

La prima novità caratterizzante il nuovo Regolamento Privacy è sintetizzato dall'espressione inglese "data protection by default and by design" *(art. 25)*, ossia dalla necessità di **configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati**. Tutto questo deve avvenire prima di procedere al trattamento vero e proprio dei dati e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari, che deve sostanziarsi in una serie di attività specifiche e dimostrabili. Così i sistemi informativi e i programmi informatici devono essere configurati con una progettazione che riduca al minimo l'utilizzazione di dati personali e di dati identificativi.

Data protection impact assessment

Un altro criterio individuato nel regolamento e finalizzato a consentire al Titolare del trattamento di dimostrare di aver rispettato la disciplina vigente è la c.d. **Valutazione d'impatto privacy**, ossia la valutazione del rischio inerente al trattamento. Cio è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione *(artt. 35-36).* All'esito di questa valutazione di impatto, il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale.

Accountability

E' il principio secondo quale **il titolare del trattamento è responsabile** per l'applicazione dei principi contenuti nel GDPR e deve essere in grado di dimostrare che le operazioni di trattamento vengono effettuiate in conformità alla nuova disciplina. Quali:

- valutare l'impatto del rischio di perdite di dati, di accesso abusivo,
- predisporre: un registro dei trattamenti (obbligatorio per le aziende con più di 250 dipendenti), in cui indicare i titolari e i responsabili del trattamento, e le misure di sicurezza dei dati; un data protection impact assessment (DPIA) per misurare impatto e conseguenze (sugli interessati) dei nuovi strumenti; l'organigramma privacy per chiarire ruoli e gerarchie nella gestione dei dati;
- prevenire le violazioni dei dati personali,
- nominare: un responsabile del trattamento (Rdp) con facoltà di nominare un subresponsabile (delle cui violazioni risponde il responsabile); un responsabile della sicurezza dei dati (il Dpo, obbligatorio per la PA) che deve operare in piena indipendenza e in assenza di conflitti di interesse, anche sulla base di un contratto di servizio;
- dimostrare l'idoneità delle misure di sicurezza adottate.

Struttura del Regolamento Ue 679/2016

Capitolo	Articoli
1 Disposizioni generali	1-4
2 Principi	5-11
3 Diritti dell'interessato	2-23
4 Titolare del trattamento e responsabile del trattamento	24-43
5 Trasferimenti di dati personali verso Paesi terzi o organizzazioni internazionali	44-50
6 Autorità di controllo indipendenti	51-59
7 Cooperazione e coerenza	60-76
8 Mezzi di ricorso, responsabilità e sanzioni	77-84
9 Disposizioni relative a specifiche situazioni di trattamento	85-91
10 Atti delegati e atti di esecuzione	92-93
11 Disposizioni finali	94-99

Il Regolamento è preceduto da 173 «considerando», che hanno solo un **valore interpretativo**, mentre va **escluso** un loro carattere **normativo.** La Corte di Giustizia ha avuto modo di spiegare che, se il corpo del testo non fosse chiaro o fosse impreciso, l'interprete può fare riferimento ai considerando, fermo restando la loro cedevolezza rispetto al testo dell'articolato, laddove difforme.

Principali definizioni (Articolo 4) Ai fini del regolamento si qualificano come

«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;

«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;

«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;

«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico

«**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;

«**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;

«**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;

«dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione
«**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
«**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
«rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

Inoltre ai sensi della ancora vigente normativa privacy
«incaricati»: le persone fisiche **autorizzate** a compiere **operazioni** di **trattamento** dal titolare o dal responsabile (art. 4, co. 1, lett. h), Codice Privacy)
«amministratore di sistema»: Le persone fisiche autorizzate a compiere **operazioni** di **trattamento** dal titolare o dal responsabile (Garante della Privacy, prot. 27.11.2008 – doc. web n. 1577499)

Trattamento dati personali - Principi generali (articolo 5)

Sono le regole a cui devono attenersi i titolari e i responsabili nel trattare i dati. Sono princìpi che, disciplinando lo svolgimento del trattamento, assicurano che i dati vengano usati legittimamente.
Liceità, correttezza e trasparenza sono le (prime) parole d'ordine per un valido trattamento, che può pertanto essere condotto solo se fondato su una specifica base giuridica di liceità e purché l'interessato sia debitamente informato di quali dati verranno trattati; come, perché, dove e chi li tratterà.
I dati oggetto di trattamento devono poi essere **adeguati, pertinenti e limitati** a quanto necessario alle finalità per le quali sono trattati (è la **minimizzazione**). Il titolare deve assicurare che non vengano impiegati dati eccedenti e non necessari al perseguimento delle finalità di trattamento: ove possibile, deve sempre preferirsi l'uso di dati anonimi, che non consentono la re-identificazione degli interessati.
I dati devono essere sempre **esatti** e **aggiornati** per prevenire rischi di falsa rappresentazione dell'identità: perciò sono riconosciuti all'interessato i diritti di rettifica e cancellazione dei propri dati. La conservazione dei dati dovrebbe poi essere limitata nel tempo e i dati dovrebbero essere cancellati (o anonimizzati) una volta perseguite le finalità di trattamento. Infine, chiunque effettui un trattamento di dati sarà tenuto ad **adottare idonee misure di sicurezza**, tali da garantire l'integrità e la riservatezza dei dati: in tal modo, si mira a scongiurare o, perlomeno, a mitigare il rischio di trattamenti non autorizzati o illeciti, perdita, distruzione e danni accidentali.
Il Regolamento, come il vigente Codice privacy, **non è invece applicabile al trattamento dei dati riferibili esclusivamente alle persone giuridiche**. La persona giuridica è un soggetto di diritto autonomo diverso dalla persona fisica. A titolo esemplificativo, si può trattare di una srl, di una spa o, ancora, si può trattare di una fondazione o di un consorzio.

Ciò significa che gli adempimenti previsti dal Regolamento non si applicano ai dati esclusivamente riferibili al bilancio delle società, né ai dati relativi alla sede o di contatto dell'impresa.

Informativa dell'interessato (articolo 13)

Al soggetto di cui tratta i dati personali (interessato), il Titolare deve fornire, prima dell'acquisizione dei dati stessi, una "**informativa" concisa, trasparente, univoca ed intellegibile** in modo da consentire al soggetto di conoscere le ragioni della richiesta.
Se, nella maggior parte dei casi, la raccolta di un consenso non è obbligatoria, l'informativa è un adempimento imprescindibile: occorre far sì che il soggetto cui i dati si riferiscono - l'interessato - e i cui dati stanno per entrare nelle attività dell'azienda (il suo server, i suoi computer o i suoi archivi) sia sempre informato di come quei dati saranno trattati, per quali fini, con che modi e tempi e, soprattutto, quali siano i diritti esercitabili su quei dati e nei confronti di chi.

L'informativa (disciplinata nello specifico dagli artt. 13 e 14 del regolamento) deve essere fornita all'interessato prima di effettuare la raccolta dei dati.
Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta.

L'art. 13 del Regolamento europeo prevede, secondo un ordine logico, gli elementi dell'informativa, dividendoli in **due blocchi**: il primo lo potremmo definire un "blocco essenziale", il secondo un blocco che mira a portare ancora più trasparenza nel trattamento.
Il primo blocco di "contenuti" deve includere l'identità e i dati di contatto del **titolare** del trattamento e, ove applicabile, del suo **rappresentante**, i dati di contatto del **responsabile** della protezione dei dati (nel caso sia previsto), le **finalità** del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento, gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali, l'intenzione del titolare del trattamento di trasferire dati personali a un Paese terzo o a un'organizzazione internazionale.
Un secondo blocco, ancora più descrittivo e ai fini di rendere il trattamento ancora più trasparente, obbliga ad indicare, nell'informativa, il **periodo di conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo, l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'**accesso** ai dati personali e la **rettifica** o la **cancellazione** degli stessi o la limitazione del trattamento che lo riguardano o di **opporsi** al loro trattamento, oltre al diritto alla **portabilità** dei dati, il diritto di proporre **reclamo** a un'autorità di controllo, se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati e l'esistenza di un processo decisionale automatizzato, compresa la profilazione e informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
In caso di trasferimento dei dati, sul nuovo titolare incombe l'obbligo di fornire, entro 30 giorni, una nuova informativa che contenga oltre a tutte le informazioni inerenti il trattamento anche l'indicazione della fonte dei

dati e quindi del titolare che li ha ceduti: «l'interessato ha sempre il diritto di conoscere anche il soggetto dal quale sono stati acquistati i dati».

Consenso dell'interessato (articoli 7-8)

Il consenso deve essere liberamente fornito dall'interessato, e **deve essere specifico, esplicito, informato ed inequivocabile** deve essere antecedente rispetto al trattamento dei dati personali.
Deve essere prestato da persone di età non inferiore a 16 anni, limite che - se non superato - impone il consenso dei genitori o di chi ne esercita la potestà.
Per i dati "sensibili" (articolo 9 del regolamento) il consenso deve essere "esplicito".
Non è ammesso il consenso tacito o presunto, per cui, anche se non è necessario che il consenso sia "documentato per iscritto" va dimostrato, in ogni caso, che l'acquisizione del consenso è stata fatta in modo "tangibile".

Uno dei diritti più importanti correlati al tipo di dato, ossia il consenso**,** è ben delineato dal Considerando n. 32. La norma dice, infatti, che il **consenso deve essere espresso mediante un atto positivo inequivocabile** attraverso il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile (appunto) di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale.
Nella società tecnologica, il conferimento del consenso con simili modalità potrebbe comprendere la selezione di un'apposita casella in un sito web, o qualsiasi altra dichiarazione o comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto.
Al contrario, non dovrebbe configurare consenso il **silenzio**, l'**inattività** o la **preselezione di caselle**.
Ci sono circostanze equivalenti al consenso, che consentono di trattare i dati personali indipendentemente dall'intervenuta acquisizione del consenso stesso. Ad esempio, il trattamento è legittimamente effettuato se necessario per l'esecuzione contrattuale di un contratto di cui l'interessato è parte. Oppure quando il trattamento dei dati sia funzionale all'adempimento di un obbligo legale.
L'aspetto principale di ogni legittimo trattamento rimane il consenso validamente prestato dalla persona, quindi libero, consapevole e informato. La persona ha il diritto di modificarlo e revocarlo in qualsiasi momento e prestarlo esclusivamente mediante un atto positivo ed inequivocabile da esprimersi per ogni specifica e singola finalità di utilizzo.
Il titolare deve essere in ogni momento in grado di dimostrare che l'interessato abbia consapevolmente acconsentito al trattamento, che il consenso sia stato validamente espresso,
Affinché il consenso sia validamente prestato è necessario che il titolare fornisca un'informativa completa relativa al trattamento, in cui dovrà esser contenuto il **periodo di conservazione del dato**, ossia il termine entro il quale lo stesso sarà cancellato.
Tale novità normativa è di importante impatto sul "sistema impresa": basti pensare anche solo agli archivi delle piccole aziende che vengono quotidianamente alimentati con preventivi e anagrafiche di possibili clienti, e che con l'entrata in vigore della norma potranno esser conservati esclusivamente per il termine indicato, spirato il quale il "dato" dovrà esser eliminato e con esso informazioni indispensabili nella prosecuzione dell'attività.

Il titolare del trattamento dati.

Il titolare del trattamento dati, come definito in precedenza, deve designare il responsabile dell'attività, formare il personale coinvolto e, se dovuto, nominare il "DPO". Deve altresì assicurarsi del costante rispetto di quanto stabilito dal Regolamento europeo in materia di «privacy.

Il DPO (Data Protection Officer - Responsabile della protezione dei dati) è un professionista con conoscenze specialistiche della normativa e delle prassi in materia di protezione dati. Normalmente è facoltativa la nomina ad eccezione dei seguenti tre casi: (i) quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico; (ii) quando i trattamenti consistono e richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; (iii) quando il trattamento riguarda, su larga scala, dati sensibili o relativi a condanne penali e reati.

Responsabilita' del titolare del trattamento. Il titolare del trattamento deve mettere in atto tutte le cautele necessarie per assicurare la protezione dei dati nonché definire i costi necessari per garantire la assenza di rischi relativi al mancato rispetto dei diritti e delle libertà delle persone fisiche.

Rischi da tenere in evidenza. Per individuare un adeguato livello di sicurezza, il titolare deve prendere in considerazione, relativamente ai dati raccolti, i possibili rischi legati a distruzione, perdita, modifica indebita, divulgazione non autorizzata, accesso accidentale o illegale, ovvero tutto quanto possa generare un danno o una violazione dei dati personali (trasmessi, conservati o comunque trattati).

Misure di sicurezza da adottare. Il titolare e il responsabile del trattamento dati dovranno procedere alla valutazione preliminare, caso per caso, dei possibili rischi e di conseguenza individuare ed implementare tutte le misure tecniche ed organizzative che garantiscano la assoluta sicurezza.

Nel GDPR, la sicurezza delle informazioni personali non si limita più a un elenco di strumenti tecnici di salvaguardia, ma si assiste a nuovi adempimenti di natura sostanziale ad un approccio che tiene continuamente conto del principio dell'***accountability*** già specificato in precedenza.
Nella pratica, questo vuole dire che la singola misura di sicurezza si inquadra in una struttura coordinata per la protezione dei dati personali. Esso serve a: (i) prevenire casi di violazioni di dati e minimizzare gli effetti nocivi in ipotesi di *data breach*; (ii) abbatte il rischio laddove – in base alla valutazione d'impatto (Dpia) - questo si presuma elevato; (iii) tutela il flusso di dati nella filiera con le terze parti e nella trasmissione degli stessi all'estero; (iv) contribuisce a dimostrare la conformità dell'azienda alla norma.

Spetta all'impresa di selezionare le misure ritenute adeguate – per qualità e tipologia - al contesto. Il legislatore prende in considerazione: (i) misure di natura tecnica cioè i tipici strumenti della protezione informatica (negli ambiti della rete, delle postazioni, delle applicazioni It) o fisica (nell'ambito della logistica); (ii) misure di natura sia organizzativa che riguardano le politiche contenenti le regole comportamentali di dipendenti e collaboratori nella gestione dei dati, le procedure standard da seguire nelle specifiche circostanze, i ruoli assegnati al personale e le istruzioni impartite, i vincoli contrattuali sottoscritti con le terze parti.

Con riferimento alle singole misure, il Regolamento non ne prevede di tassative ma certo ne mette in risalto due per la loro intrinseca duttilità: la **pseudonimizzazione** e la **cifratura**.
A nostro avviso, strumenti quali la crittografia e la pseudonimizzazione dovrebbero diventare "quotidiani", ossia non dovrebbero esistere dati trattati in azienda che non siano cifrati. Questo perché, nel quadro di minacce tecnologiche attuali, la crittografia è uno strumento davvero molto efficace per garantire la protezione delle informazioni.
Un buon sistema crittografico si basa anche, ovviamente, sulla **segretezza della chiave** (o password) necessaria per cifrare e decifrare le informazioni, un aspetto essenziale per tutto il meccanismo.

Si riepilogano le principali azioni da seguire e le misure di sicurezza da adottare per garantire un livello di sicurezza adeguato.

- In primo luogo occorre **mappare i "trattamenti"**: se il registro dei trattamenti prescritto dall'articolo 30 del GDPR sarà sufficientemente dettagliato, si potrà partire da lì.
- Quindi, occorre effettuare una **valutazione del rischio associato** a ciascun trattamento al fine di individuare tipologia del rischio e suo livello d'incidenza;
- infine, si rende necessario identificare quali **misure si ritengono appropriate «per garantire un livello di sicurezza adeguato al rischio»** applicando un corretto bilanciamento tra strumenti di tutela di natura tecnica e misure organizzative.

La misura di sicurezza appropriata riguardo ad uno specifico trattamento, tenuto conto delle sue caratteristiche, sarà quella che sarebbe ragionevole adottare, in termini di costi e di sviluppo tecnico, per fare fronte al rischio individuato.

DPIA – Valutazione d'impatto (Articolo 35).

La valutazione d'impatto sulla protezione dei dati o DPIA (acronimo di Data Protection Inpact Assessment). consiste in un'attività da svolgere prima di procedere al trattamento dei dati, dal **titolare** del **trattamento, ogniqualvolta possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche titolari dei dati trascritti.**
La valutazione avrà ad oggetto: (i) la **descrizione** dei **trattamenti** che si prevede saranno svolti; (ii) le **finalità** del trattamento; (iii) l'**interesse legittimo** per il quale il **titolare** effettua i trattamenti; (iv) la valutazione della **necessità** e della **proporzionalità** del **rischio** per i diritti e libertà dei soggetti interessati; (v) le **misure** di **sicurezza** e le **garanzie** da adottare.

Nel caso in cui dalla valutazione preventiva si evinca un **rilevante rischio** conseguente al trattamento e si sia in assenza di misure volte a contrastarlo, il titolare interessato è **tenuto** a **chiedere consulto** al **Garante** prima di dare inizio al trattamento stesso. Non è richiesta una forma specifica per la predisposizione di una DPIA, pertanto ai titolari è concessa una grande flessibilità.

Non è richiesta l'effettuazione di una DPIA nelle seguenti circostanze: (i) Quando il trattamento non è tale da presentare un rischio elevato per i diritti e le libertà delle persone fisiche; (ii) quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto.

Registro delle attività di trattamento (articolo 30)

L'**obbligo** del Registro è previsto anche per le imprese aventi **meno** di **250 dipendenti** qualora il trattamento: (i) presenti un **rischio** per i diritti e le libertà del diretto interessato; (ii) **non** sia **occasionale** e includa **dati personali sensibili**, **sanitari**, sulla **vita**, sulla **storia giudiziaria** passata, sull'**orientamento sessuale**, su dati **biometrici** o **genetici.**

L'obbligo, in sé, consiste nell'attività di **conservazione** dei documenti di tutti i trattamenti dei dati realizzati di cui si è titolari o responsabili. I **dati da conservare** riguardano: (i) l'indicazione delle **informazioni** relative al **titolare** del trattamento; (ii) lo **scopo** del trattamento dei dati; (iii) la **tipologia** di **soggetti interessati** e di **dati personali**; (iv) l'indicazione dei **soggetti destinatari** delle **informazioni** raccolte; (v) i **trasferimenti** delle informazioni personali verso un **paese terzo** o un'**organizzazione internazionale** con evidenza delle garanzie necessarie; (vi) l'indicazione dei **termini** entro i quali si prevede l'**eliminazione** dei dati; (vii) l'indicazione delle **misure** di **sicurezza tecniche** e **organizzative**.

Codici di condotta, certificazioni e formazione del personale (articoli 40 - 42)

Il titolare può dimostrare la conformità dei propri trattamenti aderendo ad un codice di condotta (redatto da una associazione o altri organismi rappresentanti le categorie di titolari ai sensi dell'art. 40 del Regolamento) o ad un meccanismo di certificazione tra quelli istituiti al fine di dimostrare la previsione di garanzie appropriate per le operazioni cui si intende procedere.

Il titolare e il responsabile del trattamento devono far sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare medesimo con formazione diretta o effettuata per il tramite di realtà specializzate.

Altre novità del Regolamento

Il GDPR arricchisce l'elenco dei diritti degli interessati aggiungendo: **Il diritto all'oblio** che consente all'interessato di domandare al titolare del trattamento la cancellazione dei dati dallo stesso detenuti in presenza di particolari condizioni: (i) quando il trattamento non sia lecito, (ii) quando i dati trattati esuberino rispetto al perseguimento delle finalità di trattamento, (iii) nel caso in cui abbia revocato il consenso o abbia esercitato il diritto di opposizione al trattamento, (iv) se è necessaria per adempiere ad un obbligo di legge.

Il diritto di limitazione riconosce all'interessato la possibilità di richiedere la sospensione momentanea di ogni trattamento dei propri dati.

Il principio di trasparenza, con il quale si prevede infatti che l'informativa debba essere chiara, trasparente, concisa e fornita all'interessato, di regola, in forma scritta. Ai fini, ad esempio, di una maggiore comprensibilità, il GDPR prevede la possibilità di utilizzare icone standardizzate.

Viene stabilito che il titolare debba dare un riscontro all'interessato entro un mese dalla richiesta, anche in caso di diniego. Può essere tuttavia concessa un'eventuale proroga, fino a tre mesi, per la risposta definitiva in caso di particolare complessità o di elevato numero delle richieste.

Sanzioni (articoli 83 – 84)

Assolutamente eccessive e sproporzionate sono le sanzioni da applicarsi in caso di omissione o inesattezze, soprattutto per le piccole e medie aziende.
Non c'è un minimo, e ci si augura una riduzione delle stesse da parte dei singoli Stati, a norma dell'art. 84 del Regolamento.
Con la normativa vigente Il rischio sarà di **10 milioni di euro,** ad esempio, per violazioni in tema di offerte commerciali e consenso di minori (articolo 8), tenuta del registro delle attività (articolo 30), misure di sicurezza del trattamento (articolo 32), certificazione (articolo 42). Il rischio massimo sarà invece di **20 milioni di euro**, ad esempio, per i principi base del trattamento (articoli 5-7 e 9) per il trasferimento dei dati in un Paese terzo (Capo V) o per l'inosservanza di un ordine dell'autorità di controllo.

Lo Studio è in grado di assisterVi per la gestione degli adempimenti in materia di privacy e rimane a disposizione per ulteriori chiarimenti.

Studio Commercialista Associato Contrino