LA PAURA DELLA NUOVA DISCIPLINA SULLA PRIVACY

Vediamo in questo scritto cosa introduce di nuovo la normativa della privacy facendo una breve panoramica introduttiva sulla disciplina che entrerà in vigore il 25 maggio 2018.

LA PAURA DELLA NUOVA DISCIPLINA SULLA PRIVACY

INTRODUZIONE

Voglio iniziare subito con una premessa e cioè dirti che questa breve guida non ha il carattere della completezza né vuole averlo.

E' un primo sguardo sulla normativa che entrerà in pieno regime questa settimana e quindi un primo sguardo a chi è digiuno su un argomento che sta destando non poche paure e preoccupazioni per chi sarà soggetto alla legge sulla privacy.

Infatti non è un segreto che la nuova normativa sulla privacy stia creando un allarmismo generale anche se non ha introdotto nulla di nuovo sotto il sole perché il GDPR era già stato recepito nel 2016.

Ma allora perché questa paura?

Semplicemente perché si annusa nell'aria che questa legge è una trappola per elevare sanzioni e non perché possa servire di fatto a qualcosa.

Qualcuno mi dovrebbe spiegare perché quando la privacy la trattiamo noi

LA PAURA SULLA NUOVA DISCIPLINA DELLA PRIVACY

Il 25 maggio 2018 entra in vigore la nuova normativa in materia di privacy. Diversi sono i nuovi incombenti che la disciplina impone. Da un lato la percezione che si ha quella di una norma studiata per fare cassa e cioè per sanzionare chi non si mette regola e non tanto per una reale necessità.

StudioLegaleBartolini

privati se magari hai tenuto la chiavina usb non criptata e sulla scrivania sei a rischio di sanzione e poi vai nei Tribunali e nei corridoi, dalla stanza delle udienze esce la cancelliera urlando: " Rossi Mario, Rossi Mario, procedimento penale n……"

Beh ……di privacy qui non se ne parla e non se ne parla ancora quando trovi abbandonati nei Tribunali i fascicoli che li potresti portare via tranquillamente e farli sparire o la bacheca ove accatastati su di un tavolo (perché nella bacheca non vi stanno più) vi sono centinai di atti consultabile anche da chiunque.

Ma siccome in Italia non sanno più cosa tassare troviamo queste trappole per levare soldi ai lavoratori.

A questa affermazione si potrà replicare che Noi (inteso come Italia) siamo stati costretti da una normativa europea e questo è anche vero ma purtroppo la normativa nasce sotto altre stelle e cioè sotto una normativa che ha altri principi e regole rispetti alla nostra, mi riferisco alla Common Law

La nuova normativa si rivolge a tutti i soggetti (anche extra UE) che offrono servizi ai cittadini UE.

AMBITO DI APPLICAZIONE DEL GDPR

1) Trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento

nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione

2) Trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: indipendentemente dall'obbligatorietà di un pagamento dell'interessato: oppure il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

3) Trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

Le novità principali di questa normativa, è bene dirlo subito, riguardano in particolar modo le aziende.

L'ambito della normativa è quello Europeo ma si applica anche al cittadino europeo che sposta i propri affari all'estero.

In generale il trattamento deve essere disposto da soggetti titolari di partita iva e quindi non riguarda le persone fisiche in sé considerate.

Per trattamento si intendono tutte le fasi dalla registrazione, lavorazione, archiviazione ecc.

Per trattare un dato personale di una persona fisica è necessaria la presenza di queste **6 condizioni di liceità:**

- consenso

- esecuzione di un contratto
- adempimento di obbligo legale
- salvaguardia di interessi vitali
- esecuzione di un compito di interesse pubblico
- esistenza di legittimo interesse del titolare.

Il GDPR nasce come accennavo prima, come norma europea e subisce in particolar modo l'influenza del Common Law circostanza che si evince dalla lettura della norma contenente non comportamenti standardizzati a cui consegue una sanzione né una tassatività di comportamenti: ovviamente però la sanzione c'è ma non a fronte di un comportamento certo!

Questo potrebbe aprire un dibattito come dicevo sulla vera funzione della norma che fa supporre (ma questa è semplicemente una mia opinione personale) un sistema volto più a sanzionare nel caso di controlli che a dare elementi certi ed utili .

Il trattamento dei dati sensibili è' vietato a meno che:

1) via sia il consenso dell'interessato: il trattamento è necessario per difendere un diritto in sede giudiziaria

2) Il trattamento è necessario per assolvere ad obblighi specifici del titolare o dell'interessato in materia di diritto del lavoro o sicurezza sociale: il trattamento è necessario per finalità di medicina preventiva

3) Il trattamento è necessario per tutelare interessi vitali dell'interessato qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio

consenso: il trattamento è necessario per motivi di interesse pubblico

4) Il trattamento riguarda dati resi manifestamente pubblici dall'interessato: il trattamento è effettuato da una fondazione, associazione senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, solo per membri ed ex membri.

ATTENZIONE: Consenso e informativa sono due cose differenti!

Consenso: si autorizza a cedere i propri dati personali

Informativa: elencare al titolare dei dati personale quali sono i suoi diritti, come verranno utilizzati i dati ecc.

Questo regolamento europeo è preceduto da una serie di "considerandum" che in parte sono stati considerati cogenti e sono stati scritti per spiegare il perché dell'articolo di riferimento anche se non sono inseriti negli articoli.

I SOGGETTI DELLA PRIVACY

Il titolare del trattamento:

- È il soggetto tenuto all'accountability
- Ha una responsabilità generale sul trattamento dei dati sia se è svolto direttamente da lui sia da terzi per suo conto
- Ha il compito di attuare la privacy by design (cioè dalla progettazione , dal momento in cui incardino il

rapporto tra me e il soggetto di cui tratterò i dati) e by default.

Di base un soggetto titolare del trattamento è colui che gestisce i dati per me.

Accountability è una auto responsabilizzazione ed è da questo concetto che nasce un GDPR diverso dal nostro codice privacy ove si delineavano degli adempimenti ben precisi da svolgere. Il titolare del trattamento deve rispettare la normativa e deve essere in grado di dimostrarlo.

Questa autoresponsaibilità si evidenzia quando, essendo stato oggetto di attacco da parte ad esempio di un hacker, dovrò autodenunciarmi al Garante della Privacy che ha un braccio armato impersonificato nella Guardia di Finanza.

Il titolare del trattamento deve condurre una gap analysis e, nei casi di trattamento a maggiore impatto sui diritti e le libertà degli interessati, condurre un vero e proprio privacy impact assessment.

Si dica che la fumosità del GDPR dovrebbe essere superata da un decreto di imminente uscita che potrebbe risolvere i molti dubbi che la normativa europea porta con sé….speriamo non ne crei di ulteriori!

Ma tornando al titolare del trattamento questi **deve valutare il livello di sicurezza del trattamento:**

il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- la pseudonimizzazione
- la cifrature dei dati personali
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la risilienza dei sistemi e dei servizi di trattamento
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

Nel valutare la sicurezza si tiene conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Art. 24. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora sia necessario. Deve adottare policy adeguate in materia di protezione dei dati personali. 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. Il titolare del trattamento mette in atto misure tecniche e

organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati necessari per ogni specifica finalità del trattamento.

Responsabile del trattamento:

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che **presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate** in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Il responsabile del trattamento è colui che tratta i dati per voi e non con voi altrimenti sarebbe un co-titolare:

- dovrà avere una formazione specifica.
- l'esecuzione di trattamenti su incarico, è regolata da contratto o altro atto giuridico che vincoli il responsabile (comma 3): si indicherà l'oggetto, la durata del trattamento, la natura e finalità del trattamento, il tipo di dati, la categoria di interessati, obblighi e diritti del responsabile.
- E' in pratica l'outsourcer cui si demanda lo svolgimento di alcuni servizi (es. commercialista, cloud, conservazione).

Se usate servizi cloud state utilizzando un outsourcer e dovrete fare un contratto dove nominate il terzo come responsabile esterno e ciò a tutela vostra perché state inviando i dati ad un terzo esterno che deve essere

obbligato agli stessi adempimenti a cui siete sottoposti voi.

Art. 28: Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato. L'accordo per il trattamento dei dati personali deve contenere l'indicazione della natura, durata e finalità del trattamento o dei trattamenti assegnati e le categorie di dati oggetto di trattamento, oltre le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare.

L'incaricato:

è definito dal regolamento quale " Terzo" (c.26) e cioè soggetto identificato come " persone autorizzate al trattamento"; non è definito formalmente, ma disciplinato indirettamente anche in relazione all'obbligo, per il titolare, di indicarli espressamente (ad esempio la segretaria).

In linea di principio valgono le nomine conferite sotto la vigenza della legge nazionale ma è necessario assicurarne la formazione, mentre i nuovi assunti (dopo il 28 maggio 2018) dovranno invece essere incaricati formalmente.

Con - titolare (art. 26):

In caso di condivisione in ordine a finalità e modalità del trattamento, il Regolamento impone ai titolari di definire con uno specifico atto il rispettivo ambito di responsabilità e i compiti con particolare riguardo all'esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente.

Rappresentante (art. 27)

Il titolare o il responsabile non stabilito nell'UE dovrà designare un rappresentante in ITALIA

Sub -responsabile (art. 28)

Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

Amministratore di sistema : figura non prevista espressamente dal Regolamento

Soggetti autorizzati (art. 29)

Il responsabile del trattamento o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri. Pur non prevedendo espressamente la figura dell'incaricato del trattamento (ex art. 30 Codice Privacy) il Regolamento non ne esclude la presenza facendo genericamente riferimento a persone non autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Data Protection Office

Il titolare del trattamento deve nominarlo obbligatoriamente se è:

- un soggetto pubblico
- se è un soggetto pubblico o privato che come attività principale svolte attività implicanti monitoraggio regolare e sistematico di interessati su larga scala
- se è un soggetto pubblico o privato che come attività principale svolge attività implicanti trattamenti di dati particolari e/o dati giudiziari su larga scala

Il DPO o RPO ovvero il Responsabile protezione dati è pertanto il soggetto che viene nominato nel caso siate un ente pubblico, se fate monitoraggio costante e tutti i soggetti la cui attività principale consiste nel

trattamento, su larga scala, dei dati sensibili per fini giudiziari. Il Dpo è in pratica un piccolo garante le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati e deve fare da consulente e consigliere del titolare del trattamento ed è responsabile dei consigli dati essendo una sorta di ponte con il Garante.

Per larga scala si intende:

- numero degli interessati
- quantità dei dati
- durata e permanenza del trattamento
- ambito geografico

Il trattamento dei dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi clienti o pazienti di un medico, legale, commercialista ecc.

IL REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

L'art. 30 del GDPR stabilisce che ogni titolare del trattamento e il suo eventuale rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. La tenuta del registro è indice di una corretta gestione dei trattamenti e permette di tenere traccia delle operazioni di trattamento effettuate e censire in maniera ordinata le banche dati e gli altri elementi rilevanti per assicurare un efficace ciclo di gestione dei dati personali.

Chi è obbligato a tenere il registro?

Obbligo di tenuta del registro non si applica alle imprese o organizzazione meno di 250 dipendenti a meno che il trattamento che effettuano possa presentare rischi per i diritti e le libertà dell'interessato, il trattamento non sia occasionale:

- Il registro può essere tenuto cartaceo o digitale e deve contenere:
- Dati del titolare
- Le finalità del trattamento
- Categoria interessati a categoria dati
- Le categorie di destinatari cui saranno comunicati i dati
- I trasferimenti dei dati ai Paesi Terzi o organizzazione internazionale
- I termini ultimi per la cancellazione dei dati
- Una descrizione generale delle misure di sicurezza tecniche ed organizzative.

L'INFORMATIVA ALL'INTERESSATO

Art. 12 e 13 prevedono l'informativa come strumento della trasparenza. E' necessario fornire all'interessato tutte le informazioni degli articoli 13,14 da 15 a 20 e 32: in forma coincisa, trasparente, intellegibile, accessibile, in modo semplice e chiaro. Informazione date per iscritto.

L'informativa di cui all'art. 13 è quella del soggetto che viene personalmente mentre l'art. 14 riguarda i dati ricevuti da terzi.

Vediamo di dati principali da indicare previsti dall'art. 13 GDPR riguardante l'informativa:

- l'identità e i dati del contatto del titolare del trattamento e, ove applicabile, del suo rappresentante
- i dati di contatto del responsabile della protezione dei dati ove applicabile
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento
- qualora il trattamento si basi sull'art 6, paragrafo 1, lettera f) i legittimi interessi perseguiti dal titolare del trattamento o da terzi
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali
- ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, nel caso di trasferimento di cui all'art. 46 o 47, o all'art. 49, secondo comma.
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione dell'art. 22.

Il consenso dovrebbe poi essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e

inequivocabile di accettare il trattamento dei dati personali che lo riguardano.

MISURE DI SICUREZZA

Secondo quanto previsto dall'art. 32 del GDPR il titolare e il responsabile del trattamento tenendo conto dello stato dell'arte e dei costi di attuazione nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento come anche del rischio, devono adottare le misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Gli adempimenti fondamentali da fare nella immediatezza per le piccole realtà sono:

- Revisione informative
- Nomina responsabili
- Nomina amministratore di sistema
- Adozione del registro dei trattamenti.

Obiettivi e misure adeguate di sicurezza da tenere sotto controllo:

- Dispositivi (inventario di dispositivi autorizzati)
- Software (inventario di software autorizzati)
- Protezione delle configurazioni hardware e software (immagini e backup)
- La vulnerabilità (valutazione e correzione continua)
- I privilegi di accesso a dispositivi e software
- Difese contro i malware

- Copie di sicurezza
- Protezione dei dati

Misure tecnologiche da adottare:

- Firewall
- Sistemi per il monitoraggio dei dispositivi e dei software
- Difesa contro i malware
- Protezione dati
- Log e Ips (Intrusion prevention system)
- Server e sistemi di backup
- Protezione dati (crittografia)
- Log di accessi
- Protezione dei livelli di accesso
- Procedure di disaster recovery
-

DATA BREACH

In caso di violazione dei dati personali a seguito di attacco informatico o anche alternazione dei dati, il titolare del trattamento notifica tale violazione al Garante 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.

La notifica deve descrivere la natura della violazione dei dati personali compresi le categorie e il numero di

interessati colpiti nonché le categorie e il numero di registrazioni dei dati personali in questione; comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto; descrivere le probabili conseguenze della violazione dei dati personali; descrivere le misure adottata o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi.

Il data breach va sempre comunicato all'interessato i cui dati personali sono stati violati eccetto i seguenti casi:

- 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;
- il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevati per i diritti e le libertà degli interessati
- 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.

CONCLUSIONI

Abbiamo percorso le tappe principali della normativa della privacy e vedremo in seguito le applicazioni pratiche sul campo.

Certamente la materia è ancora da approfondire perché questa breve guida ripeto non ha lo scopo di essere un trattato esaustivo ma solo quello di essere un primo sguardo alla normativa tra l'altro in generale in quanto gli obblighi cambiano in base ai soggetti tenuti alla osservazione della norma.

Se avete necessità di una consulenza specifica sull'argomento o se dovete mettere in regola la vostra impresa siamo disponibili a verificare la vostra situazione onde mettere a norma la vostra realtà lavorativa secondo quanto dettato dalla nuova normativa della privacy.

Per info e contatti per la consulenza dovrete semplicemente scrivere una email con i vostri dati al seguente indirizzo.

info@bartolinistudiolegale.com

INDICE

Introduzione	PAG.1
Ambito di applicazione del GDPR	PAG.2
I soggetti della privacy	PAG.5
Il registro delle attività di trattamento	PAG.12
L'informativa all'interessato	PAG.13
Misure di sicurezza	PAG.15
Data breach	PAG.16
Conclusioni	PAG.18