Ultima chiamata per la GDPR compliance: ecco il piano di verifica - Articolo di Valentina Brecevich, 15/05/2019
https://www.altalex.com/documents/news/2019/05/17/ultima-chiamata-per-la-gdpr-compliance-piano-di-verifica

Il 19 maggio 2019 scadrà il periodo di prima applicazione del **Regolamento UE 2016/79** (**GDPR**) in cui il legislatore aveva previsto un periodo di tolleranza circa l'applicabilità delle sanzioni previste dalla normativa.

L'art. 22 co. 13 del **d.lgs. 101/2018** sancisce infatti che "*Per i primi otto mesi dalla data di entrata in vigore del presente decreto, il Garante per la protezione dei dati personali tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento (UE) 2016/679, della fase di prima applicazione delle disposizioni sanzionatorie*".

Tale disposizione lungi dal rappresentare una proroga della piena operatività delle disposizioni del Regolamento europeo, di fatto pienamente applicabile in ogni sua disposizione a partire dal 25 maggio 2018, in realtà ha inteso incidere sull'entità delle sanzioni applicabili, prevedendo una fase intermedia ove l'Autorità di controllo viene invitata a tenere di conto della prima fase di applicazione delle nuove disposizioni.

Ciò comporta che dal 19 maggio 2019 alcuno sconto sarà auspicabile in termini di quantificazione della sanzione amministrativa irrogabile, pertanto eventuali inottemperanze non potranno più trovare un occhio di riguardo circa la relativa considerazione, in ragione del fatto che i destinatari delle disposizioni del GDPR non solo hanno avuto ben due anni per procedere alla implementazione delle misure tecniche e organizzative adottate, ma anche ulteriori 8 mesi successivi all'entrata in vigore del decreto di adeguamento, in cui hanno potuto fruire di una intensa attività interpretativa e chiarificatrice da parte sia del Data European Protection Board, sia del Garante italiano in ordine agli aspetti pratici-operativi delle prescrizioni europee.

Quindi, per chi non avesse ancora adempiuto agli obblighi previsti dalla normativa europea, questa rappresenta un'ultima chiamata all'ordine e una ultima occasione per interrogarsi punto per punto su quali adempimenti sono stati condotti e su quali sussiste ancora necessità di implementazione.

Tra gli spunti che è possibile offrire ai vari soggetti destinatari delle disposizioni del GDPR, siano esse aziende, gruppi societari, pubbliche amministrazioni, professionisti, associazioni o fondazioni, è possibile fornire un piano di audit integrante lo schema delle cosiddette 5 W (*What? «Che cosa?»; Who? «Chi?»; Why? «Perché?»; When? «Quando?»; Where?*

«Dove?») applicata nello stile giornalistico anglosassone e che, lungi dal voler rappresentare il percorso ufficiale per il conseguimento della piena *compliance* dei processi, può tuttavia rivelarsi utile per facilitare il Titolare, o il consulente dallo stesso incaricato, alla compilazione dei registri delle attività di trattamento richiesti all'**art. 30 GDPR**, e alla verifica degli adempimenti necessari relativi a ciascuna fase di vita del trattamento dei dati personali.

Sommario

What? «Che cosa?»

E' di fondamentale importanza capire quali categorie di dati sono oggetto di trattamento. Per dato personale di intende "*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*" (**art. 4.1 GDPR**).

L'informazione riferibile ad una persona fisica può avere gradi di "sensibilità" diverse, in quanto diverso è vicinanza della stessa alla sfera più intima della persona. Per questo il Regolamento europeo individua tra i dati personali in senso lato i **c.d. dati particolari (art. 9 GDPR)**, ossia "*dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*", e i "***dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza***" **(art. 10 GDPR).** L'importanza di identificare correttamente la natura del dato che si sta trattando attiene in primo luogo alla **corretta individuazione della base giuridica che ne legittima il trattamento**. I dati personali che non rientrano nelle categorie di cui agli **artt. 9 e 10 GDPR** possono essere trattati se a fondamento del loro utilizzo sussiste, alternativamente, il consenso dell'interessato, la necessità di dar seguito ad un obbligo contrattuale o precontrattuale, l'esecuzione di un obbligo di legge, un legittimo interesse del Titolare, la salvaguardia di interessi vitali dell'interessato o di altra persona fisica, e, infine, l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. I dati che

invece rientrano nella categoria dei dati "particolari" possono essere trattati solo in presenza delle condizioni elencate all'**art. 9 GDPR**, tra le quali figurano ad esempio il consenso esplicito dell'interessato, la necessità ad assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale o i casi in cui il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria.
Mentre invece il trattamento dei dati di cui all'**art. 10 GDPR** può avvenire solo in presenza del consenso dell'interessato e comunque soltanto sotto il controllo dell'autorità pubblica, oppure solo nei casi in cui il trattamento sia autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

Why? «Perché?»

Alla domanda di cui al punto che precede è possibile fornire una risposta esaustiva solo se la stessa risulta rapportata al **principio di finalità**. Non basta essere consapevoli della natura dei dati trattati, bensì anche del "perché" questi dati sono utilizzati e, quindi, quale sia la finalità perseguita.
Una volta individuato il motivo, ossia la "*ratio*" di trattamento, il Titolare potrà:

- **verificare che sussista una idonea base giuridica del trattamento (vedi voce What? «Che cosa?»);**
- **valutare la proporzionalità e la necessità dei dati richiesti rispetto allo scopo perseguito.**

A titolo esemplificativo è possibile richiamare il "*Parere sul disegno di legge recante interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo*" reso in data 11/10/2018 doc. web. 9051774. In questo provvedimento il Garante sottolinea come l'utilizzo di sistemi di identificazione biometrica e di videosorveglianza in sostituzione dei diversi sistemi di rilevazione automatica in uso nelle P.A. non possa prescindere da un giudizio in termini di necessità e proporzionalità in funzione della finalità di repressione del fenomeno dell'assenteismo nelle Pubbliche amministrazioni. Considerazione che ha portato il Garante ad esprimere un parere sostanzialmente positivo, ma con alcune correzioni derivanti dal rispetto dei predetti parametri. In particolare il Garante richiede, da un lato, di limitare la scelta ad un solo strumento di verifica (videosorveglianza o sistemi di identificazione biometrica) evitando quindi un utilizzo congiunto dei due strumenti di rilevazione delle presenze, di fatti non rispondente al principio di proporzionalità; dall'altro di ancorarne l'utilizzo alla sussistenza di specifici fattori di rischio, ovvero a particolari presupposti quali ad esempio le dimensioni dell'ente, il numero dei dipendenti coinvolti, la ricorrenza di situazioni di criticità che potrebbero essere anche influenzate dal contesto ambientale, in mancanza dei quali verrebbe meno il principio di necessità del trattamento.

Who? «Chi?», o meglio chi sono i soggetti coinvolti nel trattamento

In particolare uno dei primi aspetti che devono essere presi in considerazione da parte del Titolare è quello relativo alla obbligatorietà o comunque all'opportunità di nominare un Responsabile della protezione dei dati personali. Il responsabile della protezione dati personali o RDP è un soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo. Coopera con l'Autorità e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali.
Successivamente a tale valutazione preliminare il Titolare, ossia del soggetto che definisce le finalità e i mezzi del trattamento dei dati, è tenuto a verificare se tra i trattamenti dallo stesso realizzati, taluni di essi vedano il coinvolgimento, in tutto o in parte, di soggetti esterni.

Si pensi ad esempio al consulente del lavoro incaricato di svolgere per conto del Titolare tutti gli adempimenti connessi all'instaurazione, gestione e alla cessazione del rapporto lavorativo dei dipendenti, ivi compresa la elaborazione dei dati personali di quest'ultimi e dei rispettivi familiari strumentale alla compilazione dei cedolini paga; o altro ancora si pensi al server provider, che ospita sulle sue macchine i software gestionali che permettono ad un determinato Titolare del trattamento di gestire i rapporti con i rispettivi clienti.

Il Regolamento europeo, all'**art. 28** sancisce che "*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*". In esecuzione della predetta disposizione il GDPR impone al Titolare di formalizzare la decisione di affidare in tutto o parte di un trattamento dati ad un soggetto esterno attraverso un contratto avente forma scritta *che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento"*.
Tra i soggetti coinvolti nel trattamento troviamo anche i **c.d. "incaricati" o "soggetti autorizzati al trattamento"**, che, se pure non specificatamente normati all'interno del GDPR, ricoprono un ruolo ad alto impatto operativo essendo quei soggetti che rappresentano la "mano del Titolare" nelle singole attività di trattamento che vengono condotte su diretta istruzione di quest'ultimo. Per questo motivo, da una lettura congiunta degli **art. 4 co. 10** e **29 del Regolamento**, è possibile dedurre un obbligo di specifica e attenta formazione degli incaricati in ragione delle singole mansioni che gli stessi sono

chiamati ad realizzare. (Es. il dipendente incaricato di riscontrare a mezzo mail le richieste dei clienti dovrà essere informato e formato su tutti i possibili rischi derivanti da un utilizzo scorretto della posta elettronica, tra cui apertura di allegati non attendibili oppure dall'invio di comunicazioni di gruppo in CC piuttosto che in CCN).

When? «Quando?», o meglio: per quanto tempo?

L'individuazione del periodo di conservazione dei dati rappresenta uno dei pilastri fondamentali della normativa di matrice europea per un semplice motivo: il dato conservato oltre il tempo necessario al conseguimento della finalità, o comunque oltre al periodo prescritto dalla legge, è un dato esposto ad un rischio non più giustificabile dalla necessità di un trattamento. Per "*rischio*" deve intendersi uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità per i diritti e le libertà degli interessati, e da cui è possibile che si dia adito a fattispecie discriminatorie, furti o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, o qualsiasi altra tipologia di danno economico o sociale significativo.

Where? «Dove?»

Prima di ogni valutazione in merito alla idoneità delle misure tecniche e organizzative a tutelare il dato personale è fondamentale **individuare l'esatta ubicazione del dato da proteggere**. Una volta chiarito questo passaggio sarà possibile attivarsi per adottare tutte le misure necessarie alla relativa protezione. Se ad esempio i dati personali contenuti nel database aziendale sono tutti materialmente ubicati su un server esterno di proprietà di un server provider, il Titolare dovrà non solo preoccuparsi che le misure dallo stesso adottate siano idonee a proteggere il dato trattato, ma dovrà altresì procedere alla formalizzazione di un accordo scritto relativo alla protezione dei dati collocati sui predetti server esterni.

Altro aspetto rilevante è capire se tra i processi di trattamento individuati, **alcuni di essi prevedono che il dato venga trasferito e/o collocato al di fuori del territorio dell'Unione Europea**. Si pensi ad un server provider le cui macchine sono ubicate fuori dal territorio dell'Unione, o a un gruppo societario composto da società alcune delle quali hanno sede all'estero.

Partendo dal principio che il GDPR si applica «*al 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*» (**Art. 3 co.1**), ben si capisce che il CAPO V del Regolamento intitolato "Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali" mira ad assicurare che il livello di protezione delle persone fisiche garantito dal Regolamento non sia pregiudicato quando, per diverse

ragioni, i dati personali trattati da un soggetto sottoposto alle disposizioni del GDPR, vengono trasferiti fuori dall'UE.
Il GDPR agli **artt. 44 e ss.** detta le disposizioni che devono essere osservate nelle ipotesi suddette al fine di assicurare all'interessato i cui dati sono oggetto di trasferimento il medesimo livello di tutela che gli spetterebbe in base al GDPR qualora i suoi dati fossero trattati nel territorio dell'Unione.
Per questo motivo non solo sarà necessario capire con precisione se i dati trattati sono oggetto di trasferimento, ma anche se quest'ultimo è sorretto da una delle condizioni previste e disciplinate dal Regolamento agli **artt. 44 e ss**.
Sebbene non rispecchiante letteralmente lo schema delle 5W non è azzardato aggiungere anche un ultimo parametro valutativo al nostro schema di check list privacy anche la voce:

How? «Come?»
L'**art. 24 co. 1** è espressione del principio cardine dell'assetto disegnato dal Regolamento europeo, **c.d. principio di accountability**, e statuisce che "*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, 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 necessario*".
Sparisce pertanto ogni riferimento al tradizionale Allegato B del Codice della Privacy, ormai abrogato, in quanto lo scenario delle misure minime di sicurezza non rispecchia più le esigenze attuali. **Il Titolare del trattamento deve adottare misure adeguate ai dati dallo stesso trattati, alle finalità dello stesso perseguite e ai soggetti di volta in volta coinvolti nel trattamento**.
Per questo si rende necessaria una implementazione delle misure tecniche e organizzative adottate per proteggere i dati utilizzati. Implementazione che potrà avere graduazioni diverse a seconda della valutazione personalizzata che ciascun Titolare dovrà adottare circa la sicurezza dei sistemi, perché l'attenzione non si incentra più sul "se si verificherà un tentativo di violazione di dati personali" ma sul "quando si verificherà un tentativo di violazione di dati personali". Per tale motivo il Regolamento "responsabilizza" il Titolare, invitandolo a giocare in anticipo e a premunirsi quanto prima di tutte le misure tecniche e organizzative possibili tenuto conto dello stato dell'arte e dei costi di attuazione.
In pendenza dell'ultimo *count down* non ci resta che sottolineare l'importanza di una analisi preventiva relativa alla mappatura dei processi interni e al livello di rischio connesso a ciascuno di essi. Una corretta e precisa compilazione dei Registri delle attività di trattamento rappresenta sicuramente un ottimo biglietto da visita nei confronti dell'autorità di controllo fornendo alla stessa la possibilità di operare su un terreno già lavorato, incentivando così una prospettiva di cooperazione e reciproca collaborazione.