18 gennaio 2019

Studio Legale

Avv. Giorgio Majocco
Via Roma 3/10
16121 GENOVA
Tel. 010566443
Fax. 010594949
E.mail: avv.giorgiomajocco@yahoo.it
P.E.C.: avvgiorgiomajocco@cnfpec.it

[NOVITA' INTRODOTTE IN MATERIA DI PRIVACY DALL'ENTRATA IN VIGORE DEL REGOLAMENTO UE 2016/679 – G.D.P.R.]

Excursus su come cambia la normativa in materia di trattamento dei dati personali in Italia: principali novità e adempimenti.

Convegno svolto presso ODCEC di Cremona

SLIDE 1

Buonasera,

mi presento anzitutto a Voi.

Mi chiamo Giorgio Majocco e sono avvocato iscritto all'Ordine di Genova, dove svolgo la libera professione da ormai oltre dieci anni nell'ambito del diritto civile e, in particolare, del diritto commerciale all'interno dello Studio Legale dell'Avv. Renato Speciale.

Prima di iniziare, permettetemi di ringraziare gli organizzatori di questo evento: il Vostro Ordine, in persona del Presidente/consigliere_____, che oggi ci ospita nonché BM Italia S.r.l. e l'amico Andrea Martello, in particolare, che mi ha invitato qui nella veste di relatore, per me inedita, con il compito di illustrare, seppure sommariamente le novità introdotte dal Regolamento UE 2016/679, noto con l'acronimo GDPR, ossia General Data Protection Regulation, che tradotto sta per Regolamento Generale sulla Protezione dei Dati.

Quello che cercherò di fare, quindi, sarà delineare un quadro generale delle più significative novità introdotte in materia di privacy, lasciando poi agli amici di BM Trada il compito di addentrarsi maggiormente negli adempimenti e nelle procedure che il Regolamento pone a carico di chi effettui il trattamento di dati personali nonché di illustrarVi le soluzioni operative che sono già state da loro congeniate per aiutare, chi fra Voi lo desideri, ad orientarsi tra i molteplici, nuovi obblighi.

SLIDE 2

Inizierei, allora, con il chiarire velocemente quali siano attualmente le fonti normative vigenti in materia di privacy, appunto.

La prima è indubbiamente rappresentata dal **Regolamento GDPR** entrato in vigore il 25 maggio 2018 (era stata prevista una *vacatio legis* di due anni per consentire ai Parlamenti nazionali di intervenire per tempo sulle proprie legislazioni nazionali, armonizzanole), le cui norme – senza volerVi tediare con una lezione di diritto comunitario che nemmeno avrei la competenza di farvi –

come Voi tutti saprete risultano immediatamente e direttamente applicabili in tutti gli stati membri, dunque senza necessità di venire recepite con leggi nazionali come accade invece nel caso delle direttive. Una direttiva era appunto la n. 46 del 1995, costituente la previgente fonte normativa in ambito europeo ed in forza della quale in Italia era stato emesso il D.Lgs. 196/2003, che ora il Regolamento ha espressamente abrogato.

La seconda fonte è costituita dal **D.Lgs. 196/2003** ovvero ciò che ne rimane, viste le incisive modifiche ad esso apportate dal D.Lgs. 101 approvato l'8 agosto scorso (con molto ritardo rispetto alla legge delega conferita al Governo nell'ottobre 2017 che stabiliva 6 mesi per l'emanazione del Decreto da parte dell'esecutivo, di modo che si potesse giungere all'armonizzazione prima che divenisse operativo il GDPR) ed entrato in vigore il successivo 19 settembre, con cui si è provveduto appunto ad armonizzare, adeguandola, la previgente normativa nazionale – ricordo che il D.Lgs. 196/2003 costituiva il *Codice della Privay* in Italia – al contenuto delle disposizioni del Regolamento GDPR che rappresenta in ogni caso la fonte gerarchicamente superiore e pertanto prevalente in ipotesi di contrasto tra le norme.

La primissima novità conseguente all'avvento del GDPR è dunque quella di essersi determinato il superamento – vedremo meglio in seguito in che termini – del testo che per i passati quindici anni ha costituito il fulcro della legislazione in materia di privacy nel nostro paese.

Visto che non siamo qui per una lezione di stampo accademico bensì per cercare insieme delle soluzioni pratiche su come reggere l'impatto della nuova normativa sulle nostre attività, tanto per accennare soltanto alla portata dell'intervento compiuto sul D.Lgs. 196/2003, Vi basti considerare il fatto che buona parte di tutta la Parte I del testo del vecchio decreto è stata espressamente abrogata, in particolare gli artt. da 3 a 45, facendo venire meno interi Titoli quali il II sui Diritti dell'interessato e, pertanto, l'art. 7 sul Diritto di accesso o l'art.8 sull'Esercizio dei diritti, cosi come il Titolo III che al Capo I contemplava una norma fondamentale quale l'art. 13 concernente

l'informativa, mentre al successivo art. 23 sanciva il dogma del consenso, e ancora i titoli IV e V, quest'ultimo che nel proprio Capo I – di nuovo – stabiliva le misure di sicurezza e cosi i titoli VI e VII.

Tutte norme fondamentali in materia di principi generali sul trattamento dei dati personali che trovano ora nuova collocazione e riferimento all'interno del GDPR.

Sopravvive invece il D.Lgs. 196/2003, seppure emendato in molte sue parti e con ulteriori abrogazioni, nelle proprie Parti Seconda e Terza.

Quest'ultima Parte, la III appunto, era ed è di importanza non secondaria perché contiene parte delle fattispecie sanzionatorie.

Per il regime sanzionatorio occorre fare ora riferimento anzitutto al Regolamento europeo agli artt. 83 e ss. che trattano gli illeciti di natura amministrativa ma anche al vecchio Codice della privacy, all'interno del quale le fattispecie di illecito amministrativo sono state di fatto abrogate, salvo prevedere il nuovo art. 166 adottato in virtù della clausola aperta contenuta nell'art. 84 del GDPR, mentre per quanto riguarda le sanzioni penali è stata lasciata una sostanziale autonomia ai singoli Stati di prevederle, pur nel quadro dei principi stabiliti dal regolamento, cosa che il nostro legislatore ha fatto, riformando ed ampliando le previgenti ipotesi di illecito penale ed abrogandone una, come l'art. 169 perché riguardante le misure di sicurezza che non esistono più – sull'argomento, se vi sarà tempo, tornerò comunque verso la fine del mio intervento.

SLIDE 3

Abbiamo a che fare, dunque, con due fonti normative, tra loro armonizzate che delineano un quadro complesso in cui è possibile rinvenire sicuri **elementi di continuità con il passato** – LI VEDETE ELENCATI - ma anche molte ed interessanti novità.

Analizziamo velocemente, in primo luogo, gli elementi di continuità.

SLIDE 4

Partiamo dal concetto di **DATO PERSONALE**.

Costituisce dato personale, ai sensi del GDPR – LO VEDETE –, *qualsiasi informazione riguardante una persona fisica identificata o identificabile e quindi: il nome ma anche un numero identificativo, l'ubicazione, l'identificativo on-line, come anche uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale e sociale*, con una maggiore specificazione quindi rispetto al Codice della Privacy.

Oltre al concetto di dato personale vengono poi espressamente valorizzate nel GDPR talune peculiari tipologie, per meglio dire categorie, di dati che – lo vedremo in seguito – risultano, utilizzando una vecchia classificazione, "sensibilissime", al punto da prevedersi per essi, lo anticipo, un divieto generale di trattamento salvo non ricorrano specifici requisiti scriminanti per poterli trattare.

Trattasi allora dei **DATI GENETICI**, da intendersi quali dati relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica che forniscano informazioni univoche sulla fisiologia o sulla salute di detta persona *e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione*.

Cosi come è stato precisato il concetto di **DATO BIOMETRICO**, ossia quei dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentano l'identificazione univoca.

Per non parlare, infine, della specifica autonomia riconosciuta ai dati relativi alla salute: quei **DATI ATTINENTI ALLA SALUTE**, appunto, fisica o mentale di una persona, *compresa la prestazione di servizi di assistenza sanitaria*, che rivelino informazioni relative al suo stato di salute; concetto, dunque, potenzialmente molto ampio.

SLIDE 5

Anche il concetto di **TRATTAMENTO** rimane pressoché invariato salvo subire qualche modesto ampliamento.

Se con il Codice previgente esso veniva individuato in qualsiasi operazione o complesso di operazioni effettuate anche senza l'ausilio di strumenti elettronici concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, con l'introduzione del Regolamento per trattamento *dovrà d'ora innanzi intendersi qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati – ma archiviati – e applicati a dati personali o insieme di dati personali ove, quanto alle tipologie di attività, oltre a quelle già enunciate in riferimento al D.Lgs. 196/2003 che restano valide, vengono espressamente incluse* la STRUTTURAZIONE, L'ADATTAMENTO, ma anche QUALSIASI ALTRA FORMA DI MESSA A DISPOSIZIONE , compresa la LIMITAZIONE – concetto che assume nuova portata nel GDPR, lo vedremo.

SLIDE 6

Veniamo quindi ai **PRINCIPI FONDAMENTALI** che già avevamo imparato a conoscere sotto la vigenza del Codice e che ritroviamo anche nel nuovo Regolamento, assieme ad altri di cui dirò in seguito.

Ritroviamo ovviamente quelli di liceità, correttezza e trasparenza ovvero di conformità alle norme, buona fede e consapevolezza.

Ritroviamo anche il principio di minimizzazione dei dati, ossia il dovere di trattare i dati personali in maniera adeguata, pertinente e limitata a quanto necessario rispetto alle finalità per le quali sono trattati.

Certamente vige sempre il principio di esattezza dei dati raccolti che devono necessariamente essere anche tenuti aggiornati, cancellando e rettificando tempestivamente i dati inesatti, sempre rispetto alle finalità per cui i dati sono trattati, così come sempre valevoli sono quelli di integrità e riservatezza, che deve essere sempre garantita impedendo i trattamenti non autorizzati.

Fino a rinvenire un principio in parte nuovo o perlomeno nuovo rispetto all'interpretazione che ad esso veniva attribuita nella vigenza del D.Lgs.

196/2003, sostanzialmente ricondotto ai concetti di pertinenza e non eccedenza...ossia quello di **LIMITAZIONE**: ne ho accennato in precedenza parlando delle tipologie di trattamenti.

Limitazione delle finalità, ma anche Limitazione della conservazione.

Cosa significa allora Limitazione delle finalità: significa che il trattamento deve indicare in maniera chiara ed esplicita la ragione che legittima il trattamento da parte del Titolare – in sostanza perché lo fai – elemento, quello delle finalità, che diviene di tale importanza da divenire esso stesso parametro di legittimità, intimamente legato com'è con altro, nuovo concetto cardine del GDPR quello di "base giuridica", ossia le condizioni al ricorrere delle quali possa ritenersi lecito e quindi possibile il trattamento fra quelle elencate all'art. 6 - lo vedremo meglio in seguito.

Limitazione delle finalità dicevamo quindi ma anche Limitazione della conservazione, come tipologia di trattamento appunto.

Il principio in base al quale i dati che consentono l'identificazione degli interessati debbano essere conservati per un arco di tempo non superiore al conseguimento delle finalità. **ESEMPIO**

SLIDE 7

L'INFORMATIVA abbiamo detto che continua ad essere centrale in materia di privacy ma muta il suo contenuto – LO VEDETE.

Permangono taluni riferimenti indispensabili già contemplati nel Codice della Privacy previgente – vedete i puntuali riferimenti nella colonna al centro – a cui si affiancano **elementi nuovi**.

- Anzitutto circa l'identità e i dati di contatto del Titolare come del Responsabile del Trattamento, a cui si aggiungono – se previsti - quelli del DPO – Data Protection Officer – figura nuova del GDPR, di cui diremo meglio in seguito.
- In merito alle finalità di trattamento e ora anche – lo abbiamo accennato prima – alle basi giuridiche di trattamento ovverosia la condizioni di liceità del trattamento, tra cui vi è il concetto nuovo nella

sua riconosciuta autonomia di “interesse legittimo”, ci torneremo con la successiva slide.

- I destinatari, ovvero il soggetto o la categoria di soggetti a cui i dati personali possono essere comunicati o che possano venirne a conoscenza quali incaricati o responsabili per conto del Titolare, in riferimento ai quali va ora espressamente indicato se i dati saranno oggetto di trasferimenti verso paesi terzi o organizzazioni internazionali – con il divieto di farlo per quei paesi o organizzazioni che non presentino sufficienti garanzie di protezione.
- La possibilità di accedere ai dati per l’esercizio dei diritti di cui al ben noto previgente art. 7 del Codice privacy a cui si aggiungono anche l’indicazione del periodo di conservazione, il diritto di limitazione e quello di revoca del consenso. Vi segnalo fino da ora – con riserva di parlarne più nel dettaglio nel seguito – come tra i vari diritti esercitabili siano ora previsti anche il diritto di oblio e quello di portabilità.
- L’indicazione se il conferimento dei dati sia obbligatorio oppure facoltativo con la specificazione indicazione delle conseguenze previste in caso di diniego, a cui si aggiunge l’indicazione dell’esistenza o o meno di un processo automatizzato o di profilazione nonché la facoltà in ogni caso di potere presentare un ricorso all’autorità di controllo – per noi in Italia il Garante della Privacy – da parte dell’interessato.

SLIDE 8

Infine veniamo al concetto di **CONSENSO**, dapprima pietra miliare della privacy, concetto che esce invece un po’ ridimensionato dal GDPR che prevede ora – lo abbiamo detto già più volte – nuove condizioni di liceità su cui basare – da qui la definizione di basi giuridiche appunto – il trattamento.

Questa, a mio modo di vedere, la seconda grande novità apportata dal GDPR assieme a quella, esaminata all’inizio, del mutamento delle fonti normative.

Ebbene, il consenso resta sempre espressione di una intenzione libera, specifica, informata e inequivocabile di accettare il trattamento, dove il concetto di inequivoco sembra ora non ammettere più spazi di incertezza.

SLIDE 9

A mutare davvero tuttavia non è tanto il concetto di consenso quanto semmai la centralità di esso all'interno del regime della privacy.

A norma dell'**art. 6** del Regolamento divengono **CONDIZIONI CHE RENDONO LECITO IL TRATTAMENTO** non solo il consenso ma anche:

- gli **obblighi derivanti dall'esecuzione di un contratto** o di misure precontrattuali di cui l'interessato sia parte;
- l'**obbligo legale ricadente sul Titolare**;
- **la salvaguardia di interessi vitali dell'interessato**;
- **l'esecuzione di un compito di interesse pubblico o di pubblici poteri**;
- un **legittimo interesse** in capo al Titolare, da bilanciarsi con molta attenzione rispetto alle libertà e diritti fondamentali dell'interessato**,** tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento.

Ci aiuta a comprendere meglio le cose, il considerando n. 47 al Regolamento che chiarisce con un esempio come debba effettuarsi questo bilanciamento specificando come potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente ed appropriata tra l'interessato e il Titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del Titolare del trattamento… In ogni caso, tuttavia, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali: esempio.

Teniamo bene a mente che tali condizioni di liceità devono sussistere – almeno una di esse - per consentire il trattamento dei dati personali "semplici" o c.d. comuni.

SLIDE 10

Da non confondere queste condizioni legittimanti il trattamento di dati per così dire comuni con gli **ulteriori presupposti** contemplati invece all'**art. 9** nel caso di trattamenti che riguardino ***CATEGORIE PARTICOLARI DI DATI***, in qualche modo riconducibili al vecchio concetto di dati sensibili, in ordine ai quali, come già anticipato, vi è un capovolgimento della prospettiva: non dati trattabili al ricorrere di determinate condizioni di liceità, ma dati non trattabili, salvo il ricorrere di determinati presupposti. Per essi dunque è di norma previsto un vero e proprio generale **DIVIETO DI TRATTAMENTO**.

Ai sensi del paragrafo 1, si intendono come "categorie di dati particolari" *quelli che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosifiche, nonché i dati genetici e i dati biometrici intesi a identificare in modo univoco una persona fisica nonché i dati relativi alla salute o all'orientamento sessuale della persona*.

Il trattamento è ammesso e quindi il divieto di trattarli non opera nei seguenti casi previsti al secondo paragrafo dell'art. 9:

lett. a) - qualora l'interessato abbia prestato il **proprio consenso esplicito** al trattamento (di nuovo il consenso, dunque);

lett. b) - quando il trattamento sia **necessario per 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**;

lett. c) - quando il trattamento sia **necessario per tutelare un interesse vitale dell'interessato** o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

lett. d) – qualora il **trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro** che persegua finalità politiche, filosofiche,

religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'estero senza il consenso dell'interessato;

lett. e) – **il trattamento riguardi dati personali resi manifestamente pubblici dall'interessato**;

lett. f) - **il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria** o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

lett. g) – **il trattamento sia necessario per motivi di interesse pubblico** rilevante sulla base del diritto dell'Unione Europea o degli Stati membri;

lett. h) – **il trattamento sia necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità**;

lett. i) – **il trattamento si renda necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici**;

lett. j) – infine, il trattamento sia necessario ai fini di **archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici**.

Il paragrafo 3, specifica poi espressamente che il trattamento di "dati sanitari" (lett. h) può avvenire solo e nella misura in cui il Titolare o il Responsabile siano professionisti soggetti al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti (ossia un medico) o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri.

SLIDE 11

Addentriamoci, allora, un po' meglio nelle tante **VERE NOVITÀ** previste dal Regolamento implicanti un nuovo approccio operativo da parte di tutti noi al mondo della privacy.

Abbiamo cercato qui di sintetizzarle tutta in un'unica slide, LA VEDETE. Volendole leggere una una per una, trattasi dei nuovi concetti di:

- **ACCOUNTABILITY**, principio di nuova elaborazione che permea un po' tutto lo spirito del GDPR;
- del concetto di **PRIVACY BY DESIGN / BY DEFAULT**;
- di quello di **APPROCCIO BASATO SUL RISCHIO**;

concetti, Ve ne spiegherò il contenuto, che portano con sé nuovi adempimenti, quali (li avrete sentiti nominare):

- la **VALUTAZIONE D'IMPATTO**;
- il **REGISTRO DEI TRATTAMENTI**;
- la figura del **DPO**;

ma anche nuovi doveri, in caso di **DATA BREACH**, nuove **DIRITTI, ALL'OBLIO E ALLA PORTABILITÀ** nonché nuove **SANZIONI**.

Analizziamole singolarmente.

Vediamo dunque in cosa consiste il **PRINCIPIO DI ACCOUNTABILITY**, tradotto in Italia con il termine "responsabilizzazione", quindi il principio di responsabilizzazione la cui costante presenza, a prescindere dalla sua enunciazione agli art. 5, 24 e 25 del Regolamento, plasma il contenuto di un po' tutto il GDPR.

Trattasi della condotta che devono osservare gli artefici del trattamento dati che si sostanzia nell'adozione di "*comportamenti pro-attivi tali da dimostrare la comprensione prima e la concreta adozione, poi, di misure finalizzate ad assicurare l'applicazione del regolamento*", questa è al definizione utilizzata dal nostro Garante per chiarire cosa debba intendersi per responsabilizzazione, appunto.

Con la sua previsione, il legislatore europeo, in sostanza, ha voluto compiere un gesto di fiducia nei confronti dei destinatari del Regolamento, al tempo stesso

non esente per loro da responsabilità forse maggiori di prima, affidando proprio al Titolare il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dati dal medesimo posto in essere, ciò evidentemente nel rispetto delle disposizioni normative e alla luce di taluni **CRITERI GUIDA** contenuti nel Regolamento.

Il primo di tali criteri è sintetizzato dall'espressione inglese "***DATA PROTECTION BY DESIGN AND BY DEFAULT***" (art. 25), ossia dalla necessità di configurare il trattamento prevedendo fino dall'inizio (ovvero prima ancora di iniziare il trattamento) le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare così i diritti degli interessati, tenendo altresì conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Tutto questo deve avvenire "a monte", pertanto prima di procedere al trattamento dei dati vero e proprio e richiede pertanto un'analisi preventiva e un impegno applicativo da parte del Titolare che deve concretizzarsi in una serie di **attività specifiche e dimostrabili**.

Tra le attività specifiche e dimostrabili, fondamentali sono quelle concernenti il secondo nuovo, fondamentale criterio individuato nel Regolamento rispetto alla gestione degli obblighi in capo ai Titolari, quello di "**APPROCCIO BASATO SUL RISCHIO**", rischio di trattamento.

Quest'ultimo è da intendersi come rischio di impatti negativi sulla libertà e i diritti degli interessati (Considerando 75 e 77 del Regolamento), impatti che dovranno essere analizzati attraverso un apposito processo di valutazione (artt. 35 – 36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza, perché no) che il Titolare ritiene di apprestare per mitigare tali rischi.

SLIDE 12

Solamente all'esito di questa **VALUTAZIONE D'IMPATTO**, dunque, 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 – si legga il Garante – per ottenere indicazioni su come gestire il rischio residuale.

L'autorità garante, in questo frangente, non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del Titolare e potrà invece, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del Titolare, fino alla limitazione o al divieto di procedere al trattamento.

La comunicazione al Garante, che segua la valutazione d'impatto, è dunque strumento da utilizzare con estrema cura!

Quel che risulta sicuro è che l'intervento delle Autorità di controllo sarà principalmente "*ex post*" ossia si collocherà successivamente alle determinazioni assunte autonomamente dal Titolare e ciò spiega l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla Direttiva CE 95/46 e dal Codice come la notifica preventiva dei trattamenti all'autorità di controllo e il c.d. "*prior checking*" (o verifica preliminare) sostituiti invece da obblighi quali: la **TENUTA DI UN REGISTRO DEI TRATTAMENTI** da parte del Titolare/Responsabile e, appunto, dall'effettuazione della **VALUTAZIONE DI IMPATTO** con eventuale successiva consultazione del Garante.

SLIDE 11 e **13**

Vengono poi introdotti – lo abbiamo già accennato – taluni diritti nuovi con funzioni c.d. di controllo, quali il **DIRITTO ALLA PORTABILITÀ DEI DATI** personali (art. 20), che si esplica attraverso la possibilità riconosciuta in capo all'interessato di richiedere il trasferimento dei propri dati da un titolare del trattamento ad un altro, fatta espressa eccezione per gli archivi pubblici o per Titolari che si trovino in paesi extra UE che non rispettano standard di sicurezza sul trattamento dati. ESEMPIO (cambio di fornitore).

Così come viene introdotto il **DIRITTO ALL'OBLIO** (art. 17) che è qualcosa di più della semplice cancellazione già prevista nel passato e che si sostanzia nelle richiesta di cancellazione rivolta ad un Titolare che abbia reso pubblici i dati e

che importa per quest'ultimo l'obbligo di trasmettere la medesima richiesta anche a tutti coloro che li utilizzino.

ESEMPIO. Albi Ordine? ---archivio pubblico.

SLIDE 11

Mi avvio verso al conclusione, per dirVi che è stato infine previsto, tra le novità, il cosiddetto "***DATA BREACH***", consistente in tutti quegli eventi in occasione dei quali scatta l'obbligo in capo al titolare del Trattamento o del Responsabile da questi delegato di comunicare eventuali "violazioni" dei dati personali al Garante, ove per violazioni debbono intendersi: la perdita, fisica informatica, parziale o integrale, ma anche la sottrazione (fenomeni di pishing, di hackeraggio della rete), così come il danneggiamento, ad esempio per effetto di un virus e così via…da qui l'importanza di software ormai indispensabili che permettano il backup, la recovery dei dati ecc.

In tutte queste evenienze, oltre ad informare l'autorità di controllo, il Titolare dovrà anche decidere se informare o meno dell'evento anche tutti gli interessati coinvolti, a seconda che la violazione dei dati rappresenti oppure no una elevata minaccia per i diritti e le libertà delle persone coinvolte a meno non dimostri di avere già adottato idonee misure di sicurezza o, ancora, a meno che adempiere al dovere di informare gli interessati comporti uno sforzo sproporzionato al rischio.

SLIDE 11

Due parole, infine, sul **DATA PROTECTION OFFICER**, ossia sul Responsabile della Protezione dei Dati. Di cosa si tratta (?) Di una nuova figura, diversa dal Responsabile Esterno del Procedimento (che nella sostanza è un delegato del Titolare al trattamento dati che di essi venga al corrente per ragioni connesse al particolare rapporto, nella stragrande maggioranza dei casi di natura contrattuale, che lo lega al primo – si pensi appunto proprio alla Vostra categoria professionale, così come ai Consulenti del Lavoro, ad eventuali fornitori ecc.) che, al pari dei Responsabili Esterni, si caratterizza per essere una <u>figura autonoma</u> rispetto alla struttura del Titolare (in questo senso

differenziandosi entrambe le figure di Responsabile Esterno e DPO dagli eventuali, se nominati, Responsabili Interni del Procedimento) ma che deve anche esercitare le proprie funzioni in assoluta indipendenza, interfacciandosi esclusivamente con il Titolare.
Perché? Perché il DPO deve assistere il Titolare nel prendere le decisioni più opportune nel rendere effettiva l'applicazione dei principi tutti che abbiamo esaminato in precedenza e quindi l'accountability, come un modello di privacy dy design e by default o l'approccio basato sul rischio.
Il DPO viene pensato dal legislatore europeo come la figura, dotata delle competenze professionali e tecniche specifiche, per consigliare il Titolare del trattamento a porre in essere tutti quei comportamenti pro-attivi di cui si accennava prima, adattandoli alle peculiarità del Trattamento effettuato dal Titolare e, quindi, pensando a specifiche misure organizzative, amministrative, informatiche, da mantenere aggiornate a seconda anche delle continue innovazioni tecnologiche e i conseguenti crescenti rischi ad essi connessi, indicando – se non addirittura – imponendo lui al Titolare quali adempimenti porre in essere.
Quando la sua **NOMINA È OBBLIGATORIA**? In realtà non vi sono elementi precisi perché la norma contenuta nel GDPR è molto generica.
L'art. 37 infatti dispone che la nomina del DPO è obbligatoria:
a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico (ad eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali);
b) se le **attività principali**[1] (*core activities*: primarie e non accessorie) del Titolare o del Responsabile consistono in trattamenti che richiedono il **monitoraggio regolare e sistematico di interessati su LARGA SCALA**;

[1] Attività principali si possono intendere le operazioni essenziali necessarie al raggiungimento degli obiettivi perseguiti dall'azienda. Il Wp29 precisa che, tuttavia, l'esporessione attività principali non va interpretata nel senso di escludere quei casi in cui il trattamento dati, pur costituendo attività princiale, costituisce comunque una componente inscindibile dalle attività svolte. Ad esempio, l'attività principale di un ospedale è quella di

c) se le attività principali del Titolare o del Responsabile consistono nel trattamento su larga scale di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Tenete poi presente che secondo le linee guida del gruppo di lavoro "Articolo 29" in seno al Parlamento europeo e così anche secondo il nostro Garante, sebbene la designazione del DPO sia obbligatoria solo in questi casi, se ne incoraggia comunque la nomina su base volontaria, in un approccio definito "cautelativo".

Tralasciando le ipotesi a) e c) e quindi bypassando le problematiche connesse a cosa debba intendersi per autorità pubblica (non vi rientrerebbero i casi in cui una funzione pubblica sia svolta da soggetti privati, come i concessionari di pubblico servizio ma per essi sia altamente raccomandata come "good practice") e sulle categorie particolari di dati già esaminate, mi soffermerei sulla nozione che qui può risultare maggiormente di interesse ossia quella di cui alla lettera b), per comprendere la quale occorre ricostruire cosa si intenda per monitoraggio regolare e sistematico degli interessati.

Vi rientra sicuramente ogni forma di tracciamento e profilazione su internet ma, le linee guida evidenziano tuttavia che la nozione di monitoraggio non trova applicazione solo con riguardo all'ambiente on-line.

L'aggettivo "**regolare**" ha almeno uno dei seguenti significati a giudizio del gruppo di lavoro europeo:

- che avviene in modo continuo ovvero ad intervalli definiti per un arco di tempo determinato;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o ad intervalli periodici.

---

prestare assistenza sanitaria, ma non sarebbe possibile svolgerla nel rispetto della di scurezza e in modo efficace senza trattare dati relativi alla salute, come quelli contenuti nella cartella sanitaria di un paziente. Ne deriva che il trattamento di tali informazioni deve essere annoverato fra le attività principali di qualsiasi ospedale. Attività quali il pagamento delle retribuzioni al perosnale o la predisposizione di strutture standard di supporto informatico, invere, pur essendo necessarie o essenziali, sono considerate solitamente accessorie e non c"ore activities".

Del pari l'aggettivo "**sistematico"** ha invece almeno uno dei seguenti significati:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Alcuni esempi di attività che possono configurare un trattamento regolare e sistematico secondo il Wp29 sono fra gli altri: la gestione di una rete di telecomunicazioni, la prestazione di servizi di telecomunicazioni, attività di marketing basate sull'analisi dei dati raccolti, tracciamento dell'ubicazione, ad esempio da parte di appa su dispositivi mobili, programmi di fidelizzazione, utilizzo di telecamere a circuito chiuso, dispositivi per la domotica.

Quanto al concetto di "**larga scala**", bisogna fare riferimento al considerando n. 91 che fornisce alcune indicazioni, ritenendo su larga scale trattamenti "*di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato*" e precisando che, d'altra parte, "non dovrebbe essere considerato un trattamento su larga scala" il trattamento di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato" – due estremi, quelli presi in considerazione, fra cui si colloca un'ampia zona grigia.

Non esistendo, al momento, standard utili a specificare il concetto e le relative soglie applicabili, il Wp29 raccomanda di tenere conto dei seguenti fattori al fine di stabilire se un trattamento sia effettuato o meno su larga scala:

- il numero di soggetti interessati, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;

- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;

- la durata, ovvero la persistenza, dell'attività di trattamento;

- la portata geografica dell'attività di trattamento.

In virtù di quanto sopra, per verificare se sono o meno soggette all'obbligo di nominare un DPO ai sensi dell'art. 37, par. 1, lett. b), le imprese dovranno valutare:

1. se le attività di trattamento dalle stesse effettuate, per loro natura, ambito di applicazione e/o finalità, richiedono un "monitoraggio regolare e sistematico degli interessati";

2. in caso affermativo, se tale monitoraggio è effettuato su "larga scala";

3. se tale monitoraggio si può considerare come "attività principale".

SLIDE 14

Resta da accennare, in ultimo, ai **PROFILI SANZIONATORI**.

Ho già detto qualcosa all'inizio sulla necessità di fare riferimento alle due fonti GDPR e 196/2003 per ricostruire il quadro sanzionatorio.

Diciamo soltanto – al di là dei principi che devono orientare la possibilità per gli Stati nazionali nel prevedere ulteriori fattispecie sanzionatorie di farlo in un quadro di coerenza e con sanzioni equivalenti per le violazioni degli obblighi negli Stati membri (così gli artt. 63 e 70 del Regolamento) e sempre ispirandosi ad un criterio di ponderazione che tenga conto della natura, della gravità e della durata della violazione, del carattere doloso della violazione e delle misure adottate per attenuare il danno subito, del grado di responsabilità o di eventuali precedenti violazioni pertinenti, della maniera in cui l'autorità di controllo ha preso conoscenza della violazione ecc., che il GDPR ha previsto rilevanti sanzioni di natura amministrativa in caso di violazioni della normativa sulla protezione dei dati personali.

In particolare, l'art. 83 del GDPR distingue due gruppi di sanzioni amministrative: nel primo gruppo rientrano le violazioni cosiddette di **minore gravità**, per le quali sono previste le sanzioni amministrative pecuniarie fino a 10 milioni di euro o, per le imprese (da intendersi come gruppo) fino l 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, e riguardano nelle specifico le violazioni degli obblighi imposti ai seguenti soggetti:

- titolare e responsabile del procedimento (artt, 8, 11, da 25 a 39, 42 e 43 GDPR);
- l'organismo di certificazione, Accredia;
- l'organismo di controllo dei codici di condotta (art. 41 GDPR);

Il secondo gruppo di sanzioni, più pesanti in considerazione della **maggiore gravità** delle fattispecie a cui sono ricondotte, ammontano fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, e riguardano nello specifico le seguenti violazioni:

- dei principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli artt. 5, 6, 7e 9;
- dei diritti degli interessati a norma degli artt. da 12 a 22;
- i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;
- qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;
- l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dall'autorità di controllo (*rectius* Garante) ai sensi dell'art. 58, par. 2, o il negato accesso ai dati in violazione dell'art. 58, par. 1.

Il Garante è l'organo competente ad irrogare le sanzioni sopra citate. Ai sensi dell'art. 15, comma 3 del D.lgs. 101/2018: lo stesso dovrà avere cura di valutare caso per caso le violazioni, affinché le sanzioni siano sempre effettive, proporzionate e dissuasive (art. 83, comma 1 GDPR).

Il successivo art. 84, infine, lascia facoltà agli Stati membri di prevedere ulteriori sanzioni, in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie di cui all'art. 83, a condizione che esse siano sempre effettive, proporzionate e dissuasive, come già visto proprio agli esordi della mia esposizione.

Proprio in virtù di tale facoltà, il nostro legislatore, come già sappiamo attraverso il D.Lgs. 101/2018 ha novellato la parte III del previgente Codice della privacy, introducendo nuove fattispecie, tra cui il nuovo art. 166 che prevede la sanzione fino a 10 milioni di euro o al 2% del fatturato dell'impresa in caso di violazioni delle disposizioni che concernono talune situazioni specifiche tra cui la violazione dell'obbligo di informativa da rendere con linguaggio semplificato rilasciata ai minori di quattordici anni in occasione dell'offerta diretta di servizi della società dell'informazione ma, è interessante il secondo comma del medesimo art. 166 che prevede la più pesante sanzione fino a 20 milioni di euro o al 4% del fatturato dell'impresa in caso di violazioni di tutta un'altra serie di norme tra cui (ve ne cito solo alcuni) troviamo: violazione in merito alla raccolta del consenso prestato da minori di quattordici anni in occasione dell'offerta diretta di servizi della società dell'informazione; i trattamenti di dati relativi a condanne penali e reati, in relazione al trattamento dei dati sanitari, sui dati personali degli studenti, trattamenti nell'ambito di lavoro.

Per le sanzioni penali, infine, se da un lato il GDPR non ne prevede direttamente, dall'altro lato lo stesso ammette la facoltà per gli Stati membri di stabilire diposizione relative a sanzioni penali per violazioni del GDPR, nonché violazioni di norme nazionali adottate in virtù ed entro i limiti del Regolamento (Considerando 148).

Il D.Lgs. 101/2018 è appunto intervenuto a riformare le fattispecie che troviamo all'interno del Codice e per cui saranno applicabili le sanzioni penali, individuandole ne:

- **art. 167 – trattamento illecito di dati**;
- **art. 167 bis – comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala**;
- **art. 167 ter – acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala**;

- **art. 168** – **falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante**;
- **art. 170** – **inosservanza dei provvedimenti del Garante**.

***

Un'ultimissima osservazione su chi risponda delle violazioni, sia sul piano amministrativo che civilistico.

- Quanto al primo piano, si ritiene che l'unico soggetto tenuto a rispondere della sanzione amministrativa sia sempre solo e soltanto il Titolare del trattamento (inteso come l'entità nel suo complesso).

Operando in base alla legge n. 689/1981, la quale prevede che la notificazione del verbale venga effettuata al **contravventore e al responsabile in solido**, l'Autorità deputata all'accertamento dovrà notificarlo sia al **Titolare** del trattamento che al **Responsabile del trattamento**, nella misura in cui sussista un formale atto di designazione e siano riscontrate anche inadempienze gravi imputabili a tale ruolo.

- Quanto alle conseguenze civilistiche, si ritiene che la tutela apprestata nei confronti degli interessati che siano stati danneggiati dalle violazioni si esplichi attraverso il risarcimento del correlativo danno che viene posto espressamente a carico del Titolare in solido con il Responsabile del Procedimento. Nello specifico l'art. **82 GDPR** stabilisce che "*Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal Titolare o dal Responsabile del Trattamento*". Ciò premesso, la norma chiarisce che un **Titolare del trattamento risponde per il danno cagionato dal trattamento** che violi il Regolamento mente il soggetto nominato **Responsabile** ai sensi dell'art. 28 **GDPR risponde solo in caso di inadempimento degli obblighi del medesimo Regolamento specificatamente diretti ai Responsabili del trattamento** ovvero qualora abbia agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare.

Il contratto stipulato tra Titolare e Responsabile proprio per regolare tutti gli aspetti relativi alla nomina di questi nell'ambito di uno o più trattamenti di dati dovrebbe essere la sede adatta anche per prevedere allocazioni preventive di responsabilità ed eventuali azioni rimediali.

Quanto infine alla **responsabilità del DPO**, si evidenzia che lo stesso ha certamente responsabilità contrattuali nei confronti del Titolare del trattamento, ma non potrà essere responsabile nei confronti degli interessati in caso di inosservanza di obblighi in materia dei dati personali.

Tale responsabilità resta infatti in capo al Titolare e non è in alcun modo delegabile, anche in virtù del principio di *accountability*: è il Titolare che deve dimostrare la liceità del Trattamento e la non imputabilità alla propria condotta di eventuali danni a terzi per poter evitare di incorrere nelle sanzioni sopra illustrate.

Credo di averVi detto anche troppo.

Vi ringrazio per l'attenzione.

SLIDE 15

Ci sono domande?