



UNIVERSITÀ DEGLI STUDI DI SALERNO
Facoltà di Scienze Giuridiche (Scuola di Giurisprudenza)



Verso l'entrata in vigore del Regolamento UE n. 679/2016 sulla protezione dei dati personali



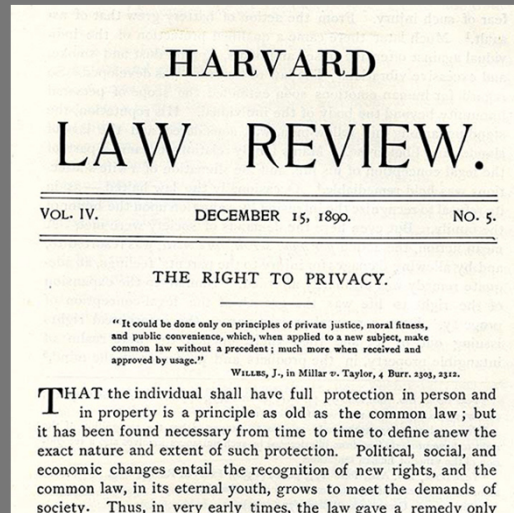
Prof. Avv. Salvatore Sica

Ordinario di Istituzioni di Diritto Privato (Università di Salerno)

Vice-Presidente della Scuola Superiore dell'Avvocatura

Privacy e Data protection in UE: la prospettiva evolutiva (1)

Dal diritto ad essere lasciati soli...



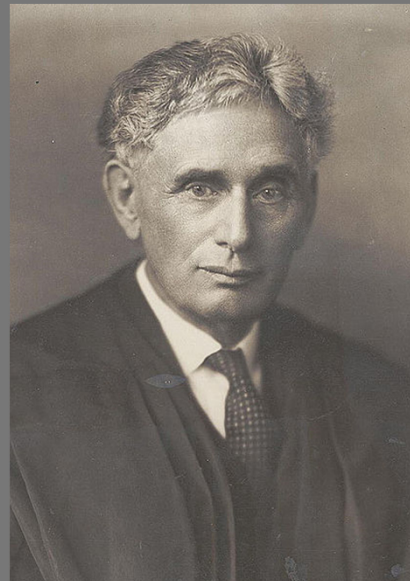
Olmstead v. United States, 277 U.S. 438 (1928)

«Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet»

(“La scoperta e l’invenzione hanno fornito al Governo mezzi molto più efficaci che origliare oltre gli scaffali, per rivelare in pubblico ciò che viene sussurrato in privato”)

S. WARREN – L. BRANDEIS, *The Right to Privacy*, 4 *Harvard L.R.* 193 (Dec. 15, 1890)

“The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle”.



Libertà negativa

«libertà come assenza di impedimento o di costrizione): situazione in cui un soggetto ha la possibilità di agire senza essere impedito, o di non agire senza essere costretto, da altri soggetti»

Privacy e Data protection in UE: la prospettiva evolutiva (2)

... all'autodeterminazione informativa

Bundesverfassungsgericht, 15 dicembre 1983, 1 BvR 209/83, in BVerfGE 65, (c.d. *Volkszählungsurteil*)

Recht auf informationelle Selbstimmung
(c.d. diritto all'autodeterminazione informativa)



«nell'ambito delle moderne modalità di trattamento dei dati personali è garantito il diritto che tutela l'individuo dalla raccolta illimitata, lo stoccaggio, l'uso e la divulgazione di informazioni personali, di cui all'articolo 2 , comma 1, della Legge fondamentale, in combinato disposto con l'articolo 1, paragrafo 1, della Legge fondamentale.

Questo diritto fondamentale è garantito nella misura in cui ogni individuo è titolare del diritto, in linea di principio, di determinare autonomamente le modalità di divulgazione e di utilizzo dei propri dati personali.

Sono consentite le restrizioni al diritto “autodeterminazione informativa” solo in caso di prevalenza dell'interesse pubblico. Tali ipotesi richiedono pertanto un fondamento costituzionale, che deve essere conforme al requisito della chiarezza. Nelle sue norme, il legislatore deve anche rispettare il principio di proporzionalità. Inoltre deve disporre misure organizzative e procedurali volte a contrastare il rischio di violazione dei diritti della personalità. 3 Uno dei requisiti costituzionali di tali restrizioni deve essere quello di poter consentire una distinzione tra i dati personali che vengono raccolti e trattati in forma non anonima ed individualizzata, e quelli che invece sono destinati ad essere utilizzati per fini statistici».

Libertà positiva

«autodeterminazione o autonomia): situazione in cui un soggetto ha la possibilità di orientare il proprio volere verso uno scopo, di prendere delle decisioni, senza essere determinato dal volere altrui

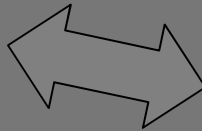
Privacy e Data protection in UE: la prospettiva evolutiva (3)

La Carta dei diritti fondamentali dell'UE e il d.lgs. 196/2003

Articolo 7 EUCFR

Rispetto della vita privata e della vita familiare

Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni.



Articolo 8 EUCFR

Protezione dei dati di carattere personale

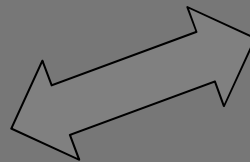
1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.



Articolo 1, d.lgs. 196/2003

Diritto alla protezione dei dati personali

Chiunque ha diritto alla protezione dei dati personali che lo riguardano.



Articolo 2, d.lgs. 196/2003

Finalità

1. Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Una disciplina in transizione



A far data dal 25 maggio 2018, il vigente Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, sarà abrogato e la nuova disciplina in materia sarà rappresentata principalmente dalle disposizioni del Regolamento immediatamente applicabili e da quelle recate dallo schema di decreto volte ad armonizzare l'ordinamento interno al nuovo quadro normativo dell'Unione Europea in tema di tutela della *privacy*.

Il nuovo Regolamento Generale sulla protezione dei dati personali - GDPR (679/2016/UE) – (1)



- L'ambito di applicazione materiale del GDPR riguarda principalmente il settore del mercato interno, con l'esclusione, quindi, di attività quali la cooperazione di polizia e giudiziaria in materia penale.
- Il GDPR non si applica al trattamento di dati effettuato da persone fisiche esclusivamente per finalità di carattere personale o domestico
- Accesso semplificato ai propri dati: maggiori informazioni sul trattamento dei propri dati, in un linguaggio semplice e chiaro.
- Diritto alla portabilità dei dati: interoperabilità e trasferimento dei propri dati personali tra più prestatori di servizi.
- Diritto all'oblio e alla cancellazione: quando l'interessato si oppone al trattamento dei propri dati – e ammesso che non sussistano ragioni legittime per la sua effettuazione – i dati devono essere cancellati o rimossi dagli indici di ricerca.
- Data breach: imprese ed enti pubblici devono notificare le gravi violazioni di dati all'autorità di controllo nazionale senza ingiustificato ritardo al fine di consentire agli interessati di adottare le misure più opportune.

Il nuovo Regolamento Generale sulla protezione dei dati personali - GDPR (679/2016/UE) – (2)



- Consenso : qualora il trattamento dei dati personali sia basato sul consenso dell'individuo interessato, il consenso deve essere prestato in modo chiaro e intellegibile.
- Responsabilizzazione dei titolari del trattamento (accountability): valutazioni del rischio derivante dal trattamento dei dati e individuazione di responsabili della protezione dei dati (DPO).
- Norme europee sul suolo europeo: alle imprese stabilite fuori dal territorio dell'Unione europea si applicano le medesime norme qualora offrano servizi nell'ambito dell'Unione.
- Un continente, una legislazione: il regolamento stabilisce un unico insieme di norme che rende più semplice e meno oneroso per le imprese svolgere attività economica nell'Unione europea.
- “Sportello unico” (one stop shop): gli operatori economici dovranno interagire con un'unica autorità di controllo.
- Protezione dei dati “by design” e “by default”: Garanzie per la protezione dei dati dovranno essere incorporate in prodotti e servizi già a partire dalle prime fasi del loro sviluppo e impostazioni di sicurezza predefinite saranno la norma, ad es., sui social network o nelle applicazioni per la telefonia mobile.
- Rimedi giudiziali e amministrativi più incisivi: sanzioni amministrative per un importo fino al 4% del loro fatturato globale annuo.

Il nuovo Regolamento Generale sulla protezione dei dati personali - GDPR (679/2016/UE) – (3)



Abolizione degli obblighi di notifica al Garante

La notificazione ex dir. 95/46/CE era una dichiarazione con la quale il titolare rendeva noto l'esistenza di una attività di raccolta e trattamento di dati personali. La notificazione rappresentava pertanto uno strumento di controllo e di conoscenza dei trattamenti posti in essere, ma anche di trasparenza, pubblicità ed effettività del diritto dell'interessato di essere informato.

Ai sensi dell'articolo 37 del Codice la notificazione veniva prevista nei casi di **dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato** (profilazione), o ad analizzare abitudini di vita o scelte di consumo, oppure a **monitorare l'utilizzo di servizi di comunicazione elettronica**, con esclusione dei trattamenti tecnicamente indispensabili per la fornitura dei medesimi servizi.

La notificazione veniva prevista dalla disciplina previgente per i seguenti trattamenti:

- dati biometrici (impronte digitali, riconoscimento iride);
- dati genetici;
- dati di geolocalizzazione (GPS);
- dati sullo stato di salute trattati a fini di procreazione assistita;
- prestazione di servizi sanitari per via telematica;
- indagini epidemiologiche;
- rilevazione di malattie mentali, infettive e diffuse, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
- dati gestiti dalle centrali rischi sulla solvibilità economica.

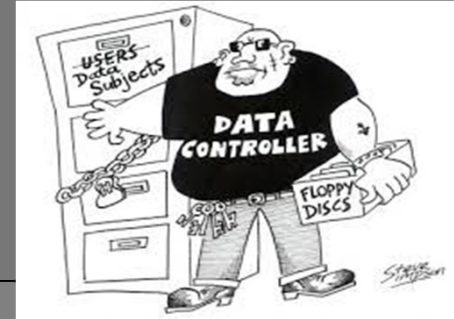
Il nuovo Regolamento Generale sulla protezione dei dati personali - GDPR (679/2016/UE) – (4)



- La notificazione veniva effettuata prima dell'inizio del trattamento, e andava trasmessa esclusivamente per via telematica utilizzando l'apposito modulo predisposto sul sito del Garante, ovvero a mezzo degli intermediari autorizzati.
- L'**omessa notificazione** era punita con la sanzione amministrativa da 20mila a 120mila euro.

Col nuovo regolamento europeo l'istituto della notifica e del *prior checking* vengono aboliti e sostituiti da verifiche *ex post*, cioè compiute successivamente alle determinazioni assunte autonomamente dal titolare del trattamento.

Risk-Based Approach e trattamento dei dati personali nel nuovo Regolamento UE



Art. 4(1) - Nozione di dato personale : estesa a tutti i dati (anche quelli pseudonimi) che, anche a seguito di combinazione con altre informazioni, possano condurre all'identificazione di una persona fisica (cc.dd. trattamenti multipli).

Art. 7 - Consenso:

Il GDPR riafferma in maniera più incisiva il principio del consenso, affiancato ai doveri di informazione e trasparenza posti in capo al titolare o responsabile del trattamento. La disciplina è declinata in maniera analitica e puntuale anche con riguardo alla tutela di particolari figure soggettive, quali i minori (v. art. 8) e, ancora, con riferimento a particolari tipologie di trattamento dei dati.

Art. 6(4) – Trattamenti secondari:

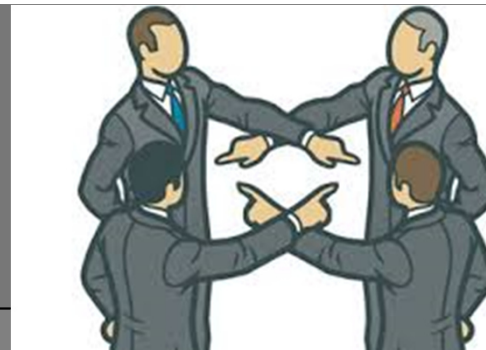
In assenza di consenso dell'interessato o di altro atto legislativo che sancisca la liceità dell'attività, il titolare è tenuto a valutare se il trattamento sia astrattamente conforme ai principi di necessità e proporzionalità di cui all'art. 23 del Regolamento, con particolare riguardo agli scopi perseguiti dal trattamento principale.

Art. 35 – Valutazione d'impatto e consultazione preventiva:

Nelle ipotesi di trattamento avente “un elevato rischio per i diritti e le libertà delle persone fisiche”, il titolare è tenuto ad attuare una valutazione preventiva dell'impatto delle attività sulla protezione dei dati personali e, ove lo ritiene opportuno, consulta preventivamente l'autorità nazionale di garanzia al fine di ottenere l'autorizzazione per svolgere il trattamento.

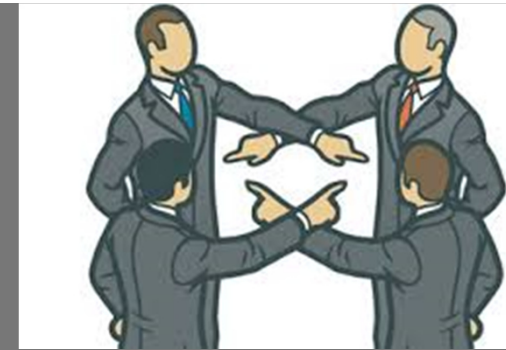
- **Registro dei trattamenti**: obbligatorio + 250 dipendenti

La c.d. *Accountability* (Responsabilizzazione) del titolare o responsabile del trattamento (1)



- La responsabilizzazione richiede l'adozione attiva di misure da parte dei titolari del trattamento dei dati per la promozione e la salvaguardia della protezione dei dati nel corso delle loro attività di trattamento.
- I titolari del trattamento sono responsabili per e devono essere in grado di dimostrare il rispetto della normativa in materia di protezione dei dati nel corso delle proprie attività di trattamento.
- I titolari del trattamento devono essere in grado di provare in ogni momento l'osservanza dei principi in materia di protezione dei dati alle persone interessate, al pubblico in generale e alle autorità di controllo. Il GDPR stabilisce nuovi obblighi in termini di responsabilizzazione che richiederanno l'adozione di nuove significative misure di carattere tecnico e organizzativo per dimostrare il rispetto del GDPR. Questi requisiti comprendono la privacy "by design", la notifica delle violazioni della sicurezza alle autorità di controllo, la nomina di un rappresentante del titolare o del responsabile del trattamento stabilito al di fuori del territorio dell'Unione europea, nonché la conduzione di valutazioni d'impatto sulla protezione dei dati per trattamenti a elevato rischio.

La c.d. *Accountability* (Responsabilizzazione) del titolare o responsabile del trattamento (2)



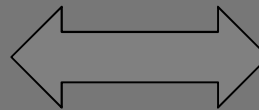
Art. 82 –

Diritto al risarcimento e responsabilità:

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 del trattamento o dal responsabile del trattamento.

2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

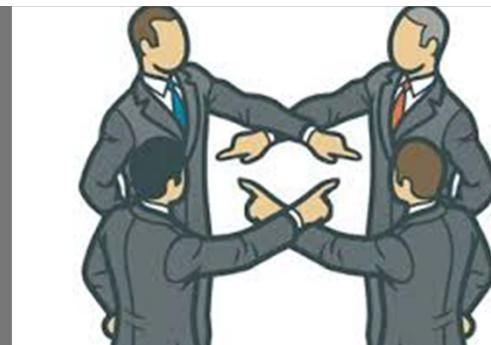


Art. 15, Codice privacy Danni cagionati per effetto del trattamento

1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

Risarcimento e solidarietà



4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.

6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.

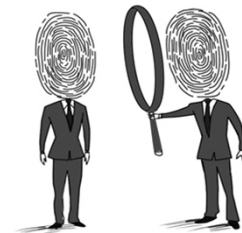
Altre sanzioni



L'articolo 84 del GDPR prevede che gli Stati membri “stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento, in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie e adottano tutti i provvedimenti necessari per assicurarne l'applicazione [...]”.

Nonostante gli Stati membri dell'Unione europea detengano un certo margine di discrezionalità nel determinare quali misure siano più appropriate per la tutela dei diritti in materia di protezione dei dati e privacy, il GDPR prevede espressamente che tali sanzioni debbano soddisfare i requisiti dell'effettività e della proporzionalità (articolo 84).

Nuove figure soggettive: il responsabile della protezione dei dati personali (c.d. *Data Protection Officer*) – (1)



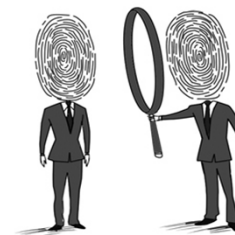
Articolo 37

Designazione del responsabile della protezione dei dati

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

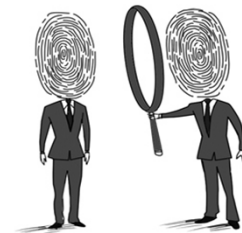
- a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
- c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Nuove figure soggettive: il responsabile della protezione dei dati personali (c.d. *Data Protection Officer*) – (2)



2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.
3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.
4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.
5. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.
6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.
7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

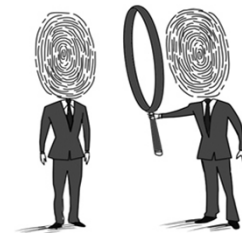
Nuove figure soggettive: il responsabile della protezione dei dati personali (c.d. *Data Protection Officer*) – (3)



La nozione di «larga scala»: esempi

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile del trattamento specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Nuove figure soggettive: il responsabile della protezione dei dati personali (c.d. *Data Protection Officer*) – (4)



«Monitoraggio regolare e sistematico»

“Regolare”:

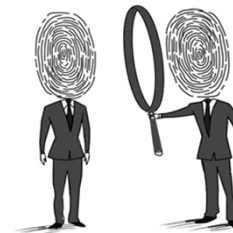
- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

“Sistematico”:

- 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.

Esempi: cura del funzionamento di una rete di telecomunicazioni; prestazione di servizi di telecomunicazioni; reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull’analisi dei dati raccolti; profilazione e scoring.

Artt. 38 e 39: Posizione e compiti del DPO



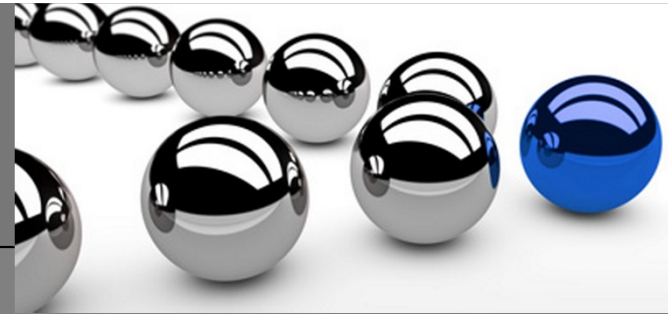
- a) deve essere adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
- b) deve essere sostenuto dal titolare del trattamento e dal responsabile nell'esecuzione dei compiti assegnati;
- c) deve avere le risorse necessarie per adempiere ai compiti assegnati;
- d) deve poter accedere ai dati personali e ai trattamenti che riguardano la struttura in cui è inserito;
- e) deve mantenere la sua conoscenza specialistica (corsi di aggiornamento);
- f) deve essere indipendente nell'esercizio delle sue funzioni;
- g) non deve essere penalizzato o rimosso per l'adempimento dei propri compiti;
- h) è tenuto al segreto e alla riservatezza in merito all'adempimento dei propri compiti;
- i) non può svolgere altre funzioni o compiti che determinino un conflitto di interessi.

I compiti del responsabile della protezione dei dati sono almeno i seguenti:

- a) informare e consigliare il titolare del trattamento o il Responsabile nonché i dipendenti;
- b) sorvegliare l'osservanza del Regolamento e delle altre leggi vigenti nell'Unione Europea in materia nonché delle policy;
- c) fornire se richiesto un parere sulla valutazione di impatto sulla protezione dei dati personali e sorvegliare lo svolgimento;
- d) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento di dati personali.

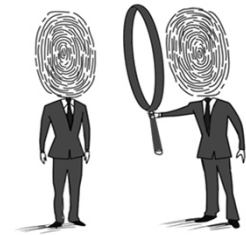
- La professione del responsabile della protezione dei dati non è regolamentata **e non è obbligatoriamente soggetta a esami, certificazioni, né all'iscrizione ad albi professionali**. In Italia, si rientra nell'ambito di applicazione della Legge 4/2013 sulle professioni non organizzate in ordini e collegi.

Le Autorità di controllo: compiti e novità



- **Funzione di controllo ex post**: abolizione della notifica preventiva dei trattamenti all'autorità di controllo e del *prior checking* (c.d. verifica preliminare). Si veda art. 17 Codice privacy.
- **Data Breach**: Tutti i titolari – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno **notificare all'Autorità di controllo le violazioni di dati personali** di cui vengano a conoscenza, entro 72 ore e comunque “senza ingiustificato ritardo”, ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.
- Le persone interessate i cui dati sono trattati in modo incompatibile con il regolamento hanno il diritto specifico di **proporre reclamo** a un'autorità di controllo (articolo 77) e le autorità di controllo devono informare il reclamante dello stato o dell'esito del reclamo.
- **Codici di condotta**: forniscono linee guida per i titolari del trattamento o responsabili del trattamento circa la precisa applicazione del GDPR e sono indicatori dell'ottemperanza di un'organizzazione alle disposizioni del regolamento; i codici di condotta devono essere approvati dalla competente autorità di controllo.
- **C.d. Autorità di controllo capofila (one stop shop)**: autorità dello stabilimento principale o unico nell'Ue del titolare o responsabile del trattamento, alla quale viene trasferita la competenza da tutte le altre autorità di controllo (definite, in questo caso, "autorità interessate") per quanto riguarda i "trattamenti transfrontalieri" di dati personali svolti da quel titolare o responsabile.

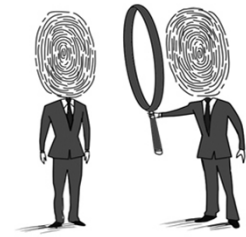
Il nuovo Regolamento nella prassi: FAQ (1)



- Il GDPR rivoluziona tutta l'organizzazione privacy fino ad ora implementata?
 - Occorre ricominciare da zero oppure qualcosa può essere salvato?
 - Posso continuare a fare riferimento alle misure di sicurezza previste dal disciplinare tecnico?

- La pluriventennale esperienza italiana in materia di protezione dei dati personali non verrà cancellata dall'entrata in vigore del Regolamento, ma subirà, come si è visto, un'evoluzione. La parte generale del Codice sarà sostituita in modo naturale dalle disposizioni del Regolamento, che su queste prevalgono e quasi nulla resta della parte generale del Codice.
- La parte speciale del Codice sarà invece trasferita, con i necessari adeguamenti imposti dal Regolamento europeo, nello schema di decreto (ad es.: Codici deontologici).
- In ossequio al principio di responsabilizzazione, non esistono più le «Misure minime di sicurezza»: nell'attesa di nuove Linee guida del garante, il Disciplinare, rimane un valido punto di riferimento per avviare una introdotti dal Regolamento.

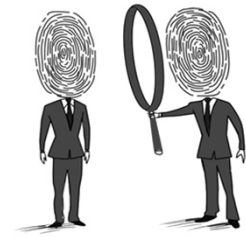
Il nuovo Regolamento nella prassi: FAQ (2)



- Da dove e come comincio a implementare il GDPR nella mia impresa?
- Posso farcela da solo, oppure occorre un consulente esterno?

- La prima operazione da svolgere è una lettura del testo del Regolamento, ampio ed articolato proprio per rendere accessibili a tutti i principi-base in materia di protezione dei dati personali.
- E' imprescindibile una verifica della conformità delle misure adottate rispetto alle nuove norme del Regolamento ai fini di una loro efficacia successiva (es.: informative e consenso al trattamento dei dati);
- Le attività di audit e consulenza svolte da soggetti qualificati rappresentano una base fondamentale per espletare in maniera corretta tutte le attività di verifica ed adeguamento alle norme introdotte dal Regolamento.

Il nuovo Regolamento nella prassi: FAQ (3)



- Ai fini di una più efficiente governance, posso traslare in ambito privacy l'istituto della delega di funzioni? Il decreto legislativo di adeguamento normativo nazionale al GDPR può disciplinarlo?

- Il Regolamento introduce un'autonomia – ed in certi punti innovativa – ripartizione dei compiti e delle responsabilità nell'ambito delle attività di trattamento;
- In ossequio al principio di responsabilizzazione e nell'ottica di un approccio interamente modellato sul rischio, il Regolamento lascia ampia libertà organizzativa al soggetto coinvolto in attività di trattamento.
- L'approccio non è di tipo precettivo (enumerazione puntuale di tutte le attività che il titolare del trattamento deve svolgere), ma focalizzato sulla promozione di *best practices* e, soprattutto, sulla prevenzione dei rischi.
- Ruolo fondamentale dei codici di condotta.



Il nuovo Regolamento nella prassi: FAQ (4)

- In che termini lo svolgimento di attività di profilazione deve considerarsi *una componente inscindibile del core business* del titolare e, quindi, un elemento idoneo a determinare a carico di quest'ultimo l'obbligo di nominare il DPO?

- Ad esempio, un'impresa che produce ad es. calzature e che le commercializza ai consumatori con i canali tradizionali e tramite e-commerce previa profilazione del consumatore, è tenuta a nominare il DPO?

- In linea generale, si segnala che il Regolamento, oltre ad un obbligo di designazione, introduce anche la facoltà di nominare un DPO.
- Nel dubbio, ogni attività di profilazione attuata per finalità commerciali andrebbe svolta in via precauzionale seguendo tutte le norme del Regolamento, compresa quella relativa alla designazione del DPO.

Il nuovo Regolamento nella prassi: FAQ (5)



- La conservazione dei dati nel caso in cui non ci sia una specifica norma di legge o contrattuale alla quale fare riferimento ovvero un provvedimento del Garante. *Quid iuris?*

(ad es.: dati contenuti nei CV, informazioni relative all'utilizzo della casella e-mail data in uso al dipendente, dati dei dipendenti a seguito della cessazione del rapporto di lavoro di rapporti di lavoro cessati).

- L'UE è al lavoro per l'approvazione di una nuova direttiva sulla data retention, che sostituirà quella invalidata dalla sentenza della CGUE resa nel caso *Digital Ireland*.
- In assenza di appigli normativi ben definiti, vige il principio di responsabilizzazione e autonoma organizzazione, da declinare unitamente al patrimonio di provvedimenti ed indicazioni fornito negli anni dal Garante.
- Un dato personale non deve essere conservato per sempre, ma solo fin quando è necessario per lo scopo per il quale i dati sono stati raccolti. Qualora non sia indicato per legge un preciso termine di conservazione, occorre comunque prevederlo.



Grazie per l'attenzione!

Studio Legale Sica Associato
sicass@tin.it