GDPR: come gestire gli adempimenti

Privacy 4.0: informativa, consenso, responsabilità, sanzioni

Con il **General Data Protection Regulation** debutta la **privacy 4.0**, studiata per rispondere alle insidie della digital transformation.

Aziende e professionisti devono prepararsi al 25 maggio 2018, data che segna la **piena operatività** del GDPR, per assicurarsi la conformità alle nuove regole.

99 articoli e numerosi adempimenti, che necessitano di interventi programmati nel tempo e calibrati in funzione della struttura organizzativa aziendale e degli studi professionali. I più urgenti sono: la nomina di un **Data Protection Officer**, la tenuta del **registro dei trattamenti** aggiornato e la corretta gestione di eventuali **data breach**.

Alcuni adempimenti vengono "ereditati" dal Codice della Privacy e rivisitati dal GDPR. E' il caso dell'**informativa** e del **consenso**.

Il sistema delle **misure di sicurezza**, poi, è stato rivoluzionato sull'idea di "accountability": una strategia operativa che pone l'accento sulla "sostanza" dell'adempimento e sulla sua verificabilità esterna.

E le **sanzioni**? Tra le più alte mai stabilite in una normativa pensata per la protezione dei dati: non solo fisse, ma anche stabilite in percentuale, con riferimento al fatturato dell'azienda.

Cosa fare per **essere compliance** alla privacy 4.0? Nel Dossier, tutte le risposte sugli adempimenti.

Gli altri dossier sul GDPR

Tutti gli adempimenti ...	... per professionisti e aziende
Quadro normativo Nuovo regolamento privacy	**Commercialisti (dal 12 aprile)** GDPR e Commercialisti: come proteggere i dati dei clienti **Consulenti del lavoro (dal 3 maggio)** GDPR e Consulenti del lavoro: proteggere i rapporti di lavoro

	PMI GDPR e PMI: gestire i dati valutando i costi **Multinazionali (dal 20 aprile)** GDPR e multinazionali: gestire i dati in ambito internazionale

COSA CAMBIA

COSA CAMBIA - 15 MARZO 2018

Privacy: informativa per i dati personali

L'informativa è un adempimento obbligatorio e fondamentale per il trattamento dei dati personali. Con il GDPR è al centro di un processo di revisione che mira ad adeguarlo ai cambiamenti legati all'uso delle nuove tecnologie. L'obiettivo è garantire un'informazione chiara sull'intero processo di trattamento dei dati anche in ambiente online. In tale ottica, il regolamento UE sulla privacy amplia i contenuti dell'informativa definendone caratteristiche e modalità.

Dal **25 maggio 2018** diventerà pienamente operativo il nuovo Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Il Regolamento sottopone ad un processo di revisione l'**informativa** in caso di **dati raccolti presso l'interessato**. Con tale adempimento il titolare del trattamento "informa" l'interessato del trattamento dei suoi dati personali: su come questi saranno trattati, per quali scopi, con quale impatto sulla sua privacy, con quali tempi e limiti.

L'informativa, inoltre, deve dare conto dei **diritti** che l'**interessato** può esercitare nei confronti di coloro che trattano le sue informazioni personali.

I **contenuti dell'informativa** sono elencati in modo tassativo dal GDPR e sono, in parte, più ampi rispetto ai contenuti previsti dal Codice della privacy. Inoltre, il regolamento UE ne specifica in modo più dettagliato caratteristiche e modalità.

Cosa cambia	Prima Fino al 24 maggio 2018	Dopo Dal 25 maggio 2018
Qualificazione	-	L'informativa è un **diritto fondamentale** dell'interessato
Tempistica	Preventiva	**Contestuale**: deve essere resa nel momento in cui i dati sono ottenuti dal titolare del trattamento
Forma	L'informativa	L'informativa è data, in linea di principio,

	deve essere fornita **oralmente** o **per iscritto**.	**per iscritto** e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online).
	-	L'informativa deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile. Occorre utilizzare un **linguaggio chiaro e semplice.**
	-	E' ammesso l'**utilizzo di icone** per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa. Tali icone dovranno essere identiche in tutta l'UE e saranno definite dalla Commissione europea. Se presentate elettronicamente, le icone dovrebbero essere leggibili da dispositivo automatico.
Contenuto	L'informativa deve indicare: · le finalità e le modalità del trattamento · la natura obbligatoria o facoltativa del conferimento dei dati · le conseguenze di un eventuale rifiuto di rispondere · i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi; · i diritti	L'informativa deve indicare: · l'identità e i dati di contatto del **titolare del trattamento** e, ove applicabile, del suo rappresentante · i dati di contatto del **responsabile della protezione dei dati**, ove applicabile · le **finalità** del trattamento cui sono destinati i dati personali, nonché la **base giuridica** del trattamento · i **legittimi interessi perseguiti** dal titolare del trattamento o da terzi qualora il trattamento sia necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi · gli eventuali **destinatari** o le eventuali categorie di destinatari dei dati personali · l'eventuale intenzione del titolare del trattamento di **trasferire dati personali a un paese terzo o a un'organizzazione internazionale,** nonché l'esistenza di una decisione della Commissione in merito al fatto che sia garantito un livello di protezione adeguato. Qualora non ci sia una decisione della Commissione in tal senso occorre fare riferimento alle garanzie appropriate o opportune ed i mezzi per ottenere una copia di tali dati o il luogo dove siano stati resi disponibili

dell'interessato

· gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato e del responsabile.

· il **periodo di conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo

· l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'**accesso** ai dati personali e la **rettifica** o la **cancellazione** degli stessi o la **limitazione** del trattamento che lo riguardano o di **opporsi** al loro trattamento, oltre al diritto alla **portabilità** dei dati

· qualora l'interessato abbia espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità oppure abbia prestato il proprio consenso esplicito al trattamento di categorie particolari di dati personali per una o più finalità specifiche, va informato dell'esistenza del **diritto di revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

· il diritto di proporre **reclamo** a un'autorità di controllo

---

· se la comunicazione di dati personali è un **obbligo legale o contrattuale** oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati

· l'esistenza di un **processo decisionale automatizzato**, compresa la **profilazione** e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste per l'interessato

· qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento deve fornire all'interessato informazioni in merito a tale diversa finalità

		e ogni ulteriore informazione pertinente.
Minori	-	Per i minorioccorre prevedere **informative idonee**.
Esonero	In caso di ricezione di curricula spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro.	- Se l'interessato **dispone già** delle **informazioni**. - Nei casi in cui il **diritto dell'Unione europea o dello Stato membro** lo **preveda** a salvaguardia di specifici interessi quali: la sicurezza nazionale e pubblica, la difesa, il perseguimento di reati, l'indipendenza della magistratura, ecc.

Leggi anche: Privacy: informativa e consenso tra i primi adempimenti

COSA CAMBIA - 20 MARZO 2018

GDPR: il consenso al trattamento dei dati

Il nuovo regolamento UE modifica la disciplina del consenso al trattamento dei dati, che deve essere effettivo ed inequivocabile. Benché possa essere manifestato oralmente - ferma restando la necessità di documentarlo - o per iscritto, il titolare del trattamento, dal 25 maggio 2018, dovrà sempre essere in grado di dimostrare che l'interessato abbia prestato il consenso ad uno specifico trattamento.

Il nuovo Regolamento UE 2016/679 considera lecito il **trattamento dei dati personali** se l'interessato ha espresso il suo **consenso**.

Il consenso è una **manifestazione di volontà** che deve essere richiesta dal titolare del trattamento all'interessato per trattare i dati di quest'ultimo.

Il consenso deve essere **esplicito** per il trattamento di dati "sensibili", ossia legati alla salute, alle abitudini sessuali, alla origine razziale o etnica o alle opinioni di una persona o per il trattamento dei dati a fini di invio di materiale promozionale o pubblicitario.

Il consenso deve essere dato liberamente e ciò, secondo le indicazioni del GDPR, è escluso nel caso in cui l'interessato non sia in grado di operare una **scelta autenticamente libera** o si trovi nell'impossibilità di rifiutare o revocare il consenso senza subire un pregiudizio.

L'interessato deve inoltre essere posto nelle condizioni di conoscere i dati trattati, le modalità e le finalità.

Il consenso deve essere sempre **revocabile**, senza obbligo di motivazione.

Infine ai minori il GDPR riserva una particolare protezione.

Il consenso è strettamente legato all'adempimento dell'informativa.

Cosa cambia	Prima	Dopo
	Fino al 24 maggio 2018	**Dal 25 maggio 2018**
Qualificazione	-	Condizione di **liceità** del trattamento
Definizione	Manifestazione del diritto dell'autodeterminazione informativa	Qualsiasi **manifestazione di volontà libera, specifica, informata e inequivocabile** dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.
Limiti all'obbligatorietà	Il consenso non è richiesto quando il trattamento è necessario: - per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria - per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato; - per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato	Il consenso non è necessario per l'**esecuzione di un contratto**, per l'adempimento di un **obbligo legale**, per la salvaguardia di **interessi vitali** per una persona fisica, per l'esecuzione da parte del titolare di un **compito di interesse pubblico** o connesso all'**esercizio di pubblici poteri**, per il perseguimento di un **legittimo interesse** ove non prevalgano i diritti e le libertà del soggetto interessato.

- ai fini dello svolgimento delle investigazioni difensive, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale

-nei casi individuati dal Garante per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;

-è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa

---

- in conformità ai rispettivi codici di deontologia, per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico o, secondo quanto previsto dai medesimi codici, presso altri archivi privati.

Inoltre quando riguarda:

- dati contenuti nei curricula, spontaneamente trasmessi

	dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro; - dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque - dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale - la comunicazione di dati tra società, enti o associazioni con società controllanti, controllate o collegate ovvero con società sottoposte a comune controllo, nonché tra consorzi, reti di imprese e raggruppamenti e associazioni temporanei di imprese con i soggetti ad essi aderenti, per le finalità amministrativo contabili, e purché queste finalità siano previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa.	
Più consensi	In presenza di più finalità connesse alla raccolta dei dati presso l'interessato sono necessarie richieste distinte di consenso	Nessuna variazione
Condizioni	Il consenso è validamente prestato solo se è informato, espresso, libero, specifico in riferimento ad un trattamento chiaramente individuato. Non è ammesso il consenso tacito o presunto (es: caselle pre-spuntate su un modulo)	Nessuna variazione
Modalità	Il consenso può essere manifestato oralmente (ma va comunque documentato) o per iscritto	Nessuna variazione
	E' obbligatorio che sia manifestato in forma scritta quando il trattamento riguarda	Deve essere **esplicito** per i dati sensibili e per trattamenti automatizzati,

	dati sensibili.	compresa la profilazione.
	-	Il titolare deve essere in grado di **dimostrare** che l'interessato abbia prestato il consenso ad uno specifico trattamento
Minori	-	E' lecito il trattamento di dati personali del minore solo se questi abbia **almeno 16 anni**. Se il minore ha un'età inferiore ai 16 anni, il trattamento è lecito soltanto se e nella misura in cui tale consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale. E' tuttavia possibile che gli Stati membri stabiliscano per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.
Revoca	Il Codice Privacy non prevede espressamente nulla in merito. La giurisprudenza prevede che la revoca del consenso al trattamento dei dati personali possa essere espressa dall'interessato con richiesta rivolta senza formalità al titolare o al responsabile del trattamento, anche per il tramite di un legale di fiducia.	L'interessato ha il diritto di revocare il proprio consenso **in qualsiasi momento**; la revoca deve poter essere fatta facilmente e non pregiudica la liceità del trattamento basata sul consenso prima della revoca.

Leggi anche: Privacy: informativa e consenso tra i primi adempimenti

COSA CAMBIA - 28 MARZO 2018

Il Data Protection Officer

Il GDPR introduce la figura del Data Protection Officer o "responsabile per la protezione dei dati", una sorta di arbitro della privacy in azienda. Il DPO deve, infatti, sorvegliare sulla corretta applicazione del Regolamento europeo e per tale motivo possedere una conoscenza specialistica della normativa e della prassi in materia di protezione dei dati. Quali sono i suoi compiti? Chi è tenuto a nominarlo?

E' una delle novità più importanti del GDPR. Il **Data Protection Officer** o "responsabile per la

protezione dei dati" ha principalmente il compito di sorvegliare sull'osservanza del GDPR, valutando i **rischi di ogni trattamento** alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità

Importante anche il suo ruolo di **"facilitatore" in azienda**: un punto di contatto per facilitare l'accesso, da parte dell'autorità di controllo, ai documenti e alle informazioni necessarie per l'adempimento dei compiti attribuiti.

Il DPO deve essere obbligatoriamente **nominato** dal titolare e dal responsabile del trattamento in alcuni casi specifici. Al di furi di tali ipotesi è prevista la possibilità di nominare il DPO volontariamente.

Può essere nominato un unico DPO:

- da un gruppo imprenditoriale a condizione che il responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento

- per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

Il DPO può essere sia un dipendente del titolare del trattamento o del responsabile del trattamento oppure può assolvere i suoi compiti in base ad un **contratto di servizi**; deve essere dotato di ampia autonomia ed indipendenza nell'espletamento dei suoi compiti ed i suoi dati di contatto vanno comunicati all'autorità di controllo.

Cosa cambia	Prima	Dopo
	Fino al 24 maggio 2018	Dal 25 maggio 2018
Definizione	-	E' una nuova figura che va nominata dal titolare del trattamento e dal responsabile del trattamento
Quando va nominato	-	- Il trattamento è effettuato da un'**autorità pubblica** o da un **organismo pubblico**, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali - 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 - Le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di **categorie particolari di 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 o di dati relativi a condanne penali e a reati

Competenze	-	Il responsabile della protezione dei dati è designato in funzione delle **qualità professionali**, in particolare della conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, e della capacità di **assolvere i compiti a lui assegnati**
Compiti	-	Il DPO deve: - **informare** e **fornire consulenza** al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati - **sorvegliare** l'**osservanza del regolamento**, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati, nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo - fornire, se richiesto, un parere in merito alla **valutazione** d'impatto sulla **protezione dei dati** e sorvegliarne lo svolgimento - cooperare con l'autorità di controllo - fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
Risorse per l'esecuzione dei compiti	-	Il titolare del trattamento e il responsabile del trattamento devono **sostenere** il **responsabile** della **protezione dei dati** nell'esecuzione dei suoi compiti, fornendogli le risorse necessarie per assolverli e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
Conflitto di interessi	-	Il DPO può svolgere anche altri compiti e funzioni ma è necessario che tali compiti e funzioni non diano adito a un conflitto di interessi.

- Privacy: dal Garante le FAQ sul DPO

- Privacy: i tre volti del Data Protection Officer

GDPR: data breach

Il GDPR ha previsto per il titolare del trattamento l'obbligo di notificare la violazione dei dati personali all'autorità di controllo competente entro 72 ore dal momento in cui ne è venuto a conoscenza. Inoltre, se la violazione presenta un rischio elevato per i diritti e le libertà delle persone deve comunicare la violazione anche all'interessato e senza ingiustificato ritardo.

La **violazione dei dati personali** può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, come ad esempio la perdita del controllo dei dati personali che le riguardano o la limitazione dei loro diritti, una discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, un pregiudizio alla reputazione, la perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Per questo motivo il Regolamento UE 2016/679 ha previsto l'obbligo di comunicare le violazioni (data breach) tempestivamente e, precisamente, **senza ingiustificato ritardo** e, ove possibile, entro 72 ore dal momento in cui il titolare del trattamento ne sia venuto a conoscenza.

Tale obbligo è presente anche nel **Codice privacy** anche se solo per specifici ambiti (società telefoniche ed internet provider) e con diverse modalità di **notifica** all'autorità di controllo e di **comunicazione** all'interessato. Altri casi sono stati, inoltre, previsti dal Garante con specifici provvedimenti (biometria, dossier elettronico sanitario, pubbliche amministrazioni).

Cosa cambia	Prima	Dopo
	Fino al 24 maggio 2018	**Dal 25 maggio 2018**
Notifica	Il fornitore di servizi di comunicazione elettronica accessibili al pubblico comunica la violazione di dati personali senza indebiti ritardi al Garante privacy.	Il titolare del trattamento deve notificare la violazione dei dati personali all'autorità di controllo competente **senza ingiustificato ritardo** e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. In caso di ritardo occorre specificare i motivi del ritardo.
Casi di esclusione	La comunicazione non é dovuta se il fornitore ha dimostrato al Garante di aver utilizzato misure tecnologiche di protezione che rendono i dati inintelligibili a chiunque non sia autorizzato ad accedervi e che tali misure erano state applicate ai dati oggetto della violazione.	La notificazione al Garante non è necessaria quando è improbabile che la violazione dei dati personali presenti un **rischio per i diritti** e le libertà delle persone fisiche.

Contenuto	In un primo momento possono essere fornite all'Autorità sommarie informazioni sulla violazione dei dati verificatasi, purché ciò avvenga immediatamente dopo l'avvenuta conoscenza della stessa, integrando poi la comunicazione in un momento successivo. Tali sommarie informazioni devono in ogni caso consentire all'Autorità di effettuare una prima valutazione dell'entità della violazione e devono comprendere: • i dati identificativi del fornitore • una breve descrizione della violazione • l'indicazione della data anche presunta della violazione e del momento della sua scoperta • l'indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se essa sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili • l'indicazione della natura e della tipologia dei dati anche solo presumibilmente coinvolti • una sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione. La comunicazione al Garante deve contenere almeno una descrizione della natura della violazione di dati personali e i punti di contatto presso cui si possono ottenere maggiori informazioni, elencare le misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione di dati personali e descrivere le conseguenze della violazione di dati personali e le misure proposte o adottate dal fornitore per porvi rimedio	La notifica del data breach deve almeno: a) descrivere la **natura della violazione** dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione b) comunicare il nome e i dati di contatto del **responsabile della protezione dei dati** o di altro punto di contatto presso cui ottenere più informazioni; c) descrivere le probabili conseguenze della violazione dei dati personali d) descrivere le **misure adottate** o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi. Se le suddette informazioni non possono essere fornite contestualmente alla notifica, possono essere indicate in fasi successive senza ulteriore ingiustificato ritardo.-
Obblighi	I fornitori tengono un aggiornato inventario delle violazioni di dati personali, ivi incluse le circostanze in cui si sono verificate, le loro conseguenze e i provvedimenti	Il **titolare del trattamento** ha l'obbligo di documentare qualsiasi violazione dei dati

	adottati per porvi rimedio, in modo da consentire al Garante di verificare il rispetto delle disposizioni della normativa.	personali, comprese le circostanze ad essa relative, le sue conseguenze ed i provvedimenti adottati per porvi rimedio. La documentazione consente all'autorità di controllo di verificare il rispetto della normativa.
Comunicazione all'interessato	Il fornitore di servizi di comunicazione elettronica accessibili al pubblico, quando la violazione di dati personali rischia di arrecare pregiudizio ai dati personali o alla riservatezza di contraente o di altra persona, comunica agli stessi senza ritardo l'avvenuta violazione. La comunicazione al contraente o ad altra persona contiene almeno una descrizione della natura della violazione di dati personali ed i punti di contatto presso cui si possono ottenere maggiori informazioni ed elenca le misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione di dati personali. La comunicazione al Garante descrive, inoltre, le conseguenze della violazione di dati personali e le misure proposte o adottate dal fornitore per porvi rimedio.	Se la violazione dei dati personali può presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve comunicare la violazione anche all'interessato senza ingiustificato ritardo. La comunicazione all'interessato deve essere fatta con un **linguaggio semplice e chiaro** e deve contenere almeno le seguenti informazioni: · comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni · descrizione delle probabili conseguenze della violazione dei dati personali · descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Casi di esclusione della comunicazione	Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni: a) il titolare del trattamento ha messo in atto le **misure tecniche e organizzative** adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati 1. la comunicazione richiederebbe **sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica o ad una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Leggi anche: Privacy: come gestire un data breach

COSA CAMBIA - 09 APRILE 2018

GDPR: profilazione

La profilazione, disciplinata nel GDPR, consiste in un trattamento automatizzato con cui si elaborano i dati messi a disposizione dell'interessato e si costruisce un suo profilo al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica,

la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato.

La **profilazione** è un **trattamento automatizzato** con cui si **elaborano i dati** dell'interessato e si costruisce un suo profilo al fine di analizzare o prevedere determinati aspetti della sua persona (ad esempio la sua situazione economica, la salute, le preferenze o gli interessi personali).

Il profilo è generalmente utilizzato per **motivi commerciali**.

L'interessato deve aver prestato il proprio consenso esplicito alla profilazione, salvo casi specifici in cui non è richiesto (ad esempio, nel caso di conclusione o esecuzione di un contratto o autorizzazione dal diritto dell'UE o dello Stato).

Il Regolamento UE 2016/679 prevede che l'interessato debba essere informato dal titolare del trattamento dell'esistenza della profilazione e debba ricevere informazioni sulla **logica utilizzata**, nonché sull'importanza e sulle conseguenze previste.

A differenza del GDPR, nel Codice Privacy la profilazione non è espressamente trattata, ma il Garante si è occupato della questione con numerosi atti, provvedimenti e chiarimenti.

Cosa cambia	**Prima**	**Dopo**
	Fino al 24 maggio 2018	**Dal 25 maggio 2018**
Cos'è	-	La profilazione è un **trattamento automatizzato** con cui si **elaborano i dati** messi a disposizione dell'interessato e si costruisce un suo **profilo** al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato.
Quando può essere effettuata	-	La profilazione è ammessa se: - necessaria per la conclusione o l'esecuzione di un **contratto** tra l'interessato e un titolare del trattamento - **autorizzata dal diritto** dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato - si basa sul **consenso esplicito** dell'interessato.
Obblighi		Chi effettua la profilazione ha l'obbligo di informare l'interessato sulla **logica utilizzata**, nonché sull'**importanza** e sulle **conseguenze** previste.
Misure da adottare		Quando la profilazione è necessaria per la conclusione o l'esecuzione di un contratto o si basa sul consenso

esplicito dell'interessato, il titolare del trattamento deve attuare **misure appropriate** per tutelare i diritti, le libertà ed i legittimi interessi dell'interessato e, almeno, prevedere il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

Leggi anche:

- Privacy, GDPR: linee guida UE su profilazione e decisioni automatizzate

- GDPR, PMI: profilazione ai fini marketing. Con quali limiti?

COSA CAMBIA - 07 APRILE 2018

GDPR: valutazione d'impatto

La valutazione d'impatto è una nuova procedura introdotta dal GDPR che permette al titolare del trattamento di valutare la necessità, la proporzionalità ed i rischi del trattamento di alcune tipologie di dati, così da approntare misure idonee di sicurezza. La norma prevede casi specifici in cui la valutazione è obbligatoria.

La **valutazione d'impatto** sulla protezione dei dati è una novità introdotta dal Regolamento UE 2016/679 ed è espressione del principio di responsabilizzazione (**accountability**) del titolare nei confronti dei trattamenti da questo effettuati.

La valutazione è necessaria quando il trattamento può presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche e va fatta, in particolare, in alcuni specifici casi previsti dal Regolamento e cioè in presenza di un **monitoraggio sistematico** dei dati o di una sorveglianza sistematica su una zona accessibile al pubblico o quando i dati sensibili sono trattati su larga scala.

Qualora, inoltre, dalla valutazione emerga che il trattamento dei dati presenti comunque un rischio elevato, il titolare del trattamento è tenuto a consultare previamente l'**autorità di controllo**.

Sono esclusi dalla valutazione d'impatto i **trattamenti in corso** già autorizzati dalle autorità competenti e che non presentino modifiche significative prima del 25 maggio 2018, data di piena applicazione del Regolamento.

Cosa cambia	Prima	Dopo
	Fino al 24 maggio 2018	Dal 25 maggio 2018
Cos'è la valutazione d'impatto	-	E' una **procedura** grazie alla quale va valutata la necessità, la proporzionalità ed i rischi del trattamento di alcune tipologie di dati, per permettere al titolare del trattamento di approntare **misure idonee di sicurezza**.

Chi deve farla	-	Deve essere fatta dal **titolare** del trattamento, consultandosi con l'eventuale responsabile della protezione dei dati (DPO).
Con quali tempi	-	Deve essere effettuata **prima del trattamento** dei dati e deve essere soggetta a revisione continua
Quando è obbligatoria	-	Il titolare deve effettuare la valutazione d'impatto quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**. La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti: · una **valutazione sistematica** e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche · il **trattamento su larga scala di dati sensibili** o relativi a condanne penali ed a reati · la **sorveglianza sistematicasu larga scala** di una zona accessibile al pubblico.
Cosa contiene	-	Deve contenere almeno: · una **descrizione sistematica dei trattamenti** previsti e delle finalità del trattamento, compreso, l'eventuale interesse legittimo perseguito dal titolare del trattamento · una **valutazione della necessità e proporzionalità** dei trattamenti in relazione alle finalità · una valutazione dei rischi per i diritti e le libertà degli interessati · le **misure previste per affrontare i rischi**, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Leggi anche: Privacy 4.0: registro dei trattamenti, valutazione di impatti, analisi dei rischi

PER AZIENDE E PROFESSIONISTI - 06 MARZO 2018

Privacy: informativa e consenso tra i primi adempimenti

di Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano

Il GDPR sottopone ad un processo di revisione l'informativa e il consenso informato, in particolare nell'ipotesi in cui l'attività del titolare del trattamento si svolga online. Nella pratica, l'informativa può essere un foglio, una pagina web, un banner, un documento affisso in una sala d'aspetto o di una registrazione vocale, consegnato all'interessato prima di trattare i suoi dati. Il Regolamento UE suggerisce l'uso di tecniche semplici e "popolari" affinché le informazioni sul trattamento arrivino anche agli utenti inesperti. Il consenso è, invece, una manifestazione di volontà richiesta prima di procedere al trattamento dei dati "sensibili": con quali modalità?

Tra gli adempimenti previsti nel Regolamento UE 2016/679 assumono un ruolo centrale i processi di revisione delle **informative** e delle modalità di **raccolta dei consensi**, soprattutto se gran parte dell'attività del titolare del trattamento si svolge online.

L'informativa e il consenso sono adempimenti antichissimi, che erano già previsti nelle prime normative sulla data protection del secolo scorso, e hanno funzioni molto chiare e fondamentali.

L'informativa...

L'informativa ha, appunto, il compito di "informare" il soggetto, prima della raccolta dei suoi dati, su che fine faranno quelle informazioni (come saranno trattate, per quali scopi, con che impatto sulla sua privacy, con che tempi e limiti) e sui diritti che il soggetto potrà esercitare nei confronti di coloro che trattano quelle informazioni.

Nella pratica, l'informativa prende la forma di **un foglio** che è **consegnato prima di trattare i dati**, o di una pagina web, di un modulo cartaceo, di un banner, di un documento affisso in una sala d'aspetto o di una registrazione vocale. Di solito la legge non richiede una forma specifica ma guarda, per così dire, più al risultato: l'informativa deve rendere edotto il soggetto di tutte le operazioni che saranno svolte con i suoi dati e di chi siano i suoi contatti nei confronti dei quali esercitare i suoi diritti.

E il consenso

Il consenso è, invece, una **manifestazione di volontà** che è richiesta prima di procedere con particolari trattamenti (soprattutto quando si è in presenza di quei dati cosiddetti "sensibili", ossia legati alla salute, alle abitudini sessuali, alla origine razziale o etnica o alle opinioni di una persona, o quando si è nell'ambito del trattamento dei dati a fini di invio di materiale promozionale o pubblicitario).

Il consenso non è sempre obbligatorio che sia reso in forma scritta, con la classica firma apposta proprio sotto l'informativa. Il timore del Regolamento, evidente, è che ben presto tutti i consensi saranno raccolti online, sul web, diminuendo le garanzie rispetto a un soggetto consapevole che appone una firma "fisica" su un modulo.

Come strutturare l'informativa

Innanzitutto, ai sensi dell'Articolo 13 del GDPR, in caso di raccolta presso l'interessato dei dati che lo riguardano, il **titolare del trattamento** deve fornirgli una serie di informazioni, che vengono a costituire, appunto, l'informativa.

Un simile elenco di informazioni da fornire deve contenere, in particolare, l'identità e i dati di contatto del titolare del trattamento (ossia del soggetto che tratta i dati, al fine di conoscere le persone cui ci si può rivolgere per eventuali problemi), i dati di contatto del **Responsabile della Protezione dei Dati** (il "famoso" Data Protection Officer, una sorta di "presidio" per la verifica della conformità al Regolamento all'interno di una realtà che tratta i dati), le finalità e la base giuridica del trattamento (ossia il motivo per cui i dati sono trattati e le norme, o il contratto, che ne consentano il trattamento), i legittimi interessi perseguiti dal titolare o da terzi (nel caso il dato sia trattato, ad esempio, senza il consenso dell'interessato), gli eventuali **destinatari dei dati personali** (ossia in che direzioni il dato "viaggerà", che tragitti prenderà durante il suo trattamento, a chi sarà trasferito o perverrà, anche elettronicamente) e l'eventuale intenzione del titolare del trattamento di trasferire i dati a un Paese terzo o a un'organizzazione internazionale (qui vi è il timore, chiaro, che il dato "esca" dall'Unione Europea e pervenga a realtà che non lo tratterebbero con lo stesso livello di sicurezza e di protezione).

Il Paragrafo 2 dello stesso Articolo prosegue, poi, prevedendo informazioni aggiuntive da fornire nel momento in cui i dati personali sono ottenuti. In particolare, tali informazioni dovrebbero includere il **periodo di conservazione dei dati personali** o, in alternativa, i criteri utilizzati per determinare tale periodo (nel caso un titolare non possa prevedere esattamente la data di "morte" del dato), l'esistenza del diritto dell'interessato di chiedere l'accesso ai dati personali e la rettifica, la cancellazione o la limitazione degli stessi, nonché il diritto alla portabilità dei dati, il diritto di proporre reclamo a un'autorità di controllo (ossia il Garante del Paese di riferimento), l'indicazione se l'interessato ha l'obbligo di fornire i dati personali, nonché le possibili conseguenze della mancata comunicazione di tali dati, e l'esistenza di un processo decisionale automatizzato (in altre parole: se i dati della persona vengono trattati da software e algoritmi senza l'intervento dell'essere umano ma generano, comunque, conseguenze giuridiche, ad esempio il rifiuto di concedere un mutuo o un prestito).

In sostanza, quindi, i principi alla base di un trattamento corretto e trasparente implicano che l'interessato debba essere informato dell'esistenza del trattamento e delle sue finalità. Il titolare del trattamento, inoltre, dovrebbe fornire eventuali, ulteriori informazioni tenendo conto delle circostanze e del contesto specifici in cui i dati personali sono trattati.

Come evidenziato nel Considerando n. 60, l'interessato dovrebbe, ad esempio, essere informato dell'esistenza di una **profilazione** e delle conseguenze della stessa. Per "profilazione" s'intende, genericamente, un'attività automatizzata che sia in grado di ricostruire gusti, preferenze, performance lavorative e abitudini di un individuo.

> Tutte le informazioni che abbiamo elencato poco sopra potrebbero essere fornite in combinazione con **icone standardizzate**, per dare in maniera facilmente comprensibile un quadro d'insieme del trattamento previsto. Il Regolamento sembra, infatti, suggerire l'uso di tecniche semplici e "popolari" (animazioni, fumetti, infografiche, schemi e disegni) affinché le informazioni sul trattamento arrivino agli utenti, anche a quelli inesperti o che non conoscono la normativa sulla data protection, nel modo più chiaro possibile.

L'interessato, dal canto suo, dovrebbe ricevere queste informazioni nel momento in cui si verifica la raccolta dei dati personali che lo riguardano o, se i dati sono ottenuti da altra fonte, entro un termine ragionevole (Considerando n. 61).

Se i dati personali possono essere legittimamente comunicati a un altro destinatario, l'interessato dovrebbe esserne informato nel momento in cui il destinatario riceve la prima comunicazione. Ai sensi del Paragrafo 3 dell'Articolo 13, qualora il titolare del trattamento intendesse trattare i dati personali per una finalità diversa da quella per cui erano stati raccolti, prima di tale ulteriore trattamento dovrebbe fornire all'interessato informazioni relative a tale diversa finalità.

Viceversa, come disposto dall'Articolo 14 del GDPR, **non è necessario imporre l'obbligo dell'informazione** se l'interessato ne è già in possesso, se la registrazione o la comunicazione dei dati sono previste per legge, se i dati devono rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri o se informare l'interessato si rivela impossibile o, comunque, un compito tale da richiedere uno sforzo sproporzionato. Quest'ultima eventualità potrebbe, ad esempio, verificarsi nei trattamenti eseguiti a fini di **ricerca scientifica o storica**, a fini statistici o di archiviazione nel pubblico interesse: in tali casi, infatti, è opportuno tener conto (come specificato nel Considerando n. 62) del numero di interessati, della vetustà dei dati e della presenza di eventuali garanzie adeguate.

Come ottenere un consenso informato

Per quanto riguarda i trattamenti basati sul consenso dell'interessato, secondo il disposto dell'Articolo 7 del GDPR, il titolare del trattamento deve essere in grado di dimostrare che l'interessato vi ha acconsentito.

Com'è noto, informativa e consenso sono due adempimenti ben distinti (la prima ci deve sempre essere, il secondo può mancare) ma, quando coesistono, sono legati a doppio filo.

Il consenso deve sempre essere manifestato liberamente (l'interessato non deve mai essere condizionato nel momento in cui lo deve conferire) anche quando viene dato online (e non attraverso la "tradizionale" firma) e deve essere il risultato di una chiara e assertiva manifestazione di volontà.

In particolare, nel contesto di una **dichiarazione scritta** che riguardi anche altre questioni contrattuali, dovrebbero esistere garanzie tali da assicurare che l'interessato sia consapevole di stare esprimendo un consenso: la relativa richiesta dovrà essere presentata in modo chiaramente distinguibile dalle altre parti del documento o della pagina web, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro, che non contenga clausole abusive. Le dichiarazioni in contrasto con il Regolamento non saranno da considerarsi vincolanti.

Come precisato chiaramente nel Considerando n. 42, ai fini di un consenso informato, l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità perseguite.

Il consenso, d'altro canto, non dovrebbe essere considerato liberamente espresso nel caso in cui l'interessato non sia in grado di operare una scelta autenticamente libera (si pensi a delle caselle di scelta su un sito web che siano pre-impostate, o al fatto che si costringa un utente a seguire obbligatoriamente un "percorso" nelle sue scelte) o si trovi nell'impossibilità di rifiutare o revocare il consenso senza subire un pregiudizio.

Il Considerando n. 43 precisa che il consenso si presume non liberamente espresso (e, quindi, non valido) se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto è subordinata al consenso, sebbene esso non sia necessario. Il primo caso è quello in cui è domandato un solo consenso per operazioni sui dati che, in realtà, sono ben distinte tra loro. Il secondo caso riguarda, invece, quei contratti dove viene chiesto un consenso obbligatorio per effettuare trattamenti che in realtà non sono connessi alla esecuzione del contratto principale (si obbliga un utente ad "accettare" un trattamento finalizzato al marketing, ad esempio, "minacciandolo" di non fornirgli il servizio principale se non dovesse accettare).

Trattamento dei dati del minore

Un ultimo cenno merita, infine, la situazione dei minori, cui il GDPR riserva una particolare protezione: l'Articolo 8 prevede, infatti, che il trattamento di dati personali relativi a tali soggetti sia lecito qualora il **minore abbia almeno 16 anni**. Nel caso in cui invece abbia un'età inferiore, il trattamento è lecito solo se il consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

Gli Stati membri possono anche stabilire un'età inferiore a tali fini, senza però scendere sotto alla soglia dei 13 anni. In ogni caso, il titolare del trattamento è tenuto ad adoperarsi in modo ragionevole per verificare la corretta prestazione o autorizzazione del consenso, tenuto conto delle tecnologie disponibili.

Considerazioni finali

Questi primi due adempimenti, l'informativa e il consenso, sono due autentiche pietre miliari nel sistema della protezione dei dati, perché mirano a funzioni fondamentali e ineludibili.

Nessuna persona può vedere i suoi dati trattati se, prima, non è informata nel dettaglio sul destino di quei dati. Il consenso, soprattutto quando conferito online, deve sempre essere una chiara, libera e inequivocabile manifestazione di volontà.

Nella pratica, accanto a una revisione delle informative per renderle più dettagliate, sarò opportuno pensare a **modalità efficaci** per raccogliere e custodire i consensi espressi online, che saranno sempre più comuni.

DATI PERSONALI E DIRITTI

PREVISTE ANCHE DEROGHE - 07 MARZO 2018

Privacy e dati personali 4.0: quali tutele?

di Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano

Accanto all'idea di dato personale tradizionale si profila, nel GDPR, l'idea di dato "più moderno" legato all'era degli smartphone, dei social network e degli algoritmi di profilazione, che meritano lo stesso livello di protezione. Le persone fisiche oggi possono, infatti, essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP. E tali identificativi sono idonei a lasciare tracce che, se combinate con altre informazioni ricevute dai server, possono essere utilizzate per creare profili e identificare le persone. Quali tutele prevede il nuovo regolamento privacy UE?

L'articolo 4 del GDPR contiene una precisa definizione di "dato personale", inteso come qualsiasi informazione riguardante una persona fisica identificata o identificabile, denominata

“interessato”.

In particolare, si considera identificabile la **persona fisica** a cui ci si può riferire – direttamente o indirettamente – tramite un identificativo, come un nome, un dato relativo all’ubicazione, un numero di identificazione, o tramite uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Le persone fisiche possono, infatti, essere associate a **identificativi online** prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP (Considerando n. 30). Tali identificativi sono idonei a lasciare tracce che, se combinate con altre informazioni ricevute dai server, possono essere utilizzate per creare profili e identificare le persone fisiche. Sulla base di tali osservazioni, si ritiene dunque auspicabile un’applicazione dei principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile.

Il Considerando n. 26 precisa che per stabilire l’identificabilità di una persona è opportuno considerare tutti i mezzi di cui il titolare del trattamento, o un terzo, possono ragionevolmente disporre per identificare detta persona. In particolare, si dovrebbe tenere conto dell’**insieme dei fattori obiettivi**, tra cui i costi e il tempo necessario per identificazione, tenendo presenti altresì le tecnologie disponibili al momento del trattamento.

Viceversa, i principi di protezione dei dati non dovrebbero applicarsi, neppure per finalità statistiche o di ricerca, a informazioni anonime, ossia a informazioni che non si riferiscono a una persona fisica identificata o identificabile, o che si riferiscono a dati personali resi sufficientemente anonimi da impedire l’identificazione dell’interessato.

Il Regolamento, inoltre, non si applica ai dati personali delle **persone decedute**, con riguardo ai quali i singoli Stati membri possono prevedere specifiche norme.

Categorie di dati personali

L’Articolo 4 del GDPR prosegue, poi, individuando alcune specifiche categorie di dato personale: troviamo, innanzitutto, i dati genetici, ossia i dati relativi alle **caratteristiche genetiche, ereditarie o acquisite**, di una persona fisica, idonee a fornire informazioni univoche sulla sua fisiologia o salute e risultanti dall’analisi di un campione biologico dell’interessato, in particolare – come specificato dal Considerando n. 34 – dall’analisi dei cromosomi, del DNA, del RNA o di altro elemento che consenta di ottenere informazioni equivalenti.

In secondo luogo, vengono menzionati i **dati biometrici**, vale a dire i dati ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona, che ne consentono o ne confermano l’identificazione univoca; sono tali, ad esempio, l’immagine facciale o i dati dattiloscopici.

Infine, troviamo la categoria dei **dati relativi alla salute**, in cui dovrebbero rientrare tutti i dati riguardanti lo stato di salute fisica o mentale presente, passata o futura dell'interessato.

Tra questi, come spiegato nel Considerando n. 35, sono comprese:

- le informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di **assistenza sanitaria**

- un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari

- le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica

- più in generale, qualsiasi informazione riguardante **malattie, disabilità, anamnesi mediche**, trattamenti clinici o stati fisiologici dell'interessato, indipendentemente dalla fonte.

Tutele per i dati particolarmente sensibili ...

Il Considerando n. 51 evidenzia come meritino una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali: per tale ragione, l'Articolo 9 del GDPR vieta il trattamento dei dati genetici, biometrici, relativi alla salute o alla vita sessuale di una persona, nonché dei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni filosofiche o religiose o l'appartenenza sindacale, a tutela dei diritti e delle libertà dell'interessato.

... e deroghe

Quanto disposto, tuttavia, non trova applicazione in una serie di circostanze, e in particolare quando:

1) l'interessato abbia prestato esplicitamente il proprio **consenso al trattamento** di tali dati, fatta eccezione per il caso in cui il diritto dell'Unione o degli Stati membri dispone che il divieto non sia revocabile

2) 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 e protezione sociale, in presenza di garanzie appropriate

3) 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

4) il trattamento sia effettuato, nell'ambito delle sue legittime attività e con **adeguate garanzie**, da una fondazione, associazione o altro organismo senza scopo di lucro, a condizione che il trattamento riguardi unicamente le persone che hanno regolari contatti con l'organismo in questione e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato

5) il trattamento riguardi dati personali resi manifestamente pubblici dell'interessato

6) il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziale, amministrativa o stragiudiziale

7) il trattamento sia necessario per motivi di interesse pubblico, rilevante sulla base del diritto dell'Unione o degli Stati membri. Questo si verifica nel caso anche nel caso in cui il trattamento di dati personali sia effettuato a cura di autorità pubbliche allo scopo di realizzare fini, previsti dal diritto costituzionale o dal diritto internazionale pubblico, di associazioni religiose ufficialmente riconosciute.

8) 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. In particolare, questo è possibile se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti, o da altra persona anch'essa soggetta all'obbligo di segretezza;

9) il trattamento sia necessario per motivi di interesse pubblico nel settore della sanità pubblica. Come precisato dal Considerando n. 54, in tale contesto la nozione di "sanità pubblica" dovrebbe essere interpretata secondo la definizione del regolamento CE n. 1338/2008 del Parlamento europeo e del Consiglio, dunque come l'insieme di tutti gli elementi relativi alla salute, quali lo stato di salute, morbilità e disabilità incluse, i determinanti aventi un effetto su tale stato di salute, le necessità e le risorse in materia di assistenza sanitaria, l'effettiva prestazione e l'accesso universale a essa, la spesa sanitaria e il relativo finanziamento, le cause di mortalità

8) il trattamento sia necessario a fini di **archiviazione nel pubblico interesse**, di ricerca scientifica o storica o a fini statistici.

È dunque possibile e opportuno prevedere espressamente deroghe al divieto generale di trattare le suddette categorie particolari di dati personali, purché siano fatte salve le adeguate

garanzie.

Il Paragrafo 4 dell'Articolo 9, infine, contiene una formula di chiusura che consente agli Stati membri di mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento dei c.d. "dati sensibili", senza tuttavia ostacolare la libera circolazione dei dati personali all'interno dell'Unione quando tali condizioni si applicano al trattamento transfrontaliero degli stessi.

Considerazioni conclusive

L'idea alla base del Regolamento è quella di presentare un dato personale "più moderno" e più legato all'era degli smartphone, dei braccialetti fitness, dei social network, degli algoritmi di profilazione e di decisioni automatizzate.

Accanto, quindi, all'idea di dato personale più tradizionale, che rimane, sono evidenziati dati che sono collegati alla vita elettronica della persona e alla sua identità sui social network e che meritano, oggi, lo stesso livello di protezione.

ANCHE PER L'UTILIZZO DI NUOVE TECNOLOGIE - 08 MARZO 2018

GDPR: maggiori tutele per gli interessati al trattamento dei dati

di Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano

Pur presentando elementi di continuità rispetto alla normativa precedente, il GDPR ha previsto nuovi diritti per gli interessati dal trattamento dei dati, avendo sempre ben presente i pericoli e i rischi che derivano dall'uso delle nuove tecnologie. Si parte da un principio di fondo. Il titolare che tratta il dato non ne diventa "proprietario", ma deve essere consapevole che l'interessato - ossia la persona fisica cui i dati si riferiscono - può, in ogni momento, esercitare una sorta di "potere di controllo" su quei dati. I poteri di controllo sono indicati chiaramente dal GPR: quali sono?

Il **GDPR**, per quanto concerne il tema dei diritti degli interessati al trattamento, presenta diversi elementi di continuità rispetto alla normativa precedente (D.Lgs. 196/2003 e Direttiva 95/46/CE).

A ben vedere, però, il Legislatore europeo ha introdotto, nella lunga elencazione (che va dall'art. 15 al 22 del GDPR), **nuove prerogative** riconosciute agli interessati dal trattamento, tenendo in considerazione l'attuale sviluppo delle nuove tecnologie che, potenzialmente, può determinare nuovi **pericoli e rischi** per i diritti e le libertà degli stessi.

Cosa si intende per “diritti degli interessati”

Per diritti degli interessati si intendono quei diritti che un soggetto può esercitare con riferimento ai propri dati. In altre parole, il titolare che tratta il dato non ne diventa “proprietario” ma deve sempre essere consapevole che l’interessato – ossia la persona fisica cui i dati si riferiscono – può, in ogni momento, esercitare una sorta di “**potere di controllo**” su quei dati, e tali poteri di controllo sono ben indicati nel testo di legge.

Ai sensi dell’Articolo 15 del GDPR, infatti, l’interessato ha il diritto di ottenere innanzitutto dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano, ossia di conoscere se un determinato soggetto sia in possesso o meno di sue informazioni.

In tal caso, se il **trattamento è in corso**, la persona ha diritto di accedere ai dati e alle informazioni riguardanti le finalità del trattamento, le categorie di dati personali in questione, i destinatari o le categorie di destinatari a cui i dati personali sono, o saranno, comunicati, in particolare se destinatari di Paesi terzi o organizzazioni internazionali (compreso il diritto di essere informato circa l’esistenza di garanzie adeguate relative al trasferimento).

Quando possibile, l’interessato ha anche il diritto di sapere il **periodo di conservazione** dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare questo periodo, l’esistenza del diritto dell’interessato di chiedere la rettifica, la cancellazione o la limitazione del trattamento dei dati personali che lo riguardano, il diritto di proporre reclamo a un’Autorità di controllo.

Qualora i dati non siano raccolti presso l’interessato, il soggetto ha diritto di ricevere tutte le informazioni disponibili sulla loro origine e sull’esistenza di un processo decisionale automatizzato, compresa l’eventuale **attività di profilazione** nei confronti dell’interessato al trattamento.

In base a tali disposizioni, quindi, un interessato dovrebbe avere il diritto di accedere ai dati personali raccolti che lo riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. Ove possibile, il titolare del trattamento dovrebbe fornire l’**accesso remoto a un sistema sicuro** che consenta all’interessato di consultare direttamente i propri dati personali (ad esempio un pannello o un’area riservata su un sito web che faciliti una simile operazione da remoto). Tale diritto non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, anche se tali considerazioni non dovrebbero condurre a un diniego a fornire all’interessato tutte le informazioni.

Nel caso in cui un titolare del trattamento tratti una notevole quantità di informazioni riguardanti l’interessato, dovrebbe poter richiedere che quest’ultimo precisi l’informazione o le attività a cui la sua richiesta si riferisce. Egli, inoltre, dovrebbe adottare tutte le misure ragionevoli per verificare l’identità dell’interessato che domanda l’accesso, in particolare nel contesto di servizi e identificativi online.

Rettifica dei dati personali

L’Articolo 16 del GDPR stabilisce che l’interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo, nonché l’integrazione dei dati personali incompleti.

Il “diritto all'oblio”

L’Articolo 17, poi, prevede il “diritto all'oblio” nel caso in cui la conservazione dei dati violi lo stesso GDPR o il diritto dell’Unione o degli Stati membri cui è soggetto il titolare del trattamento.

In particolare, l’interessato dovrebbe avere il diritto di chiedere che siano **cancellati** e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le

quali erano stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al Regolamento.

Tale diritto è particolarmente importante se l'interessato ha prestato il proprio **consenso quando era minorenne**, quindi non pienamente consapevole dei rischi derivanti dal trattamento, e decida, successivamente, di eliminare questo tipo di dati personali (in particolare da Internet). L'interessato dovrebbe poter esercitare tale diritto indipendentemente dal fatto che non sia più un minore.

Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un **obbligo legale**, per eseguire un compito di interesse pubblico, per motivi inerenti al settore della sanità pubblica, per fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

Per rafforzare il diritto all'oblio nell'ambiente online, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati di cancellare qualsiasi link, copia o riproduzione degli stessi. Nel fare ciò, è opportuno che il titolare del trattamento adotti misure ragionevoli tenendo conto della tecnologia e dei mezzi a disponibili.

Il diritto alla limitazione

Un'altra novità che merita un approfondimento specifico è il diritto di limitazione introdotto dall'Articolo 18 del GDPR.

Il diritto alla limitazione è una sorta di **sospensione temporanea** (ma che può, in determinate condizioni, diventare anche permanente) del trattamento in corso – con l'unica eccezione consentita alla sola conservazione – che deve essere adottata dal Titolare previa valutazione di una serie di circostanze.

L'effetto principale della limitazione, dunque, consiste nel non sottoporre i dati a ulteriori trattamenti (salvo, appunto, la sola conservazione): la limitazione, infatti, può essere chiesta **al posto della cancellazione** (e ciò avviene, ad esempio, in attesa di definire l'esattezza o l'obsolescenza di un dato o per continuare a utilizzare il dato per specifiche finalità) e in sostituzione del blocco del trattamento.

In particolare, l'interessato ha il diritto di ottenere la limitazione del trattamento dei dati personali quando:

- contesta l'**esattezza dei dati**, per il periodo necessario al titolare del trattamento per effettuare le opportune verifiche

- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati (chiedendo, al suo posto, che ne sia limitato l'utilizzo)

- benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, oppure,

- l'interessato si è opposto al trattamento, in attesa della verifica se i motivi legittimi del titolare del trattamento prevalgano su quelli dell'interessato.

Come suggerito dallo stesso Legislatore europeo nei Considerando al Regolamento, dal punto di vista pratico le modalità per limitare il trattamento dei dati personali potrebbero consistere, tra l'altro, nel **trasferire temporaneamente i dati** selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito web.

Negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe, in linea

di massima, essere assicurata mediante **dispositivi tecnici**, in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato.

Il diritto alla portabilità

Infine, all'Articolo 19 si trova riconosciuto il diritto alla portabilità, che consiste nella facoltà per l'interessato di ricevere – in un formato strutturato, di uso comune e leggibile da dispositivo automatico – i dati personali che lo riguardano forniti a un titolare del trattamento e di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare originario.

In conclusione

Il quadro dei diritti dell'interessato appare, in conclusione, estremamente potenziato, soprattutto con riferimento alla possibilità di cancellare informazioni, "congelare" archivi contenenti dati e rendere i dati portabili da un sistema informatico all'altro.

DAL REGOLAMENTO UE - 09 MARZO 2018

Privacy 4.0: nasce la portabilità dei dati personali

di Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano

Il GDPR introduce il diritto alla portabilità dei dati: gli interessati possono ricevere, in un formato di uso comune e leggibile meccanicamente, i dati personali forniti al titolare del trattamento e trasmetterli ad un diverso titolare senza alcun impedimento. La portabilità dei dati rappresenta uno dei diritti più importanti nella società dell'informazione: oltre a garantire continuità nel servizio, aumenta la concorrenza tra i fornitori di servizi e, di conseguenza, migliora la qualità del servizio offerto. Quali sono i maggiori problemi che possono sorgere nell'operatività? Quali le differenze con il diritto di accesso?

L'articolo 20 del **GDPR** introduce il **diritto alla portabilità dei dati**, che permette agli interessati di ricevere, in un formato strutturato, di uso comune e leggibile meccanicamente, i dati personali da loro forniti al titolare del trattamento e di trasmetterli a un diverso titolare senza impedimenti.

L'idea di un diritto alla portabilità dei dati è molto simile a quella che sta alla base della portabilità di un numero di telefono cellulare, per cui una persona può scegliere di mantenere lo stesso numero e di "portarselo" presso un altro gestore che offra condizioni più convenienti.

In molte infografiche e icone che descrivono questo nuovo diritto, vi è il disegno di una persona che si è caricata in spalla tutti i suoi dati e li porta senza problemi da un gestore (ad esempio una banca, o un provider) all'altro.

Differenze con il diritto di accesso

Sebbene questo nuovo diritto appaia strettamente connesso al diritto d'accesso previsto dall'originaria Direttiva sulla protezione dei dati (95/46/CE), è importante sottolineare come, invece, per molti aspetti se ne distanzi.

Innanzitutto, mentre l'esercizio del diritto di accesso è vincolato al **formato** che il titolare decide di utilizzare nel fornire le informazioni richieste (in altre parole: un soggetto va a domandare di accedere ai suoi dati e i dati gli vengono forniti nel formato scelto dal titolare), il nuovo diritto alla portabilità intende promuovere il controllo degli interessati sui propri dati personali, facilitando la circolazione, la copia o la trasmissione dei dati da un ambiente informatico all'altro. Per tale ragione è previsto che il dato sia rilasciato "in un formato strutturato, di uso comune e leggibile da dispositivo automatico".

In secondo luogo, il diritto alla portabilità si presenta come un'integrazione del diritto di accesso, in quanto comprende il diritto dell'interessato di ricevere un "sottoinsieme" dei dati personali che lo riguardano e di conservarli, su un supporto personale o su un cloud privato, in vista di un utilizzo ulteriore per scopi personali.

Per quanto riguarda, poi, la **trasmissione** di tali dati da un titolare del trattamento a un altro, l'interessato può anche richiedere che essa avvenga direttamente tra i titolari, ove ciò sia tecnicamente possibile.

Così, pur non essendovi uno specifico obbligo in tal senso, si tenta di promuovere lo sviluppo di formati interoperabili tra i titolari, al fine di favorire una **condivisione di dati personali** in piena sicurezza e sotto il controllo dell'interessato.

Occorre anche precisare che il titolare che dia seguito alla richiesta di portabilità non è responsabile dell'osservanza delle norme in materia di protezione dei dati da parte del titolare ricevente (ad esempio: un altro provider che riceve i dati di posta elettronica dell'interessato), visto che quest'ultimo non viene da lui selezionato (non sarà quindi responsabile se capiterà, ad esempio, una violazione dei dati nel nuovo servizio scelto dall'interessato). Al contempo, il titolare cui l'interessato si rivolge dovrebbe prevedere **garanzie idonee** a far sì che ogni sua attività corrisponda alle richieste dell'interessato stesso.

Considerato l'ampio ventaglio di tipologie di dati potenzialmente oggetto di trattamento, il GDPR non contiene indicazioni precise sul formato da adottare. La scelta dovrà essere, allora, la più idonea in rapporto al singolo settore di attività ed essere sempre orientata all'obiettivo ultimo di garantire un ampio margine di portabilità. Qualora non vi siano formati di impiego comune in un determinato contesto, i titolari dovrebbero utilizzare formati aperti (ad esempio: l'XML).

La portabilità non impone al titolare alcun obbligo di **conservazione dei dati** per un periodo superiore al necessario, o ulteriore, rispetto a quello eventualmente specificato. Al contempo, tuttavia, essa non pregiudica l'esercizio degli altri diritti: l'interessato può, quindi, continuare a fruire e beneficiare del servizio offerto dal titolare anche dopo che sia compiuta un'operazione di portabilità, che – è bene ribadirlo – non comporta la cancellazione automatica dei dati conservati nei sistemi del titolare, e non incide sul periodo di conservazione previsto originariamente per i dati oggetto di trasmissione. Analogamente, l'interessato può esercitare il diritto di cancellazione (o "diritto all'oblio") previsto dall'Articolo 17 del Regolamento.

Ai sensi del GDPR, il diritto alla portabilità dei dati presuppone che il trattamento si basi sul consenso dell'interessato oppure su un contratto di cui è parte l'interessato. Non è, invece, previsto un diritto generale alla portabilità dei dati il cui trattamento non si fondi su uno di questi due elementi.

Inoltre, tale diritto sussiste esclusivamente se il trattamento è "effettuato con mezzi automatizzati" e non si applica, di conseguenza, alla maggioranza degli archivi o dei registri cartacei.

Dati portabili

Per quanto concerne i dati "portabili", l'articolo 20, Paragrafo 1, stabilisce che sono tali i **dati personali** che riguardano l'interessato e sono stati forniti dall'interessato a un titolare.

Con riferimento alla prima condizione, va osservato che un dato anonimo, o non relativo all'interessato, non ricade nell'ambito di applicazione del diritto in questione. In molti casi, tuttavia, i titolari trattano informazioni contenenti dati personali relativi a una pluralità di interessati. Non è possibile, pertanto, dare un'interpretazione eccessivamente restrittiva dell'espressione "dati personali che riguardano l'interessato". Per esempio, i tabulati telefonici riferiti a un abbonato, la messaggistica interpersonale o i dati VoIP comprendono, talora, informazioni su terzi in riferimento alle chiamate in entrata e in uscita. Anche se si tratta di tabulati contenenti dati personali relativi a una pluralità di individui, l'abbonato deve avere la possibilità di ottenere tali informazioni a seguito di una richiesta di portabilità, dal momento che essi contengono (anche) dati a lui relativi.

La seconda condizione, invece, limita l'ambito della portabilità ai dati "forniti da" un interessato. Sono qualificabili come tali i dati forniti consapevolmente e attivamente dall'interessato (indirizzo postale, nome utente, età, etc.) e i dati osservati forniti dall'interessato attraverso la fruizione di un servizio o l'utilizzo di un dispositivo. Questa categoria comprende i "**dati grezzi**", come la cronologia delle ricerche effettuate sul web, i dati relativi al traffico, quelli relativi all'ubicazione, etc.

Non sono, invece, ricompresi in tale nozione i **dati inferenziali**, né i dati generati dal titolare utilizzando come input i dati osservati o forniti direttamente, come ad esempio il profilo-utente creato a partire dall'analisi dei dati grezzi generati da un contatore intelligente.

Limiti all'esercizio del diritto

L'articolo 20, Paragrafo 4, stabilisce un'ulteriore condizione, prevedendo che l'osservanza del diritto alla portabilità non deve ledere i diritti e le libertà altrui. Tale disposizione è intesa a evitare il recupero e la trasmissione a un nuovo titolare di informazioni contenenti i dati personali di altri interessati che a ciò non abbiano acconsentito.

Per evitare di ledere diritti e libertà dei terzi interessati, il trattamento dei dati personali in questione da parte di un diverso titolare è consentito soltanto nella misura in cui i dati rimangano nell'**esclusiva disponibilità dell'utente** che ne aveva richiesto la portabilità e siano utilizzati esclusivamente per finalità personali o domestiche.

Il nuovo titolare non può utilizzare i dati riferiti a terzi per le proprie finalità, né per ricavare informazioni sugli stessi e creare profili specifici; in caso contrario, è verosimile che il trattamento risulti illecito e violi il principio di correttezza. Inoltre, per ridurre ulteriormente i rischi, sarebbe opportuno che i titolari rendessero disponibili strumenti per consentire agli interessati di scegliere i dati che desiderano trasmettere e ricevere, escludendo (se del caso) i dati di altri interessati.

Ai titolari è fatta espressa raccomandazione di informare gli interessati dell'esistenza del diritto alla portabilità. Qualora i dati personali in questione siano raccolti direttamente presso l'interessato, l'informativa deve essere fornita nel momento in cui i dati sono ottenuti. Se, invece, i dati personali non sono stati ottenuti direttamente dall'interessato, l'Articolo 14, Paragrafo 3, prevede che l'**informativa** sia fornita entro un termine ragionevole e, comunque, non superiore a un mese dall'ottenimento dei dati.

Autenticazione e tempistiche

Il GDPR non contiene prescrizioni specifiche rispetto all'eventuale **autenticazione di un interessato** che eserciti il suo diritto alla portabilità. Tuttavia, qualora il titolare nutra ragionevoli dubbi circa l'identità di questi, può chiedere informazioni ulteriori che siano tali da confermarla. Tali richieste non devono essere eccedenti, né comportare la raccolta di dati

personali che non siano pertinenti o necessari. Se l'interessato fornisce effettivamente tali informazioni ulteriori, il titolare non può rifiutarsi di dare seguito alla richiesta.

Per quanto riguarda le tempistiche, in base all'articolo 12, Paragrafo 3, il titolare fornisce informazioni all'interessato "**senza ingiustificato ritardo**", e comunque entro un mese dal ricevimento dalla richiesta o, in casi di particolare complessità, entro un massimo di tre mesi, purché l'interessato venga informato delle motivazioni di tale proroga entro un mese dal ricevimento della richiesta iniziale. I titolari che oppongono un diniego alla richiesta di portabilità devono indicare all'interessato i motivi dell'inottemperanza e la possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso. I titolari devono rispettare l'obbligo di ottemperare nei termini previsti, anche in caso di diniego.

Considerazioni finali

La portabilità si presenta, in conclusione, come uno dei diritti più interessanti esercitabili nella società dell'informazione.

Oltre a garantire continuità nel servizio (si pensi a un utente che per anni utilizzi un servizio di posta elettronica e voglia migrare a un altro che ritiene migliore senza perdere tutti i messaggi), aumenta la concorrenza tra fornitori di servizi, che si vedranno costretti a lavorare sulla qualità del servizio offerto per evitare la migrazione di massa degli utenti verso altre società simili.

I problemi maggiori, in un'ottica di adempimento, sorgeranno qualora i dati siano trattati con **strumenti o software proprietari:** sarà indispensabile uno strumento di conversione per renderli realmente "portabili" anche verso sistemi di concorrenti commerciali.

PORTATA INNOVATIVA DEL REGOLAMENTO UE - 10 MARZO 2018

Privacy e cancellazione dei dati: nuovi adempimenti per il titolare del trattamento

di Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano

Per proteggere realmente i diritti dell'individuo diventa essenziale prevedere la "morte" del dato soprattutto nell'ambiente online che tutto ricorda e diffonde. Ed è per questo che il GDPR rafforza il diritto alla cancellazione dei dati personali unitamente al diritto all'oblio, e non solo in presenza di un motivo specifico, ma anche, genericamente, perché non ha più senso che le informazioni, pur raccolte legittimamente, restino in vita. Tuttavia è nei doveri specifici posti a carico del titolare del trattamento la vera portata innovativa del regolamento UE: quali sono?

Tra le principali novità introdotte dal **GDPR** merita una menzione particolare il rafforzamento del diritto alla **cancellazione dei dati personali** che è unito, nel testo del Regolamento, al **diritto all'oblio**, un diritto inizialmente riconosciuto solo a livello giurisprudenziale sia in campo europeo che nazionale e che, invece, nelle nuove norme trova un espresso cenno che ne indica portata e limiti.

Questo specifico aspetto è disciplinato dall'articolo 17 del Regolamento, che prevede un diritto che non ha carattere assoluto, in quanto dev'essere inevitabilmente contemperato con altri interessi (primo fra tutti: il diritto di cronaca) e che può essere definito come "l'interesse di un singolo a essere dimenticato".

La sua concretizzazione consiste nella cancellazione (o, in alcuni casi, nella de-indicizzazione) dei contenuti, dalle varie pagine web, di precedenti informazioni (spesso pregiudizievoli) che non rappresentano più la vera identità dell'interessato. Quanto detto, tuttavia, non può avvenire in modo incondizionato e, prima le Corti nazionali e comunitarie, poi la regolamentazione contenuta nel GDPR, hanno stabilito quali debbano essere le condizioni necessarie per un **corretto esercizio del diritto** in questione, soprattutto ai fini della sua compatibilità con il diritto d'informazione che, nei casi di interesse pubblico, dovrà comunque prevalere sull'interesse del singolo.

Cancellazione dei dati personali

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano **senza ingiustificato ritardo** e il titolare del trattamento ha l'obbligo di cancellare tali dati se essi non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati. Questo primo principio mira a far sì che i dati non siano conservati in eterno quando hanno obiettivamente esaurito la loro funzione, ed era già previsto anche nella normativa precedente (per amore di precisione, potremmo dire che in questo caso stiamo parlando di cancellazione dei dati personali custoditi da un titolare e non di diritto all'oblio in senso stretto).

La cancellazione può essere, inoltre, richiesta qualora l'interessato abbia **ritirato il proprio consenso** o si sia opposto al trattamento dei dati personali che lo riguardino, o ancora quando tale trattamento sia stato effettuato illecitamente o in maniera non conforme allo stesso GDPR, o nel caso in cui si debba adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o, infine, se i dati personali siano stati raccolti relativamente all'offerta di servizi della società dell'informazione.

Tale diritto è, in particolare, rilevante se l'interessato ha prestato il proprio consenso quando era minorenne, quindi non pienamente consapevole dei rischi derivanti dal trattamento, e decida, in un secondo momento, di eliminare un certo tipo di dati personali, in particolare da Internet. L'interessato dovrebbe poter esercitare il diritto in esame indipendentemente dal fatto che non sia più un minore.

Deroghe consentite

D'altra parte, tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati personali in una serie di specifiche circostanze, e in particolare:

1) qualora sia necessaria per esercitare il **diritto alla libertà di espressione e di informazione** (in questo caso entrano "in conflitto" due diritti, quello alla protezione dei dati e quello a una libera informazione, che si devono obbligatoriamente bilanciare)

2) per adempiere un **obbligo legale**

3) per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento

4) per motivi di **interesse pubblico** nel settore della sanità pubblica

5) a fini di archiviazione, di ricerca scientifica o storica o a fini statistici

6) per accertare, esercitare o difendere un diritto in sede giudiziaria.

Adempimenti del titolare del trattamento

Sulla base di quanto detto, si potrebbe ritenere che l'Articolo 17 non introduca modalità davvero innovative rispetto al diritto alla cancellazione previsto dalla precedente Direttiva, salvo alcune precisazioni legate a nuove tutele contenute nel Regolamento stesso.

Tuttavia, la portata innovativa della nuova disposizione c'è, e riguarda il dovere specifico posto a carico del **titolare** che riceva una richiesta di cancellazione quando i dati che ne sono oggetto siano stati "resi pubblici" dal titolare stesso. Una sorta di **obbligo di "rincorrere"** i dati quando il titolare che riceve la richiesta di cancellazione li ha già comunicati ad altri titolari e, quindi, messi in circolazione.

Come specificato nei Considerando al Regolamento, infatti, per rafforzare il **diritto all'oblio** nell'ambiente online è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a comunicare ai titolari che trattano tali dati di cancellare qualsiasi link, copia o riproduzione degli stessi. Nel fare ciò, è opportuno che si adottino misure ragionevoli, anche tecniche, tenendo conto della tecnologia disponibile e dei **costi di attuazione**.

L'obbligo di segnalazione scatta sempre quando l'interessato non si sia limitato a chiedere la sola cancellazione dei suoi dati in capo al titolare a cui si rivolge, ma abbia domandato la cancellazione di "qualsiasi immagine, copia o riproduzione dei suoi dati personali". Questo è il motivo per cui va innanzitutto valutato l'oggetto della richiesta dell'interessato.

In secondo luogo, occorre che il titolare sia a conoscenza di quali sono gli altri titolari che stanno trattando i dati sulla base del fatto che lui li ha "resi pubblici".

In terzo luogo, il titolare destinatario della richiesta sembra avere solo il dovere di segnalazione, lasciando alla **responsabilità degli altri titolari** valutare se essa debba, o meno, essere accolta anche da loro, tenendo conto della base giuridica specifica in virtù della quale ciascuno di essi opera. Infatti, il titolare a cui è stata rivolta la richiesta ha solo il dovere di effettuare la segnalazione, non anche quello di accertarsi del comportamento degli altri titolari e di informare di questo l'interessato. Inoltre, come detto, lo stesso dovere di segnalazione trova un limite nella tecnologia disponibile e nei costi di attuazione ragionevoli.

Sarà molto interessante, nei prossimi mesi, vedere se aumenteranno le richieste di cancellazione e di "oblio" che perverranno ai titolari e se, quindi, il diritto sarà percepito come (giustamente) importante nell'attuale società dell'informazione, anche in un'ottica di **tutela dei consumatori/utenti** o se, al contrario, una tale esigenza non sarà percepita come essenziale.

Considerazioni finali

Di certo, il prevedere la "morte" del dato diventa essenziale, in una **società tecnologica** che tutto ricorda, per proteggere realmente i diritti dell'individuo non solo quando ha un motivo specifico per domandare la cancellazione delle informazioni che lo riguardano (perché, ad esempio, sono state raccolte in violazione di legge) ma anche, genericamente, perché non ha più senso che le informazioni, pur raccolte legittimamente, restino in vita, in quanto si è esaurita la funzione per la quale erano state raccolte.

CONSENSO E INFORMATIVA - 16 MARZO 2018

Dal GDPR maggiori tutele per il trattamento dati dei minori sul web

di Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano

La prima connessione in rete avviene tra i 7 e gli 8 anni. Ciò comporta che già verso i 13 anni di età un minore ha almeno 5 anni di "vita" online durante la quale ha espresso preferenze, tenuto comportamenti facilmente rilevabili e, soprattutto, "seminato dati". E' per questo che il GDPR rafforza la disciplina in tema di protezione dei dati personali dei minori, prevedendo specifiche modalità di applicazione dei principi sulla privacy e riconoscendo precisi diritti agli interessati. Con riguardo soprattutto all'utilizzo dei dati personali dei minori ai fini di marketing o di creazione di profili utente.

I **minori**, in rete e sui social network, sono considerati ormai un "nuovo mercato", un esercito di piccoli consumatori i cui dati hanno un valore incalcolabile per tutte le società/piattaforme, e non solo per quelle che offrono prodotti o servizi mirati ai bambini e agli adolescenti.

In molti Paesi, quali ad esempio l'Italia, la prima connessione in rete avviene tra i 7 e gli 8 anni. Ciò comporta che già verso i 13 anni di età un minore ha almeno **5 anni di "vita" online** durante la quale ha espresso preferenze, tenuto comportamenti facilmente rilevabili e, soprattutto, seminato dati. In altre parole, sono **soggetti facilmente profilabili**, al fine di generare nuovi, preziosi contenuti da quelli già esistenti. Non deve quindi apparire strano che la normativa sulla data protection si occupi anche dei minori, individuandoli come soggetti da tutelare con maggior attenzione nell'era tecnologica attuale.

Il Regolamento UE 2016/679 offre così maggiori tutele nei confronti dei minori, i quali, come specificato nel Considerando n. 38, meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere **meno consapevoli dei rischi**, delle conseguenze e delle misure di salvaguardia interessate, nonché dei loro diritti in relazione al trattamento dei dati personali. Sono, allora, tre i motivi per cui il GDPR prevede una tutela rafforzata: la loro età, l'invasività della società tecnologica e la presunzione che non conoscano la legge e i loro diritti.

Tutele rafforzate per i minori

Il GDPR, in quest'ottica, rafforza la disciplina in tema di protezione dei dati personali, prevedendo specifiche modalità di applicazione dei principi sulla privacy e riconoscendo precisi diritti agli interessati. Questa specifica protezione dovrebbe riguardare, in particolare, l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili utente.

L'Articolo 8 prevede innanzitutto che, per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali è lecito ove il **minore abbia almeno 16 anni**.

Nel caso in cui, invece, abbia un'**età inferiore**, il trattamento è lecito solo se il consenso è prestato o autorizzato dal titolare della responsabilità genitoriale. Il consenso di tale figura non sembra invece essere necessario nel quadro dei servizi di prevenzione o consulenza forniti direttamente a un minore.

Gli Stati membri possono anche stabilire un'età inferiore a tali fini, senza però scendere sotto la soglia dei 13 anni. In ogni caso, il titolare del trattamento è tenuto ad adoperarsi in modo ragionevole per verificare la corretta prestazione o autorizzazione del consenso, in considerazione delle tecnologie disponibili.

Il Paragrafo 3, infine, precisa che quanto dettato dalla disposizione in esame non pregiudica il diritto generale degli Stati membri in tema di contratti, riferendosi nello specifico alle norme riguardanti la validità, la formazione o l'efficacia di un contratto nei confronti di un minore.

Richiesta del consenso al genitore

Il primo punto su cui opera il Regolamento è, allora, la richiesta del consenso al genitore. Si tratta di un aspetto molto innovativo ma, al contempo, delicato. La raccolta del consenso del genitore dovrà infatti essere perfezionata con **modalità** che non "burocratizzino" eccessivamente l'operazione (se i controlli fossero troppo accurati e richiedessero troppo

tempo, ci sarebbe il rischio di migrazione dei clienti verso altri servizi) e che, al contempo, non siano falsificabili dal minore stesso (ossia, occorrerà fare in modo che il minore non si possa sostituire agevolmente al genitore al momento del conferimento del consenso online).

Come deve essere resa l'informativa

La peculiare figura del minore è presa in considerazione anche da un'altra disposizione del GDPR, ossia l'Articolo 12, dedicato all'informativa in tema di trattamento dei dati personali.

L'Articolo dispone che il titolare del trattamento debba fornire informazioni e comunicazioni all'interessato adottando **misure appropriate**, e in particolare in forma concisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro. Ciò si rivela particolarmente importante nel caso in cui l'interessato sia un minore, in quanto tale – come detto – meritevole di una protezione specifica.

Anche l'Articolo 57, nel delineare i compiti spettanti a ciascuna autorità di controllo sul proprio territorio, fa espresso riferimento ai minori, stabilendo che sono oggetto di particolare attenzione le attività volte a promuovere la consapevolezza e a favorire la comprensione riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento destinate specificamente ai minori.

Anche questo secondo punto apre a considerazioni molto interessanti e innovative: se il primo diritto in capo a un interessato è quello di essere informato, i minori devono essere informati con un **linguaggio a loro comprensibile**, con informative che abbandonino burocrazia e termini giuridici (per loro) incomprensibili e forniscano invece loro piena consapevolezza di che cosa sta per capitare ai dati che si riferiscono a loro.

Infine, merita di essere menzionata la nuova tutela contenuta nell'Articolo 17 e disposta a favore del soggetto interessato che richieda la cancellazione dei propri dati. Si tratta del c.d. diritto all'oblio, ossia il diritto alla cancellazione dei propri dati personali, che nel GDPR riceve un "rafforzamento" rispetto alla precedente normativa.

Cancellazione dei dati

Infatti, oltre all'obbligo del titolare del trattamento di procedere senza ingiustificato ritardo alla cancellazione dei dati personali dell'interessato che ne faccia richiesta, è altresì previsto l'obbligo per i titolari che abbiano reso pubblici i dati personali in questione di informare della richiesta di cancellazione anche gli altri titolari che li trattano, ricomprendendo qualsiasi link, copia o riproduzione degli stessi.

Tale diritto, come specificato nel Considerando n. 65, è in particolare rilevante se l'interessato ha prestato il proprio consenso quando era minorenne, dunque non pienamente consapevole dei rischi derivanti dal trattamento, e decida – in un momento successivo – di eliminare un certo tipo di dato personale. L'interessato, prosegue il Considerando, dovrebbe poter esercitare tale diritto indipendentemente dal fatto di non essere più minore.

TUTELA DEI DATI PERSONALI - 30 MARZO 2018

Privacy, GDPR: linee guida UE su profilazione e decisioni automatizzate

Per il pieno riconoscimento e la tutela dei diritti e delle libertà degli utenti l'attività di profilazione deve essere trasparente e bisogna evitare decisioni completamente automatizzate per la raccolta on line dei dati di una persona. Sono questi i principi, messi in evidenza dal Garante per la protezione dei dati personali, che ispirano le Linee guida su profilazione e decisioni automatizzate adottate dalle autorità di protezione dati europee allo scopo di fornire indicazioni a chi tratta i dati per mettersi in regola con il GDPR.

Il Garante per la protezione dei dati personali, nella newslettter del 30 marzo, pone l'attenzione sulle linee guida UE elaborate dal "Gruppo Art. 29" in materia di **processi decisionali automatizzati** e **profilazione** come definite in base alle previsioni del GDPR.

In particolare, ai fini del pieno riconoscimento e **tutela dei diritti** e delle **libertà degli utenti**, viene richiesta una profilazione più trasparente ed una raccolta dati on line non completamente automatizzata che potrebbe produrre effetti giuridici negativi per la persona o che incidano su di essa in modo significativo.

Consulta il Dossier GDPR: come gestire gli adempimenti

Sistemi di profilazione

Per profilazione si fa riferimento all'attività di **raccolta** e **trattamento dei dati** al fine di ricostruire un quadro del soggetto riguardante i gusti commerciali, il suo stato di salute ed anche le sue performance lavorative.

In taluni casi oltre ad essere spesso poco trasparenti, questi trattamenti di dati possono confinare una persona all'interno di una determinata categoria fino a **limitare le scelte**, suggerirne altre sulla o impedire l'accesso a determinati servizi o prodotti.

Linee guida UE

Nelle Linee guida , aggiornate il 29 marzo 2018, le autorità europee forniscono indicazioni ai soggetti che trattato i dati per mettersi in regola con la nuova normativa introdotta dal GDPR in materia di profilazione e decisioni automatizzate.

Le società dovranno, innanzitutto, improntare il trattamento dei dati ai principi di **privacy by design** e **privacy by default** e porre particolare attenzione agli obblighi di trasparenza richiesti dal GDPR.

Leggi anche: GDPR, PMI: impostare procedure di privacy by default e by design

Le aziende dovranno quindi:

- informare chiaramente gli utenti sull'attività di profilazione;

- garantire loro il diritto di conoscere quali dati e quali categorie di dati personali sono stati utilizzati.

Le autorità europee richiedono, inoltre, una particolare attenzione per i trattamenti di dati che riguardano i **minori** a fronte della loro **maggiore vulnerabilità** rispetto a trattamenti particolarmente invasivi.

A cura della Redazione

RUOLI E RESPONSABILITÀ

SICUREZZA DEI DATI - 12 MARZO 2018

Privacy, titolare e responsabile del trattamento: quali responsabilità?

di Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano

Titolare e responsabile del trattamento dei dati personali non sono figure nuove nel panorama della privacy. Il primo è il soggetto che determina le finalità e i mezzi del trattamento di dati. Il secondo tratta i dati personali per conto del titolare del trattamento e, per questo motivo, deve presentare garanzie sufficienti, in particolare, in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del GDPR. E, a tali fini, l'applicazione di un codice di condotta o di un meccanismo di certificazione può essere utile a dimostrare il rispetto degli obblighi.

Il Regolamento 2016/679 dedica il Capo IV a due figure fondamentali: quella del titolare e del responsabile del trattamento.

Titolare ...

Il Titolare del trattamento, che non è una figura nuova ma è "ereditata" dalla normativa originata dalla Direttiva del 1995 sulla protezione dei dati, è la persona fisica o giuridica, l'autorità pubblica, il servizio o qualunque altro organismo che, singolarmente o insieme ad altri, determina le **finalità** e i mezzi del trattamento di dati personali. Viene di solito individuato, per comodità, nel **"vertice" dell'azienda** o dell'organo. Colui, insomma, che decide circa il trattamento dei dati e le sue modalità.

... e Responsabile del trattamento ...

Il Responsabile del trattamento, anche questa una figura già presente nella normativa precedente, è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

... un contratto per regolare il rapporto

Il rapporto tra il titolare e il responsabile del trattamento deve essere regolato da un contratto stipulato per iscritto che, oltre a vincolare a vicenda le due figure, deve prevedere in dettaglio quale sia materia disciplinata, la durata del trattamento, la natura e le finalità del trattamento nonché il tipo di dati personali e le categorie di interessati a cui gli stessi dati si riferiscono.

Responsabilità del titolare

Innanzitutto, l'Articolo 24 stabilisce la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare deve essere in grado di

dimostrare la **conformità delle attività di trattamento** con il Regolamento stesso e deve mettere in atto misure adeguate ed efficaci volte a garantire ciò. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

Questi ultimi, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale. Nei Considerando al Regolamento si precisa che questo si verifica, in particolare, nelle seguenti ipotesi:

a) quando il trattamento comporta **discriminazioni**, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo

b) quando gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o viene loro impedito l'esercizio del controllo sui dati personali che li riguardano

c) se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute, dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza

d) in caso di **valutazione di aspetti personali**, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali

e) se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori

f) se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Come detto, dunque, la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate sulla base di una valutazione oggettiva, con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento, che spetta, appunto, ai vertici, ossa al titolare.

Gli orientamenti per la messa in atto di opportune misure potrebbero essere forniti, in particolare, mediante **codici di condotta** o certificazioni approvate, linee guida o indicazioni fornite da un responsabile della protezione dei dati.

Inoltre, al fine di dimostrare la conformità delle sue azioni con il Regolamento in esame, il titolare del trattamento dovrebbe adottare **politiche interne** e attuare misure che soddisfino i principi della protezione dei dati di default e fin dalla progettazione. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, creare e migliorare le caratteristiche di sicurezza, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali e consentire all'interessato di controllare il trattamento dei dati.

Gli stessi produttori di servizi, prodotti e applicazioni, infine, dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati nel momento di sviluppo e progettazione.

Contitolari del trattamento

L'Articolo 26, poi, prevede l'ipotesi di contitolari del trattamento, che si configura quando due o più titolari determinano congiuntamente le finalità e i mezzi del trattamento: anche in questo caso è necessaria una **chiara ripartizione delle responsabilità**, che viene determinata sulla base di un accordo interno, con particolare riguardo all'esercizio dei diritti dell'interessato (per evitare che un soggetto che abbia intenzione di rivolgersi al titolare per esercitare i suoi diritti non sappia a chi rivolgersi).

Quando un titolare del trattamento o un responsabile del trattamento non stabilito nell'Unione

Europea tratta dati personali di interessati che si trovano nell'Unione e le sue attività di trattamento sono connesse all'offerta di beni o alla prestazione di servizi a tali interessati, è opportuno che egli designi un rappresentante, fatta eccezione per il caso in cui il trattamento sia occasionale, non includa il trattamento -su larga scala - di categorie particolari di dati o il trattamento di dati personali relativi alle condanne penali e ai reati, ed è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche o, infine, se il titolare del trattamento è un'autorità pubblica o un organismo pubblico.

Il rappresentante dovrebbe essere esplicitamente incaricato, mediante **mandato scritto del titolare** o del responsabile del trattamento, ad agire per conto di questi ultimi, con riguardo agli obblighi loro spettanti e con la possibilità di essere interpellato da qualsiasi autorità di controllo. È importante, tuttavia, sottolineare che la designazione di tale rappresentante non incide sulla responsabilità generale del titolare del trattamento o del responsabile del trattamento.

Attività del titolare e del responsabile del trattamento

Come stabilito all'Articolo 28, quando il titolare del trattamento affida delle attività a un responsabile del trattamento, dovrebbe ricorrere unicamente a responsabili che presentino **garanzie sufficienti**, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del GDPR, soprattutto in tema di sicurezza del trattamento. L'applicazione da parte del responsabile del trattamento di un codice di condotta approvato o di un meccanismo di certificazione approvato può essere utilizzata come elemento per dimostrare il rispetto degli obblighi da parte del titolare del trattamento. L'esecuzione dei trattamenti da parte di un responsabile del trattamento dovrebbe essere disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, in cui siano stipulati la materia disciplinata e la durata del trattamento, la natura e le finalità dello stesso, il tipo di dati personali, le categorie di interessati, i compiti e le responsabilità specifiche nel contesto del trattamento da eseguire e del relativo rischio.

Il titolare del trattamento e il responsabile del trattamento possono scegliere di usare un **contratto individuale o clausole contrattuali-tipo** che sono adottate direttamente dalla Commissione o da un'autorità di controllo. Dopo il completamento del trattamento per conto del titolare, il responsabile dovrebbe, a scelta del titolare del trattamento, restituire o cancellare i dati personali, salvo che il diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento ne prescrivano la conservazione.

Per dimostrare la conformità alle disposizioni contenute nel GDPR, il titolare e il responsabile del trattamento dovrebbero tenere un **registro delle attività di trattamento** effettuate sotto la loro responsabilità. Essi dovrebbero, inoltre, cooperare con l'autorità di controllo e mettere, su richiesta, tali registri a sua disposizione a fini di monitoraggio.

Altro compito fondamentale è quello di **garantire la sicurezza del trattamento**: a tale scopo, il titolare e il responsabile del trattamento dovrebbero valutare gli eventuali rischi, determinandone origine, natura, particolarità e gravità, e mettere in atto le misure tecniche e organizzative atte a prevenirli o, quantomeno, a limitarli. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, tenuto conto dello stato dell'arte e dei costi di attuazione. Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune, prima del trattamento si dovrebbe consultare l'autorità di controllo.

Violazione dei dati personali

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche. Pertanto, ai sensi dell'Articolo 33, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento deve **notificarla all'autorità di controllo** competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che egli non sia in grado di dimostrare che è improbabile che la suddetta violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale

notifica dovrebbe essere corredata dalle ragioni del ritardo.

Il titolare del trattamento dovrebbe, altresì, comunicare all'interessato la violazione dei dati personali **senza indebito ritardo**, qualora essa sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni intese ad attenuare i potenziali effetti negativi. Tali **comunicazioni agli interessati** dovrebbero essere effettuate non appena ragionevolmente possibile, in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti.

La Direttiva 95/46/CE aveva introdotto un obbligo generale di notificare alle autorità di controllo alcuni tipi di trattamento di dati personali. Tale obbligo comportava **oneri amministrativi e finanziari**, ma non sempre contribuiva a migliorare la protezione dei dati personali. Con il GDPR si è, pertanto, scelto di abolire tali obblighi generali e indiscriminati di notifica e di sostituirli con meccanismi e procedure efficaci che si concentrino su quei tipi di trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità. Tali tipi di trattamenti includono, in particolare, quelli che comportano l'utilizzo di nuove tecnologie: in questi casi, è opportuno che il titolare del trattamento effettui una **valutazione d'impatto** sulla protezione dei dati prima del trattamento.

Se dalla valutazione d'impatto sulla protezione dei dati risulta che il trattamento, in mancanza delle garanzie, delle misure di sicurezza e dei meccanismi per attenuare il rischio, presenterebbe un rischio elevato per i diritti e le libertà delle persone fisiche e il titolare del trattamento è del parere che il rischio non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e costi di attuazione, è opportuno **consultare l'autorità di controllo** prima dell'inizio delle attività di trattamento.

L'autorità di controllo che riceve una richiesta di consultazione dovrebbe darvi seguito entro un termine determinato; tuttavia, la mancanza di reazione entro tale termine dovrebbe far salvo ogni intervento della stessa nell'ambito dei suoi compiti e dei suoi poteri, compreso quello di vietare tali trattamenti.

ASSOLUTA NOVITÀ DEL GDPR - 13 MARZO 2018

Privacy: i tre volti del Data Protection Officer

di Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano

Una delle novità più rilevanti del GDPR è rappresentata dalla figura del Responsabile della Protezione dei Dati (RPD), ossia il Data Protection Officer. Il DPO ha il compito di sorvegliare

l'osservanza del GDPR, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità. Il DPO, inoltre, deve essere in grado di adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse. Forte l'impatto sul sistema organizzativo delle realtà aziendali dove tale figura si presenta con un profilo a tre volti: quali?

Il **GDPR** offre un quadro di riferimento in termini di **compliance per la protezione dei dati** in Europa aggiornato e fondato sul principio di responsabilizzazione (accountability). I Responsabili della Protezione dei Dati (RPD), altrimenti noti come **Data Protection Officer** (DPO), si trovano esattamente al centro di questo nuovo quadro giuridico e sono chiamati a facilitare l'osservanza delle disposizioni.

Chi è tenuto a designare un DPO

Secondo il GDPR, alcuni titolari e responsabili del trattamento sono tenuti a nominare un DPO. In base all'Articolo 37, paragrafo 1, del GDPR, questo vale, in particolare:

- per tutte le **amministrazioni** e gli enti pubblici, indipendentemente dai dati oggetto di trattamento (fatta eccezione per le autorità giudiziarie)

- per quei soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono un **monitoraggio regolare e sistematico degli interessati** su larga scala

- per tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di **dati sensibili**, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Anche ove il Regolamento non imponga in modo specifico la designazione di un DPO, può risultare utile procedere alla **nomina su base volontaria**. In tal caso, troveranno applicazione tutti i requisiti di cui agli Articoli 37-39 per quanto concerne la nomina stessa, lo status e i compiti del DPO.

L'Articolo 37 non distingue fra titolari del trattamento e responsabili del trattamento in termini di applicabilità: a seconda di chi soddisfi i criteri relativi all'obbligatorietà della nomina, potrà essere il solo titolare del trattamento, ovvero il solo responsabile del trattamento, oppure sia l'uno sia l'altro, a dover nominare un DPO. Questi ultimi saranno poi tenuti alla reciproca collaborazione.

Il Paragrafo 2 consente a un **gruppo imprenditoriale** di nominare un unico DPO a condizione che quest'ultimo sia "facilmente raggiungibile da ciascuno stabilimento".

Il concetto di raggiungibilità si riferisce ai compiti del DPO in quanto punto di contatto per gli interessati, l'autorità di controllo e i soggetti interni all'organismo o all'ente. Infatti, il DPO, se necessario con il supporto di un team di collaboratori, deve essere in grado di comunicare con gli interessati in modo efficiente e di collaborare con le autorità di controllo coinvolte. Ciò significa che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa.

Analogamente, ai sensi dell'Articolo 37, Paragrafo 3, è ammessa la **designazione di un unico DPO** per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

Per garantire l'accessibilità del DPO (soprattutto da parte di chi deve esercitare i suoi diritti) è raccomandata la sua collocazione **nel territorio dell'Unione Europea**, indipendentemente dall'esistenza di uno stabilimento del titolare o del responsabile in tale sede. Tuttavia, non si può escludere che, in alcuni specifici casi, un DPO sia in grado di adempiere ai propri compiti con maggiore efficacia operando al di fuori dell'UE.

La figura del DPO ...

In base all'Articolo 37, Paragrafo 5, il DPO "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".

Il livello di **conoscenza specialistica** richiesto non trova una definizione tassativa; piuttosto, deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento. Inoltre, non sono specificate le qualità professionali da prendere in considerazione nella nomina di un DPO. Tuttavia, sono pertinenti, al riguardo, la conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, anche in termini di misure tecniche e organizzative, nonché un'approfondita conoscenza del GDPR.

Non sono richieste **attestazioni formali** o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio o professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze.

Per "capacità di assolvere i propri compiti", poi, si deve intendere sia tutto ciò che è legato alle qualità personali e alle conoscenze del DPO, sia ciò che dipende dalla posizione del DPO all'interno dell'azienda o dell'organismo.

Le qualità personali dovrebbero comprendere, per esempio, l'integrità ed elevati standard deontologici.

Il DPO, inoltre, deve essere in grado di adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse. In linea di principio, ciò significa che non può trattarsi di un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali.

Il DPO dovrà operare alle dipendenze del titolare o del responsabile del trattamento dati, oppure sulla base di un **contratto di servizio**.

In quest'ultimo caso, il DPO sarà esterno e le sue funzioni saranno esercitate sulla base di un contratto di servizi stipulato con una persona fisica o giuridica.

... e i compiti

I compiti stabiliti per il DPO potranno essere assolti efficacemente da un team operante sotto l'autorità di un contatto principale "responsabile" per il singolo cliente. In tal caso, è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale DPO soddisfi tutti i requisiti fissati nel GDPR. Per favorire efficienza e correttezza, e prevenire **conflitti di interesse** a carico dei componenti del team, è opportuno procedere ad una chiara ripartizione dei compiti e prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente.

L'Articolo 39, Paragrafo 1, lettera b), affida al DPO, fra gli altri, il compito di **sorvegliare l'osservanza del GDPR**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità. Il titolare del trattamento (o il responsabile del trattamento), infatti, dovrebbe essere assistito dal DPO nel controllo del rispetto a livello interno del regolamento.

Fanno parte di questi compiti di controllo svolti dal DPO, in particolare, la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità e l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

In secondo luogo, il DPO svolge un ruolo di primo piano nella collaborazione con il titolare del trattamento per quanto riguarda la conduzione di una valutazione di impatto sulla protezione dei dati (DPIA).

L'Articolo 35, Paragrafo 2, prevede in modo specifico che il titolare si consulti con il DPO quando svolge una DPIA. A sua volta, l'Articolo 39, Paragrafo 1, lettera c) affida al DPO il compito di "fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'Articolo 35".

In particolare, la consultazione dovrebbe avvenire sulle seguenti tematiche:

1) se condurre o meno una DPIA

2) quale metodologia adottare nel condurre una DPIA

3) se condurre la DPIA con le risorse interne ovvero esternalizzandola

4) quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate

5) se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte siano conformi al GDPR.

Con riferimento al ruolo di **"facilitatore" attribuito al DPO**, ricordiamo inoltre che egli deve fungere da punto di contatto per facilitare l'accesso, da parte dell'autorità di controllo, ai documenti e alle informazioni necessarie per l'adempimento dei compiti attribuiti.

Deve, inoltre, informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e dalle altre disposizioni dettate in materia.

Infine, il DPO è chiamato a supportare il titolare/responsabile in ogni attività connessa al trattamento dei dati personali, inclusa quella relativa alla realizzazione di un registro contenente tutte le attività di trattamento svolte.

Considerazioni finali

Il DPO è una figura completamente nuova che ha un forte impatto anche sul sistema organizzativo di una realtà. Già il fatto che debba essere un soggetto che non sia in posizione di conflitto di interessi, libero e non "istruito", lo rende un elemento molto particolare all'interno di un'azienda o di un ente.

Si presenta, poi, come un profilo a tre volti. Un volto è diretto verso i **vertici dell'azienda**, in quanto il DPO diventa il consulente del titolare. Un secondo volto è verso il Garante, perché il DPO è non solo il punto di contatto con cui dialoga l'autorità di controllo in caso di bisogno ma anche un **presidio del sistema normativo** dentro l'attività di trattamento dei dati affinché sia garantita la corretta applicazione del Regolamento. Infine, un terzo volto è orientato **verso gli interessati**, che possono esercitare i loro diritti dialogando con il DPO. Una funzione "una e trina" che, nella pratica, riserverà non poche sorprese.

PER IL SETTORE PRIVATO - 27 MARZO 2018

Privacy: dal Garante le FAQ sul DPO

Il Garante per la protezione dei dati personali, con delle nuove FAQ, ha fornito chiarimenti in

merito ai compiti e alla nomina nel settore privato del Responsabile della Protezione dei Dati, ossia il Data Protection Officer. Con particolare riferimento ai requisiti viene chiarito che il DPO deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di privacy ed essere in grado di offrire la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali. Quali sono i compiti del DPO? Come e da chi deve essere nominato?

In vista dell'entrata in vigore del **GDPR**, prevista per il 25 maggio 2018, il Garante per la protezione dei dati personali ha pubblicato on line delle nuove FAQ per meglio chiarire il ruolo del Data Protection Officer (**DPO**), con particolare riferimento al settore privato.

Consulta il Dossier GDPR: come gestire gli adempimenti

Requisiti professionali

Con riferimento ai requisiti che il responsabile della protezione dei dati personali deve possedere il Garante chiarisce che il DPO deve possedere un'approfondita conoscenza della **normativa** e delle **prassi in materia di privacy**, nonché delle norme e delle **procedure amministrative** che caratterizzano lo specifico settore di riferimento.

Deve, inoltre, poter offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per **progettare**, verificare e mantenere un **sistema organizzato di gestione dei dati personali**, coadiuvando il titolare nell'adozione di un complesso di misure di sicurezza e garanzie adeguate al contesto in cui è chiamato a operare. Il responsabile della protezione dei dati personali deve poter disporre delle risorse necessarie per l'espletamento dei propri compiti.

Compiti

Nelle FAQ viene chiarito che il Data Protection Officer deve assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR. Inoltre, deve cooperare con il Garante e rappresentare un punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali.

Nomina

Il Garante stabilisce nelle FAQ che i soggetti privati tenuti alla designazione del responsabile della protezione dei dati personali sono il **titolare** e il **responsabile del trattamento** che rientrino nei casi previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679.

Nei casi diversi da quelli previsti dal citato art. 37 la designazione del responsabile del trattamento **non è obbligatoria** ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti.

Resta **comunque raccomandata** la nomina di un DPO anche alla luce del principio di "**accountability**" che permea il GDPR.

Gruppi imprenditoriali

Le FAQ chiariscono che nell'ambito di un gruppo imprenditoriale è possibile designare un **unico responsabile** della protezione dei dati personali, purché tale responsabile sia facilmente raggiungibile da ciascuna struttura produttiva. Inoltre, il DPO dovrà essere in grado di comunicare in modo efficace con gli interessati e di collaborare con le autorità di controllo.

A cura della Redazione

TRA I PRINCIPI CARDINE - 14 MARZO 2018

Misure di sicurezza e “accountability”: il nuovo approccio del GDPR

di Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell’Università degli Studi di Milano

Il GDPR “rifonda” le misure minime di sicurezza alla base del sistema di protezione dei dati personali. Rispetto ai limiti del Codice della privacy, dove tali misure si concretizzano in un elenco dettagliato e uguale per tutti (sia per chi tratta pochi dati e sia per chi ne tratta molti), il regolamento europeo cambia approccio, lasciando al titolare del trattamento ampio margine di libertà di scelta in funzione della realtà produttiva nella quale opera. Il nuovo sistema si basa su alcuni principi cardine, ineludibili. I primi tre sono: la necessità di un’analisi del rischio, l’attenzione ai costi da supportare e l’applicazione della nozione di “accountability”. In cosa consistono?

Una delle grandi novità del **GDPR** è l’aver ripensato completamente al sistema di protezione dei dati che il titolare del trattamento deve progettare e implementare nella sua realtà produttiva. I vent’anni precedenti, in base alle regole contenute nella Direttiva 95/46, ci avevano abituato all’idea, innanzitutto, delle **misure minime di sicurezza**.

I limiti del vecchio Codice della privacy

Le misure minime di sicurezza, contenute nell’Allegato B al Codice Privacy del 2003, prendono la forma di un elenco molto dettagliato di misure, tecniche e comportamenti che il Legislatore ha ritenuto che potessero, se rispettate, garantire appunto un livello minimo di sicurezza in qualsiasi ambiente.

Il grosso limite di simili elenchi di misure minime è facilmente individuabile anche dal non esperto: sono **uguali per tutti**, per chi tratta pochi dati e per chi ne tratta molti, per chi tratta dati delicatissimi e per chi, invece, tratta dati comuni. Al contempo, per **piccole realtà commerciali** può essere molto costoso rispettare tutte le misure minime elencate.

E le soluzioni del GDPR

Il Regolamento europeo ha eliminato la nozione di misure minime e ha lasciato un amplissimo **margine di libertà al titolare di scegliere** quali possano essere le misure di sicurezza adeguate in base al tipo di trattamenti effettuati e di dati trattati.

Da un lato, quindi, il titolare non è più vincolato a un elenco di misure; dall’altro, però, sono previste **sanzioni molto più alte** nel caso in cui, in questo quadro di libertà, il titolare ne approfitti per non proteggere le informazioni e per non rispettare le regole.

I cardini del nuovo sistema

Questo nuovo sistema si basa su alcuni principi cardine che sono ineludibili. I primi tre sono, certamente,

- la necessità di un’analisi del rischio

- la stretta connessione con la migliore tecnica e i costi da supportare

- la comprensione e l'applicazione costante della nozione di "accountability".

Analisi del rischio

Il primo punto, la necessità di un'analisi del rischio, è molto lineare da comprendere: se non vengono fornite regole specifiche, occorre, prima di scegliere come operare, analizzare i rischi reali che i dati che si trattano, e gli interessati a loro riferiti, possono soffrire.

In questo caso, occorre rappresentarsi prima tutti i rischi possibili – che variano molto a seconda del "peso" del dato che viene trattato – e da quella analisi si prendono le mosse per predisporre un insieme di misure adeguate di sicurezza.

L'analisi del rischio può essere un procedimento estremamente semplice o, al contrario, particolarmente complesso in quanto è strettamente legato ai tipi di dati che sono trattati, alla molteplicità (o meno) di trattamenti e ai rischi che corrono gli interessati in caso di attacco alle loro informazioni. Realtà che trattano dati ad alto rischio (cliniche, ospedali, laboratori medici) dovranno fare un'analisi estremamente curata e specifica; realtà che, invece, trattano soprattutto dati comuni, avranno ovviamente analisi del rischio più semplici da completare.

Commisurazione alla "forza commerciale"

Il secondo punto, l'**attenzione ai costi** e allo stato dell'arte della tecnica, è altrettanto interessante.

Il Regolamento, in più punti, ribadisce che tutto il sistema di protezione dei dati disegnato dal provvedimento europeo deve sempre tenere presente i costi (ossia la capacità che ha un'azienda o un ente di investire denaro per la compliance) e i migliori strumenti tecnici e informatici disponibili sul mercato. Tutti gli sforzi per proteggere i dati non devono arrivare a minare l'economia e i bilanci dell'azienda, ma devono sempre essere accuratamente calibrati con la **realtà economica effettiva**.

Per la prima volta, quindi, si specifica che ogni azione per la protezione dei dati debba essere commisurata alla "forza commerciale" e alla capacità di investire della singola realtà. Questo porterà un vantaggio soprattutto in quelle realtà che hanno budget limitati.

Principio della accountability

Infine, tutto il sistema deve essere visto sotto due aspetti, al fine di rispettare anche il principio della accountability: non solo gli adempimenti devono esser concretamente svolti ("sostanza") ma tutto ciò che viene fatto deve essere anche **formalmente verificabile** ("verificabilità"), sia dall'interno, sia da eventuali operazioni di auditing esterno. Ciò comporta la necessità di tenere traccia di qualsiasi operazione effettuata in un'ottica di protezione dei dati, al fine di poter ripercorrere in maniera obiettiva, in ogni momento, il percorso seguito e di valutare i risultati.

L'Articolo 32 del GDPR, infine, è quello più importante con riferimento all'implementazione di misure di sicurezza vere e proprie e intese nel senso stringente del termine.

Questa norma stabilisce come, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento debbano mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Esempi di misure di sicurezza

Nonostante sia stato abbandonato l'approccio delle misure minime, con elenchi molto

dettagliati, l'articolo prevede comunque quattro esempi di misure:

1) la pseudonimizzazione e la **cifratura dei dati personali**

2) la capacità di assicurare su base permanente la **riservatezza**, l'**integrità**, la **disponibilità** e la **resilienza** dei sistemi e dei servizi di trattamento

3) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico

4) una procedura per testare, verificare e valutare regolarmente l'**efficacia** delle **misure tecniche e organizzative** al fine di garantire la sicurezza del trattamento.

Da un lato, quindi, è stato abbandonato un elenco tassativo e dettagliato di misure di sicurezza minime; dall'altro, al contempo, è il Legislatore stesso a fornire **suggerimenti utili sugli obiettivi** che le misure dovrebbero aiutare a raggiungere, con riferimento, in particolare, a riservatezza, integrità e disponibilità costante del dato.

MISURE DI SICUREZZA E ISTRUZIONI - 20 MARZO 2018

Privacy 4.0: perché redigere una policy aziendale

di Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano

Gran parte dei problemi di sicurezza dei dati sono, oggi, cagionati da comportamenti errati, soprattutto nelle realtà aziendali dove la componente tecnica è avanzata e la sicurezza informatica è a un buon livello. In tali contesti, infatti, gli attacchi informatici sono diretti a generare azioni sbagliate che possono aprire falle in sistemi altrimenti inviolabili. Anche con il GDPR, Il ricorso ad una policy che vieti, ad esempio, di aprire allegati non attesi, di cliccare su link fraudolenti, di non rispondere a richieste di credenziali o di codici provenienti da (asserite) banche, servizi postali, società emittenti di carte di credito, potrebbe eliminare alla radice ogni rischio.

Per mantenere un quadro sicuro con riferimento alla protezione dei dati, di grandissima utilità e suggeriti anche tra le righe del **GDPR**, sono documenti contenenti **istruzioni, regole o indicazioni di comportamento** che possano orientare le attività di chi si trova quotidianamente a trattare dati.

La presenza, nella realtà produttiva, di soggetti che trattano i dati che siano istruiti dal titolare o dal responsabile comporta, di default, un **innalzamento della sicurezza** complessiva dell'ambiente, soprattutto se le regole sono presentate come stringenti e uniformi.

Tali regole possono riguardare, ad esempio, l'**uso** delle **risorse informatiche** (sia hardware e software, sia di rete), il corretto utilizzo della posta elettronica o degli spazi cloud, l'impostazione di una politica di ridondanza del dato che sia capace di fronteggiare ogni evenienza, la cifratura delle informazioni e degli archivi, una verifica costante degli antivirus, sino ad arrivare a vere e proprie politiche di sicurezza dettagliate.

Policy e misure di sicurezza

Nell'ottica del GDPR e delle sue misure di sicurezza, importante sarebbe, innanzitutto, far comprendere il "peso" del dato, ossia evidenziare come non tutti i dati siano uguali e, quindi, non tutti debbano essere protetti allo stesso modo.

Il comunicare a chi tratta i dati che, in un'ottica di responsabilità e di rischio, un dato sanitario è, nella maggior parte dei casi, più delicato di altri e, di conseguenza, richiede un sistema di protezione più solido, porta lo "spirito" del Regolamento nel contesto produttivo.

Su questo punto, occorrerebbe insistere per far comprendere il ruolo cruciale che rivestono nella società tecnologica odierna **la cifratura dei dati** e la **pseudonimizzazione**. Sono due misure di sicurezza che si rivelano preziose soprattutto in caso di attacco agli archivi o in occasione di data breach, smarrimento dei dispositivi e altre esfiltrazioni non volute di informazioni.

Uso corretto delle dotazioni informatiche

Un secondo gruppo di indicazioni che dovrebbe essere veicolata tramite policy riguarda l'uso corretto degli strumenti informatici che sono consegnati a chi tratta i dati.

Per uso corretto, da un punto di vista della sicurezza, non s'intende soltanto un **uso "etico" dello strumento tecnologico** (ossia, ad esempio, non usarlo per scopi privati o per navigare su siti web non consoni alle mansioni lavorative svolte) ma, soprattutto, un uso che mantenga sempre i dispositivi e gli ambienti operativi aggiornati e sicuri, sia verificando la presenza di vulnerabilità nel sistema usato, sia non attivando (o disattivando) funzioni che possano aprire falle di sicurezza nel sistema stesso.

Molto utili sono anche istruzioni che riguardino l'uso corretto di risorse condivise, ad esempio cartelle in comune, spazi sul cloud o sulla rete aziendale, indirizzi di posta elettronica condivisi tra più soggetti.

Una "mappa" costante di dove siano, e di come circolino, i dati, con indicazioni precise su dove, e in che modo, memorizzare le informazioni, diventa al contempo essenziale per una **governance efficace** su tutti i dati trattati.

Una policy per la ridondanza del dato (ad esempio i backup) e un **uso obbligatorio degli antivirus** permetterebbe, d'altro canto, di poter fronteggiare le minacce più comuni che possono attentare alla riservatezza, all'integrità e alla disponibilità dei dati.

I vantaggi di una policy

Gran parte dei problemi di sicurezza dei dati sono, oggi, cagionati da comportamenti errati, soprattutto in quelle realtà dove la componente tecnica è molto avanzata e, quindi, per definizione più sicura.

Nei contesti dove la sicurezza informatica è a un buon livello, sono numerosi i criminali che cercano di attaccare i comportamenti e la mente di chi tratta i dati, tentando di generare azioni sbagliate che aprano delle falle in sistemi altrimenti inviolabili.

Regole precise che vietino, ad esempio, di aprire allegati non attesi, di cliccare su link fraudolenti, di non rispondere a richieste di credenziali o di codici provenienti da (asserite) banche, servizi postali, società emittenti di carte di credito, sarebbero in grado di eliminare alla radice tutti quegli **attacchi ai dati** che cercano di arrivare all'accesso alle informazioni

ingannando l'essere umano.

Il recente Regolamento non prevede espressamente la figura dell'**incaricato** come era prevista nel Codice Privacy e che prendeva la forma, in sintesi, di chiunque in un contesto aziendale o altro ente trattasse un dato. L'incaricato era solitamente istruito con regole e istruzioni precise, spesso per iscritto. Nel regolamento si indica espressamente l'obbligo per il titolare di "istruire" chiunque tratti dati all'interno della realtà produttiva. Il quarto Paragrafo dell'Articolo 32 sulle misure di sicurezza stabilisce chiaramente, infatti, che "Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri". Questa figura del **soggetto "istruito" al trattamento dei dati** non può che essere creata attraverso delle regole impartite durante l'attività quotidiana.

Le regole possono essere spiegate in aula, con corsi ad hoc, per unire a un "freddo" documento scritto un'attività di chiarimento che rende tutta l'operazione molto più efficace.

Con l'evoluzione tecnologica, le regole vanno aggiornate, sia in base alle novità in ambito informatico che ogni giorno si presentano, sia in base a una valutazione del passato, riflettendo su errori o **vulnerabilità/falle di sicurezza** che si sono già manifestate.

NUOVO REGOLAMENTO UE - 17 MARZO 2018

Crittografia e pseudonimizzazione nel GDPR

di Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano

Cifratura dei dati e pseudonimizzazione sono strumenti differenti tra loro, ma con un medesimo fine: oscurare il dato per renderlo incomprensibile a coloro che non hanno i codici per accedervi. La crittografia si basa, di solito, su un algoritmo di cifratura e su una passphrase che "apre" e "chiude" i dati. La pseudonimizzazione garantisce i dati personali, facendo in modo che gli stessi non siano attribuibili ad una persona fisica identificata o identificabile. Entrambe sono comunemente considerate dal GDPR alcune delle tecniche più efficaci per garantire una reale protezione delle informazioni.

Nonostante il sistema di misure di sicurezza contenuto nel **GDPR** non preveda più un elenco tassativo e specifico di misure minime come nel Codice Privacy precedente, in diversi passaggi si indicano la **cifratura dei dati** e degli archivi e la **pseudonimizzazione delle informazioni** come tecniche ideali per aumentare la protezione dei dati, soprattutto di quelli sensibili.

L'idea è quella che un'eventuale fuga di questi dati faccia sì che le informazioni reperibili siano visibili ma assolutamente incomprensibili o destrutturate, ossia separate da altre informazioni che sarebbero in grado di dar loro un senso.

Si pensi al caso di un **furto di dati da un server**, o allo smarrimento di un computer portatile o di uno smartphone: il soggetto che ha rubato i dati, o ha trovato il portatile, non sarà in grado di comprendere i dati stessi, dal momento che algoritmi e tecnologie li avranno resi non intelligibili.

Cifratura dei dati e pseudonimizzazione sono strumenti differenti tra loro che mirano, però, allo stesso fine: oscurare il dato affinché sia incomprensibile a tutti coloro che non hanno i codici corretti per accedervi.

Cifratura dei dati

La crittografia si basa, di solito, su un algoritmo di cifratura e su una passphrase (una password, ma più lunga e complessa) che "apre" e "chiude" i dati (di solito al momento dell'autenticazione). Si tratta di una procedura che è trasparente per l'utente ma che protegge l'informazione con modalità che sono, nella maggior parte dei casi, insuperabili.

Il GDPR ha in mente la cifratura dei grandi server, dei sistemi che gestiscono credenziali, di quelli che trattano dati sensibili (si pensi al settore sanitario), di quei computer che processano una grande mole d'informazioni per profilare i consumatori e, in generale, di tutti quegli achivi che contengono dati personali.

L'idea del Legislatore europeo è di far sì che ben presto, nella società dell'informazione, tutti i dati da "in chiaro" diventino "offuscati". Ciò comporterebbe un innalzamento della sicurezza non solo dei sistemi ma anche degli utenti comuni.

Nel Considerando n. 83 si indica proprio la cifratura delle informazioni quale sistema per mantenere la sicurezza e prevenire trattamenti in violazione al Regolamento. Il titolare del trattamento, o il responsabile del trattamento, hanno infatti il compito di ridurre i rischi inerenti al trattamento e attuare misure per limitare tali rischi, e tra tali misure è indicata specificamente la cifratura.

Pseudonimizzazione delle informazioni

La pseudonimizzazione è descritta, nel Regolamento, come il trattamento dei dati personali eseguito in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive.

La condizione essenziale è, però, che tali informazioni aggiuntive siano **conservate separatamente** e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Anche questa tecnica, che opera attraverso l'**uso di codici e pseudonimi**, diventa particolarmente interessante quando viene completamente automatizzata, ossia inserita nel processo (e nel software) stesso di trattamento dei dati di modo che non sollevi complicazioni inutili, nell'utilizzo, per l'utente comune.

Nel testo del Regolamento, l'idea di pseudonimizzazione viene infatti spesso affiancata alle nozioni di "**privacy by design**" e di "**privacy by default**", ossia al fatto che sia il sistema stesso, sin dalla nascita o con istruzioni ad hoc, a essere configurato sin dall'inizio come un ambiente rispettoso della privacy degli utenti.

Considerazioni finali

Non è un caso che sia la pseudonimizzazione, sia la cifratura siano messi come primi due elementi nell'articolo del Regolamento che "suggerisce" alcune misure di sicurezza adeguate alla società dell'informazione (l'Articolo 32 che tratta, appunto, della "sicurezza del

trattamento"): sono comunemente considerate come due tra le **tecniche più efficaci** per garantire una reale protezione delle informazioni.

In un'ottica di adempimenti, queste tecniche indicate esplicitamente nel GDPR comportano una serie di passaggi obbligati.

Il primo adempimento consiste nella verifica se i dati di una realtà che è presa in considerazione (ad esempio: il database di una assicurazione, l'archivio di un ospedale, i dati di una banca) siano cifrati o meno, e con quali tecniche. In questo caso il titolare si deve chiaramente confrontare con il **reparto IT** per avere delucidazioni se la crittografia sia presente o meno. In caso di risposta negativa, è obbligatorio, soprattutto in caso di trattamento di dati particolarmente delicati, migrare verso un sistema cifrato, anche se è comunque consigliabile per qualsiasi tipo di dato.

In secondo luogo, crittografia e pseudonimizzazione, se presenti, richiedono comunque un **minimo di regole** ("policy") per una corretta gestione del sistema. Si pensi, ad esempio, all'indicazione chiara di chi detenga le chiavi di cifratura, oppure all'obbligatorietà, per tutti i dipendenti, di ricevere smartphone, chiavette USB e portatili già cifrati, e così via. La crittografia è, infatti, uno strumento estremamente sicuro, soprattutto in caso di **data breach**, se però, al contempo, anche i comportamenti degli utenti sono corretti. Altrimenti anche il migliore strumento di sicurezza esistente rischia di crollare inesorabilmente.

NUOVO REGOLAMENTO UE - 28 MARZO 2018

Privacy: il Garante aggiorna la Guida applicativa

È online l'aggiornamento 2018 della Guida all'applicazione del nuovo Regolamento UE sulla privacy. Lo ha reso noto il Garante per la protezione dei dati personali con comunicato del 27 marzo 2018. La Guida è stata in parte modificata ed integrata alla luce dell'evoluzione della riflessione a livello nazionale ed europeo.

Il Garante per la protezione dei dati personali ha messo a disposizione l'**aggiornamento 2018** della **Guida all'applicazione del Regolamento UE 2016/679** in materia di protezione dei dati personali.

Il documento - che traccia un quadro generale delle principali innovazioni introdotte dal Regolamento e fornisce indicazioni utili sulle prassi da seguire e gli adempimenti da attuare per dare corretta applicazione alla normativa - è stato in parte **modificato e integrato** alla luce dell'evoluzione della riflessione a livello nazionale ed europeo.

Preleva la Guida all'applicazione del Regolamento UE 2016/679

Il testo potrà subire ulteriori aggiornamenti, allo scopo di offrire sempre nuovi contenuti e garantire un aggiornamento costante.

Leggi anche Privacy: dal Garante le FAQ sul DPO

Consulta il Dossier GDPR: come gestire gli adempimenti

A cura della Redazione

ANALISI DEI RISCHI

TRE ADEMPIMENTI - 15 MARZO 2018

Privacy 4.0: registro dei trattamenti, valutazione di impatti, analisi dei rischi

di Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano

Valutazione dei rischi e dell'impatto del trattamento dei dati personali anche in caso di uso di nuove tecnologie unitamente ad una mappa di tutti i trattamenti, dei dati e delle misure di sicurezza adottate in azienda. Sono tappe fondamentali nella gestione della privacy aziendale. Con il registro dei trattamenti dei dati, in particolare, vengono fornite tutte le informazioni essenziali per comprendere la strategia di compliance seguita. Il Privacy Impact Assessment deve essere elaborato soltanto in determinati casi, ma è importante soprattutto quando i dati trattati possono mettere in pericolo i diritti degli interessati. Al centro di tale documento, l'analisi della probabilità e della gravità del rischio.

Ci sono **tre adempimenti**, nel GDPR, che uniscono l'aspetto "burocratico" (la compilazione di un registro, l'elaborazione di formule, la preparazione di elenchi, previsioni e regole) e la possibilità concreta di disegnare un'utilissima mappa del trattamento dei dati in una determinata realtà (mappa che diventa indispensabile nelle realtà molto complesse e con tanti trattamenti eterogenei tra loro).

Registro dei trattamenti

Il primo adempimento, il registro dei trattamenti (che deve essere redatto soltanto da specifiche categorie di titolari elencate nel Regolamento) ha due finalità.

La prima, più pratica, è di **esibirlo all'autorità di controllo** nel caso il Garante lo richiedesse. Perché sia utile all'autorità di controllo, dovrebbe consentire di avere un quadro completo di tutti i trattamenti, dei dati e delle misure di sicurezza già "a prima vista".

La seconda funzione, più programmatica, è che tramite la compilazione di un registro dei trattamenti, e un suo costante aggiornamento, si può impostare sin dall'inizio un **approccio alla sicurezza** molto corretto, che tenga in ogni momento sotto controllo la vita del dato e i comportamenti di chi tratta il dato stesso.

L'Articolo 30 descrive il contenuto minimo dei registri delle attività di trattamento, che dovrebbero contenere tutte le seguenti informazioni:

a) il **nome** e i **dati di contatto del titolare del trattamento** e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile

della protezione dei dati (ciò consente di individuare all'istante i vertici del trattamento)

b) le **finalità del trattamento** (ossia per quali fini i dati sono stati raccolti)

c) una descrizione delle categorie di **interessati** e delle categorie di **dati personali**

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la **cancellazione** delle diverse categorie di dati (questa si tratta di una delle novità più interessanti, strettamente correlata a una previsione esplicita della data di "morte" del dato);

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative predisposte.

Il registro dei trattamenti non è, quindi, un semplice registro, ma contiene tutte le informazioni essenziali per comprendere la strategia di compliance adottata nel contesto concreto.

Il Privacy Impact Assessment

Anche il Privacy Impact Assessment, o valutazione d'impatto, deve essere elaborato soltanto in determinati casi, ma assume una fondamentale importanza soprattutto quando i dati trattati sono in grado **di mettere in pericolo i diritti degli interessati**.

La valutazione d'impatto sulla protezione dei dati è prevista dall'Articolo 35.

Quando un tipo di trattamento, allorché preveda in particolare l'**uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve effettuare, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

Il titolare del trattamento, allorquando svolga una valutazione d'impatto sulla protezione dei dati, si consulta con il **responsabile della protezione dei dati**, qualora ne sia designato uno.

La valutazione d'impatto è richiesta, in particolare, in **tre ipotesi**.

a) quando il titolare opera una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche

b) quando il titolare procede al trattamento, su larga scala, di **categorie particolari di dati** personali o di dati relativi a condanne penali e a reati

c) quando il titolare opera attività di sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare, in concreto, da trattamenti di dati personali suscettibili di cagionare un **danno fisico, materiale o immateriale**.

In particolare:

a) se il trattamento può comportare **discriminazioni, furto o usurpazione d'identità**,

perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo

b) se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano

c) se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'**appartenenza sindacale**, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;

d) in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali

e) se sono trattati dati personali di **persone fisiche vulnerabili**, in particolare minori

f) se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Analisi del rischio

Il Privacy Impact Assessment è un documento complesso, che può arrivare anche a diverse decine di pagine in caso di numerosi trattamenti, e che deve avere, al centro, l'analisi della probabilità e della gravità del rischio.

La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportino un rischio o un rischio elevato.

In conclusione

Questi tre adempimenti, se richiesti, sono tra i più complessi del GDPR. Il **registro**, però, diventa fondamentale per redigere una mappa, costantemente aggiornata, dei dati e della loro "vita". Il **Privacy Impact Assessment** ha invece al centro la previsione dell'impatto che il trattamento di dati particolarmente delicati può avere sui diritti delle persone e riguarda quindi direttamente i diritti di libertà degli individui. L'**analisi del rischio**, infine, è il principale metodo per impostare una politica di protezione dei dati che non sia solamente efficace ma anche strettamente collegata a una realtà concreta.

CONTRO IL RISCHIO DI VIOLAZIONE DEI DATI - 19 MARZO 2018

Privacy: come gestire un data breach

di Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano

Il data breach consiste in una violazione dei dati che determina la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzati ai dati personali. E' in definitiva un'anomalia che colpisce i dati dell'interessato, che fuoriescono da un archivio custodito e iniziano a circolare e a diventare pubblici. Il GDPR vuole che tali eventi siano comunicati al Garante della privacy e agli interessati: la mancata notifica espone l'azienda all'applicazione di elevate sanzioni. Come evitare il rischio di data breach? Quali misure è opportuno adottare?

Il Regolamento UE 2016/679 - **GDPR** in materia di protezione dei dati personali dedica una disciplina specifica al "**data breach**", ossia all'ipotesi di una **violazione dei dati** idonea a comportare – accidentalmente o come conseguenza di un illecito – la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Si tratta dell'incubo peggiore previsto dal Legislatore europeo nella nuova società dell'informazione, dove anche **grandi piattaforme e server**/servizi custodiscono i dati di milioni di utenti con indirizzi e-mail, credenziali, indirizzi e numeri di carte di credito.

Una violazione di questi tipi di dati personali può, se non affrontata in modo adeguato e tempestivo, provocare **danni gravissimi** alle persone fisiche.

Tali danni possono consistere, ad esempio, nella **perdita del controllo dei dati** da parte degli interessati stessi, nella limitazione o soffocamento dei loro diritti, nella discriminazione nel contesto sociale dove vivono e lavorano, nell'usurpazione o nel furto di identità, in perdite finanziarie, nella decifratura non autorizzata della pseudonimizzazione, in un pregiudizio alla reputazione, nella perdita di riservatezza dei dati personali protetti da segreto professionale e, in generale, in tantissimi danni economici o sociali significativo.

Notifica al Garante

Per tale ragione, l'Articolo 33 del GDPR prevede che, in caso di violazione di archivi contenenti dati personali (ma, anche, in caso di smarrimento o furto di una chiavetta, di un hard disk esterno o di un computer portatile) il titolare del trattamento debba **notificare** la suddetta violazione **all'autorità di controllo competente** (ossia: al Garante) entro 72 ore dal momento in cui ne è venuto a conoscenza.

La comunicazione deve essere fatta anche a tutti gli utenti/interessati cui i dati si riferiscono, a meno che sia improbabile che quella violazione dell'archivio rappresenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale comunicazione deve essere accompagnata dalle ragioni del ritardo nell'agire in tal senso.

La notifica, in particolare, deve descrivere la **natura della violazione**, indicando – ove possibile – le categorie e il numero approssimativo dei dati personali violati e degli interessati coinvolti. Deve, inoltre, contenere il nome e i dati di contatto del responsabile della protezione dei dati o di un altro punto di contatto presso cui sia consentito ottenere più informazioni. Infine, deve descrivere le probabili conseguenze della violazione e le misure adottate, o di cui si propone l'adozione, al fine di porre rimedio alla violazione o di attenuarne i possibili effetti negativi.

Comunicazione all'interessato

Ai sensi dell'Articolo 34, poi, quando la violazione dei dati personali è suscettibile di presentare un **rischio elevato per i diritti** e le libertà delle persone fisiche, il titolare del trattamento dovrebbe comunicarla senza indebito ritardo anche all'interessato stesso, consentendogli, in tal modo, di prendere le precauzioni necessarie.

La comunicazione dovrebbe descrivere la **natura della violazione** e contenere raccomandazioni per la persona fisica interessate dirette ad attenuare i potenziali effetti negativi (ad esempio: il suggerimento di cambiare immediatamente le credenziali). Essa, inoltre, dovrebbe essere effettuata non appena ragionevolmente possibile, in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti.

La comunicazione all'interessato non è tuttavia richiesta se si ravvisano una serie di **circostanze specifiche**.

La prima ricorre quando il titolare del trattamento ha messo in atto, e applicato ai dati che sono stati oggetto di violazione, tutte le necessarie misure tecniche e organizzative di protezione, comprese quelle destinate a rendere i dati personali incomprensibili ai soggetti non autorizzati (come, ad esempio, la cifratura delle informazioni).

La seconda è prevista quando il titolare del trattamento abbia successivamente adottato misure per scongiurare il verificarsi di un rischio elevato per i diritti e le libertà degli interessati.

La terza si presenta quando la comunicazione stessa richiederebbe **sforzi sproporzionati** e, in tal caso, si può procedere a una comunicazione pubblica o ad altra soluzione analoga, così da informare gli interessati in maniera ugualmente efficace.

In sostanza, dunque, è opportuno procedere a un duplice controllo.

Da un lato, occorre verificare che siano state adottate le **misure di protezione adeguate**, così da poter stabilire se c'è stata violazione dei dati personali e informare, di conseguenza, l'autorità di controllo e gli interessati. Dall'altro, si deve stabilire se la notifica è stata trasmessa senza ingiustificato ritardo, tenendo conto, in particolare, della natura e della gravità della violazione, nonché delle sue conseguenze ed effetti negativi per l'interessato.

Sanzioni

Il mancato rispetto dell'obbligo di notifica pone l'autorità di controllo nella condizione di poter applicare le sanzioni a sua disposizione. Queste possono consistere nell'**esercizio dei poteri** previsti dall'Articolo 58 del GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere i flussi di dati) e nell'imposizione di **sanzioni amministrative** ex Articolo 83, il cui importo può arrivare fino a 10 milioni di euro o, se superiore, al 2% del fatturato totale annuo dell'esercizio precedente.

> Dato che l'obbligo di notifica spetta al titolare, è molto importante che, nell'affidare servizi a responsabili del trattamento, questi, preliminarmente, si accerti della **capacità del fornitore** nel gestire tempestivamente e adeguatamente un incidente di sicurezza e preveda, quindi, idonee clausole contrattuali, come stabilito dall'Articolo 28, Paragrafo 3 del GDPR, che regolino il rapporto di fornitura in modo da garantire il rispetto del Regolamento stesso.

Considerazioni finali

Gli obblighi della notifica e della comunicazione, sebbene richiedano adempimenti specifici, non possono essere letti e interpretati correttamente senza considerare la loro correlazione con l'intero GDPR. In particolare, in tal senso, sono fondamentali gli Articoli 24 e 32 del GDPR, che

impongono ad ogni titolare di:

1) mettere in atto misure tecniche e organizzative adeguate per garantire il rispetto del GDPR

2) essere in grado di dimostrare che il trattamento sia effettuato conformemente al GDPR

3) riesaminare e aggiornare tali misure quando necessario

4) garantire un **livello di sicurezza** adeguato al rischio.

Non si può, infatti, pensare di gestire correttamente un possibile data breach (soprattutto in una realtà complessa) se il lato organizzativo (istruzioni, dialogo tra le varie "parti" dell'azienda, chiarezza nei processi) non sia impeccabile.

Il data breach, nell'ottica dell'interessato – e ricordiamo sempre che l'interessato è posto al centro del Regolamento – è visto come **un'anomalia** che colpisce i suoi dati i quali, improvvisamente, fuoriescono da un archivio custodito e iniziano a circolare e a diventare pubblici. Ciò che la legge vuole è che questi eventi siano sia comunicati all'autorità che è in grado di intervenire da un punto di vista della verifica ed, eventualmente, delle sanzioni, sia agli interessati stessi, che hanno diritto di conoscere.

Si noti, anche in questo contesto, l'importanza della **cifratura degli archivi**: un data breach su un archivio di dati cifrato allo stato dell'arte può evitare grandi responsabilità in capo al titolare e annullare qualsiasi effetto dannoso dell'evento nei confronti di chiunque, titolare, interessati e terzi.

CRITERI DI APPLICAZIONE - 21 MARZO 2018

GDPR: sanzioni pecuniarie fisse e proporzionali al fatturato

di Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano

Il GDPR ridisegna l'impianto sanzionatorio in tema di privacy. Un elemento centrale del nuovo assetto è rappresentato dalle sanzioni amministrative pecuniarie. Una volta accertata la violazione di una o più norme del GDPR, l'autorità di controllo competente individua le misure correttive più appropriate. Le sanzioni applicate devono essere equivalenti in tutti gli Stati membri e rispondere adeguatamente alla natura, alla gravità e alle conseguenze della violazione. L'aspetto più preoccupante è quello relativo alle sanzioni d'importo non fisso, ma commisurato al fatturato globale annuo della società. Quali le possibili conseguenze per le imprese?

L'Unione Europea, con il **GDPR**, ha voluto attuare una riforma completa del quadro normativo sulla protezione dei dati.

Una simile riforma si è dovuta fondare su alcuni **principi fondamentali**: norme specifiche e coerenti, procedure consultive e di accertamento semplificate, azioni coordinate anche tra i vari Paesi, utenti messi al centro del sistema di protezione, informazioni sui diritti più efficaci e rafforzamento dei poteri indirizzati a far rispettare le norme previste.

Le **sanzioni amministrative** pecuniarie rappresentano, in particolare, un **elemento centrale** di questo nuovo regime, in quanto rientrano nell'insieme degli strumenti di applicazione che sono messi a disposizione della autorità di controllo in ogni singolo Paese.

Una volta accertata la violazione di alcune norme del GDPR, l'autorità di controllo competente può individuare le **misure correttive** più appropriate per affrontare la situazione che si è così venuta a creare. Le disposizioni di cui all'Articolo 58, Paragrafo 2, indicano gli strumenti messi a disposizione per far fronte a un'inadempienza da parte di un titolare o di un responsabile del trattamento.

Sanzioni equivalenti in tutti gli Stai membri

Innanzitutto, la violazione del GDPR dovrebbe comportare l'imposizione di "sanzioni equivalenti". Infatti, al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione Europea, il **livello di protezione** dovrebbe essere equivalente in tutti gli Stati membri. Per garantire questo, occorrono – tra l'altro – poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali, nonché sanzioni equivalenti in caso di violazione.

Il Regolamento offre una base più solida rispetto alla Direttiva 95/46/CE, in quanto lo stesso è direttamente applicabile negli Stati membri, ed esorta a una maggiore coerenza, da garantire principalmente mediante il meccanismo di cooperazione.

Sanzioni pecuniarie proporzionate e dissuasive

Come tutte le misure correttive, le sanzioni amministrative pecuniarie dovrebbero rispondere adeguatamente alla natura, alla gravità e alle conseguenze della violazione. Le autorità di controllo dovranno allora valutare tutte le circostanze del caso in maniera coerente e oggettivamente giustificata: la valutazione di quanto le misure siano effettive, proporzionate e dissuasive in ciascun caso dovrà riflettere anche l'obiettivo che esse perseguono, che potrà essere quello di ripristinare la conformità alle norme o quello di punire un comportamento illecito.

Il Regolamento, fissando **due diversi massimali** per le sanzioni amministrative pecuniarie (10 e 20 milioni di euro), fornisce già un'indicazione sul fatto che la violazione di alcune disposizioni del Regolamento si può presentare più grave rispetto alla violazione di altre.

Nel caso in cui l'autorità di controllo ritenga che la violazione non crei un rischio significativo per i diritti degli interessati e non incida sull'essenza dell'obbligo in questione, la sanzione può talvolta essere **sostituita da un ammonimento**. Tale sostituzione può avvenire anche nel caso in cui il titolare del trattamento sia una persona fisica e la sanzione pecuniaria che dovrebbe essere imposta costituisca un onere sproporzionato per la "vittima" di tale provvedimento.

Come si determina la gravità della violazione

La natura della violazione, l'oggetto o la finalità del trattamento in questione, nonché il numero di interessati lesi dal danno e il livello del danno da essi subito, possono fornire chiaramente un'indicazione della gravità della violazione.

Occorre valutare, in particolare, il numero di interessati coinvolti al fine di stabilire se si tratti di

un evento isolato oppure un sintomo di una violazione sistematica o, addirittura, dell'assenza volontaria e perdurante di prassi adeguate alla protezione dei dati in quel contesto specifico.

Se, poi, gli interessati hanno subito un danno, occorre considerarne l'entità.

Un'ulteriore distinzione che deve essere operata è quella tra **violazione colposa e violazione dolosa**: quest'ultima è generalmente riconosciuta come più grave e, dunque, potrebbe essere idonea a giustificare l'applicazione di una sanzione amministrativa pecuniaria.

Tra le circostanze indicanti il carattere doloso di una violazione potrebbe figurare il trattamento illecito autorizzato esplicitamente dall'alta dirigenza del titolare, oppure effettuato ignorando le politiche esistenti. Altre circostanze, invece, come l'errore umano o l'incapacità di apportare aggiornamenti tecnici in maniera puntuale, potrebbero essere sinonimo di negligenza.

Non possono essere legittimate violazioni della normativa, e questo risulta chiaro nel Regolamento, facendo appello a una carenza di risorse economiche o di personale. I **titolari del trattamento** e i **responsabili del trattamento**, infatti, hanno l'obbligo di attuare misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio, di condurre valutazioni d'impatto sulla protezione dei dati e di mitigare i rischi arrecati ai diritti e alle libertà personali.

Quando si verifica una violazione e ne derivano danni, la parte responsabile dovrebbe fare quanto in suo potere per **ridurre le conseguenze negative**: tale comportamento responsabile (o la sua assenza) sarà preso in considerazione dall'autorità di controllo nella scelta della misura correttiva e della sanzione da imporre.

In passato, l'esperienza disciplinare delle autorità di controllo nell'ambito della Direttiva 95/46/CE ha dimostrato che può essere opportuno mostrare un certo **livello di flessibilità** nei confronti di quei titolari/responsabili del trattamento che hanno ammesso la violazione e che si sono assunti la responsabilità di correggere o limitare l'impatto delle loro azioni.

Aumenta il grado di responsabilità del titolare del trattamento

Il Regolamento ha introdotto un livello ben superiore di responsabilità del titolare del trattamento rispetto alla Direttiva 95/46/CE sulla protezione dei dati.

Il suo grado di responsabilità, valutato sulla base dell'adozione di una misura correttiva appropriata, può dipendere dai seguenti aspetti:

· se sono state attuate **misure tecniche** che seguono i principi della protezione dei dati fin dalla progettazione o per impostazione predefinita;

· se sono state adottate misure **organizzative** che attuano i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita a tutti i livelli dell'organizzazione;

· se è stato messo in atto un livello di sicurezza adeguato;

· se le **prassi/politiche** pertinenti in materia di protezione dei dati sono conosciute e applicate al livello adeguato di gestione dell'organizzazione.

L'Articolo 25 e l'Articolo 32 del Regolamento UE (GDPR) prevedono che i titolari del trattamento tengano 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".

Anziché imporre un obbligo di risultato, tali disposizioni introducono **obblighi di mezzi**, il che significa che il titolare del trattamento deve condurre le valutazioni necessarie e giungere alle opportune conclusioni.

L'autorità di controllo, inoltre, dovrebbe valutare eventuali precedenti violazioni pertinenti commesse dal titolare o dal responsabile del trattamento, osservando in particolare se si è trattato della medesima violazione o di una violazione eseguita con le stesse modalità.

E se le violazioni sono molteplici?

È possibile comminare sanzioni amministrative pecuniarie in risposta ad una vasta serie di violazioni.

Il Regolamento stabilisce che ogni caso sia **valutato singolarmente**: pertanto, al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singola fattispecie, si deve tenere conto di una serie di elementi espressamente elencati dalla disposizione in esame. A seguito di tale valutazione, l'autorità di controllo ha la responsabilità di scegliere la misura più adeguata, nonché il canale più appropriato per portare avanti l'intervento.

Controversie e rapporti tra le autorità

In caso di controversie tra le autorità, in particolare in merito alla determinazione dell'esistenza di una violazione, sarà il Comitato Europeo per la Protezione dei dati ad adottare una decisione vincolante, esaminando anche se, e in che modo, la misura correttiva adottata nel singolo caso rispetti i principi di efficacia, proporzionalità e deterrenza richiesti dal regolamento.

Un approccio armonizzato richiede altresì la **partecipazione attiva** delle autorità di controllo e lo **scambio d'informazioni** tra le stesse. Per alcune autorità di controllo nazionali, i poteri sanzionatori rappresentano una novità nel settore della protezione dei dati e sollevano numerose questioni in termini di risorse, organizzazione e procedura.

Ad ogni modo, le diverse autorità dovrebbero collaborare tra loro e, ove necessario, con la Commissione europea, al fine di sostenere scambi formali e informali di informazioni. Tale cooperazione si concentrerà sulla loro **esperienza e pratica** nell'applicazione di poteri sanzionatori, con l'obiettivo di raggiungere una maggiore coerenza complessiva dell'intero sistema.

Sanzioni proporzionali al fatturato

La parte che più preoccupa, con riferimento alle sanzioni, è quella che prevede sanzioni non d'importo/massimale fisso ma commisurate al fatturato globale annuo della società.

L'idea di prevedere sanzioni in percentuale al fatturato è nata per cercare di "intimorire" anche le grandi società o piattaforme nordamericane (ma non solo) e intaccare direttamente il loro business, cosa che con sanzioni fisse, seppur alte, non sarebbe stato possibile fare. Al contempo, simili sanzioni, che l'autorità di controllo può riferire al **fatturato mondiale** (o della casa madre che dir si voglia), sono pensate per responsabilizzare anche le business unit e sedi operative locali di grandi multinazionali con sede centrale al di fuori dell'Italia. Una violazione del GDPR perpetrata da una di queste sedi, anche se piccola, inciderà infatti, in punto di sanzioni, sul bilancio di tutta la società.

DAL CONSIGLIO DEI MINISTRI - 22 MARZO 2018

GDPR: primo via libera al decreto attuativo

Durante la riunione del 21 marzo 2018, il Consiglio dei Ministri ha approvato, in esame preliminare, il decreto legislativo utile all'adeguamento della normativa nazionale alle disposizioni dettate dal nuovo Regolamento europeo per la protezione dei dati personali delle persone fisiche e per la libera circolazione degli stessi. La direttiva attualmente in vigore cesserà di essere applicata dal 25 maggio 2018.

Il Consiglio dei Ministri, su proposta del Presidente Paolo Gentiloni e del Ministro della giustizia Andrea Orlando, ha approvato, in esame preliminare, un decreto legislativo che, in attuazione dell'art. 13 della legge di delegazione europea 2016-2017, introduce disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Contestualmente, a partire dal 25 maggio 2018, viene abrogata la direttiva 95/46/CE, che contiene il Regolamento generale sulla protezione dei dati. E sarà necessario armonizzare l'ordinamento interno al nuovo quadro normativo dell'Unione Europea in tema di tutela della *privacy*.

Il nuovo Regolamento sulla privacy

ll Regolamento introdurrà regole più chiare e semplici in materia di informativa e consenso, puntando a garantire maggiori tutele per i cittadini. Il regolamento diventerà immediatamente applicabile senza bisogno di essere recepito con provvedimenti nazionali: un testo unico valido in tutti i paesi UE che mirerà a rendere omogeneo ed elevato il livello di protezione dei dati personali e a favorire la circolazione degli stessi all'interno dell'Unione Europea, salva la facoltà degli Stati Membri dell'Unione rimarrà di introdurre ulteriori regole e condizioni.
L'informativa andrà resa in forma concisa, trasparente, intellegibile, facilmente accessibile e con un linguaggio semplice e chiaro; le informazioni saranno fornite per iscritto o con altri mezzi, anche in formato elettronico, e, se richiesto dall'interessato, potrà essere fornita anche oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.
Per quanto attiene il consenso, sarà valida qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile con la quale l'interessato accetta, con dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento. Viene esclusa ogni forma di consenso tacito oppure raccolto attraverso la presentazione di opzioni già selezionate. Il consenso potrà essere revocato in ogni momento. Il trattamento effettuato fino a quel momento dal titolare sulla base del consenso rimarrà comunque legittimo.

Diritto all'oblio

Verrà introdotto il cosiddetto «diritto all'oblio»: il diritto da parte di un interessato ad ottenere la cancellazione dei propri dati personali, anche on line, da parte del titolare del trattamento, qualora ricorrano alcune condizioni previste dal Regolamento: i dati saranno trattati solo sulla base del consenso; se i dati non saranno più necessari per gli scopi rispetto ai quali sono stati raccolti; se i dati sono trattati illecitamente; oppure se l'interessato si oppone legittimamente al loro trattamento. Il diritto all'oblio potrà essere limitato solo in alcuni casi specifici: per esempio, per garantire l'esercizio della libertà di espressione o il diritto alla difesa in sede giudiziaria; per tutelare un interesse generale (ad esempio, la salute pubblica); oppure quando i dati, resi anonimi, sono necessari per la ricerca storica o per finalità statistiche o scientifiche.

Portabilità dei dati

Il nuovo regolamento introduce la portabilità dei dati per favorire una maggiore fluidità del mercato digitale. Tra le possibilità che il regolamento permette c'è il trasferimento dei dati da un titolare del trattamento ad un altro, si potrà cambiare il provider di posta elettronica senza perdere i contatti ed i messaggi salvati, salvaguardando il diritto di essere totalmente dimenticato da chi ha raccolto i dati inizialmente.

Tutele rafforzate

Previste inoltre più garanzie per i minori: i fornitori di servizi Internet ed i social media, dovranno richiedere il consenso ai genitori o a chi esercita la potestà genitoriale per trattare i dati personali dei minori di 16 anni.
Viene introdotta la nuova figura del Data Protection Officer (DPO), responsabile della protezione dei dati.
A cura della Redazione