80015
9 772282 452006

Chiuso in redazione il 21 maggio 2018

I FOCUS DEL SOLE 24 ORE
Il Sole 24 ORE, Milano, Sett. n. 15.
In vendita abbinata obbligatoria con Il Sole 24 ORE a € 2,00* (I focus del Sole 24 ORE € 0,50 + Il Sole 24 ORE € 1,50)

NORME & TRIBUTI FOCUS

Il Sole 24 ORE

Giovedì 24 Maggio 2018
www.ilsole24ore.com/focus

Speciale GDPR

ILLUSTRAZIONE DI STEFANO MARRA

DOMANI IL VIA ALLE NUOVE REGOLE UE

PRONTI PER LA PRIVACY?

Pronti per la privacy?
LE NORME AL DEBUTTO

Nuovi diritti e obblighi targati Ue

Dalla portabilità dei dati alla nomina del Dpo domani è l'inizio di un cammino

di **Antonello Cherchi**

Dopo due anni di transizione, domani la privacy cambia volto: diventa operativo il regolamento europeo 679, approvato dalla Ue nella primavera del 2016 con la clausola che ne rimandava l'applicazione a dopo un biennio, proprio per dare modo a tutti - singoli cittadini, pubbliche amministrazioni e imprese - di metabolizzare le novità.

E ce ne sono molte. A cominciare dal fatto che da domani in tutti i Paesi dell'Unione la normativa di riferimento sulla tutela dei dati sarà il regolamento, altrimenti conosciuto con l'acronimo Gdpr (General data protection regulation). Questo significa che le disposizioni nazionali sopravviveranno solo se compatibili con le nuove regole europee.

UN QUADRO UNITARIO

Un cambio di prospettiva dettato dalla volontà di andare oltre la frammentazione legislativa che fino a oggi ha contraddistinto la normativa sulla privacy a livello europeo. Tutto era nato 23 anni fa con la direttiva 95/46, che ciascun Paese aveva declinato a modo proprio, dando così vita a sistemi legislativi differenti l'uno dall'altro. Un approccio non più sostenibile in tempi di condivisione online dei dati, che impongono un approccio transfrontaliero alla loro tutela.

A questa esigenza è strettamente legata l'altra che ha portato al regolamento Ue: l'incessante sviluppo delle nuove tecnologie, che fanno nascere sempre nuovi problemi di protezione dei dati personali, per rispondere ai quali occorre dotarsi non solo di norme comuni, ma anche flessibili, in grado di stare al passo, per quanto possibile, con la velocità della Rete.

DIRITTI E OBBLIGHI

Da qui, per esempio, la nascita di nuovi diritti della privacy, come quello della portabilità dei dati, e il rafforzamento degli altri: dalla necessità di informative chiare e sintetiche nel momento in cui si consegnano i propri dati personali, informative in grado di trasformarsi in un consenso veramente consapevole, al diritto di accesso, opposizione, rettifica e cancellazione (il diritto all'oblio) nel caso ci si accorga che i nostri dati sono trattati irregolarmente.

L'altra faccia della medaglia sono i soggetti che quei diritti devono garantire, ovvero le pubbliche amministrazioni e le imprese chiamate da domani ad applicare il regolamento. Anche loro si troveranno alle prese con diverse novità, a cominciare dal mutamento di prospettiva che informa le nuove regole europee e che si regge sul principio di accountability: il farsi parte attiva e responsabile nella valutazione del livello di tutela dei dati necessario per la propria azienda e all'interno della pubblica amministrazione in cui si lavora. Una volta raggiunta tale consapevolezza, si tratta di progettare il sistema di di privacy in modo da organizzare al meglio la gestione dei dati personali e ridurre al minimo i rischi, per esempio di perdita o furto.

Un passaggio importante sarà la designazione del Data protection officer (Dpo) o responsabile della protezione dei dati: una figura nuova, che avrà il compito di monitorare l'applicazione delle nuove regole e, conservando la necessaria indipendenza, fare da tramite tra il proprio datore di lavoro, sia esso privato o pubblico, e il Garante della privacy.

L'INIZIO DI UN PERCORSO

Domani è solo l'inizio di un cammino iniziato due anni fa. L'applicazione del regolamento è, infatti, soltanto un primo, seppure importante, passo, al quale si accompagneranno una serie di altri interventi. Intanto l'indispensabile coordinamento tra le norme Ue e quelle nazionali che fino a oggi hanno disciplinato la materia della privacy. Si parla, in particolare, del codice (il decreto legislativo 196 del 2003), che deve essere emendato delle parti incompatibili con il regolamento.

E poi c'è tutto il lavoro di rivisitazione della "legislazione" fin qui prodotta dal Garante, in particolare i codici deontologici e di buona condotta e le autorizzazioni generali. Si tratta, in entrambi i casi, di provvedimenti che disciplinano la gestione dei dati personali in ambiti particolari e delicati, che richiedono un attento bilanciamento dei diritti. È il caso, per esempio, del giornalismo, regolato da vent'anni dal codice deontologico, il primo dei vademecum di buona condotta a vedere la luce e che ora si dovrà verificare se regge al vaglio di compatibilità con il regolamento.

Il glossario e i riferimenti normativi della nuova privacy

Accountability
Termine traducibile con «responsabilizzazione». Sta a indicare, per Titolari e responsabili, l'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento

Anc
Autorità nazionale di controllo di ogni Stato Ue, vale a dire l'autorità competente per la gestione dei reclami a essa proposti o di eventuali violazioni del Gdpr e delle norme nazionali in materia di protezione dei Dati, se l'oggetto riguarda unicamente uno stabilimento nel suo Stato membro o incide in modo sostanziale sugli interessati unicamente nel suo Stato membro

Autorità capofila
Autorità di controllo capofila disciplinata dall'articolo 56 del Gdpr. È l'autorità di controllo dello stabilimento principale, dello stabilimento unico del Titolare e del Trattamento o responsabile del Trattamento, competente ad agire in qualità di autorità di controllo capofila

Codice privacy
Decreto legislativo 30 giugno 2003, n. 196 recante «Codice in materia di protezione dei dati personali», in Gazzetta Ufficiale 29 luglio 2003, n. 174

Comitato o Cepd
Comitato europeo per la protezione dei Dati, istituito dall'articolo 68 del Gdpr. Il Comitato è composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal garante europeo della protezione dei Dati, o dai rispettivi rappresentanti

Consenso
Manifestazione di volontà libera, specifica e informata dell'Interessato con cui questi accetta espressamente che i suoi Dati personali siano fatti oggetto di Trattamento

Data breach
Violazione dei Dati personali consistente nella perdita, distruzione, diffusione indebita di Dati personali che si verifica a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità

Data protection officer (Dpo) o Responsabile dei dati personali (Rpd)
Professionista, generalmente nell'organico della società, che il Titolare nomina al fine di avere al suo interno un "focal point" (cioè, un punto di riferimento) esperto di privacy e di facilitare l'osservanza delle disposizioni del Gdpr

Dati biometrici
Tutti i Dati personali ottenuti da un Trattamento relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i Dati dattiloscopici

Dati genetici
Tutti i Dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di questa persona, e che risultano in particolare dall'analisi di un campione biologico

Dati giudiziari
Dati personali che rivelano l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio provvedimenti penali di condanna definitivi, liberazione condizionale, divieto o obbligo di soggiorno, misure alternative alla detenzione)

Dati personali o Dati
Qualunque informazione relativa a una persona fisica, identificata o identificabile, anche indirettamente, attraverso altre informazioni, ivi compreso un numero di identificazione personale

Dati sanitari
Dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute

Dati sensibili
Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altra genere, le opinioni politiche, l'adesione a partiti, sindacati o associazioni od organizzazioni a carattere religioso, filosofico, polito o sindacale, nonché i Dati personali idonei a rivelare stato di salute e vita sessuale

Direttiva e-Privacy
Direttiva 2002/58/CE del 12 luglio 2002, relativa al «trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)», in Guce [2002] L 201

Direttiva madre
Direttiva 95/46/CE del 24 ottobre 1995, relativa alla «tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati», in Guce [1995] L 46

Dossier sanitario
Strumento costituito presso un organismo sanitario in qualità di unico Titolare del trattamento (ad esempio, ospedali, aziende sanitarie, case di cura) al cui interno operano più professionisti, attraverso il quale sono rese accessibili informazioni, inerenti i Dati sanitari di un Interessato

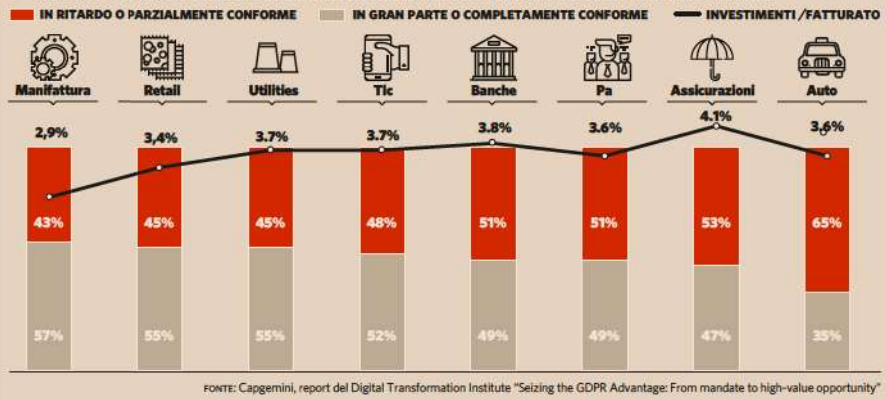
Dpia
Data Protection Impact Assessment, ovvero la valutazione d'impatto sulla protezione dei dati che il Titolare del trattamento è obbligato a fare quando può esserci un rischio elevato per i diritti e le libertà delle persone interessate

Finalità (del Trattamento)
Scopo determinato, esplicito e legittimo che viene perseguito dal Titolare con il Trattamento

Garante
Autorità garante per la protezione dei Dati personali: l'Anc preposta alla vigilanza e al controllo della normativa sulla protezione dei Dati personali

La risposta dei settori

Conformità GDPR, per settore. Dati basati su interviste a 1.000 dirigenti e 6.000 clienti in 8 mercati



FONTE: Capgemini, report del Digital Transformation Institute "Seizing the GDPR Advantage: From mandate to high-value opportunity"

Il sistema. Insieme al regolamento Ue resta l'attuale codice

Il quadro normativo diventa più complesso

di **Giusella Finocchiaro***

A distanza di oltre vent'anni dalla prima normativa europea in materia, la direttiva-madre 46 del 1995, è giunto il momento di voltare pagina. Prendendo atto dei cambiamenti tecnologici (nel 1995 non esistevano gli smartphone) che hanno indotto grandi cambiamenti sociologici (basti pensare alla vita che si svolge sui social network). È cambiato anche il contesto economico: oggi i dati sono il nuovo petrolio, come scrive l'Economist. E quello politico: l'Europa si è impegnata nel mercato unico digitale.

Il Regolamento europeo 679/2016, che entra in vigore domani, riflette tutti questi cambiamenti e volta pagina. Innanzitutto detta una disciplina unitaria per tutti gli Stati membri, salvo alcuni spazi lasciati al legislatore nazionale, definendo così uno spazio unico anche sotto il profilo giuridico, all'interno e verso l'esterno.

Afferma con forza il principio della libera circolazione dei dati, la quale «non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali», come recita l'articolo 1 del regolamento.

Il diritto alla protezione dei dati personali, sancito dalla Carta dei diritti fondamentali dell'Unione europea, è soggetto a un necessario bilanciamento. I dati personali possono essere al tempo stesso gli elementi su cui si definiscono l'immagine e l'identità dell'individuo, nonché beni economici oggetto di scambio.

Il patrimonio italiano costituito dalla nostra elaborazione normativa, giurisprudenziale e dottrinale, è ormai patrimonio giuridico europeo e in questa prospettiva va correttamente inquadrata la nuova fase della protezione dei dati personali. I principi fondamentali già consolidati sono confermati dal regolamento europeo: così informativa, consenso e altri presupposti di legittimità del trattamento.

Muta però la filosofia di fondo: si passa dall'approccio autorizzatorio a quello fondato sull'accountability. E questo comporta la modifica nella governance: la gestione dei dati personali diviene gestione del rischio, non più soltanto competenza del legale o dell'It.

In Italia, con grande ritardo, è stata incaricata una commissione legislativa - che ha concluso i lavori in due mesi, il 19 marzo - di predisporre il testo di un decreto legislativo per adeguare la normativa italiana a quella europea. Opera non strettamente necessaria, essendo il regolamento direttamente applicabile, ma utile per operare un coordinamento.

La commissione ha verificato la compatibilità delle norme presenti nell'ordinamento italiano con quelle del regolamento europeo, che direttamente le sostituiscono. Ha quindi proceduto con un'operazione non frequente: l'abrogazione espressa delle norme italiane sostituite. Si tratta di un'operazione culturale di grande rilevanza, volta a chiarire agli operatori e agli interpreti il quadro normativo di riferimento.

Questa verifica ha condotto all'abrogazione della maggior parte delle norme del codice privacy, ormai sostituite dal Gdpr. La conseguenza ovvia sarebbe stata l'abrogazione del codice, non più tale, per favorire la leggibilità complessiva.

Questa proposta non è stata accolta dal Governo, che ha preferito un'altra tecnica normativa che ha condotto alla formulazione di un testo di decreto che detta delle inserzioni nel codice, che ne abroga una grande parte e che formula delle disposizioni ulteriori. Il risultato è un quadro normativo di inutile complessità, che non aiuta certo gli operatori. Il Governo, con una scelta su cui ha certamente influito anche la vicenda Cambridge Analityca, ha inoltre introdotto nuove fattispecie penali.

La commissione ha effettuato alcune scelte nei settori in cui gli Stati conservano competenza e ha operato un raccordo fra il ricco quadro complessivo previgente e il Gdpr, mantenendo la continuità. Sono fatti salvi per un periodo transitorio i provvedimenti del Garante (si pensi, per esempio a quello in materia di biometria) e le autorizzazioni, che saranno oggetto di successivo riesame. Sono stati mantenuti anche i codici deontologici vigenti (ad esempio, quello dei giornalisti). Si è rafforzato il meccanismo delle consultazioni pubbliche e il coinvolgimento delle categorie interessate in molteplici casi. Per le micro, piccole e medie imprese si è previsto che il Garante promuova modalità semplificate di adempimento degli obblighi del titolare del trattamento.

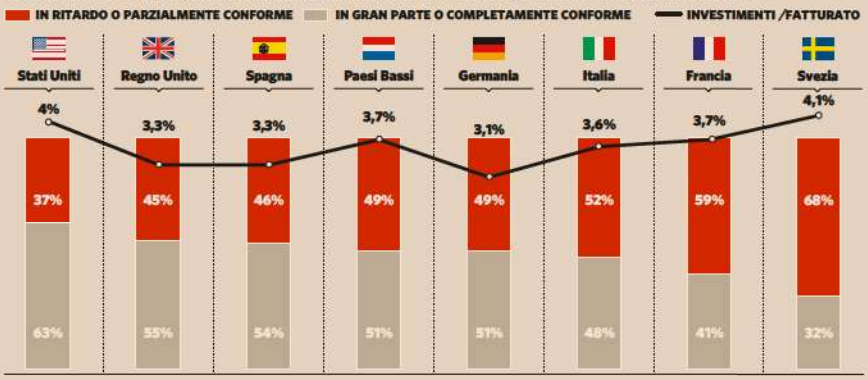
Da domani, dunque, si volta pagina. Maggiore libertà e maggiore responsabilità per i titolari del trattamento che potranno, da un lato, sfruttare le nuove aperture contenute nel Gdpr, come la base giuridica del "legittimo interesse", ma dall'altro lato saranno chiamati a motivare e a documentare le scelte.

Un ruolo nuovo per il Garante, che dovrà guidare il processo di adeguamento alle nuove disposizioni anche con un nuovo approccio e nuove competenze, relative, per esempio alla gestione del rischio. E infine per gli operatori, che dovranno rendersi parte attiva e quanto prima attivare i processi normativi che li possono vedere direttamente coinvolti, come l'elaborazione di codici di condotta.

** Presidente della commissione incaricata di adeguare la normativa italiana sulla privacy al regolamento europeo*

In corso di adeguamento

Conformità GDPR, per paese. Dati basati su interviste a 1.000 dirigenti e 6.000 clienti in 8 mercati



FONTE: Capgemini, report del Digital Transformation Institute "Seizing the GDPR Advantage: From mandate to high-value opportunity"

Gdpr
Acronimo di «General Data Protection Regulation», cioé «Regolamento generale sulla protezione dei dati», ovvero il Regolamento Ue 2016/679.

Gruppo di lavoro ex Articolo 29 o Gla29
Gruppo per la tutela delle persone con riguardo al Trattamento dei Dati personali, istituito dall'articolo 29 della Direttiva madre. È un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei Dati personali designate da ciascuno Stato membro, dal Garante europeo della protezione dei Dati (European Data Protection Supervisor), nonché da un rappresentante della Commissione

Incaricato (del Trattamento)
Persona fisica autorizzata a compiere operazioni di Trattamento sulla base delle istruzioni ricevute dal Titolare e/o dal Responsabile, ove designato

Informativa
Documento (o insieme di informazioni) contenente le informazioni che il Titolare deve fornire all'Interessato per chiarire se quest'ultimo è obbligato o meno a rilasciare i Dati personali, le conseguenze di un eventuale rifiuto al rilascio dei Dati personali, quali sono le finalità e le modalità del Trattamento, i soggetti che entrano in contatto con i suoi Dati personali, come circolano i Dati personali e in che modo esercitare i diritti riconosciuti dal Gdpr

Informazioni personali identificabili o Pii
Informazioni Personali Identificabili o «Personally identifiable information» (Pii).

Interessato
Persona fisica cui si riferiscono i Dati personali

Misure di sicurezza
Complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione

Ott
L'Autorità per le Garanzie nelle Comunicazioni definisce "Over-the-top" le imprese che forniscono, attraverso la rete Internet, servizi, contenuti (soprattutto video) e applicazioni di tipo *rich media* (ad esempio, le pubblicità che appaiono "sopra" la pagina di un sito web mentre lo si visita e che dopo una durata prefissata scompaiono)

Regolamento o Gdpr
Regolamento (Ue) 2016/679 del 27 aprile 2016 relativo alla «protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)», in Gazzetta Ufficiale dell'Unione europea [2016] L 119, pagine 1-88

Registro dei Trattamenti o Registro
Registro delle attività di Trattamento, disciplinato dall'articolo 30 Gdpr, il quale deve essere conservato da ogni Titolare

Responsabile (del Trattamento)
Persona, fisica o giuridica, Pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al Trattamento

Tfue
Trattato sul funzionamento dell'Unione europea (versione consolidata), come modificato dall'articolo 2 del Trattato di Lisbona del 13 dicembre 2007 ratificato dalla legge 2 agosto 2008, n. 130, in Guue 8 agosto 2008, n. 185

Titolare (del Trattamento)
Persona, fisica o giuridica, pubblica amministrazione e qualsiasi altro ente, associazione o organismo cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del Trattamento e agli strumenti utilizzati, compreso il profilo della sicurezza

Tlc
Telecomunicazioni, vale a dire qualunque sistema di comunicazione (ad esempio, radio, telefono e televisione) che permetta di trasmettere suoni o immagini a distanza

Trattamento
Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di Dati personali, anche se non registrati in una banca di Dati

Tue
Trattato sull'Unione europea (versione consolidata), come modificato dall'articolo 1 del Trattato di Lisbona 13 dicembre 2007 ratificato dalla legge 2 agosto 2008, n. 130, in Guue 8 agosto 2008, n. 185

Vip o Dpia
Valutazione di Impatto Privacy o Data Protection Impact Assessment, da cui il relativo acronimo (Dpia)

LA DOCUMENTAZIONE

LA «GUIDA» ALLA NUOVA DISCIPLINA

Il Glossario riportato in queste pagine è un estratto di quello contenuto nella Guida «Privacy - La nuova disciplina europea», in vendita su Il sito del Sole 24 Ore, in formato cartaceo e in pdf

www.shopping24.ilsole24ore.com
L'indirizzo per acquistare la Guida

Pronti per la privacy?

ASPETTI CRITICI

Facebook e gli altri social aggiornano le strategie

Si innalza il limite di età per l'accesso e diventano severi i requisiti sulla riservatezza

di **Marisa Marraffino**

Le nuove norme sulla privacy introdotte dal Regolamento Ue 2016/679, noto come Gdpr, impattano anche sui social network che trattano dati degli utenti dell'Unione Europea. Per questi soggetti occorrerà quindi semplificare i modelli delle informative, ampliare i diritti degli interessati (ad esempio garantendo la portabilità dei dati) e verificare l'età minima dell'utente, che viene innalzata dai 13 ai 16 anni. Di fatto, però, al social network basterà l'autodichiarazione dell'utente, ovvero far spuntare un pop-up in cui l'interessato dichiari di avere almeno 16 anni.

PER I MINORI

Una battaglia di principio, più che una verifica effettiva, visto che a oggi non esiste alcuna norma internazionale che imponga ai provider controlli sulla veridicità delle dichiarazioni rilasciate dagli interessati. L'articolo 8 del Regolamento UE 2016/679 prevede poi che ogni Stato membro possa abbassare l'età minima di iscrizione ai social network fino a tredici anni. In questo caso, tuttavia, occorrerà il consenso dei genitori. Difficile ipotizzare che le piattaforme prevedano forme di validazione diverse per ogni Stato membro, chiedendo al minore se ha acquisito il consenso dei genitori.

Più problematica la questione relativa al trattamento dei dati degli utenti già iscritti che abbiano dichiarato di avere meno di sedici anni. Teoricamente il social network dovrebbe cessare di trattare i loro dati dal momento dell'entrata in vigore del Gdpr oppure, più realisticamente, affrettarsi a chiedere loro prima di tale data se hanno acquisito il consenso dei genitori.

Si tratta complessivamente di una riforma culturale che – di fatto – impone ai genitori un maggior controllo sui figli, ma che non sposta di molto la responsabilità dei social network.

MAGGIORE SICUREZZA

Più effettivo invece potrà essere il controllo sulle misure di sicurezza adottate dai social network per evitare violazioni dei dati, ovvero data breach. Per il trattamento massivo di dati occorrerà dimostrare di aver adottato misure idonee e dovrà essere nominato un rappresentante Ue che si occupi di far rispettare le nuove norme e di comunicare agli utenti, senza ritardo, eventuali accessi non autorizzati. In questi casi le norme sono provviste di sanzioni che possono arrivare fino a 20 milioni di euro o al 4% del fatturato (per il dettaglio delle sanzioni, si veda a pagina 14).

Il cosiddetto "consenso granulare" impone poi che per ogni finalità di trattamento dei dati, ad esempio geolocalizzazione, profilazione, marketing, debba essere rilasciato un consenso distinto. Già con l'entrata in vigore della prima legge sulla privacy, la legge 675/96, il Garante per la protezione dei dati personali italiano aveva pubblicato una guida dal titolo «il primo Garante sei tu»: un titolo che diventa oggi, alla luce del Gdpr, addirittura profetico. Sarà infatti l'utente a dover leggere con più attenzione le informative che saranno più brevi e semplici, ma che non dovranno più essere ignorate come avveniva in passato. Affinché tutto cambi, infatti, occorre che nulla resti com'è, a partire dalla consapevolezza degli utenti.

In azienda. Le mosse dei big della telefonia per l'adeguamento

Dispositivi mobili, il fronte più esposto

Tra le preoccupazioni delle imprese per il debutto del Regolamento Ue sulla privacy, c'è anche anche la gestione dei dispositivi di telefonia mobile. Passaggio cruciale, perché il traffico sui siti che arriva da browser mobili è ormai più importante di quello da desktop. Per una configurazione dei dispositivi mobili conforme al Gdpr sono numerosi i punti da prendere in considerazione (si veda la scheda): dalla configurazione delle connessioni disponibili (wifi, Vpn, bluetooth, Nfc, gps) e dispositivi di archiviazione (schede SD) fino alla configurazione di fotocamera e audio e alla gestione degli aggiornamenti delle applicazioni. È inoltre fondamentale la manutenzione del sistema operativo.

I grandi operatori del settore, come Samsung e Apple, sono attvi da tempo, come ha segnalato nei giorni scorsi Biagio Simonetta sul sito del Sole 24 Ore. La casa coreana, leader del mercato smartphone con sistema operativo Android, punta tutto sulla piattaforma Samsung Knox, che - spiega la stessa azienda - «fornisce una serie di meccanismi di sicurezza volti a tutelare i dati contenuti nei dispositivi mobili», dando «la libertà di lavorare ovunque e in qualunque momento». La piattaforma Knox ha una vasta gamma di funzioni, dalla custodia separata dei dati personali e di quelli aziendali fino alla gestione remota degli smartphone aziendali. «Abbiamo sviluppato un sistema di cifratura dei dati integrato sia nell'hardware sia nel software dei nostri terminali», spiega il sito dell'azienda coreana.

L'altro macrocosmo mobile porta il nome di Apple. L'azienda di Cupertino ha investito nell'adeguamento al Gdpr e può vantare un background importante in fatto di sicurezza e di impenetrabilità dei dati. Apple spiega di aver già da tempo intrapreso la strada della "privacy by design": progettazione di apparecchi e servizi pensati da subito per minimizzare la raccolta dei dati e dare il massimo del controllo agli utenti. Inoltre, sono state recentemente introdotte alcune novità, fra cui le nuove info sulla privacy e la nuova icona, resa disponibile su tutte le piattaforme, per rendere più chiaro il modo in cui Apple userà i dati dei clienti quando sottoscrivono o attivano determinate funzioni.

SETTE MOSSE ANTI-INCONVENIENTI

1. Gestione centralizzata
Ogni politica per la sicurezza dei dispositivi mobili dovrebbe basarsi sulla gestione centralizzata dei dispositivi e dei profili utente

2. Autorizzazioni guidate
La segmentazione riveste un'enorme importanza. Vanno definiti i profili utente in base alle funzioni e va regolato l'accesso agli strumenti amministrativi per consentire la delegazione delle funzioni amministrative e stabilire le norme per l'assegnazione dei dispositivi

3. Controllo dell'accesso
Occorre considerare non solo le password, ma anche le norme correlate e l'accesso in generale (ad esempio: quanti tentativi prima di sbloccare un dispositivo? Qual è il livello di accesso necessario? Deve essere consentita l'attivazione delle fotocamere?)

4. Garanzia dell'integrità del sistema operativo
A ogni accensione del dispositivo è necessario verificare l'integrità del sistema operativo e dei relativi aggiornamenti

5. Messa in sicurezza di app e dati
È necessario imporre un certo grado di controllo sugli "app store" e individuare eventuali problemi relativi alle app installate

6. Distinzione tra utilizzo professionale e personale
È necessario garantire che gli strumenti e le app personali non compromettano i dati aziendali (la responsabilità potrebbe ricadere sull'azienda)

7. Capacità di intervenire da remoto
Furti e smarrimenti dei telefoni sono frequenti e rappresentano il rischio più grande per le aziende. La soluzione è garantire la capacità di formattare o bloccare i dispositivi da remoto e in sicurezza, in modo che oltre al telefono non vengano rubati anche i dati

Fonte: Samsung - Gdpr Campaign

APPUNTAMENTI PER LA NUOVA PRIVACY

DAL «SOLE 24 ORE»

Forum Facebook sul debutto

Prosegue l'attività di informazione e divulgazione del Sole 24 Ore per il Regolamento Ue (si vedano anche le iniziative a pagina 15 di questo inserto: sulla pagina Facebook del Sole (www.facebook.com/ilsole24ore/) il Forum gratuito con gli esperti che si è svolto ieri, per approfondire i vari aspetti del Gdpr e per fornire tutti i chiarimenti sui nuovi obblighi.
Tra i video consultabili sulla pagina resta inoltre a disposizione il Forum realizzato il 14 maggio sempre in materia di privacy e Regolamento Ue. In quell'occasione hanno risposto alle domande dei partecipanti il segretario generale dell'Autorità per la protezione dei dati personali, Giuseppe Busia, l'avvocato Riccardo Imperiali, i giornalisti Antonello Cherchi e Francesca Milano.

OGGI A BOLOGNA

Incontro del Garante con gli «Rpd»

Oggi a Bologna (Palazzo dei Congressi - Piazza della Costituzione 4), il Garante privacy incontra i responsabili della protezione dei dati (Rpd). L'incontro ha inizio alle ore 10 e si protrarrà fino alle 17.45. Saranno presenti tutti i componenti del Collegio dell'Autorità.
Obiettivo della giornata è offrire a questa nuova figura del «Rpd» - centrale nel processo di attuazione del principio di «responsabilizzazione» (accountability) - le prime indicazioni utili per l'attuazione dei compiti e per la definizione delle modalità di relazione con l'Autorità.
L'evento è organizzato in collaborazione con Regione Emilia-Romagna e LepidaSpA ed è aperto alla partecipazione dei Responsabili della Protezione dei Dati sia pubblici che privati.
Rientra in un più ampio progetto promosso dall'Autorità per favorire la conoscenza delle nuove norme e offrire supporto nell'attuazione degli adempimenti previsti dal Regolamento.

Pronti per la privacy? Le novità in 10 domande

I PUNTI FONDAMENTALI DELLE DISPOSIZIONI UE

1 | A chi si applica il Regolamento sulla protezione dei dati?

Con il «Gdpr» le norme di tutela diventano anche un nuovo standard per il mercato

di **Rosario Imperiali**

Se si considera l'intreccio di possibilità, come sintetizzato nella scheda qui accanto, appare subito chiaro che le disposizioni contenute nel regolamento Ue syl trattamento dei dati personali (Gdpr) non sono solo norme europee ma costituiscono piuttosto uno standard internazionale.

Che sia stata l'Europa a dettare le regole è comprensibile, visto il valore del mercato Ue dei dati (cioè dei dati digitali scambiati come prodotto o servizio) che, secondo una ricerca della Commissione del marzo di quest'anno (Smart 2016/0063), è oggi pari a 65 miliardi di euro e toccherà i 77 miliardi (60 per l'Ue a 27) nel 2020, mentre l'economia dei dati (cioè lo sfruttamento dei dati mediante l'odierna tecnologia) ammonta a 335 miliardi (dati 2017) con una previsione che tocca i 452 miliardi di euro (365 senza il Regno Unito) nel 2020.

DATI, MERCATO E FIDUCIA

Dati e dati personali - come si vedrà nelle pagine successive - sono quasi sinonimi e la pregiudiziale per sostenere e sviluppare la data economy è la tutela della fiducia dell'individuo circa il corretto utilizzo dei propri dati personali da parte del mercato.

Per «dato personale» il Regolamento intende «qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica,fisiologica, genetica, psichica, economica, culturale o sociale».

Il Gdpr contribuisce significativamente a tutelare la fiducia di chi affida i propri dati, da un lato proteggendo i diritti del singolo riguardo all'uso dei propri dati personali, sulla scia della natura fondamentale riconosciutagli dal trattato di Lisbona e, dall'altro lato, rimuove gli ostacoli alla circolazione dei dati personali all'interno dell'Unione. Nell'attuale mondo globalizzato, quindi, non è sufficiente stabilire autonomamente il livello di adempimento al Gdpr che l'azienda, anche se meramente locale, possa decidere di conseguire, in quanto - da ultimo - sarà la filiera delle relazioni commerciali con fornitori e clienti ad imporle lo standard da rispettare.

RICADUTE GLOBALI

Le aziende con sede in uno dei Paesi della Ue dovranno necessariamente fare i conti con le prescrizioni del Gdpr e, in caso alimentino flussi di dati all'interno dell'Unione, dovranno anche individuare quale sia l'autorità guida competente per le qUestioni data protection relative a qUel flusso.

Se il flusso, invece, riguarda paesi terzi (non Ue), qualora riguardi dati personali di soggetti che si trovano nella Ue, esso dovrà essere regolato da apposite clausole contrattuali che vincolino i partner importatori di dati a comportamenti conformi ai dettati del Gdpr. In aggiunta, se i trattamenti sui dati personali effettuati dalle medesime aziende non-Ue le qualificano come titolari o responsabili in base al Gdpr, qUeste stesse aziende saranno soggette alle pertinenti prescrizioni del regolamento e dovranno nominare per iscritto un proprio rappresentante in uno degli Stati membri dell'Unione.

Non deve apparire un paradosso, quindi, il presentimento che individua nel mercato, piuttosto che nello spauracchio delle alte sanzioni o nella compliance in sé, il vero innesco che determinerà la citata metamorfosi del Gdpr, da norma di competenza europea a standard universale.

IL TRATTAMENTO DEI DATI NELL'UNIONE EUROPEA E OLTRE

Trattamento dei dati nella Ue

- Questa è l'ipotesi più evidente, in cui il trattamento si svolge in territorio Ue; ci si potrebbe chiedere se questo sia vero anche nell'ipotesi, ad esempio, di un CRM contenente solo dati di clienti che si trovino fuori della Ue, cui si ritiene debba darsi risposta affermativa in considerazione della natura fondamentale del diritto alla protezione dei dati personali

Trattamento dei dati fuori dalla Ue

- Se il trattamento è effettuato fuori della Ue ma per conto di un titolare o un responsabile ubicato nella Ue.
- Può esserci il caso in cui operazioni di trattamento vengano demandate a terzi che si trovino oltre i confini della Ue.
- Oppure l'ipotesi di un'azienda titolare che si avvale di altra azienda in funzione di responsabile del trattamento oppure di un ulteriore sub-appaltatore (sempre localizzato fuori della Ue)
- Se il trattamento rientra in origine nella competenza del Gdpr, è indifferente dove sono ubicate le aziende che eventualmente effettuino operazioni di trattamento per conto del titolare; tali operazioni dovranno comunqUe rispettare le prescrizioni del Gdpr

Trattamento «connesso»

- Può accadere che il trattamento, anche se effettuato fuori della Ue, sia strettamente connesso alle attività di uno stabilimento localizzato nella Ue. Questa ipotesi è un po' più difficile da comprendere e discende dal caso Google Spain della Corte di Giustizia Ue, in cui è stato elaborato il principio della «inestricabile connessione» come criterio di attrazione della competenza data protection
- In quella circostanza, l'attività di gestione del motore di ricerca Google effettuata nello stabilimento di Google Inc. in California (meglio, il trattamento di dati personali ad essa connesso) è stata ritenuta «inestricabilmente legata» all'attività di raccolta pubblicitaria svolta presso lo stabilimento di Google Spain in Spagna, in quanto la raccolta pubblicitaria è elemento essenziale del modello di business che consente la fruizione (apparentemente) gratuita del motore di ricerca di Google da parte degli utenti

Trattamento svolto da azienda non Ue

Il trattamento svolto da un'azienda estera non Ue, ad esempio giapponese o americana, ma che riguarda dati personali di individui che si trovano nella Uem è la novità espressamente prevista dal Gdpr (articolo 3, 2).

LE INDICAZIONI DEL REGOLAMENTO 2016/679

ARTICOLO | 1
Oggetto e finalità

1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.
2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

ARTICOLO | 2
Ambito di applicazione materiale

1. Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.
2. Il presente regolamento non si applica ai trattamenti di dati personali:
a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V,capo 2, TUE;
c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

ARTICOLO | 3
Ambito di applicazione territoriale

1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.
2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.
3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

Pronti per la privacy?
LE NOVITÀ IN DIECI DOMANDE

2 | Quali dati personali riguarda e come vengono distinti?

Gradi differenti di protezione secondo la sensibilità delle informazioni

di **Rosario Imperiali**

Quando si affronta il tema dei dati personali viene alla mente la raffigurazione di una piramide ad ampia base, che racchiude tutte le ipotesi che consentono di qualificare un'informazione, come personale, ai fini dell'applicabilità della normativa data protection. Le parti alte della figura sono occupate da quelle categorie speciali di dati a più alto tasso di sensibilità riguardo ai diritti ed alle libertà degli interessati e, conseguentemente, a più elevato rischio; in Italia, siamo abituati a indicarle come dati sensibili o giudiziari.

Da ultimo, il vertice della figura è occupato dall'informazione più intima tra tutte: un multi-dato spesso ignoto allo stesso interessato, quello genetico.

La scala dei valori sul dato personale viene ribadita nel Gdpr, con poche novità. A beneficio di altri contesti nazionali, dove il dibattito sulla qualificazione dell'informazione come dato personale era stato più incerto, diversamente che da noi, il legislatore comunitario rende inequivoca l'attrazione nella cerchia di dato personale di qualsiasi identificativo - incluso lo pseudonimo - che sia in grado di individuare, anche in via indiretta, l'interessato.

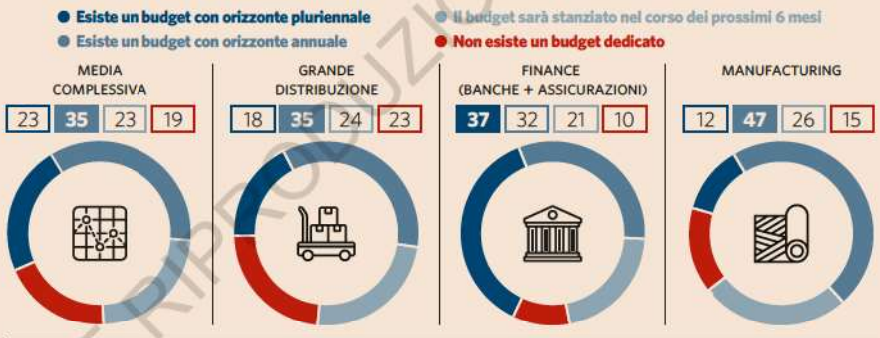
Rimangono fuori dall'ambito solo i dati anonimi, cioè quelli non riconducibili in alcun modo ad un individuo determinato, insieme a quelli per i quali il processo di re-identificazione possa considerarsi ragionevolmente improbabile a causa della necessità di avvalersi per lo scopo di mezzi eccessivi, prendendo in considerazione l'insieme dei fattori obiettivi, tra cui i costi, il tempo necessario per l'identificazione e le tecnologie disponibili al momento.

Per i dati sensibili e giudiziari sono previste maggiori salvaguardie e garanzie volte a ridurre il pericolo di violazioni a danno degli interessati: maggiore è l'obbligo di trasparenza, il consenso deve essere esplicito e non solo inequivocabile, i processi decisionali automatizzati sono di regola vietati, in presenza di tali speciali categorie di dati l'obbligo di tenuta del registro dei trattamenti permane anche per le piccole e medie imprese e, infine, se essi sono presenti su larga scala presuppongono la valutazione d'impatto (Dpia) e la designazione del Dpo.

In cima alla piramide, i dati genetici includono il campione biologico della persona fisica dalla cui analisi possono essere desunti, così come dati genetici e campioni biologici possono essere fonte di dati riguardanti lo stato di salute fisica o mentale dell'interessato. Il Gdpr, in applicazione del principio di sussidiarietà, riconosce la libertà degli Stati membri di introdurre ulteriori condizioni o limitazioni riguardo al trattamento di dati genetici, biometrici o relativi alla salute che il legislatore nostrano si appresta a precisare nel decreto di adeguamento della normativa nazionale.

Le imprese e la privacy

? **La percentuale di aziende italiane, divise per settore di mercato, che ha stanziato un budget dedicato a misure di risposta al GDPR**



FONTE: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano; IDC 2017

DAL CODICE ITALIANO DELLA PRIVACY ALLE NUOVE DISPOSIZIONI EUROPEE

Il «dato personale»
Il concetto di dato personale non è sostanzialmente mutato nel Gdpr, rispetto a quello definito nella direttiva 95/46 e nella norma italiana di recepimento che è il codice privacy: il criterio della identificabilità diretta o indiretta dell'individuo continua a caratterizzare l'ampia portata di questa definizione

Gli «identificatori»
Gli identificatori, come i numeri di identificazione, gli identificativi on line, i dati relativi all'ubicazione, sono considerati dati personali proprio in quanto sono in grado di identificare una persona, se a essa collegati

Gli pseudonimi
Pseudonimi, cioè i dati personali oscurati con codici per non consentire la diretta identificazione dell'interessato, ma di cui si conserva disponibile la chiave di decodifica, continuano ad essere dati personali in virtù del permanere della possibilità di identificazione

I dati crittografati
Dati crittografati, diversamente dagli altri concetti, attengono a una modalità di elaborazione dei dati che li rende non intelligibili.
per la lettura in chiaro occorre disporre della chiave di decrittazione per cui, a differenza della pseudonimizzazione, la crittografia determina l'oscuramento totale del testo e non solo dei dati identificativi della persona

I «dati sensibili»
La categoria dei dati sensibili, nota a noi italiani, è stata sostituita dalla locuzione «categorie particolari di dati personali»includendovi espressamente anche i dati genetici e biometrici, peraltro già considerati tali dagli interpreti

I dati giudiziari
La categoria dei dati giudiziari, analogamente a quella dei dati sensibili, non gode più di un elemento definitorio nel Gdpr e, in via parzialmente diversa dal Codice privacy, riguarda solo dati personali relativi a condanne penali o a reati, per cui è dubbio che possa continuare a rientrarvi la qualità di imputato o indagato, come previsto nel Codice Privacy ante-Gdpr

LE INDICAZIONI DEL REGOLAMENTO 2016/679

ARTICOLO | 5
Principi applicabili al trattamento di dati personali

1. I dati personali sono:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

Pronti per la privacy?
LE NOVITÀ IN DIECI DOMANDE

3 | Ho predisposto l'informativa e la raccolta del consenso?

Il requisito fondamentale è la chiarezza nei confronti degli interessati

di **Rosario Imperiali**

L'obbligo di informare l'interessato è adempimento fondamentale che ammette limitate deroghe, in attuazione del principio di trasparenza che costituisce uno dei capisaldi della legittimità del trattamento.

L'informativa correttamente formulata e fornita risponde a una molteplicità di funzioni essenziali per la tutela dei diritti e delle libertà degli interessati. Informando preventivamente l'individuo di cui si intende utilizzare i dati personali, gli si consente di avere un quadro complessivo delle finalità e modalità di utilizzo degli stessi e di poter esprimere un consenso realmente consapevole e, allo stesso tempo, di conoscere su quale ulteriore fondamento giuridico si sostanzia il trattamento. In aggiunta, l'informativa mette l'interessato in grado di poter esercitare i propri diritti in relazione al titolare di riferimento, avvalendosi dei canali di contatto e comunicazione in essa indicati.

Il Gdpr dedica l'intero articolo 12 per la determinazione delle modalità di redazione e di fornitura dell'informativa. Sotto il profilo redazionale, si sottolinea la necessità di utilizzare un linguaggio chiaro, non tecnico, facilmente comprensibile; attenzione viene prestata alla concisione ed al formato della struttura del documento, atto a facilitarne la lettura. Appare evidente un arduo sforzo di bilanciamento tra esigenze apparentemente confliggenti: quella dell'esaustività e tassatività delle informazioni anche di dettaglio e, in contro-tendenza, l'esigenza di concisione, semplificazione e immediatezza.

Anche a livello operativo e funzionale è prevedibile una forte dialettica tra coloro che vorranno privilegiare la tecnica redazionale di stampo giuridico ed i più propensi all'informalità di approccio, ben sapendo che la soluzione ottimale è nel mezzo: l'uso di una forma discorsiva che non sia a detrimento degli argomenti da trattare.

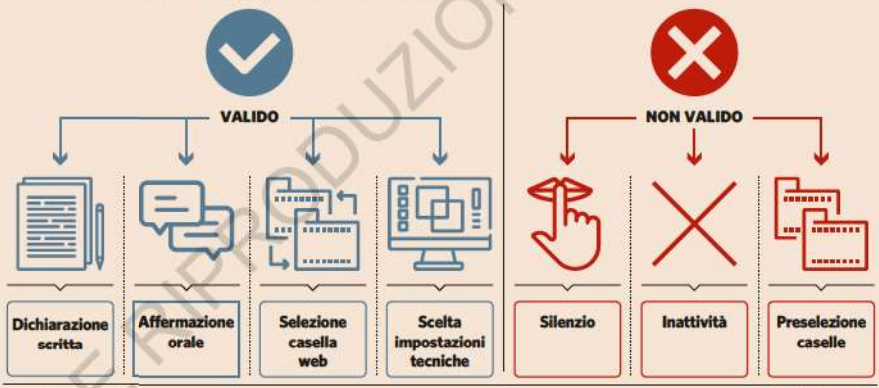
In questa direzione, le linee guida del Gruppo di lavoro dell'Articolo 29 sottolineano l'opportunità di ricorrere a tecniche multi-livello, specie nell'ambito online, che permettano di indirizzare l'individuo verso l'argomento di specifico interesse; oppure di fare ricorso alla scissione fra un primo messaggio conciso ed essenziale che rinvii poi a un'informativa completa facilmente accessibile.

Riguardo al consenso, si registrano importanti novità rispetto al Codice Privacy: esso non è più considerato il fondamento giuridico preferenziale ma uno fra i molti ed addirittura, in taluni casi, persino residuale o inadeguato, anche grazie alla nuova disciplina sull'interesse legittimo che ora è oggetto di autonoma valutazione del titolare e non più rimesso al giudizio del Garante.

Infine, la forma scritta non è più obbligatoria, né a fini probatori (come previsto dal Codice per i dati non sensibili) né costitutivi (per i dati sensibili).

La forma del consenso

Il consenso deve essere espresso con atto positivo ed inequivocabile



FONTE: @Ros_Imperiali

IL LEGAME TASSATIVO TRA INFORMATIVA E CONSENSO

Informativa e consenso
- Informativa e consenso sono strettamente connessi; nel senso che non esiste un valido consenso se privo di una preliminare informativa, mentre possono aversi circostanze in cui, ai fini della legittimità del trattamento, all'informativa può non seguire necessariamente il consenso del soggetto interessato, in quanto il consenso è solo una delle basi legali per un trattamento legittimo

I contenuti dell'informativa
- Il Gdpr prevede due gruppi di informazioni da fornire agli interessati; apparentemente, la distinzione potrebbe venire interpretata nel senso che il primo gruppo contenga informazioni tassative da fornire in ogni caso, mentre il secondo includa informazioni da aggiungere per una maggiore trasparenza
- Secondo il Gruppo di lavoro dell'articolo 29, organo consultivo della Commissione Ue su questi temi, le informazioni di entrambi i gruppi sono parimenti tassative

Le modalità
- Il Gdpr fornisce indicazioni sui contenuti e sulla forma delle informazioni da fornire nonché sulle modalità di comunicazione
- La forma può essere scritta o orale ma sempre semplice e facilmente comprensibile
- La modalità richiede che l'informazione sia fornita piuttosto che resa disponibile: nel senso che spetta all'azienda produrla direttamente all'interessato oppure indirizzare l'interessato su dove reperirla, evitando che quest'ultimo sia costretto a cercarla autonomamente

La richiesta
- La richiesta del consenso deve essere chiaramente distinguibile da altri contesti; l'azienda dovrà essere in grado di dimostrare che l'interessato abbia acconsentito mediante una dichiarazione o azione positiva inequivocabile

LE INDICAZIONI DEL REGOLAMENTO 2016/679

ARTICOLO | 7
Condizioni per il consenso
1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

ARTICOLO | 8
Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione
1. Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale. Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.
2. Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.
3. Il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore.

Pronti per la privacy?
LE NOVITÀ IN DIECI DOMANDE

4 | Sono in grado di garantire i diritti degli interessati?

Dal diritto di accesso a quello all'oblio, il titolare deve avere un canale elettronico per le richieste

di **Giuliano Fonderico**

I diritti degli interessati non sono una novità del Regolamento, già erano previsti dalla direttiva del 1995 e dal Codice italiano della riservatezza del 2003. Il Regolamento, però, li rafforza e ne prevede di nuovi.

Come in passato, gli interessati possono chiedere di "accedere" ai loro dati – per conoscerne il contenuto e l'origine, le finalità ecc. – o che i loro dati siano "rettificati" a fronte di errori o di omissioni. Un altro diritto che già esisteva è quello di "opposizione", che il Regolamento articola in più ipotesi. L'interessato può sempre opporsi ai trattamenti per scopi di marketing, a quelli che si basano sul "legittimo interesse" del titolare o che sono necessari per eseguire compiti di interesse pubblico. In questi ultimi due casi, i trattamenti potrebbero proseguire ugualmente se vi sono "motivi legittimi cogenti" per farlo.

I diritti nuovi sono anche quelli che potrebbero essere più onerosi da soddisfare. Il "diritto all'oblio", in realtà, corrisponde al diritto alla cancellazione che esisteva anche prima. Il Regolamento, codificando le decisioni della Corte di giustizia, lo presenta però in una veste nuova legata al fenomeno dei social network e dei motori di ricerca. In particolare, se chi tratta i dati li ha resi pubblici deve informare gli altri titolari dei trattamenti della richiesta di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. C'è poi il "diritto di limitazione", in pratica è come se l'interessato chiedesse di "congelare" i dati che lo riguardano, ad esempio perché ha chiesto che i dati siano corretti e occorre tempo per verificare l'esattezza delle informazioni. A quel punto, chi li tratta li potrà usare solo per fini specifici – come difendersi in giudizio – sino a che la limitazione non sia venuta meno. Infine, il Regolamento introduce il "diritto alla portabilità", che evoca la portabilità delle numerazioni che è da tempo applicata nella telefonia. A certe condizioni, l'interessato può chiedere che il titolare gli ritrasmetta i suoi dati o li trasmetta a un altro titolare, in un formato "strutturato" di uso comune. Nei casi più semplici, il diritto potrebbe riguardare dati anagrafici, di pagamento ecc. Le prime interpretazioni ne prefigurano un uso più esteso, ad esempio per gli indirizzari di posta elettronica o le cronologie internet trattati dai fornitori di servizi web.

Garantire i diritti degli interessati vuole dire anche organizzarsi per farlo. Il titolare deve anzitutto informare gli interessati dei diritti di cui dispongono, deve avere un canale elettronico per ricevere le richieste ed essere in grado di rispondere di regola entro un mese. I diritti, per una volta, sono gratis. Solo per le richieste infondate ed eccessive, perché ad esempio ripetitive, è possibile chiedere un contributo spese all'interessato.

AGF

Marketing. L'interessato può sempre opporsi ai trattamenti per scopi pubblicitari

TRA VECCHI E NUOVI DIRITTI DELL'INTERESSATO

Diritto di accesso
Si usa per chiedere la conferma che ci siano trattamenti dei propri dati personali, quali siano i dati, le finalità del trattamento, i tempi di conservazione. L'interessato può chiedere anche una copia dei dati: la prima è gratuita, per le successive può essere chiesto un contributo spese

Diritto di rettifica
Si usa per far correggere o integrare i propri dati quando siano trattati in modo inesatto o incompleto

Diritto di opposizione
Si usa per bloccare i trattamenti per finalità di marketing. I dati possono essere conservati e trattati ancora, ma non più per la finalità di marketing. Si può usare anche per i trattamenti basati su un "legittimo interesse" del titolare o sull'esercizio di funzioni di pubblico interesse, sempre che vi siano motivi legittimi per proseguirli

Diritto alla cancellazione o di oblio
Si usa per far cancellare i dati trattati illecitamente o quelli per cui non vi sia più una ragione legittima di conservazione, ad esempio perché l'interessato revoca il consenso che in precedenza aveva rilasciato. Se i dati sono stati resi pubblici, ad esempio su internet in un motore di ricerca, il titolare deve informare tutti gli altri titolari che stanno trattando i dati della richiesta di cancellare link, copie, riproduzioni. La cancellazione non è possibile se i dati sono trattati per esercitare la libertà di espressione o informazione (es., organi di stampa), per obblighi legali, per archiviazioni o ricerche storico-scientifiche, per difendersi in giudizio

Diritto di limitazione
Si usa per "congelare" i trattamenti garantendo che nel frattempo i dati siano conservati

Diritto di portabilità
Si usa per farsi ritrasmettere dati propri o per farli trasmettere ad altri titolari. Il formato di trasmissione deve essere "strutturato", deve cioè seguire una schema di archiviazione che ne consenta l'elaborazione, e di uso comune. Il diritto si esercita per i dati forniti dall'interessato e trattati in modo automatizzato in base al consenso o per l'esecuzione di un contratto con l'interessato

LE INDICAZIONI DEL REGOLAMENTO 2016/679

ARTICOLO | 16
Diritto di rettifica

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

ARTICOLO | 17
Diritto alla cancellazione («diritto all'oblio»)

1. 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 senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.
2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.
3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Pronti per la privacy?
LE NOVITÀ IN DIECI DOMANDE

5 | Ho designato le figure-chiave di responsabile e incaricati?

Le mansioni dall'organigramma aziendale agli incarichi a società terze

di **Luigi Fruscione** e **Benedetto Santacroce**

Titolare, responsabile, incaricato e Dpo: sono queste le figure che possono comporre l'organigramma privacy delle aziende. In particolare, qualora il titolare ritenga di dover nominare un responsabile del trattamento dati occorre che questi lo designi attraverso un contratto (o altro atto giuridico conforme al diritto nazionale) con cui si vadano a disciplinare tassativamente le tematiche riportate al paragrafo 3 dell'articolo 28 del Gdpr. Tra queste, ad esempio, che il responsabile garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza; garantisca il titolare per il rispetto delle misure relative alla sicurezza del trattamento (articolo 32), alla valutazione d'impatto (articolo 35) e alla comunicazione all'interessato di una violazione dei dati personali (articolo 34).

L'atto che lega il responsabile al titolare del trattamento deve obbligatoriamente far riferimento ai seguenti aspetti: la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Occorre segnalare che qualora il responsabile designato intenda nominare, a sua volta, un sub-responsabile avrà bisogno di una autorizzazione scritta, specifica o generale, del titolare del trattamento; qualora si ottenga un'autorizzazione scritta generale, il responsabile del trattamento avrà l'onere di informare il titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare la possibilità di opporsi.

In caso di nomina di un sub-responsabile occorre che il responsabile originario gli imponga, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati gravanti su di lui.

Sul punto l'Autorità Garante ha rilevato che «i titolari del trattamento dovrebbero verificare che i contratti o altri atti giuridici che attualmente disciplinano i rapporti con i rispettivi responsabili siano conformi a quanto previsto, in particolare, dall'articolo 28, paragrafo 3, del Gdpr. Dovranno essere apportate le necessarie integrazioni o modifiche, in particolare qualora si intendano designare sub-responsabili».

Figura particolarmente importante nell'organigramma privacy è quella che nell'ancora vigente Codice privacy è denominata «incaricato al trattamento dati» che nel Gdpr viene qualificata quale «persona autorizzata al trattamento dei dati personali» permanendo nella sostanza una identità di ruoli e modalità di nomina.

Sul punto la stessa Autorità Garante ha stabilito che l'organizzazione degli incaricati può permanere immutata.

I manager della cybersicurezza nelle aziende italiane non finanziarie

Dati in percentuale

	Risorse interne	Dentro il gruppo	Fuori dal gruppo	Interni + outsourcing	No cybersecurity	Non sa/ Non risponde
Area geografica						
Nord-ovest	35,2	5,0	27,2	29,1	0,7	2,8
Nord-est	30,0	6,9	28,3	31,1	1,9	1,8
Centro	42,8	6,1	22,9	22,7	2,2	3,2
Sud e isole	46,8	4,1	24,1	20,1	2,0	3,0
Numero dipendenti						
20 - 49	35,4	4,6	30,6	24,5	1,7	3,1
50 - 199	39,6	7,6	19,7	30,2	1,5	1,4
200 - 499	46,6	5,4	7,8	37,7	–	2,5
Più di 500	42,9	10,4	5,1	36,9	0,1	4,7

Fonte: Banca d'Italia, Occasional papers febbraio 2017

I PROFILI DEL RESPONSABILE E DEGLI INCARICATI DEL TRATTAMENTO DATI

Il Responsabile del trattamento dati

- Il responsabile del trattamento dati è una figura facoltativa
- Si ricorre alla nomina di un responsabile qualora un trattamento debba essere effettuato per conto del titolare da parte di soggetti terzi
- Il contratto o altro atto giuridico stipulato tra titolare e responsabile ha la forma scritta e può essere redatto anche in formato elettronico
- Il responsabile ha obblighi propri derivanti dal Gdpr distinti da quelli del titolare
- Il responsabile deve garantire al titolare la predisposizione di misure tecniche e organizzative adeguate a consentire il rispetto sia delle istruzioni impartite dal titolare medesimo che, in via generale, delle disposizioni contenute nel regolamento
- In caso di nomina di un sub-responsabile occorre l'autorizzazione del titolare
- Qualora un responsabile del trattamento violi il regolamento determinando le finalità e i mezzi del trattamento è da considerarsi un titolare del trattamento

Gli incaricati del trattamento dati

- L'autorità Garante ha precisato che «in tema di misure tecniche e organizzative di sicurezza si ritiene che titolari e responsabili del trattamento possano mantenere in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante»

LE INDICAZIONI DEL REGOLAMENTO 2016/679

ARTICOLO | 28
(PARAGRAFI DA 1 A 3)
Responsabile del trattamento

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

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:
a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste ai sensi dell'articolo 32;
d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
h) e metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Pronti per la privacy?
LE NOVITÀ IN DIECI DOMANDE

6 | Devo nominare il «Dpo» e con quali responsabilità?

Attività e ambito quali criteri per l'obbligo del«Data protection Officer»

di **Luigi Fruscione**
Benedetto Santacroce

Attività principale e larga scala: su questi parametri si basa l'obbligo di nomina del Dpo (Data Protection Officer o Rpd, responsabile della protezione dei dati, nella versione italiana del Regolamento) per i soggetti privati da parte del titolare del trattamento, come indicano le lettere b) e c) nel primo paragrafo dell'articolo 37 del Gdpr.

Qual è il perimetro del concetto di «attività principale» del titolare? In base al Considerando n.97 vi rientrano «le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria». A integrazione dello scarno dettato normativo il Gruppo di lavoro Articolo 29 (documento WP 243 rev. 01 del 5 aprile 2017) precisa che l'espressione «attività principali» «non va interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte dal titolare del trattamento o dal responsabile del trattamento» (si veda la scheda).

Per il concetto di «larga scala», invece, il Considerando 91 stabilisce che tali sono quelle attività «che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato».

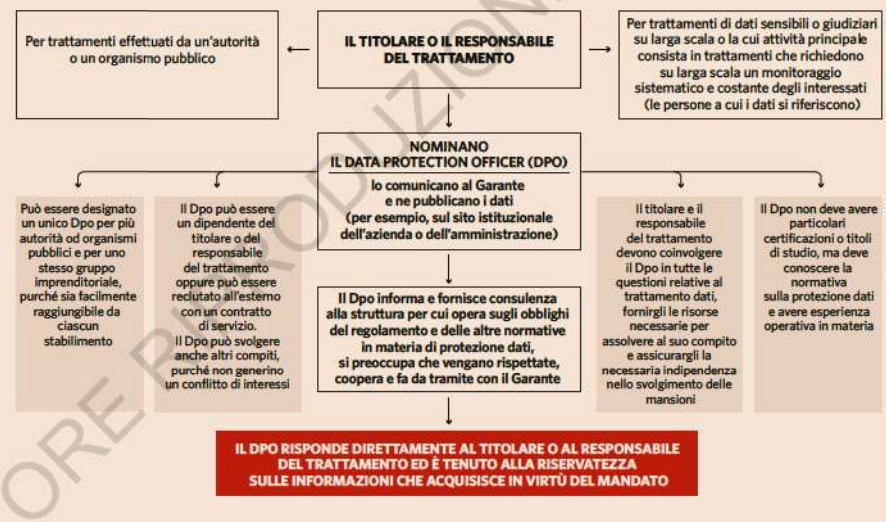
Anche qui, a integrazione della normativa, il Comitato individua dei parametri al fine di stabilire se un trattamento sia effettuato su larga scala, ad esempio: il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento.

Inquadrati i requisiti applicabili ad entrambi i casi di nomina del Dpo previsti alle lettere b) e c) dell'articolo 37 esaminiamo l'ulteriore requisito previsto dalla lettera b): il «monitoraggio regolare sistematico» degli interessati. L'aggettivo «regolare» può essere inteso, secondo il Comitato, nelle seguenti accezioni: che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito; ricorrente o ripetuto a intervalli costanti; che avviene in modo costante o a intervalli periodici.

L'aggettivo «sistematico», invece, può intendersi: che avviene per sistema; predeterminato, organizzato o metodico; svolto nell'ambito di una strategia.

La seconda ipotesi di obbligo di nomina del Dpo – lettera c) dell'articolo 37 del Gdpr – riguarda i casi in cui le attività principali del titolare del trattamento consistano in trattamenti su larga scala dei dati particolari (gli ex sensibili) o dei dati giudiziari previsti dall'articolo 10 del Gdpr; in tal caso, richiamati i criteri di «attività principale» e «larga scala», la disposizione non si presta particolari dubbi interpretativi essendo necessario verificare solo se il trattamento attiene a dati particolari.

Il battesimo e i compiti del «Data protection officer»



COME VANNO INTERPRETATI I REQUISITI PER LA NOMINA DEL «DPO»

Un esempio di «attività principale»

- Un'impresa di sicurezza privata incaricata della sorveglianza di più centri commerciali e aree pubbliche. L'attività principale dell'impresa consiste nella sorveglianza, e questa, a sua volta, è legata in modo inscindibile al trattamento di dati personali. Ne consegue che anche l'impresa in oggetto deve nominare un DPO

Esempi di «larga scala»

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

Esempi di «monitoraggio regolare e sistematico»

- Curare il funzionamento di una rete di telecomunicazioni
- La prestazione di servizi di telecomunicazioni
- Il reindirizzamento di messaggi di posta elettronica
- Attività di marketing basate sull'analisi dei dati raccolti

LE INDICAZIONI DEL REGOLAMENTO 2016/679

ARTICOLO | 37

Designazione del responsabile della protezione dei dati

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

2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.

3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.

5. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.

6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Pronti per la privacy?
LE NOVITÀ IN DIECI DOMANDE

7 | Sono tenuto a effettuare la valutazione di impatto?

Per decidere sull'obbligatorietà vanno identificati correttamente i gradi di rischio

di **Alessandro Curioni**

La valutazione di impatto è obbligatoria quando il trattamento presenta un «rischio elevato» e la questione che tipicamente affligge i titolari è comprendere in quali circostanze si è vincolati a svolgerla.

In realtà, se l'organizzazione ha correttamente interpretato i temi posti dalla protezione fin dalla progettazione e per impostazione predefinita saprà precisamente quali sono i trattamenti ad alto rischio. Quindi la valutazione d'impatto sulla protezione dei dati deriva da una presa d'atto di quanto emerso da un'attività svolta in precedenza. Questo fermo restando che, in alcuni casi, lo stesso Regolamento la richiede. Si tratta di situazioni in cui si effettua una valutazione continua e complessiva di determinate attività dell'interessato, oppure quando si svolgono attività su larga scala di sorveglianza o trattamento di categorie particolari di dati.

In generale il tema appare ostico, tanto da indurre il legislatore a prevedere che il titolare consulti il Dpo sulla materia. Un ulteriore aiuto dovrebbe arrivare dalle autorità di controllo, alle quali il Regolamento richiede di stabilire quali trattamenti siano soggetti alla valutazione ed eventualmente quelli che possano essere esclusi. La norma, infine, segnala come eventuali codici di condotta redatti dalle associazioni di categoria e approvati dall'autorità di controllo potrebbero fornire indicazioni in materia e la previsione di raccogliere il parere degli interessati, per esempio tramite le associazioni dei consumatori, che potrebbe dare utili elementi per meglio definire le casistiche.

Tuttavia, considerando la rapida evoluzione delle tecnologie - basta pensare all'Internet delle cose e ai Big data - la possibilità che tali indicazioni diventino prima o poi esaustive è remota e ancora una volta riemerge il tema dell'accountability per il titolare, al quale vengono rimesse le decisioni finali anche su questa materia e l'onere di dimostrare la correttezza delle sue scelte.

Quell'attività di analisi e valutazione del rischio, da svolgere in ossequio alla protezione dei dati fin dalla progettazione, è di certo il punto di partenza per comprendere se e quali trattamenti richiedono l'approfondimento di una valutazione d'impatto. Questo porta a pensare che nell'ambito del Regolamento la protezione dei dati fin dalla progettazione e la valutazione d'impatto possano collassare in un'unica attività completamente integrata. Le implicazioni sono significative perché i reali adempimenti sarebbero all'interno della protezione fin dalla progettazione, mentre la valutazione d'impatto finirebbe per essere una specifica formalizzazione per formulare un'eventuale richiesta di consultazione preventiva all'autorità di controllo. La vera domanda diventa non tanto se effettuarla o meno, ma se vale la pena rischiare la non conformità per non formalizzare un'attività già svolta.

I passi per strutturare il sistema

La progettazione iniziale e la valutazione d'impatto (Dpia)

REQUISITO	PRINCIPI DI PRIVACY BY DESIGN E DI PRIVACY BY DEFAULT	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI
Ambito di applicabilità	Progettazione o sviluppo di ogni nuovo trattamento di dati personali o di sostanziale modifica di trattamenti esistenti	Trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli individui
Analisi dei rischi	Concertazione interna tra responsabile progetto, data protection officer e responsabili dei dipartimenti dell'azienda per analisi dei rischi in materia di privacy e identificazione delle misure per proteggere i dati e garantire che il trattamento sia ridotto al minimo	Descrizione sistematica dei trattamenti e delle loro finalità; valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; valutazione dei rischi per i diritti e le libertà degli interessati; indicazione delle misure per affrontare i rischi
Adozione delle misure concordate	Implementazione delle misure organizzative e tecniche volte a garantire il rispetto degli obblighi dettati dal regolamento privacy europeo	Implementazione dei correttivi identificati a seguito della valutazione d'impatto (Dpia) ed eventuale consultazione con il Garante

TUTTE LE TAPPE DELLA VALUTAZIONE DI IMPATTO

I contenuti
- I contenuti della valutazione d'impatto sostanzialmente sono analoghi a quelli una normale attività di gestione del rischio. Essi richiedono di descrivere nel dettaglio:
- l'oggetto dell'analisi (trattamento e sue finalità);
- la valutazione vera e propria del rischio spesso mettendo in relazione elementi come le caratteristiche di sicurezza del bene (integrità, disponibilità e riservatezza) e l'evento che può comprometterle (minaccia);
- la descrizione delle contromisure che si intendono mettere a presidio

Chi deve occuparsene
- La valutazione d'impatto non è un'attività in capo al Dpo, che si deve limitare a fornire consulenza e a sorvegliarne l'esecuzione

Le valutazioni preliminari
- Nel valutare l'opportunità di una consultazione preventiva, è bene tenere presente che esistono delle autorizzazioni generali predisposte dall'autorità di controllo, per esempio relative ai trattamenti di dati inerenti i contratti di lavoro, per i quali potrebbe non essere necessaria, questo dipendentemente dalle tecnologie utilizzate

L'esecuzione
- Per svolgere correttamente la valutazione è necessario calcolare sia il rischio assoluto (in assenza di qualunque contromisura) sia quello residuo
- L'obbligo di consultazione preventiva, infatti, scatta qualora il trattamento presenti un rischio elevato in assenza delle misure adottate dal titolare

Le linee guida
- Il Gruppo Articolo 29 ha prodotto delle linee guida in materia che possono fornire alcune indicazioni per individuare quali sono i trattamenti che presentano un rischio elevato

Il «rischio elevato»
- In generale, la valutazione d'impatto deve essere eseguita anche sui trattamenti già in essere laddove si rilevi il rischio elevato, poiché il Regolamento prevede che i suoi risultati siano periodicamente riesaminati

LE INDICAZIONI DEL REGOLAMENTO 2016/679

ARTICOLO | 35
(*PARAGRAFI DA 1 A 6*)
Valutazione d'impatto sulla protezione dei dati

1. 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, il titolare del trattamento effettua, 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.

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

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:
a) 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) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.

5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

Pronti per la privacy?
LE NOVITÀ IN DIECI DOMANDE

8 | Ho predisposto le adeguate misure di sicurezza?

Standard Iso e codici di condotta possono aiutare nella messa a punto delle tutele

di **Alessandro Curioni**

Il contenuto dell'articolo 32 è "centrale" perché parlare di sicurezza del dato nel contesto di una norma che ha per oggetto la protezione dei dati significa prendere in considerazione la ragione stessa dell'esistenza della norma. Adempiere a questa previsione significa rispondere al suo dettato.

Il vero problema è rappresentato dall'interpretazione del concetto di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

In primo luogo, si deve tenere presente come esso ricalca quanto già affermato nell'articolo 25, che tratta della protezione dei dati fin dalla progettazione. Il legislatore, poi, suggerisce una serie di indicazioni che ritiene utili per raggiungere l'obiettivo tra i quali la pseudonimizzazione e la cifratura dei dati personali, aggiungendo temi più generali come la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento e quella di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

Di fronte a questo approccio è facile restare spiazzati se non si ha una certa dimestichezza con tematiche di analisi e gestione del rischio. Tuttavia una ciambella di salvataggio arriva quando nel paragrafo dell'articolo 32 si legge come l'adesione a un codice di condotta o a un meccanismo di certificazione può essere utilizzata come elemento per dimostrare la conformità. Esistono, infatti, un certo numero di *best practice* in materia di sicurezza che possono fungere da guida per rispondere alle richieste del Regolamento.

GLI STANDARD

In particolare, la Iso ha sviluppato la serie 27000 che costituisce ormai il riferimento internazionale. I due standard verso i quali rivolgere l'attenzione sono:

- la Iso/Iec 27001 Information security management systems - Requirements
- la Iso/Iec 27002 - Code of practice for information security controls.

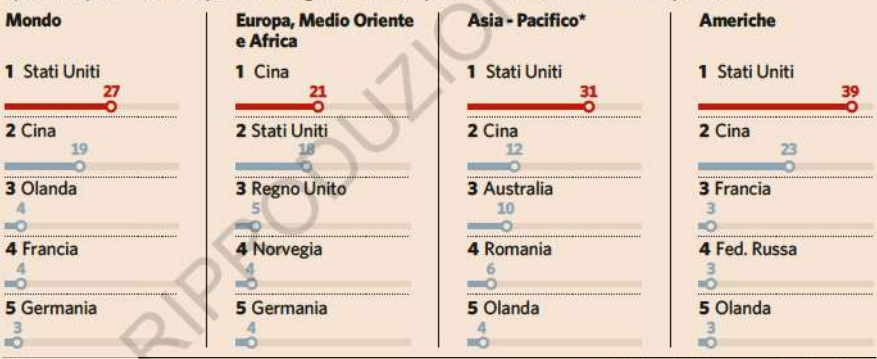
La prima appartiene alla categoria delle norme per la quali è possibile sottoporsi a un percorso di verifica con un ente e al termine ottenere la relativa certificazione. Per intendersi è lo stesso iter attraverso il quale si ottiene la Iso 9001.

La seconda, la 27002, funziona come una guida per meglio comprendere i requisiti espressi dalla 27001.

Utilizzare questi standard come riferimento è un buon punto di partenza, proprio per il costante richiamo del Regolamento a delle certificazioni. La stessa Iso, infatti, ha annunciato la prossima pubblicazione di una nuova norma certificante, la Iso/IEC 27552 - Enhancement to Iso/Iec 27001 for privacy management, e ha già pubblicato la Iso/Iec 29151:2017 - Code of practice for personally identifiable information protection. Senza dubbio si tratta della candidatura più importante al richiamato meccanismo di certificazione.

Cybersicurezza, la geografia degli attacchi

I primi cinque Paesi da cui provenivano gli attacchi compiuti nel 2017 nelle varie aree. In percentuale



(*) Escluso Giappone

FONTE: «Global threat intelligence report 2018» di Ntt Security

LE ATTIVITÀ VANNO CONSIDERATE DAL PUNTO DI VISTA DEGLI INTERESSATI

L'adeguatezza
L'adeguatezza può essere dimostrata soltanto se la sicurezza è gestita come un processo coerente, strutturato e periodicamente verificato. Questo implica che le attività ad essa connesse, come l'analisi dei rischi, siano ricorsive

L'approccio
L'approccio alla sicurezza deve essere basato sull'analisi e la valutazione dei rischi, in modo da riuscire a dimostrare che le misure di adottate non sono "casuali"

La prospettiva
Nel caso del Regolamento il rischio da valutare non è quello per l'organizzazione, ma per l'interessato. Si richiede, quindi un cambio di prospettiva

Cos'è il rischio
Il rischio è normalmente il risultato di una combinazione di elementi. L'evento esterno (minaccia) che sfruttando una condizione particolare (vulnerabilità) compromette il bene (asset)

Per chi ha il Registro
Nell'effettuare un'analisi dei rischi nel contesto del Regolamento l'asset potrebbe essere rappresentato da ognuna delle attività di trattamento che sono censite nell'apposito Registro

Per chi non ha il Registro
Per le organizzazioni che non hanno l'obbligo del Registro delle attività di trattamento potrebbe essere utile concentrarsi sui sistemi e i processi attraverso cui i dati sono elaborati

Gli standard/1
La Iso/Iec 27001 contiene un elenco di controlli (114) che possono essere utilizzati per mappare le proprie attività di sicurezza e quindi dargli un senso di organicità e di coerenza. Utile per rispondere al requisito dell'accountability richiesto dalla norma

Gli standard/2
La Iso/Iec 27002 è importante per comprendere "praticamente" cosa implicano i controlli della 27001 che ai non addetti a lavori possono sembrare piuttosto vaghi

Vantaggio competitivo
Va considerato che una certificazione approvata può essere un vantaggio competitivo, soprattutto per quelle aziende i cui servizi implicano trattamenti di dati su vasta scala o appartenenti a categorie particolari. Per esempio società di paghe contributi, recupero crediti, sorveglianza eccetera

LE INDICAZIONI DEL REGOLAMENTO 2016/679

ARTICOLO | 32
Sicurezza del trattamento

1. 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 mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

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

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. 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.

Pronti per la privacy?
LE NOVITÀ IN DIECI DOMANDE

9 | In caso di violazione dei dati, so come comportarmi?

Un «data breach» può originare sia dall'esterno che dall'interno dell'impresa

di **Alessandro Curioni**

Spesso le organizzazioni non hanno ben chiaro cosa sia un data breach e nel loro immaginario si riduce alla divulgazione di dati, come quelle subite da Yahoo! Nel 2012 e nel 2013. In realtà il Regolamento offre una definizione più ampia descrivendolo come la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Un incauto utente che modifica erroneamente un database o un malware che crittografa una cartella di rete diventano entrambe potenziali violazioni dei dati personali che, secondo le previsioni dell'articolo 33, il titolare deve notificare.

La domanda è molto semplice: come si può strutturare un processo di gestione degli incidenti in modo da essere ragionevolmente conformi ai requisiti della norma? La questione risulta talmente spinosa che il Gruppo di lavoro dell'Articolo 29 (Article 29 Data Protection Working Party, quello che diventerà il comitato europeo delle Autorità Garanti) ha prodotto delle linee guida in materia che forniscono materia di riflessione.

In primo luogo, viene evidenziato che il ciclo di vita di un incidente può essere molto lungo. L'esempio è legato a una violazione di riservatezza di dati crittografati, un caso in cui non dovrebbe essere necessaria la comunicazione. Tuttavia, se in futuro il titolare dovesse perdere il controllo della chiave di cifratura oppure l'algoritmo si rivelasse vulnerabile, ecco come il tema della notifica per quello stesso incidente tornerebbe d'attualità.

Un secondo aspetto è legato alla distinzione tra «rischio» e «alto rischio». La lettura della norma evidenzia come nel primo caso il *data breach* deve essere portato alla conoscenza dell'autorità garante, nel secondo l'informazione dovrebbe essere estesa agli interessati coinvolti. Questo determina la necessità di effettuare per ogni incidente un'analisi d'impatto per categorizzarlo correttamente.

Proprio il tema della classificazione della gravità dell'incidente viene affrontato piuttosto in profondità e sono evidenziati quelli che dovrebbero essere i criteri di cui tenere conto nella valutazione.

La caratteristica della sicurezza del dato a essere violata (integrità, riservatezza o disponibilità), la natura e la quantità di dati coinvolta, la facilità con cui possono essere identificati gli interessati, la gravità delle conseguenze che potrebbero subire, il numero delle vittime e le particolari caratteristiche del titolare.

Quest'ultimo aspetto è determinante, poiché a parità di tutti gli altri indicatori potrebbe diventare il vero discrimine e della valutazione. Per esempio, la violazione della riservatezza delle anagrafiche di centomila abbonati a un giornale avrà un rischio per i soggetti coinvolti nettamente inferiore a quello che deriverebbe se la stessa base dati fosse stata detenuta da un ospedale.

Quando c'è una violazione dei dati personali

Perdita di un *device* non cifrato	Anche un semplice smarrimento di un telefonino aziendale può costituire una valida ragione di un *Data breach* nel caso in cui contenga Dati personali e non sia stato opportunamente cifrato
Un *device* viene infettato da un *Ransomware*	Un *ransomware* è un tipo di *malware* che limita l'accesso del dispositvo che infetta, richiedendo un riscatto (*ransom* in Inglese) da pagare per rimuove la limitazione
Perdita di disponibilità del Dato personale	Un esempio potenziale di perdita di disponibilità del dato è quando un Dato personale viene inviato per errore a un terzo non autorizzato
Cosa fare in caso di *Data Breach*	
Perdita di un *device* non cifrato	Il Titolare del Trattamento deve notificare non appena viene a conoscenza che il *device* è stato smarrito. Il fatto che il Titolare non sia a conoscenza che vi sia stato o meno accesso al *device* da soggetto non autorizzato non rileva
Il Titolare del Trattamento viene reso edotto di attacco informatico	Il Titolare del Trattamento deve tempestivamente verificare se sono stati violati dei Dati personali e una volta verificato deve procedere alla verifica nelle 72 ore
Un "cybercriminale" contatta la società con una richiesta di riscatto dopo averla attaccata	Il Titolare del Trattamento deve notificare al Garante da subito tale violazione

LE PRECAUZIONI E IL PERCORSO DA SEGUIRE

La procedura
- Una violazione dei dati personali dovrebbe rientrare nelle attività di una crisi, quindi va prevista una rapida procedura di escalation gerarchica verso i vertici aziendali

Per l'efficienza
- Nelle organizzazioni che hanno un piano di continuità operativa, potrebbe essere utile inserire in questo contesto anche la gestione dei data breach, rendendo più efficienti le attività di crisi

Funzioni da coinvolgere
- Considerando la varietà di violazioni possibili, è indispensabile prevedere che diverse funzioni aziendali possano essere coinvolte nella gestione dell'incidente. Per esempio, se i dati colpiti sono quelli dei dipendenti, servirà il contributo delle direzione risorse umane

Gli standard
- Esiste uno standard che offre una base di partenza, si tratta del Iso/Iec 27035 dedicato all'«Information security incident management» che fornisce una traccia per costruire i contenuti di un'appropriata notifica all'autorità e le successive attività da svolgere

La valutazione d'impatto
- Un'osservazione importante è legata al tema della valutazione d'impatto sulla protezione dei dati. In quel frangente si parla di «rischio elevato» al fine di identificare i trattamenti da sottoporre a questo tipo di verifica
- La logica conseguenza è quella di prevedere che la notifica agli interessati sia probabile qualora il trattamento sia stato oggetto di questa attività.

L'annotazione
- Il Regolamento richiede che sia tenuta traccia di tutti gli incidenti che hanno convolto dati personali, anche di quelli per i quali non è necessaria la notifica
- Si tratta di un documento vero e proprio che deve essere costantemente aggiornato

Autorità e interessati
- Spesso la valutazione della gravità di una violazione richiede tempo, quindi prima di decidere se e come comunicarla agli interessati, può essere utile il confronto con l'autorità

Segmentare le attività
- Un elemento chiave per rispettare le 72 ore richieste dalla norma è la capacità di un'organizzazione di segmentare le diverse attività.
- Per esempio: comprendere la portata di un furto di dati potrebbe richiedere lunghe analisi, quindi la notifica dovrebbe avvenire quando le investigazioni sono ancora in corso

Il ruolo del Dpo
- Il coinvolgimento del Dpo, se designato, sin dai primi sospetti di data breach è essenziale perché agirà da punto di contatto privilegiato per l'autorità di controllo

LE INDICAZIONI DEL REGOLAMENTO 2016/679

ARTICOLO | 33
Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 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.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo

Pronti per la privacy?
LE NOVITÀ IN DIECI DOMANDE

10 | Inadempienze o mancanze: quali sono le sanzioni?

Una traccia europea che gli Stati potranno integrare

di **Giuliano Fonderico**

Uno degli aspetti più innovativi del Regolamento, e più delicato per chi dovrà rispettarlo, sono le sanzioni. La direttiva del 1995 rimetteva agli Stati membri di stabilire le sanzioni per le violazioni delle norme sulla riservatezza. Nel Codice della riservatezza del 2003 le sanzioni erano per lo più definite per illeciti puntuali – ad esempio omissioni d'informativa, trattamenti senza consenso ecc. – e, di regola, avevano singolarmente un valore non elevatissimo che cominciava a crescere solo quando fossero coinvolte intere banche dati o nel caso di violazione degli obblighi sul «data breach», la violazione dei dati personali. Vi erano poi alcune sanzioni penali.

Il Regolamento contiene un proprio sistema di sanzioni pecuniarie che sono applicabili sia a illeciti puntuali sia a disfunzioni organizzative considerate nel loro insieme, come ad esempio, un modello aziendale non rispettoso dei principi generali sul trattamento o difetti di gestione dei rapporti con i responsabili del trattamento.

Questo evita alcune incongruenze del sistema precedente, che operava più per cumulo di sanzioni minute (come una sanzione per ogni caso di omessa informativa). Al contempo, nel nuovo sistema le sanzioni possono arrivare a somme ben più elevate perché, coerentemente all'impostazione di fondo, sono calcolate sul fatturato complessivo dell'impresa e, a certe condizioni, su quello del gruppo di appartenenza, secondo la stessa logica del diritto antitrust Ue. I massimali variano dal 2% al 4% del fatturato mondiale, in relazione alle norme violate.

Non finisce qui. Il Regolamento demanda ai diritti nazionali di definire le «altre sanzioni», per le violazioni che esso già non sottopone a sanzioni pecuniarie, e di stabilire se le sanzioni possano essere applicate anche ai soggetti pubblici. La legge di delegazione europea n. 163/2017 contiene al riguardo un criterio generico e l'ultima bozza di decreto delegato prevede sia altre sanzioni amministrative, dichiarate applicabile anche ai soggetti pubblici, sia sanzioni penali.

Nella primissima fase di applicazione del regolamento, potrebbe esserci un approccio più "morbido" nell'applicazione delle sanzioni, almeno nei casi frutto di semplice negligenza. A mano che la consapevolezza degli obblighi derivanti dal regolamento si diffonda, le sanzioni potrebbero farsi più gravi.

Occorrerà poi mettere in conto il risarcimento del danno da azioni private. Quasi ogni violazione alle norme del Regolamento potrebbe tradursi in illeciti risarcibili. In più, il Regolamento ammette espressamente, rimettendo però la scelta alle norme nazionali, azioni portate avanti mediante enti esponenziali (articoli 81 e 82), che potrebbero di fatto divenire di tipo collettivo. Se la normazione italiana dovesse esercitare questa facoltà, il rischio di azioni per danni potrebbe crescere di molto.

ADOBESTOCK

L'IMPIANTO SANZIONATORIO GUARDA AL FATTURATO

Le condotte sanzionate
- La violazione di obblighi strumentali, per garantire trattamenti rispettosi dei diritti degli interessati (ad esempio le violazioni in tema di privacy by design/default, sui rapporti con i responsabili dei trattamenti, sul registro dei trattamenti, su sicurezza e data breach, sulla valutazione d'impatto)
- La violazione di obblighi finali, di tutela diretta degli interessati (ad esempio la violazione dei principi sul trattamento, sul consenso o sulle altre condizioni di liceità dei trattamenti, e dei diritti degli interessati all'accesso, all'oblio, alla portabilità)

I massimali
- Dal 2 al 4% del fatturato mondiale, secondo le norme violate

La base di calcolo
- Si fa riferimento all'impresa come entità economica, come nel diritto antitrust Ue; il fatturato da considerare potrebbe essere quello del gruppo societario di appartenenza

La quantificazione
- Varierà secondo il dolo, la colpa, la recidiva, la natura, la gravità e la durata della violazione, il numero di interessati coinvolti, i danni prodotti, il «ravvedimento operoso»
- Potrà essere ridotta se le misure di sicurezza predisposte dal titolare sono già elevate o se il titolare aderisce ai codici di condotta e ai sistemi di certificazione

Il «cumulo giuridico»
- Quando ci sono più violazioni relative al medesimo trattamento o a trattamenti collegati, la sanzione complessiva non supera l'importo previsto per la violazione più grave

Le altre sanzioni nel diritto nazionale
- Sanzioni pecuniarie
- Sanzioni penali

Le azioni di risarcimento del danno
- Il titolare e il responsabile dei trattamenti sono esenti da responsabilità solo se dimostrano che il danno «non gli è in alcun modo imputabile»

LE INDICAZIONI DEL REGOLAMENTO 2016/679

ARTICOLO | 83 (PARAGRAFI 1, 4, 5 E 6)

Condizioni generali per infliggere sanzioni amministrative pecuniarie

1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.(...)

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:
a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;
b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;
c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:
a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;
b) i diritti degli interessati a norma degli articoli da 12 a 22;
c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;
d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;
e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

6. In conformità del paragrafo 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. (...)

Pronti per la privacy?
LE INIZIATIVE DEL GRUPPO 24 ORE

Sul sito del «Sole» gli strumenti per accompagnare il debutto

Dossier dedicati, notizie e analisi, fascicoli a disposizione dei navigatori

Un dossier con notizie, analisi e approfondimenti, la sezione «Tecnologia», gli ebook sulla cybersicurezza e la privacy: è molto ampia e in continuo aggiornamento l'offerta digitale del Sole 24 Ore in avvicinamento alle nuove regole europee sulla tutela dei dati personali, da domani al debutto. E naturalmente i navigatori hanno sempre la possibilità di effettuare ricerche mirate, utilizzando la finestra che compare in alto a sinistra nella home page del sito. Vediamo in dettaglio alcuni percorsi a disposizione.

IL DOSSIER
«Privacy, come mettersi in regola con il Gdpr» è il titolo del dossier ospitato nella sezione Tecnologia del sito. Il dossier raccoglie articoli, contributi video, grafici e infodata. I richiami contenuti all'interno dei signoli articoli consentono di approfondire la ricerca. L'indirizzo completo del dossier è www.ilsole24ore.com/dossier/tecnologie/2018/diritto-privacy/index.shtml

LA CYBERSICUREZZA
Digitando www.ilsole24.com/ebook è possibile invece accedere o acquistare i fascicoli dedicati alla cybersicurezza, allegati al quotidiano nei mesi di marzo e aprile e ora disponibili in versione digitale. In particolare, i numeri 5 e 6 della collana (che si estendeva anche in alcune puntate del programma «2024») sono stati dedicati al Regolamento Ue e alle sue ricadute all'interno delle imprese. La collana comprende anche il dossier «Cybersicurezza», con articoli, analisi e contributi video dedicati al tema.

LA SEZIONE «TECNOLOGIA»
Ogni giorno viene infine alimentata la sezione Tecnologia (raggiungibile dal link in home page, sotto la testata «Il Sole 24 Ore»), che riprende, aggiorna e amplia quanto viene pubblicato ogni domenica sulle pagine di «Nòva24»

DALL'8 GIUGNO MASTER A ROMA PER I «DPO»

Partirà l'8 giugno a Roma il Master part time dedicato alle ricadute del Gdpr. «**Il Data Protection Officer e il nuovo Regolamento Europeo sulla privacy**». In questa settima edizione, che si concluderà il 28 luglio, il Master si concentrerà sulla fase di prima applicazione del Regolamento Ue: con la definitiva applicazione del General Data Protection Regulation, infatti, le imprese e le pubbliche amministrazioni devono obbligatoriamente dotarsi di una nuova figura organizzativa, il responsabile della protezione dei dati personali (Data Protection Officer).

Il Master organizzato da 24 ORE Business School offre un quadro della normativa in materia di trattamento dei dati personali, ne analizza gli impatti applicativi, organizzativi e gestionali e approfondisce il nuovo ruolo del responsabile della protezione dei dati personali.
Il master è a numero chiuso e a frequenza obbligatoria, si sviluppa su 7 weekend per 84 ore complessive di formazione. Sono disponibili borse di studio per studenti meritevoli.

bs.ilsole24ore.com/master-data-protection
Il sito per le informazioni sul Master

IL MANUALE PER GESTIRE IL «GDPR»

Un manuale per il debutto e la prima applicazione del Gdpr, utile a chi si occupa della protezione dei dati in azienda, a chi vuole comprendere nel dettaglio la materia, a chi vuole prepararsi per un ruolo nella gestione e nella tutela dei dati personali. Il «**Manuale per il trattamento dei dati personali**», edito da Il Sole 24 Ore, è uno strumento con molteplici obiettivi: è una guida per chiunque sia chiamato a svolgere la funzione di Dpo (Responsabile della Protezione dei Dati) o voglia formarsi per questo ruolo; è un vademecum per studenti che vogliono comprendere contenuti e impatto del Regolamento Ue 679/2016; è un aggiornamento essenziale per chi è già un esperto deputato alla compliance in tema di privacy e dati personali; è un corso di formazione per i responsabili della sicurezza informatica che vogliono ampliare l'attività alla tutela giuridica dei dati personali; è un perfezionamento per consulenti giuristi che vogliono specializzarsi nella protezione dei dati personali. In vendita su:

www.shopping24.ilsole24ore.com

IL FUTURO IN ONDA A «2024»

L'economia dei dati, la cybersicurezza, la nostra vita digitale ogni settimana vanno in onda a «2024», la trasmissione di Radio24 condotta da Enrico Pagliarini, **ogni venerdì alle 22 e ogni domenica alle 13**.
«2024» affronta tutte le ricadute della tecnologia: nel nostro ufficio e in cucina, nell'automobile e a scuola, nel modo di viaggiare e lavorare, di ascoltare la musica e di telefonare. E sono le tecnologie a determinare le grandi variabili su cui si basa la vita: gli approvvigionamenti di energia, la cura della salute, la coltivazione del cibo. La velocità con cui le innovazioni si sviluppano è esponenziale, inquietante e affascinante. E «2024» si espande, allarga gli orizzonti, per parlare del presente e guardare al futuro. Tre le grandi aree di contenuti: i nuovi prodotti hi-tech di largo consumo, il mondo dei video giochi, le novità tecnologiche che stanno cambiando il mondo.

www.radio24.it
Il sito per i contenuti del programma e per i podcast

IL ROADSHOW FA TAPPA A TORINO

La digitalizzazione pervade la vita quotidiana, da casa al lavoro. E non solo per via dei computer e dei telefoni. Le automobili e le telecamere per il controllo degli accessi nelle case, i robot in linea di montaggio, le piattaforme che governano la micrologistica cittadina e i satelliti che tengono monitorato il clima in ogni istante, le macchine per le analisi mediche e i mezzi di comunicazione: i chip e il software sono ovunque e sono connessi alla rete. Alimentano le opportunità e i rischi. Favoriscono lo sviluppo di servizi ai cittadini e suggeriscono nuovi modelli di business per le imprese, attraverso la gestione dei processi di approvvigionamento, produzione e vendita tramite le tecnologie di rete. Ma offrono il fianco a sempre nuove e pericolose azioni di cyber crime, in grado di violare il "sistema impresa" e minarne drasticamente la capacità competitiva.
Nòva 24 - Il Sole 24 Ore, in collaborazione con il Cini, organizza per lunedì 8 ottobre 2018 a Torino la quinta tappa del roadshow **«Cyber Security. L'evoluzione della sicurezza nell'ecosistema 4.0»**, un percorso iniziato nel 2017, rivolto ad aziende e professionisti che ha l'obiettivo di diffondere la conoscenza sul tema della sicurezza informatica e sulle ricadute del fenomeno sul sistema imprenditoriale, attraverso un confronto tra università e istituzioni, mondo delle aziende e associazioni di categoria. Per informazioni scrivere a:
cybersecurity@ilsole24ore.com

I FOCUS DEL SOLE 24 ORE
Settimanale - Registrazione Tribunale di Milano n. 170 del 07-06-2013
DIRETTORE RESPONSABILE
Guido Gentili
COORDINAMENTO
Jean Marie Del Bo, Mauro Meazza
CAPOREDATTORE
Maria Carla De Cesari
INSERTO A CURA DI
Antonello Cherchi, Andrea Marini, Mauro Meazza