CONFINDUSTRIA RADIO TELEVISIONI

GDPR

Il nuovo regolamento privacy

Istruzioni per l'uso

CRTV LAB

LUISS

Il volume nasce dalla collaborazione tra Confindustria Radio Televisioni (CRTV) e @LawLAB, il laboratorio per lo svolgimento e la promozione di attività di ricerca, studio, analisi e consulenza, coordinato dai Professori Maurizio Mensi e Pietro Falletta della LUISS, in materia di diritto digitale.

Collana di Studi e Ricerche sul settore radiotv a cura di CRTV LAB

Stampato Aprile 2018 - **Confindustria Radio Televisioni**

Progetto grafico: Andrea Veronese

Impaginazione e stampa: ELLECI di Boselli A. e L. snc

Immagine di copertina 123RF ID58199746

CONFINDUSTRIA RADIO TELEVISIONI

CRTV LAB

LUISS

Presentazione

Il Regolamento generale sul trattamento dei dati personali (GDPR) è un cantiere aperto che impone una rinnovata consapevolezza dei diritti della persona nel settore dei media globali in un'ottica "sia aziendalistica, sia volta a creare valore nella società" come efficacemente chiosato nel capitolo introduttivo.

Con la nuova normativa, che diventa direttamente applicabile nel nostro ordinamento, le aziende (e tutti gli organismi, anche pubblici) sono infatti responsabilizzate e chiamate ad approntare un sistema di tutele e garanzie per il trattamento dei dati personali in risposta alla sensibilità e il valore che essi assumono nell'economia digitale. L'ottica più responsabilizzante comporta adempimenti e oneri aggiuntivi per gli operatori che trattano i dati, ma al tempo stesso mira a rendere il sistema più flessibile rispetto al precedente. Una sfida per le aziende, e in particolare per quelle del settore radiotelevisivo, che aggiungono ai nuovi adempimenti richiesti - fra cui per esempio progettazione del sistema di tutele, valutazioni di impatto, modulistica per i database di clienti, fornitori, utenti, dipendenti - trattamenti di dati particolarmente sensibili. Ci riferiamo per esempio ad adempimenti specifici per i quali la tutela della *privacy* deve essere bilanciata con valori fondanti per il pluralismo e la democrazia, come nel caso dell'esercizio dell'attività giornalistica; o alle problematiche legate alla gestione del consenso nell'esposizione mediatica, o al diritto all'oblio.

Le imprese dei media televisivi e i giornalisti hanno la consapevolezza che, nell'epoca della Rete aperta, un quadro condiviso di regole a tutela dei diritti dell'uomo e delle libertà individuali e collettive quali il diritto dei cittadini a ricevere una informazione professionale onesta, leale e indipendente sia la sfida centrale e qualificante su cui investire. Questi sono i pilastri di un'economia e una società digitale veramente inclusiva e rispettosa dei valori fondanti delle libertà civili. Le vicende recenti di utilizzo anomalo e scorretto dei dati nel mondo della comunicazione *social* dimostrano la stringente attualità di una assunzione di responsabilità concorrenti di soggetti diversi per evitare derive pericolose per gli individui, o per la creazione di posizioni dominanti e pervasive.

Questo manuale di CRTV, in fruttuosa sinergia con LUISS, vuol essere uno strumento utile per gli operatori del settore. Si tratta di un lavoro in parte inedito, anche se per chi opera nel campo dell'informazione professionale la tutela della *privacy* è già connaturato nell'esercizio dell'attività (giornalisti) e del business (editori): per le imprese del nostro settore, è fondamentale estendere il rapporto di fiducia instaurato con i cittadini, (ascoltatori, utenti, clienti) anche al sistema della rete.

Un cantiere importante, si diceva in apertura, cruciale per ribadire il ruolo centrale e responsabile degli editori radiotelevisivi; ma al tempo stesso un cantiere che richiede, mattone dopo mattone, la costruzione di un sistema di tutela solido per gli utenti da un lato, ed equo e sostenibile per le aziende del settore, dall'altro.

Un cantiere aperto che CRTV non mancherà di continuare a presidiare: con il lavoro dei professionisti delle imprese coinvolte, nonché con strumenti a sostegno delle aziende del settore radiotelevisivo che rappresenta - piccole e medie imprese, nazionali e locali, pubbliche e private - e con interlocuzioni istituzionali. Nell'ottica di sistema che contraddistingue e ispira l'attività associativa.

Francesco Angelo Siddi
Presidente Confindustria Radio Televisioni

Introduzione

Il prossimo 25 maggio diverrà integralmente applicabile il Regolamento UE 2016/679 (GDPR) del Parlamento europeo e del Consiglio del 27 aprile 2016.

Il regolamento innova profondamente la normativa sul tema della privacy in risposta all'accelerazione imposta dalla digitalizzazione dell'economia e al peso e al valore che la raccolta e l'elaborazione delle informazioni personali hanno assunto in essa.

Un aggiornamento atteso, imprescindibile per normare attività che si basano sulla raccolta e la profilazione dei dati, ma non pienamente concluso dalla nuova norma, come viene sottolineato nella "prefazione tecnica" ad opera di Giuseppe Colaiacomo.

L'intervento europeo sposta il focus della tutela sulla responsabilizzazione delle aziende e degli organismi che devono operare un trattamento di dati per svolgere le proprie attività, con una serie di obblighi e oneri aggiuntivi importanti.

Sono molti i nuovi adempimenti richiesti ai titolari e responsabili del trattamento dei dati: dall'implementazione di una organizzazione delle attività di raccolta e trattamento *privacy friendly* (e ciò sin dalla progettazione iniziale del sistema nell'ambito del quale viene trattato il dato, quello che il regolamento definisce *privacy by design*); alla nomina di nuove figure (il *data protection officer*, DPO); alla predisposizione della documentazione di supporto (valutazione di

impatto, registro dei trattamenti, etc.); al recepimento di nuove tutele per il diritto all'oblio o alla portabilità dei dati che hanno assunto rinnovata importanza. E questo solo per fare qualche esempio.

Sono molte, a poche settimane dal 25 maggio, anche le aree "grigie" della nuova normativa sulle quali dovranno (e potranno) esprimersi gli Stati Membri con disposizioni specifiche e l'Autorità Garante con suoi provvedimenti.

Il nostro settore è ampiamente coinvolto dalle novità, con peculiarità che riguardano, tra l'altro, l'attività di informazione giornalistica. Peculiarità che richiedono attenta considerazione.

Non a caso il progetto di CRTV per accompagnare i propri associati – grandi, piccole e medie imprese del settore radiotelevisivo – nella delicata fase di adeguamento alla nuova normativa si è strutturato in un *work in progress*, che ha previsto innanzitutto la creazione di un gruppo di lavoro interno, coordinato dal nostro ufficio Normativa e Regolamentare. Il gruppo coinvolge le figure professionali che si occupano del tema nelle aziende associate, ed è mirato a condividere criticità, strumenti interpretativi e organizzativi, e a delineare interventi coordinati di settore.

L'Associazione collabora poi con le strutture centrali di Confindustria che si interfacciano con il Garante sui temi più controversi.

Soprattutto, CRTV lavorerà all'elaborazione di un codice di condotta di settore, che è compito precipuo delle Associazioni di categoria, e alla redazione di formulari standard per alcuni adempimenti, quali la nomina del DPO e le informative.

Per questa pubblicazione, primo tassello del progetto, ci siamo avvalsi della collaborazione del @LawLab della Luiss, struttura di ricerca specializzata sul tema, per elaborare delle linee guida generali sul regolamento, che costituiscono la parte centrale di questa pubblicazione (testo e schede sintetiche per una consultazione rapida). Sotto forma di schede è anche la parte relativa all'attuazione del GDPR nell'ordinamento italiano a cura dell'ufficio Normativa e

Regolamentare di CRTV. Nel primo capitolo, a cura dell'Avv. Giuseppe Colaiacomo, si iniziano a delineare alcune problematiche specifiche di settore, a normativa e strumenti interpretativi attuali. CRTV si attrezzerà anche per fornire aggiornamenti, approfondimenti e strumenti di lavoro attraverso il sito associativo.

Da ultimo, rivolgo un particolare ringraziamento ai Professori Maurizio Mensi e Pietro Falletta, responsabili e coordinatori di @LawLab; ai componenti del Gruppo di Lavoro istituito in CRTV: Francesco Canini, Laura Canu, Claudia Cignitti, Barnaba Costalonga, Gianluca De Matteis Tortora, Marcello Dolores, Anna Maria Genzano, Pietro Grignani, Diego Facchini, Raffaella Forchino, Arianna Fusco, Ottavia Marotta, Tiziana Mennuti, Valentina Alessia Pezzuto, Roberta Quintavalle, Sara Rinaldi, Germana Scalco, Gilda Serafini, Claudia Venturini, Cecilia Vicedomini; ai colleghi Elena Cappuccio, Annamaria La Cesa e Andrea Veronese.

Rosario Alfredo Donato
Direttore Generale Confindustria Radio Televisioni

Indice

Il GDPR e la sua attuazione per il settore RadioTv
Avv. Giuseppe Colaiacomo

Linee guida sul Regolamento
Prof. Pietro Falletta (@Lawlab, LUISS)

Schede tecniche

Roadmap del GDPR nell'ordinamento Italiano

Avv. Annamaria La Cesa (Normativa e Regolamentare, CRTV)

Contenuti del Regolamento

Dott.ssa Michela Tresca, Dott.ssa Giulia Di Carlo (@Lawlab, LUISS)

Il GDPR e la sua attuazione per il settore RadioTv

Avv. Giuseppe Colaiacomo

Il GDPR e il tempo presente

Il Regolamento generale sul trattamento dei dati personali (Regolamento Europeo in materia di protezione dei dati personali 2016/679, approvato in data 14 aprile 2016 dal Parlamento Europeo e pubblicato sulla Gazzetta Ufficiale Europea del 4 maggio 2016, in breve GDPR [1]) è per più versi un evento singolare nel panorama della normativa europea.

Esso interrompe una linea di intervento sulla materia del trattamento dei dati che era caratterizzata fino ad ora dall'adozione di direttive (a

[1] Si è preferito, in questo scritto, adottare l'acronimo inglese, che sta per "*General Data Protection Regulation*", in quanto pare ormai più diffuso, nella prassi, del corrispondente italiano RGPD.

partire dalla direttiva "madre" 95/46/CE), quindi da norme destinate ad essere recepite nelle legislazioni nazionali con appositi provvedimenti legislativi.

L'uso dello strumento "regolamento" (norma destinata a produrre per sé sola tutti gli effetti giuridici che promanano dalle sue disposizioni) sta a segnare un nuovo e peculiare approccio dell'Unione al tema dei dati.

Il contesto di riferimento di tale nuova impostazione sta nella *roadmap* dell'agenda digitale europea [2], quell'ambizioso progetto che dovrà portare la legislazione degli Stati membri nel nuovo mondo digitale, dove peraltro l'economia già si trova da anni.

Una simile transizione non è socialmente sostenibile se non si stabilisce un quadro di tutela dei dati personali. Quadro che non può essere costituito dalle disposizioni della direttiva 95/46/CE, emanata quando meno dell'uno percento della popolazione europea era su internet.

I dati erano allora, ancora per buona parte, una questione cartacea, fatta di moduli, formulari, firme a inchiostro. Eravamo, insomma, in un mondo non troppo dissimile (sotto l'aspetto dell'archiviazione e della catalogazione) da quello di fine '800.

L'avvento della disciplina del trattamento dei dati è stato, per molti, una sorpresa, e ha smosso non poca polvere da quegli archivi, che si formavano e organizzavano ancora nel modo che Gogol descriveva.

……..

[2] Lanciata nel maggio 2010, l'Agenda Digitale per l'Europa contiene 101 azioni, raggruppate intorno a sette aree prioritarie intese a promuovere le condizioni per creare crescita e occupazione in Europa: nuovo e stabile quadro normativo per quanto riguarda la banda larga; nuove infrastrutture per i servizi pubblici digitali attraverso prestiti per collegare l'Europa; avviare una grande coalizione per le competenze digitali e per l'occupazione; proporre una strategia per la sicurezza digitale dell'UE; aggiornare il framework normativo dell'UE sul copyright; accelerare il cloud computing attraverso il potere d'acquisto del settore pubblico; lanciare una nuova strategia industriale sull'elettronica.

Ma la risposta è stata ancora una volta simile a quegli stessi archivi: lenta, burocratica e, inesorabilmente, cartacea.

La rivoluzione digitale, in pochi anni, ha spazzato via molti fogli di carta, ma ha messo al centro del suo sviluppo le informazioni che una volta erano ristrette, a fatica, su tali fogli. I dati sono diventati merce preziosa, e sono stati raccolti in quantità enorme.

Dove sia la maggior parte di tale merce è noto: la custodiscono i grandi operatori OTT come Google, Facebook, etc.

Questi ultimi godono del fatto di aver consentito agli utenti l'accesso a una serie amplissima di servizi: ciò, in apparenza, gratuitamente. In realtà, l'utente paga con i propri dati personali.

Anche tale meccanismo è noto: a chi accede a determinati siti viene fornito senza contropartita ciò che normalmente paga (musica, video, etc.). Nel frattempo però i server raccolgono i dati che generosamente (e a volte inconsapevolmente) vengono immessi nella rete.

L'evoluzione tecnologica si muove dunque, apparentemente, in una direzione che nega – nel vorticoso superamento della carta in favore delle infinite possibilità del dato informatico – la stessa possibilità di consentire alle persone fisiche un effettivo controllo sulle informazioni della loro vita, che vengono in tal modo "reificate" [3] e separate dal contesto dell'identità personale dell'individuo.

Il regolamento rappresenta il tentativo di fornire un'ossatura alla tutela normativa di tali informazioni: esso sancisce principi inderogabili, ma si affida in parte non piccola alla responsabilità delle imprese, alle forme di autoregolamentazione attraverso i codici di condotta e all'intervento dei legislatori nazionali.

……..

[3] Di reificazione ha parlato espressamente S. Rodotà in Tecnologie e diritti, Bologna, 1995, p. 27.

Le voci critiche hanno rilevato che tale tentativo spinge sempre di più verso la denunciata "reificazione" del dato, allontanando il tema della tutela di quest'ultimo dalla più generale tutela dei diritti della personalità. Si è osservato che l'art. 1 della Direttiva 95/46/CE, stabiliva che gli Stati membri devono garantire "la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali", mentre l'art. 1, par. 2, del Regolamento, pone tra i suoi vari obiettivi la necessità di "proteggere i diritti e le libertà fondamentali delle persone e in particolare il loro diritto alla protezione dei dati personali". Si può notare che è venuto meno l'espresso riferimento al diritto alla riservatezza, strettamente connesso alla costruzione dell'identità personale, il che porterebbe a pensare che vi sia "una cesura netta tra la protezione dei dati e il rispetto della vita privata" e che "la dimensione economica dei dati sia destinata a prendere il sopravvento". [4]

Come si è detto, però, questa dimensione economica è ormai immanente al sistema, e crescerà sempre di più nei prossimi anni.

Il dato, anche se relativo alla persona umana, è divenuto una risorsa imprenditoriale e come tale lo considera il Regolamento, che in quest'ottica sposta l'attenzione dai diritti dell'interessato (e la preoccupazione, talvolta formalistica, per il suo consenso) alla responsabilità dei soggetti che raccolgono e utilizzano le informazioni.

Il tema della responsabilità torna continuamente nel testo: significativo è il considerando 74: "È opportuno stabilire la responsabilità generale

……..

[4] Così, A. Thiene, Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo regolamento europeo, NLCC 2017, pp. 412 s., secondo il quale "Per apprezzare pienamente la portata delle nuove regole è, invece, necessario non solo mantenere ferma la lettura dualistica dei diritti della personalità, concepiti, lo sappiamo, come la somma di due distinte situazioni giuridiche soggettive, ma, ora più che mai, recuperare l'originaria radice personalistica in cui la dimensione ideale e quella patrimoniale, quella dell'essere e quella dell'avere, si intersecano e si confondono. Non pare dunque condivisibile l'impostazione che distingue nettamente i profili patrimoniali e aspetti personali del diritto sui propri dati".

del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche".

Le "misure adeguate ed efficaci" rappresentano la base e il contenuto della *privacy by design* e *by default* [5]: l'impresa deve essere organizzata e strutturata per gestire i dati di cui viene in possesso, secondo modelli e sistemi rigorosamente preparati per essere adeguati ai rischi concretamente presenti nell'attività svolta ed efficacemente attuati. In proposito occorrerà riflettere sull'integrazione tra le nuove misure imposte dal regolamento e i modelli di organizzazione e controllo per la prevenzione dei reati, ex D.Lgs. 231/2001 sulla responsabilità amministrativa da reato degli enti.

Altro aspetto rilevante da considerare è legato al tipo di strutture tecnologiche da implementare nelle organizzazioni aziendali. A seguito dell'entrata in vigore del GDPR sono comparsi sul mercato numerosi *software* (soluzioni *cloud*, *software as a service*, servizi e applicazioni) creati per garantire la conformità dei sistemi alle norme

[5] Il concetto di *privacy by design* si fonda su un "approccio proattivo alla tutela dei dati personali nel contesto di prodotti e servizi informatici, basato sull'inserimento degli strumenti posti a tutela della *privacy* in tali prodotti sin dall'inizio della loro progettazione, partendo da quelli che sono principi universali di tutela della *privacy*". Invece, "la *privacy by default* implica l'utilizzo di determinate impostazioni in automatico, con una scelta predisposta da parte di chi costruisce il sistema informatico, sempre fatta salva la possibilità di cambiamento da parte dell'utente dell'opzione prescelta" (cfr. per queste definizioni e per una puntuale ricostruzione di tali concetti A. Principato, Verso nuovi approcci alla tutela della privacy: *privacy by design* e *privacy by default settings*, in Contratto e Impresa Europa 2015, pp. 197 ss.

sul trattamento dei dati [6]: la scelta di uno piuttosto che un altro è ancora una volta oggetto di una decisione che l'impresa dovrà assumere e adeguatamente motivare.

L'adozione di entrambi i tipi di strumenti, organizzativi e tecnologici, costituirà la base, insieme alla valutazione dei rischi, per la *compliance* delle imprese rispetto al GDPR.

Si può dire che ormai la *privacy by design* e *by default* rappresenta a pieno titolo uno dei contenuti della Responsabilità Sociale delle Imprese (RSI) o *Corporate Social Responsibility* (CSR) ossia "l'integrazione su base volontaria, da parte delle imprese, delle preoccupazioni sociali ed ambientali nelle loro operazioni commerciali e nei loro rapporti con le parti interessate" secondo la definizione Libro Verde della Commissione Europea del luglio 2001 [7].

In quest'ottica, sia aziendalistica che rivolta a creare valore nella società (ottica più responsabilizzante certo, ma anche più flessibile rispetto al precedente sistema) dovrà indirizzarsi la riorganizzazione delle imprese.

……..

[6] Come si legge in F. Fabbri, Data protection, mercato globale software a 120 miliardi di dollari nel 2022, in https://www.key4biz.it/data-protection-mercato-globale-software-120-miliardi-dollari-nel-2022/213981/, "Un nuovo studio ReportsnReports ha stimato il valore del settore attorno ai 57 miliardi di dollari a fine 2017. Grazie ad un tasso di crescita annuo (Carg 2017-2022) atteso al 16%, il mercato delle soluzioni per la *data protection* dovrebbe sfiorare i 120 miliardi di dollari nel 2022. I *verticals* che registreranno i maggiori incrementi di spesa, secondo il Report, sono i segmenti della *disaster recovery*, della data *loss prevention* e della data backup and recovery, seguiti comunque da data archiving and *ediscovery, encryption, tokenization* e *identity* and *access management*".

[7] Comunicazione della Commissione europea al Parlamento europeo e al Consiglio COM (2011) 681 definitivo.

Il GDPR e l'ordinamento italiano

Si è detto, nel precedente paragrafo, che cifra caratterizzante dell'intervento europeo è proprio la scelta di adottare un regolamento anziché una direttiva.

Il regolamento "ha portata generale. Esso è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri" (art. 288 TFUE), senza la necessità di atti di recepimento nei singoli Stati nazionali. Si è osservato che "Non si tratta più di uno strumento di armonizzazione, ma invece di un mezzo di uniformazione del diritto per gli Stati europei, eliminando così in radice quelle piccole differenze che rendono difficile realizzare compiutamente un mercato unico" [8].

Eppure, molte disposizioni del GDPR appaiono, sotto questo profilo "ibride", perché demandano agli Stati membri (in alcuni casi, vedremo, anche a strumenti di autoregolamentazione) la disciplina di aspetti non secondari.

Di seguito si indicheranno alcuni esempi.

In linea generale, il considerando 13 del GDPR invita le istituzioni, organi e agenzie dell'Unione, gli Stati membri e le Autorità di controllo a considerare le esigenze specifiche delle micro, piccole e medie imprese.

Vi sono poi casi in cui il Regolamento consente agli Stati membri di mantenere o introdurre disposizioni specifiche, dirette a precisare alcuni punti della disciplina per adattarli alle singole realtà nazionali [9].

……..

[8] G. Finocchiaro, Introduzione al regolamento europeo sulla protezione dei dati, NLCC 2017, p. 6.

[9] F. Pizzetti, Guida alla lettura del Regolamento 2016/679, I, Napoli 2016, p. 21, parla a tale proposito di legislazione o regolazione statale interstiziale, in quanto destinata a intervenire sugli "interstizi" lasciati aperti dalle norme regolamentari che, nel definire tutti gli elementi essenziali a regolare aspetti specifici, consentono agli Stati di introdurre precisazioni o requisiti ulteriori.

Un esempio che può essere molto rilevante per il settore dell'informazione e dell'intrattenimento è rappresentato dall'art. 8, par. 1 del Regolamento, che, per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, dispone che il consenso al trattamento di dati personali sia da considerare lecito ove il minore stesso abbia almeno 16 anni (in caso contrario occorre il consenso di chi esercita la responsabilità genitoriale). Gli Stati membri, però, possono stabilire per legge un'età più bassa a tali fini, purché non inferiore ai 13 anni.

Infine, alcuni passaggi fondamentali della disciplina sono interamente demandati agli Stati, come la determinazione delle sanzioni minime applicabili e, aspetto ancor più rilevante, la riorganizzazione delle Autorità garanti al fine di adeguarne i poteri e il funzionamento alle nuove norme del GDPR (cfr. in proposito l'art. 51 del Regolamento).

Orbene, a poca distanza dalla data fatidica del 25 maggio 2018, il legislatore italiano si è mosso con alcuni interventi.

In particolare, con l'art. 13 della Legge di delegazione europea 2017 (Legge 20 novembre 2017, n. 167), è stato demandato al Governo il compito di adottare i decreti legislativi per adeguare, entro 6 mesi dall'entrata in vigore della legge, il quadro normativo nazionale al GDPR.

Il ritardo con cui si è mossa l'Italia è evidente. Se il Governo dovesse sfruttare tutti i sei mesi concessigli dal Parlamento, il Decreto delegato potrebbe arrivare il 6 maggio 2018, quindi a ridosso della data di efficacia delle norme del GDPR.

D'altra parte, la stessa legge delega è piuttosto generica in merito al contenuto che dovrà avere l'intervento governativo. Esso dovrà abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali incompatibili con le disposizioni contenute nel Regolamento (precisazione inutile, dato che

prevarrebbero comunque le norme del GDPR, anche senza un intervento normativo nazionale); e modificare quelle non incompatibili, al fine di dare attuazione alle disposizioni non direttamente applicabili contenute nel Regolamento.

L'art. 13 citato impone inoltre al Governo di prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali e di adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle nuove disposizioni con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione.

Si tratta, come ben si vede, di delega amplissima e in gran parte rimessa ad una discrezionalità (per quanto "tecnica") del Governo.

Manca, e sarebbe stata opportuna, una previsione in merito a misure di mitigazione degli obblighi per il trattamento dei dati personali in relazione a imprese micro, piccole e medie.

A complicare il quadro è arrivata la legge di bilancio del 2018 (Legge 27 dicembre 2017, n. 205, G.U. n.302 del 29-12-2017) commi da 1020 a 1024.

Per quanto riguarda la posizione del Garante, tale legge ha previsto, ai commi 1020 e 1021, che esso debba assicurare "la tutela dei diritti fondamentali e delle libertà dei cittadini", e a tali fini debba, con proprio provvedimento da adottare entro due mesi dalla data di entrata in vigore della legge:

a) disciplinare le modalità attraverso le quali il Garante stesso monitora l'applicazione del Regolamento e vigila sulla sua applicazione;

b) disciplinare le modalità di verifica, anche attraverso l'acquisizione di informazioni dai titolari dei dati personali trattati per

via automatizzata o tramite tecnologie digitali, della presenza di adeguate infrastrutture per l'interoperabilità dei formati con cui i dati sono messi a disposizione dei soggetti interessati, sia ai fini della portabilità dei dati ai sensi dell'articolo 20 del Regolamento, sia ai fini dell'adeguamento tempestivo alle disposizioni del regolamento stesso;

c) predisporre un modello di informativa da compilare a cura dei titolari di dati personali che effettuano un trattamento fondato sull'interesse legittimo che prevede l'uso di nuove tecnologie o di strumenti automatizzati;

d) definire linee-guida o buone prassi in materia di trattamento dei dati personali fondato sull'interesse legittimo del titolare.

A breve, pertanto, dovrebbe arrivare un complesso provvedimento del Garante diretto a fornire un quadro applicativo per il GDPR. Resta da vedere quanto tempo, in concreto, occorrerà alle imprese per adeguarvisi (ricordando che la scadenza di maggio è alle porte).

Si può parlare quindi di un lento approccio al tema che implica, a cascata, un rallentamento dell'intero sistema in vista del raggiungimento dell'adeguamento alle nuove norme.

I punti critici attualmente privi di una disciplina di dettaglio sono molti, e a taluni abbiamo fatto cenno. Per limitarci ad alcuni esempi, si possono citare anche l'assenza di criteri certi sulla compilazione della valutazione di impatto *privacy*, svariati aspetti legati al consenso al trattamento dei dati, la mancanza di un format per il contratto tipo per la nomina del responsabile esterno del trattamento (per le attività in outsourcing).

La situazione è, come si vede, tuttora liquida e gravida di incertezza.

Lasciando ad altre, ormai numerose e ponderose, pubblicazioni l'esame dei problemi più generali posti dal nuovo Regolamento, ci si

concentrerà, nelle prossime pagine, su alcuni aspetti che ineriscono più direttamente al settore radiotelevisivo.

L'intervento del legislatore italiano sul tema dell'interesse legittimo

Il legislatore è già intervenuto in merito al trattamento dei dati fondato su di un "interesse legittimo", ai sensi del Considerando 47 del Regolamento.

Brevemente, ai sensi del GDPR, se il trattamento è basato sui legittimi interessi non occorre il consenso dell'interessato, purché non prevalgano gli interessi o i diritti e le libertà fondamentali (in special modo se questi è un minore) tenuto conto delle ragionevoli aspettative dello stesso in base alla relazione col titolare del trattamento (Considerando 47 del GDPR).

Occorre però informare l'interessato del fatto che i suoi dati sono trattati in base ai legittimi interessi. Sussiste l'interesse legittimo al trattamento se: a) il titolare ha necessità di elaborare il dato per fini propri o di terzi; b) gli interessi del titolare e quelli dell'interessato sono bilanciati; c) il trattamento delle informazioni è equo e rispetta i principi di protezione dei dati.

Il Regolamento esemplifica alcuni casi (per es., corrisponde a interesse legittimo, il trattamento dei dati in caso di esistenza di "una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento"), ma non c'è dubbio che sia il titolare a dover individuare il proprio "interesse" e bilanciarlo con i diritti coinvolti.

Una tale soluzione può sorprendere: in sostanza è chi tratta il dato a decidere, sotto la sua responsabilità, quanto la sua condotta è lecita e quanto gli interessi altrui possono essere compressi.

In realtà è l'intero GDPR a proporre una prospettiva rovesciata rispetto alla tradizione normativa: mentre in precedenza l'accento era sull'interessato e i suoi diritti, l'ottica è ora opposta, e il trattamento viene considerato piuttosto dalla parte dei doveri del "controller". [10]

A quest'ultimo spetta un'attenta valutazione al fine di verificare se i diritti dell'interessato possano prevalere sui legittimi interessi del titolare.

L'azienda dunque, prima ancora di iniziare il trattamento dei dati sulla base dei suoi legittimi interessi, deve effettuare tutte le valutazioni del caso e assicurarsi di essere in grado di documentare i passaggi di tali valutazioni.

Il legislatore italiano è intervenuto sulla materia con la richiamata legge di bilancio del 2018 (Legge 27 dicembre 2017, n. 205, G.U. n.302 del 29-12-2017) che, come si è visto, ha demandato al Garante di definire linee-guida o buone prassi in materia di trattamento dei dati personali fondata sull'interesse legittimo del titolare.

La norma ha inoltre previsto che i responsabili del trattamento dei dati che analizzano i dati personali mediante mezzi automatizzati o nuove tecnologie sulla base dei legittimi interessi debbano:

- inviare una notifica preventiva all'Autorità Garante per la protezione dei dati, allegando una nota informativa (secondo le indicazioni del Garante);

……..

[10] Sul tema F. Pizzetti, Privacy e il diritto europeo alla protezione dei dati personali, I, Torino 2016, p.154.

- attendere l'approvazione dell'Autorità, salvo che essa rimanga inerte per 15 giorni dall'invio del materiale: in tal caso si può iniziare il trattamento.

La norma è stata aspramente criticata, perché introduce una forma di notifica preventiva che non pare compatibile con l'impianto del regolamento. Inoltre, il concetto stesso di controllo preventivo pare in contrasto con il principio, prima accennato, per cui la responsabilità di determinare quale sia il trattamento lecito spetta in primo luogo a chi lo effettua.

L'unico caso di consultazione preventiva previsto nel Regolamento è infatti quello disciplinato nell'art. 36, per il quale "Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio".

Secondo il GDPR, dunque, se un'impresa ritiene di stare trattando dei dati secondo un interesse legittimo (ad esempio, in ossequio a doveri imposti da norme di legge) e, secondo la valutazione d'impatto che ha eseguito (e che può dimostrare documentalmente di aver eseguito) non emerge, anche senza misure adeguate, un elevato rischio, non ha bisogno di autorizzazioni preventive.

Il legislatore italiano, evidentemente, ha ritenuto che l'utilizzo di "mezzi automatizzati o nuove tecnologie" imponga invece il ricorso ad un *prior checking*.

Al di là della legittimità, in chiave di conformità alle norme europee, di tale scelta, essa non appare condivisibile. Le stesse espressioni "mezzi automatizzati o nuove tecnologie" sono irrimediabilmente vecchie: ogni mezzo di trattamento dei dati è automatizzato in qualche sua fase, e le "nuove tecnologie" sono difficilmente distinguibili dalle

vecchie, in un'epoca di rapidissimi cambiamenti. Senza contare che una tecnologia più avanzata è spesso più sicura per i fini perseguiti dal Regolamento.

Inoltre, ma il dato non pare secondario, il Garante potrebbe essere subissato di comunicazioni, in gran parte inutili.

Il GDPR e l'informazione giornalistica

L'informazione è per certi aspetti l'esatta controparte della tutela del dato personale.

Per tale ragione l'applicazione della disciplina della privacy all'attività giornalistica è assolutamente peculiare: i diritti di stampa e di informazione devono contemperarsi con quelli individuali alla tutela dei dati personali, e necessariamente questi ultimi finiscono, in molti casi, per subire un arretramento. Non si può informare senza trattare dati, né si può attendere, per tale trattamento, sempre il pieno consenso dell'interessato.

Condizione essenziale per l'esercizio del diritto / dovere di cronaca è infatti la possibilità di raccogliere, registrare, conservare e diffondere notizie che contengono dati, anche sensibili, su persone.

Per tale motivo, il legislatore ha introdotto delle deroghe ai consueti princìpi in materia di trattamento dei dati (cfr. art. 9 della direttiva 95/46/CE e artt. 136 sc. D.Lgs. 196/2003)

Il Garante ha precisato tali deroghe emanando il Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (cfr. Provvedimento del Garante del 29 luglio 1998, Gazzetta Ufficiale 3 agosto 1998, n. 179).

In sintesi:

1. il giornalista che raccoglie notizie deve rendere note la propria identità, la propria professione e le finalità della raccolta salvo che ciò comporti rischi per la sua incolumità o renda altrimenti impossibile l'esercizio della funzione informativa; non è obbligato a rendere l'informativa sul trattamento dei dati;

2. se i dati personali sono raccolti presso banche dati di uso redazionale, le imprese editoriali sono tenute a renderne nota l'esistenza al pubblico;

3. il giornalista può conservare i dati raccolti per tutto il tempo necessario al perseguimento delle finalità proprie della sua professione.

Nel raccogliere dati personali sensibili il giornalista garantisce il diritto all'informazione su fatti di interesse pubblico, nel rispetto dell'essenzialità dell'informazione, evitando riferimenti a congiunti o ad altri soggetti non interessati ai fatti.

La divulgazione di notizie di rilevante interesse pubblico o sociale non contrasta con il rispetto della sfera privata quando l'informazione, anche dettagliata, sia indispensabile in ragione dell'originalità del fatto o della relativa descrizione dei modi particolari in cui è avvenuto, nonché della qualificazione dei protagonisti.

Il quadro non sembra cambiato, nella sua sostanza, con l'entrata in vigore del Regolamento, che al considerando 153 così si esprime: "Il diritto degli Stati membri dovrebbe conciliare le norme che disciplinano la libertà di espressione e di informazione, comprese l'espressione giornalistica, accademica, artistica o letteraria, con il diritto alla protezione dei dati personali ai sensi del presente regolamento. Il trattamento dei dati personali effettuato unicamente a scopi giornalistici o di espressione accademica, artistica o letteraria dovrebbe essere soggetto a deroghe o esenzioni rispetto ad alcune disposizioni del presente regolamento, se necessario, per conciliare il

diritto alla protezione dei dati personali e il diritto alla libertà d'espressione e di informazione sancito nell'articolo 11 della Carta. Ciò dovrebbe applicarsi in particolare al trattamento dei dati personali nel settore audiovisivo, negli archivi stampa e nelle emeroteche".

All'art. 85 dello stesso GDPR si prevede che "Il diritto degli Stati membri concilia la protezione dei dati personali ai sensi del presente regolamento con il diritto alla libertà d'espressione e di informazione, incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria. Ai fini del trattamento effettuato a scopi giornalistici o di espressione accademica, artistica o letteraria, gli Stati membri prevedono esenzioni o deroghe rispetto ai capi II (principi), III (diritti dell'interessato), IV (titolare del trattamento e responsabile del trattamento), V (trasferimento di dati personali verso paesi terzi o organizzazioni internazionali), VI (autorità di controllo indipendenti), VII (cooperazione e coerenza) e IX (specifiche situazioni di trattamento dei dati) qualora siano necessarie per conciliare il diritto alla protezione dei dati personali e la libertà d'espressione e di informazione".

Come accade in altre parti del Regolamento, le possibilità per il legislatore nazionale di derogare alla disciplina generale sono amplissime, e si traducono in una sostanziale "delega" a regolare la materia secondo i princìpi della normativa nazionale, con il solo limite di dover notificare alla Commissione le norme adottate e le loro successive modifiche.

Si è visto che il Legislatore italiano non ha previsto, nei suoi scarni interventi, alcunché in merito al diritto di informazione e alla sua relazione con la tutela dei dati.

Se ne deve inferire che il quadro regolatorio è rimasto quello delineato dal D.lgs. 196/2003 e dalle norme deontologiche successivamente emanate, in base al quale l'attività giornalistica è una forma di trattamento dei dati, seppur caratterizzata da interesse pubblico.

In proposito la giurisprudenza ha affermato che "La divulgazione di un dato di interesse pubblico mediante dichiarazioni o comportamenti pubblici non è configurabile come una forma di consenso tacito al suo trattamento, in quanto l'interessato potrebbe anche essere contrario a che l'informazione da lui resa nota abbia una ulteriore e più ampia diffusione. La ratio della norma di cui all'art. 137, D. Lgs. n. 196 del 2003 (Codice della *Privacy*), può essere, dunque, colta nell'opportunità di dare prevalenza all'interesse pubblico all'informazione, seppure riguardante profili non essenziali rispetto alla vicenda o al personaggio di interesse pubblico cui si riferisce, quando le dichiarazioni o i comportamenti in pubblico dell'interessato abbiano già compromesso in misura significativa l'interesse alla riservatezza dei dati trattati. La deroga, pertanto, concerne l'essenzialità del dato trattato e non l'interesse pubblico, il quale va apprezzato autonomamente" (Cass. civ. Sez. I, 06/12/2013, n. 27381).

Tale pronuncia conferma che il trattamento dei dati per scopi di informazione non è, nel nostro ordinamento, qualcosa di ontologicamente diverso da ogni altro trattamento.

Il GDPR si fa portatore, però, di un'ottica per la quale la tutela del dato personale non è un diritto inderogabile, ma è destinato piuttosto a cedere di fronte agli interessi che siano ad esso sovraordinati.

Come si è osservato, il considerando 4 del Regolamento richiama la "funzione sociale" del dato. Se esso supera la sfera individuale riferita all'interessato, ed è strumentale al soddisfacimento di un ulteriore interesse, degno evidentemente di riconoscimento giuridico, l'assolutezza del contenuto del diritto può subire una limitazione. "La «funzione sociale» è quindi un limite alla pienezza del diritto alla protezione dei dati personali, connaturale alla sua essenza e alla sua dimensione di tutela, che richiede di contemperare l'interesse

individuale dell'interessato, le particolari esigenze dei titolari del trattamento e le possibili esigenze collettive". [11]

Peculiare dimostrazione di come opera, nel regolamento, questa tensione verso la funzione sociale, specialmente nel mondo dell'informazione, è la nuova disciplina del diritto all'oblio.

L'art. 17 del GDPR definisce quest'ultimo come l'interesse di un individuo a "ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo".

Si tratta quindi, in realtà, di un diritto alla cancellazione dei dati, che opera quanto: 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; c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1 (casi particolari) o ai sensi dell'articolo 21, paragrafo 2 (marketing); d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo legale; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.

Tale diritto, però, secondo l'art. 17, comma 3, non è opponibile dal suo titolare nel caso in cui il trattamento sia necessario, tra l'altro "per l'esercizio del diritto alla libertà di espressione e di informazione".

Ci troviamo di fronte, nuovamente, ad una clausola generale contenuta nel GDPR, e ad una sfida per gli interpreti.

Contemperare diversi interessi (nella specie, l'interesse di chi invoca l'oblio, e quello generale all'informazione) è tradizionalmente compito del legislatore, ma nel Regolamento l'asse del controllo e del

[11] Così A. Ricci, Sulla «funzione sociale» del diritto alla protezione dei dati personali, Contratto e impr. 2017, p. 586.

discrimine tra lecito e illecito si sposta sempre, l'abbiamo più volte rilevato, verso chi opera il trattamento.

Quando l'uno o l'altro interesse debba prevalere è difficile dirlo. È stato rilevato in proposito che "Principio di correttezza e principio di identità fungono da criteri di composizione del conflitto; criteri che, in quanto elastici, dinamici ed empirici, rimodulano nel tempo i contenuti e la forza assiologica degli interessi implicati, sicché un trattamento che risulta lecito in un dato momento storico, potrebbe non esserlo più in un momento successivo in cui è mutata l'identità dell'interessato" [12].

In questo momento successivo, vengono meno le ragioni stesse della libertà di pensiero e informazione, perché il contenuto veicolato non è più attuale, e quindi non più veritiero. A questo punto, l'interessato potrà utilmente richiedere di esercitare il suo diritto all'oblio.

È probabile che le imprese potenzialmente coinvolte da tali richieste si debbano dotare di strumenti idonei, quali i *software* di *Privacy Enhancing Technologies*, che sono in grado di cancellare automaticamente i dati personali decorso un certo lasso di tempo o a richiesta.

Il senso della responsabilità di cui abbiamo più volte parlato è infatti rappresentato sia dalla capacità di contemperare i diversi interessi al momento del trattamento, sia dalla capacità tecnologica di cancellare il dato, consentendo all'interessato di realizzare appieno il suo diritto all'oblio, ciò in ottemperanza agli obblighi generali di precauzione, di carattere tecnico e organizzativo, che sono previsti in capo al titolare. In particolare, ci si riferisce alle misure tecniche e organizzative adeguate per garantire, ed essere in grado di

[12] R. Senigaglia, Reg. ue 2016/679 e diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza nell'ordine della dignità personale, in NLCC 2017, p. 1035.

dimostrare, che il trattamento è "effettuato conformemente" al Regolamento.

Si spera che anche su questi punti, delicatissimi per il mondo dell'informazione, il Garante fornisca linee di condotta chiare e puntuali, in modo che le imprese possano orientare opportunamente i loro investimenti tecnologici.

Il codice di condotta

Gli aspetti fino ad ora esaminati hanno evidenziato più dubbi che certezze.

Il punto fondamentale della nuova disciplina, come già ripetuto più volte, è la responsabilità dell'impresa nel valutare: a) i rischi che i dati trattati corrono; b) l'adeguatezza della propria struttura a garantire il trattamento nel modo più consono alla tutela degli interessati; c) le misure occorrenti a tale tutela.

Il pericolo, per le imprese, di perdersi in questo complicato processo, è serio, per questo il GDPR ha previsto l'adozione di strumenti di indirizzo in chiave di autoregolamentazione, ossia i codici di condotta.

L'art. 40 del testo prevede: "Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese". Al secondo comma la norma prevedere che "Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici

di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente regolamento". [13]

I Codici di condotta potranno essere proposti dalle associazioni di categoria alle Autorità Garanti. Se approvati dalle Autorità Garanti nazionali (quando relativi a trattamenti di dati personali con portata nazionale), o dalla Commissione previo parere del Comitato Europeo dei Garanti (quando relativi a trattamenti che si svolgono in vari Stati europei), i Codici di condotta integreranno il GDPR con norme di dettaglio e semplificazioni, valide per le imprese aderenti. Il rispetto dei Codici determinerà una presunzione di conformità in caso di procedimento da parte del Garante.

Non si tratta di una novità assoluta del Regolamento, essendo tali codici già previsti nella direttiva madre, ma lo strumento acquista una nuova centralità, e ci avvicina al sistema statunitense.

L'articolo 28 del Regolamento e il considerando 81 prevedono infatti espressamente che l'adesione ad un codice di condotta, sia un elemento per dimostrare l'adempimento agli obblighi del titolare.

Tra i vantaggi, in termini di efficienza, vi è quello di evitare duplicazioni in termini di valutazioni del rischio. Ad esempio, un "controller" potrebbe, in base al codice, evitare di effettuare una verifica su determinati sistemi di "data processor" che sono già ritenuti sicuri dalla sua associazione di categoria [14].

Il punto più delicato è rappresentato dalle semplificazioni, che chi propone il codice dovrà proporre calibrando attentamente le norme in ragione delle caratteristiche delle imprese cui sono rivolte e del tipo di dati da trattare.

……..

[13] Cfr. R. Senigaglia, op. cit., p. 1056.
[14] Cfr. R. Heimes, Top 10 operational impacts of the GDPR. Part. 9 – Codes of Conduct and certifications, in https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-9-codes-of-conduct-and-certifications.

Si tratterà comunque di uno strumento atto a indirizzare l'azione delle imprese nell'ottica della privacy.

I codici etici rappresentano una espressione particolarmente forte dell'autoregolazione societaria [15], nonché lo strumento attraverso il quale l'impresa attesta la propria intenzione di adottare determinate strategie "socialmente responsabili" e conformi agli standard legislativi.

Senonché, i meccanismi necessari per l'approvazione, e quindi l'operatività dei codici di condotta, al pari di quelli per le certificazioni previste nel Regolamento, sono ancora privi di una disciplina.

Ciò avviene nonostante vi sia una notevole attenzione per questi temi nel nostro Paese, che conosce già strumenti di autoregolamentazione etica e certificazione ben funzionanti (si pensi al rating di legalità e al rating d'impresa). Non a caso l'Italia, nei tavoli di lavoro europei, ha proposto l'introduzione di un obbligo di certificazione privacy per poter accedere alla partecipazione di specifici bandi di gara.

Ad oggi si deve però registrare un fermo su questi temi e non risulta sia stato approvato alcun codice di condotta. Né esiste la possibilità di certificare la conformità di uno specifico trattamento, o di una intera organizzazione aziendale, al GDPR.

Il DPO, quando va nominato

In alcuni casi, il Regolamento impone al titolare e al responsabile la nomina di un *Data Protection Officer* (DPO) con vari compiti, che vanno dalla consulenza, alla vigilanza, al contatto con gli interessati e con il Garante.

[15] Sul punto cfr. C. Angelici, Responsabilità sociale dell'impresa, codici etici e autodisciplina, in Giur. comm., I, 2011, p. 168 ss.

Non si tratta di una figura nuova a livello europeo, ma di certo è peculiare per il diritto italiano.

Vi si trovano infatti, allo stesso tempo, caratteristiche proprie del collaboratore dell'impresa e del soggetto indipendente dalla stessa.

Il DPO deve essere legato al titolare o al responsabile del trattamento da un contratto (anche di lavoro subordinato), ma godere di indipendenza rispetto all'organizzazione aziendale.

Non pare di poter individuare nella nostra esperienza nazionale qualcosa di simile, a parte forse (ma con evidenti differenze) l'Organismo di Vigilanza previsto dalla normativa sulla responsabilità amministrativa degli enti (D.Lgs. 231/2001).

Neppure il Responsabile del Servizio di Prevenzione e Protezione previsto dal Testo unico per la sicurezza sul lavoro sembra avere le stesse garanzie di indipendenza del DPO.

È lecito chiedersi se la previsione di tali cautele non sia eccessiva.

Se lo sono sicuramente chiesto le Istituzioni europee, dato che la relativa norma del DGPR (art. 37) ha subìto più rimaneggiamenti di qualunque altra, prima della definitiva approvazione. In particolare le opzioni hanno oscillato tra la previsione di una generalizzata imposizione dell'obbligo di nominare il DPO, e soluzioni molto più blande [16].

Nella versione finale, evidentemente di compromesso, il Regolamento ha indicato tre casi di obbligatorietà:

……..

[16] Per una ricostruzione del dibattito e delle relative posizioni cfr. L. Moerel, GDPR conundrums: The data protection officer requirements, in https://iapp.org/news/a/gdpr-conundrums-the-data-protection-officer-requirement/

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;

c) oppure 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.

In questa sede pare ultroneo esaminare il caso sub a).

Il caso sub b) si riferisce, evidentemente e principalmente, a quelle imprese che fanno della profilazione e del monitoraggio delle abitudini e dei dati delle persone il loro core business. Mentre sono scritte queste righe infuria l'affaire Cambridge Analytica, e si tratta certamente di un buon esempio di ciò che il regolamento intende disciplinare con la norma in esame.

Tuttavia, l'ambito cui si applica l'obbligo è ben più ampio.

Si deve partire, innanzitutto, dal concetto di "larga scala", che consente di escludere almeno una parte significativa delle imprese dall'obbligo.

Nel Regolamento non c'è una definizione cui poter fare appiglio, ma il considerando 91 specifica che il riferimento è a 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".

Non si tratta, come si vede, di un grosso aiuto: al limite può autorizzare a considerare esclusi dall'obbligo i soggetti che operano in ambito locale (se per locale non intendiamo, però, una grande città).

Qualche chiarimento proviene dalle raccomandazioni del WP29 (gruppo formato dai Garanti Europei), in base alle quali va tenuto conto, per individuare la "larga scala": a) del numero di soggetti interessati, sia in via assoluta che in percentuale; b) del volume dei dati e delle diverse tipologie di essi; c) della durata dell'attività di trattamento; d) della portata geografica di quest'ultima.

Sono indicati come esempi di trattamento su larga scala: il trattamento di dati relativi ai pazienti svolto da un ospedale, il trattamento di dati relativi agli spostamenti di utenti del servizio di trasporto pubblico, il trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche, l'attività di banche, assicurazioni, motori di ricerca, fornitori di servizi telefonici o telematici.

A parte questi casi quindi occorrerà usare il buon senso e verificare se il trattamento ha effettivamente le dimensioni che giustificano la nomina di un DPO.

Nemmeno il "monitoraggio regolare sistematico degli interessati" è definito dal Regolamento.

Il considerando 24 menziona "il monitoraggio del comportamento degli interessati". Il successivo considerando 26 riferisce tale monitoraggio al "comportamento" dei soggetti.

Ancora una volta è chiaro chi sia il convitato di pietra: i grandi soggetti che lavorano sulla profilazione in Internet.

Le raccomandazioni del gruppo WP29 ci assicurano che per essere definito "regolare" il monitoraggio deve almeno avvenire: in modo continuo ovvero a intervalli definiti per un arco di tempo definito,

ovvero essere ricorrente o ripetuto a intervalli costanti. Oppure deve avvenire in modo costante o a intervalli periodici.

Il monitoraggio è inoltre "sistematico" se: avviene per sistema, è predeterminato, organizzato e metodico, ha luogo nell'ambito di un progetto complessivo di raccolta di dati oppure è svolto nell'ambito di una strategia.

Ancora una volta gli esempi chiariscono le idee meglio delle definizioni. Eseguono tale tipo di monitoraggio, secondo il gruppo WP29, i soggetti che curano: 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; profilazione e *scoring* per finalità di valutazione del rischio; tracciamento dell'ubicazione; programmi di fidelizzazione; pubblicità comportamentale; utilizzo di telecamere a circuito chiuso; utilizzo di dispositivi connessi.

Quanto al concetto di "attività principale", la previsione normativa consente di escludere dall'obbligo in esame i casi di monitoraggio meramente "ancillare" rispetto al *core business* dell'impresa. L'esempio più frequentemente fatto é il trattamento dei dati dei dipendenti delle grandi imprese.

D'altra parte, possono considerarsi riferiti all'attività principale dell'impresa quei trattamenti che costituiscono componenti inscindibili delle attività svolte dal titolare o dal responsabile. E qui l'esempio da fare è quello degli ospedali che trattano i dati dei pazienti.

In definitiva, per comprendere se un'impresa debba nominare il DPO occorre fare riferimento a numerosi fattori. Tra tali fattori non sono compresi né il numero di dipendenti né il fatturato.

Calare la questione nella realtà delle imprese radiotelevisive non è semplice.

Nelle "Nuove FAQ sul Responsabile della Protezione dei Dati (RPD) in ambito privato" del Garante del 27.3.2018 vengono espressamente incluse, tra le imprese che debbono dotarsi della figura in esame, le "società che erogano servizi televisivi a pagamento".

L'indicazione è piuttosto chiara, anche se sembra eccessivamente rigorosa (manca un riferimento, che sarebbe stato opportuno, alla "larga scala").

Al di fuori di tale caso, espressamente menzionato, c'è una ampia gamma di situazioni incerte.

A parere di chi scrive, una emittente che si limiti a irradiare il proprio segnale non tratta alcun dato, se non quelli dei dipendenti e degli inserzionisti: possiamo escludere che debba nominare un DPO.

Se invece l'emittente ha un sito internet la questione si complica.

Occorre valutare se tale sito utilizzi cookies di profilazione e se essi siano sfruttati dall'emittente medesima per monitorare i comportamenti di chi vi accede.

Se tale monitoraggio sussiste, ne vanno considerate le dimensioni e le finalità.

Chiaramente, laddove un'emittente usi il sito solo come occasionale vetrina per i suoi programmi, e abbia pochi accessi, anche un monitoraggio tramite profilazione potrebbe non rilevare ai fini che qui ci interessano.

Se, infine, si offrono servizi on-line e/o in abbonamento "su larga scala", è pressoché certo che vada nominato il DPO, e ciò è confermato dalle FAQ del garante, come si è visto.

Insomma, tra i due estremi che qui abbiamo indicato (semplice emittente e offerta di servizi on-line e in abbonamento) c'è una larga zona d'ombra.

Va inoltre esaminato un profilo legato alla lettera c) della norma, che impone la nomina del DPO se vengono trattate su larga scala categorie particolari di dati ai sensi dell'art. 9 del Regolamento (origine razziale o etnica, convinzioni religiose, etc.) o dati relativi a condanne penali e reati.

Può capitare che nel sistema televisivo alcune imprese trattino estesamente tali dati tramite gli archivi dei loro servizi giornalistici.

Anche in questo caso, la nomina di un DPO può risultare obbligatoria.

Si deve aggiungere che il Garante raccomanda "In ogni caso [...] anche alla luce del principio di *accountability* che permea il Regolamento, la designazione di tale figura" (cfr. le richiamate FAQ del 27.3.2018).

In conclusione, la miglior politica in merito alla scelta sulla nomina di un esperto di privacy quale DPO sembra quella di affidarsi ad un esperto di *privacy* che faccia le valutazioni del caso, le focalizzi in un documento e le lasci all'impresa per il suo dossier.

La soluzione può apparire tautologica, ma occorre tener presente che, come si è molte volte scritto in precedenza, la valutazione "ex ante" è un elemento imprescindibile nel cammino di adeguamento al GDPR.

Il buon senso, la professionalità degli esperti, e l'orientamento alla tutela dei diritti degli interessati consentiranno di affrontare tale cammino in modo ottimale.

La tutela dei minori e il consenso

Nel precedente paragrafo si è visto come la fornitura di servizi in abbonamento sia, per le emittenti radiotelevisive, fattore di rischio per il trattamento dei dati, tanto da indurre il Garante a "consigliare" la nomina del GDO.

A maggior ragione tale rischio sussiste per i servizi che vengono forniti on-line a pagamento o comunque previa registrazione.

In tali casi, evidentemente, i soggetti che maggiormente vanno tutelati sono i minori che vengono in contatto con le imprese.

Le problematiche sono intuibili: il minore, soggetto debole per eccellenza, e peraltro incapace, in base alle regole civilistiche, di compiere validi atti che comportino la manifestazione della sua volontà e la produzione di effetti giuridici, è notoriamente tra i primi e più assidui fruitori dei servizi della società dell'informazione. [17] Ovviamente, nel farlo, lascia i suoi dati, che vengono trattati.

Il Regolamento, al considerando 38, afferma che "I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore".

L'attuazione di tali principi si rinviene nell'art. 8 del Regolamento che, in sintesi, prevede quanto segue:

- il consenso al trattamento dei dati prestato dal minore nell'ambito dei servizi della società dell'informazione è valido se il minore stesso ha almeno 16 anni (ma il legislatore nazionale può abbassare la soglia fino a 13 anni). Altrimenti occorre

……..

[17] Il tema è in realtà molto complesso, e ci sono studi contrastanti. Si sostiene da alcuni che, in realtà, i minori siano gli utenti più *skilled* della rete, e che le limitazioni all'accesso non facciano altro che indurli a mentire sulla loro età. Cfr. in proposito L. Bolognini, C. Bistolfi, L'età del consenso digitale. Privacy e minori on line, riflessioni sugli impatti dell'art. 8 del Regolamento 2016/679(UE), in http://anticyberbullismo.it/wp-content/uploads/2017/06/Età_del_consenso_digitale_IIP_CNAC_2017.pdf

l'autorizzazione dell'esercente la responsabilità genitoriale o il consenso di quest'ultimo;

- il titolare del trattamento deve attivarsi "in ogni modo ragionevole" per verificare l'esistenza dell'autorizzazione dell'esercente la potestà genitoriale;

- non sono pregiudicate le norme nazionali che disciplinano la validità dei contratti stipulati dai minori.

Va aggiunto che le informazioni e le comunicazioni relative al trattamento devono essere, se il destinatario è un minore, redatte con linguaggio chiaro e semplice.

Ai sensi dell'art. 4 del Regolamento, per servizio della società dell'informazione si intende il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, "vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi".

Vi rientrano quindi tutti i servizi forniti on-line "normalmente retribuiti".

La norma non pare tanto indirizzata verso i social network [18](i cui servizi sono essenzialmente gratuiti) e sui siti di streaming, quanto su quelle realtà, come alcune piattaforme on-line delle emittenti radiotelevisive, che consentono di scaricare a pagamento file od offrono streaming su abbonamento.

Senza entrare nel tema, complesso e meritevole di più ampia trattazione, del tipo di capacità che si configura, per il consenso, in capo al minore, si possono segnalare due profili rilevanti nella pratica: a) il Regolamento ha sancito l'esistenza di una "maggiore età digitale"

……..

[18] E ciò, pare, differentemente da quanto ritiene la dottrina che individua in "Facebook, et similia", il principale campo di applicazione della norma: cfr. A. Thiene, Segretezza e riappropriazione, cit., 418.

per il consenso al trattamento dei dati che scatta a 16 anni (salvo che il legislatore nazionale voglia abbassare tale soglia); b) restano ferme le norme nazionali sulla capacità di agire dei minori, e in particolare l'art. 1425 del codice civile, che rende annullabili i contratti stipulati da minorenni (ma anche l'art. 1426 dello stesso codice, che ritiene validi gli stessi contratti se il minore ha, con raggiri, nascosto la propria età).

Entrambi i punti rendono evidente la necessità, per chi fornisce "i servizi della società dell'informazione", di dotarsi degli strumenti tecnologici necessari a verificare l'età di coloro che accedono ai siti o comunque richiedono di sottoscrivere abbonamenti.

Lo scopo è duplice: garantire la validità del consenso al trattamento dei dati e garantire la validità del contratto che si va a stipulare.

Si tratta di uno sforzo, anche in termini di investimenti tecnologici, sicuramente significativo, ma indispensabile per garantire un ordinato svolgimento della propria attività.

Linee guida sul Regolamento

Prof. Pietro Falletta

Nel gennaio 2012 la Commissione europea ha avviato il processo di riforma del quadro normativo in materia di protezione dei dati personali con lo scopo di garantire, all'interno dell'Unione europea, maggiore coerenza e armonizzazione in materia. Il 24 maggio 2016 è entrato ufficialmente in vigore il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati), che abroga la Direttiva 95/46/CE. Il Regolamento diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018.

Entro tale data le aziende sono pertanto chiamate ad adeguare la propria struttura organizzativa e a modificare le attività inerenti al

trattamento, in modo da conformarsi al nuovo quadro normativo in materia di protezione dei dati.[19]

Ambito di applicazione

Il Regolamento supera il principio di stabilimento previsto dalla Direttiva, in base al quale fino ad oggi le aziende o gli organismi non stabiliti sul territorio dell'Unione – cioè non aventi una sede o una succursale in uno Stato membro – non erano soggetti alla normativa europea in materia di protezione dei dati, a meno che non processassero fisicamente dati in Europa.

Il Regolamento amplia l'ambito di applicazione di tutela della *privacy* dei cittadini europei ogni qual volta siano destinatari di beni o servizi o i loro comportamenti siano oggetto di monitoraggio, anche da parte di aziende o organismi che non sono stabiliti sul territorio europeo.

Il Regolamento si applica (art. 3):

a) al titolare / responsabile stabilito sul territorio dell'UE, a prescindere dal fatto che anche il trattamento sia effettuato nell'Unione;

b) al titolare / responsabile del trattamento non stabilito nel territorio dell'UE nel caso in cui:

- offra beni o servizi a interessati che si trovano nell'Unione;
- svolga un monitoraggio del comportamento degli interessati comunque presenti nell'Unione;

……..

[19] Per l'elaborazione delle presenti linee guida, oltre al testo del Regolamento, sono stati consultati la pagina informativa del Garante per la protezione dei dati personali (disponibile all'indirizzo http://www.garanteprivacy.it/regolamentoue) e i working papers del Gruppo di lavoro Art. 29 (nello specifico: WP242, Linee-guida sul diritto alla "portabilità dei dati", 13 dicembre 2016; WP243, Linee-guida sui responsabili della protezione dei dati (RPD), 13 dicembre 2016; WP248, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 4 aprile 2017).

- sia stabilito in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico (disposizione già presente nella Direttiva 95/46/CE).

Qualora gli interessati non siano residenti nell'Unione, invece, il Regolamento si applica solo nei casi in cui:

- il titolare / responsabile ha uno stabilimento nell'UE;
- il trattamento sia fisicamente effettuato nel territorio dell'UE.

Privacy by default, by design, valutazione di impatto

Il Regolamento si basa su un nuovo approccio alla *privacy*. La tutela della protezione dei dati non è più intesa come adempimento successivo a fronte del trattamento dei dati personali, ma come presupposto di ogni trattamento. Prima di procedere al trattamento dei dati, è necessario adottare tutte le misure che assicurino le garanzie indispensabili per soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà dei soggetti coinvolti.

Il Regolamento privilegia la responsabilizzazione (*accountability*) dei titolari/responsabili del trattamento. Spetta a quest'ultimi stabilire autonomamente le modalità, le garanzie e i limiti del trattamento. In quest'ottica, sono favoriti interventi proattivi dei titolari/responsabili del trattamento, rispetto a interventi ex post delle autorità di controllo.

Da tale prospettiva derivano degli obblighi per il titolare/responsabile, che sono conformati ai criteri della c.d. *privacy by design* e *privacy by default*, nonché ad un approccio basato sul rischio, che comporta

l'attenzione ad eventuali impatti negativi del trattamento sui diritti e sulle libertà degli interessati (valutazione d'impatto sulla *privacy*).

Per *privacy by default* (art. 25) si intende il fatto che:

- il trattamento sia effettuato solo qualora sia necessario per le finalità specifiche per le quali i dati sono stati raccolti;
- la raccolta e la conservazione dei dati avvenga in quantità minima, tale per cui sia limitata al raggiungimento delle predette finalità;
- la conservazione dei dati sia limitata al tempo necessario a fornire il bene o il servizio per cui il trattamento è stato effettuato.

La *privacy by default* costituisce il livello minimo di tutela dell'interessato, che consiste nel garantire a quest'ultimo che il trattamento dei dati che lo riguardano avvenga solo per scopi leciti e solo nell'ambito delle finalità per le quali il trattamento è stato autorizzato o è necessario.

Tale principio, in realtà, era già alla base della Direttiva ed è stato recepito nel Codice in materia di protezione dei dati personali nel c.d. principio di necessità (art. 3 d.lgs. 196/2003).

Per *privacy by design* (art. 25) si intende l'esigenza di garantire la tutela della *privacy* sin dalle fasi di progettazione del sistema con il quale il trattamento dei dati verrà effettuato.

Si tratta di un principio introdotto ex novo dal Regolamento, in base al quale l'azienda deve provare di aver adottato tutte le misure indispensabili per garantire la tutela della *privacy* dell'interessato.

La valutazione d'impatto sulla *privacy* (art. 35), introdotta dal Regolamento, è un processo volto a valutare la necessità e la proporzionalità di un trattamento e a gestire i rischi che ne possono

derivare per i diritti e le libertà delle persone fisiche. Si tratta di uno degli strumenti che rispondono alla logica di responsabilizzazione dei titolari / responsabili del trattamento, in quanto aiuta quest'ultimi a soddisfare i requisiti richiesti dal Regolamento, ma soprattutto a dimostrare che siano state adottate le misure adeguate per garantirne il rispetto.

La valutazione di impatto riguarda i trattamenti di dati creati successivamente al mese di maggio 2018, oppure i casi in cui vi sia stato un cambiamento significativo nel trattamento.

La valutazione di impatto si riferisce a una singola operazione di trattamento di dati; tuttavia, i trattamenti che presentano rischi simili possono essere valutati insieme.

Nel caso di variazione del rischio connesso al trattamento, il titolare è tenuto a verificare nuovamente la conformità di questo alla valutazione di impatto.

Qualora sia designato un responsabile della protezione dei dati (DPO, vedi par. 4), il titolare si consulta con quest'ultimo al fine della valutazione. Il titolare può anche raccogliere le opinioni degli interessati o dei loro rappresentanti, nel rispetto degli interessi commerciali o pubblici e della sicurezza dei trattamenti.

Il Regolamento prevede dei contenuti minimi della valutazione di impatto che sono:

- la descrizione dei trattamenti e delle loro finalità;
- la valutazione circa la necessità e la proporzionalità del trattamento alla luce delle suddette finalità;
- la valutazione dei rischi per i diritti e le libertà degli interessati;
- la definizione delle misure previste per affrontare i rischi e la prova della conformità del trattamento al Regolamento.

La valutazione è richiesta nel caso in cui il trattamento possa presentare elevati rischi per i diritti e le libertà delle persone fisiche e, in particolare, nel caso di:

- trattamento automatizzato che comporti una valutazione sistematica e globale di aspetti personali relativi a persone fisiche (tra cui la profilazione) da cui derivano decisioni aventi effetti giuridici o che influenzano significativamente la persona;
- trattamento su larga scala di dati sensibili e di dati relativi a condanne penali o a reati;
- sorveglianza sistematica e su larga scala di una zona accessibile al pubblico.

Tale elenco, tuttavia, non è esaustivo. [20]

In tali circostanze e in linea con il principio della *privacy by default*, il titolare del trattamento deve effettuare la valutazione di impatto prima di procedere al trattamento, nel rispetto dei codici di condotta approvati (vedi par. 8.1). Potrà essere necessario un aggiornamento della valutazione, una volta che il trattamento sia effettivamente iniziato.

La valutazione non è necessaria:

- se i trattamenti sono imposti da un obbligo legale al quale è soggetto il titolare / responsabile o se sono in esecuzione di un compito di interesse pubblico o comunque connesso all'esercizio di

[20] Il Gruppo di lavoro Art. 29 ha ricavato dalle disposizioni del Regolamento una serie di circostanze al ricorrere delle quali il trattamento può ritenersi "suscettibile di provocare un rischio elevato"; in particolare: valutazioni di aspetti personali e/o trattamenti di dati aggregati; trattamenti automatizzati aventi effetti giuridici (o analoghi) sull'interessato; monitoraggio sistematico; trattamento di dati sensibili; dati processati su larga scala; banca dati originata da un incrocio di dati/trattamenti; trattamento di dati che riguardano soggetti vulnerabili; uso di soluzioni tecnologiche o organizzative innovative per il trattamento dei dati; trasferimento di dati al di fuori del territorio UE; trattamento che impedisce di per sé all'interessato l'esercizio di un diritto, l'uso di un servizio o la conclusione di un contratto.

pubblici poteri. In entrambi i casi è necessario che i trattamenti abbiano una base giuridica nel diritto dell'UE o nel diritto dello Stato membro e che, in tale contesto, sia stata già effettuata una valutazione di impatto nell'ambito di una valutazione di impatto generale (art. 35, par. 10);

- se il trattamento non è suscettibile di provocare un rischio elevato per i diritti e le libertà delle persone fisiche;

- se la natura, la portata, il contesto e le finalità del trattamento siano simili a un trattamento per cui la valutazione sia stata già effettuata per cui possono esserne utilizzati i risultati;

- se il trattamento è incluso nella lista opzionale delle operazioni di trattamento per cui non è necessaria la valutazione di impatto.

Il Regolamento demanda all'autorità di controllo il compito di redigere un elenco dei trattamenti per i quali è richiesta una valutazione di impatto e, se necessario, anche di quelli che ne sono esclusi; tale elenco è comunicato al Comitato europeo per la protezione dei dati.[21]

Qualora non sia chiaro l'obbligo di provvedere ad una valutazione di impatto, si consiglia in ogni caso di effettuarla, trattandosi di uno strumento utile per conformare il trattamento al quadro normativo in materia di protezione dei dati.

Una volta effettuata la valutazione, il titolare / responsabile può iniziare il trattamento adottando tutte le misure necessarie per ridurre al minimo il rischio, oppure procedere alla consultazione dell'autorità di controllo.

Qualora dalla valutazione di impatto risulti un rischio elevato per il trattamento, il titolare deve procedere a una consultazione preventiva

[21] Il Comitato europeo per la protezione dei dati (artt. 68 e ss.) è un organismo dotato di personalità giuridica e di indipendenza, con il compito di garantire l'applicazione coerente del Regolamento che sostituisce il Gruppo di lavoro Art. 29.

del Garante per la protezione dei dati personali (art. 36). In questi casi, l'autorità non autorizza al trattamento, ma indica le eventuali e ulteriori misure che il titolare è tenuto ad adottare e, se necessario, prende tutte le misure correttive di cui dispone, dall'ammonimento al titolare / responsabile, alla limitazione o al divieto di procedere al trattamento. In caso di consultazione preventiva, la valutazione di impatto deve essere comunicata al Garante. Non sussiste un obbligo di pubblicazione; tuttavia si raccomanda di procedere alla pubblicazione, anche solo di una parte della valutazione, in modo da promuovere la fiducia nelle operazioni di trattamento dei dati e da garantire responsabilità e trasparenza.

Se l'autorità ritiene che il trattamento sia in violazione del Regolamento, fornisce una consulenza scritta entro 8 settimane, che possono essere prorogate fino a 6 in caso di trattamenti particolarmente complessi, purché ne sia data informazione al titolare / responsabile entro 1 mese dalla richiesta di consultazione.

In ogni caso, anche qualora il titolare decida di non effettuare una valutazione di impatto, dovrà redigere un registro delle attività di trattamento. Il registro delle attività di trattamento (art. 30) deve essere tenuto da tutti i titolari/responsabili del trattamento, ad eccezione di imprese e organizzazioni con meno di 250 dipendenti, sempre che non effettuino trattamenti a rischio, che l'attività di trattamento sia occasionale, o che il trattamento non includa dati sensibili o dati relativi a condanne penali e a reati.

Il registro deve essere tenuto in forma scritta, su supporto cartaceo o elettronico e, qualora richiesto, deve essere messo a disposizione del Garante.

Questo strumento è importante al fine della supervisione da parte del Garante e per la tenuta di un quadro aggiornato dei trattamenti all'interno dell'azienda/organismo pubblico; è indispensabile ai fini

della valutazione e analisi del rischio e utile per garantire l'esercizio dei diritti dell'interessato.

Il Regolamento fissa le informazioni che il registro deve contenere operando una distinzione tra titolare e responsabile del trattamento.

Se il registro è tenuto dal titolare del trattamento e, qualora presente, dal suo rappresentante, è necessario riportare le seguenti informazioni:

- il nome ed i dati di contatto del titolare del trattamento e, se presenti, del contitolare del trattamento, del rappresentante del titolare e del DPO;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie dei dati personali;
- i destinatari cui i dati sono o saranno comunicati (compresi quelli di Paesi terzi / organizzazioni internazionali);
- se previsti, i trasferimenti di dati personali verso Paesi terzi / organizzazioni internazionali (con relativa identificazione) e la documentazione delle garanzie adeguate per i trasferimenti dei dati presi dai pubblici registri (vedi par. 9.3);
- se possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative messe in atto.

Se il registro è tenuto dal responsabile del trattamento e, qualora presente, dal suo rappresentante, è necessario riportare le seguenti informazioni:

- il nome e i dati di contatto di ogni titolare per conto del quale agisce il responsabile, del responsabile/i del trattamento, del rappresentante del responsabile del trattamento in alternativa a quello del titolare e, ove presente, del DPO;

- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- se previsti, i trasferimenti di dati personali verso Paesi terzi / organizzazioni internazionali (con relativa identificazione) e la documentazione delle garanzie adeguate per i trasferimenti dei dati presi dai pubblici registri (vedi par. 9.3);
- se possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative messe in atto.

Al di là dei contenuti necessari, il titolare / responsabile può aggiungere informazioni ulteriori. Tale strumento coincide, quanto ai contenuti, con la notifica dei trattamenti prevista dal Codice *privacy* (artt. 37-38), superata dal Regolamento ad eccezione del caso di violazione di dati personali (vedi par. 7). Come già accade per la notificazione, il Garante sta valutando l'opportunità di predisporre sul proprio sito un modello di registro dei trattamenti.

Titolare e responsabile del trattamento

Le caratteristiche soggettive e le responsabilità del titolare e del responsabile del trattamento rimangono invariati rispetto a quanto previsto dal Codice.

Il titolare del trattamento è la persona fisica o giuridica che determina le finalità e i mezzi del trattamento dei dati personali. Spetta al titolare porre in essere le misure adeguate a garantire che il trattamento avvenga conformemente al Regolamento e deve essere in grado di dimostrarlo (art. 24).

Il Regolamento inserisce la disciplina della contitolarità del trattamento (art. 26). In tali casi i titolari devono stabilire in modo trasparente, con un accordo interno giuridicamente vincolante, le rispettive

responsabilità e funzioni, con riferimento specifico all'esercizio dei diritti degli interessati. Questi ultimi possono rivolgersi indifferentemente a ognuno dei titolari che opera congiuntamente.

Il responsabile del trattamento è la persona fisica o giuridica, autorità pubblica, servizio o qualsiasi altro organismo che tratta i dati per conto del titolare del trattamento. Il responsabile deve essere dotato di garanzie sufficienti a mettere in atto misure idonee per conformare il trattamento al Regolamento. (art. 28)

Il Regolamento specifica le caratteristiche dell'atto di designazione del responsabile del trattamento da parte del titolare, per cui non è più sufficiente la semplice forma scritta, ma è richiesta la stipula di un contratto o altro atto giuridico conforme al diritto nazionale. Al fine di dimostrare che il responsabile fornisca garanzie sufficienti e operi conformemente a quanto disposto dal Regolamento, l'atto in questione deve disciplinare necessariamente: la materia e la durata del trattamento; la natura e la finalità; il tipo di dati oggetto di trattamento e le categorie degli interessati; gli obblighi e i diritti del titolare del trattamento.

Sono previsti obblighi specifici in capo al responsabile del trattamento, da ritenere distinti da quelli riconosciuti in capo ai titolari e in particolare: la redazione di un registro dei trattamenti (art. 30, par.2); l'adozione di misure tecniche e organizzative di sicurezza (art. 32); la designazione del DPO (art. 37); la designazione di un rappresentante in Italia del titolare / responsabile non stabilito nell'UE nel caso in cui i dati dell'interessato siano trattati nell'ambito dell'offerta di beni e servizi o siano soggetti a monitoraggio (art. 27).

È prevista la possibilità di nominare sub-responsabili (art. 28, par. 4) per specifiche attività di trattamento, i quali sottostanno agli stessi obblighi previsti dal contratto tra il titolare e il responsabile principale. È in ogni

caso quest'ultimo che risponde davanti al titolare per eventuali inadempimenti del sub-responsabile.

Il Regolamento non prevede più espressamente la figura dell'incaricato del trattamento; tuttavia non è esclusa la possibilità della sua presenza in quanto si fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (art. 4, n. 10).

Nel caso di titolare / responsabile non stabilito sul territorio dell'UE, il Regolamento prevede la designazione di un rappresentante (art. 27), con esclusione dei casi in cui il trattamento sia occasionale o sia effettuato da un'autorità o da un organismo pubblico. Tale figura svolge, in particolare, la funzione di interlocutore delle autorità di controllo e degli interessati.

Responsabilità del titolare / responsabile del trattamento

In caso di violazione del Regolamento chiunque ha il diritto di ottenere il risarcimento del danno (materiale o immateriale) dal titolare / responsabile del trattamento (art. 82). Il titolare del trattamento risponde per danni causati da un trattamento effettuato in violazione del Regolamento; il responsabile risponde per il danno causato dal trattamento solo se non ha adempiuto agli obblighi che il Regolamento gli impone o se ha agito in modo differente o contrario rispetto alle istruzioni fornite dal titolare del trattamento. Entrambi sono esonerati dalla responsabilità se è dimostrato che l'evento dannoso non è loro imputabile in alcun modo.

Se più titolari/responsabili del trattamento oppure se entrambi sono coinvolti nello stesso trattamento e sono responsabili dell'eventuale danno causato da esso, ciascuno è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo del soggetto interessato. Nel caso in cui un titolare / responsabile del

trattamento paghi l'intero risarcimento del danno, ha il diritto di reclamare dagli altri titolari/responsabili coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno.

Responsabile della protezione dei dati (Data Protection Officer)

Il responsabile della protezione dei dati è una nuova figura introdotta dal Regolamento, che risponde alla logica di responsabilizzazione del titolare e del responsabile, essendo volta a facilitare l'attuazione del nuovo quadro normativo in materia di protezione dei dati. (artt. 38, 39)

La sua nomina è obbligatoria nel caso in cui (art. 37):

- il trattamento sia effettuato da un'autorità pubblica o da organismo pubblico (con l'eccezione delle autorità giurisdizionali) indipendentemente dai dati oggetto di trattamento;
- l'attività principale [22] dell'azienda consiste nel monitoraggio regolare e sistematico [23] su larga scala;
- l'attività principale dell'azienda consiste nel trattamento su larga scala [24] di dati sensibili o dati relativi a condanne penali o a reati.

[22] Con attività principale si intendono le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi del titolare / responsabile del trattamento; in esse sono ricomprese anche i casi in cui il trattamento costituisce una componente inscindibile dalle attività svolte.

[23] Per monitoraggio regolare e sistematico si intendono le forme di tracciamento e profilazione su Internet (sebbene non sia legato al solo contesto online) svolta in modo continuo, ricorrente o costante nell'ambito di una strategia, di un progetto complessivo di raccolta di dati, predeterminato, organizzato.

[24] Il trattamento su larga scala tiene conto del numero dei soggetti interessati dal trattamento, della quantità di dati e delle tipologie, della durata dell'attività di trattamento, nonché della sua portata geografica.

Anche nei casi in cui il Regolamento non prevede come obbligatoria la designazione del DPO, può essere utile nominare tale figura su base volontaria.

Il Regolamento non differenzia in merito alla titolarità del potere di nomina del DPO tra titolare e responsabile; è da intendere che possa essere nominato a seconda dei casi dall'uno, dall'altro o da entrambi.

I gruppi di imprese possono nominare un solo responsabile per la protezione dei dati, ma questo deve essere raggiungibile da tutti gli stabilimenti.

Anche le autorità o organismi pubblici possono nominarne uno solo, sempre tenendo conto della loro dimensione e struttura organizzativa.

Una volta nominato, i dati di contatto del DPO devono essere pubblicati e comunicati all'autorità di controllo.

Spetta al titolare / responsabile assicurare che il DPO sia "tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati" (art. 38). Ciò comporta che sia tra gli interlocutori all'interno della struttura del titolare / responsabile e che prenda parte ai gruppi di lavoro in merito alle attività di trattamento. Il DPO dovrebbe, quindi, essere inserito dalle fasi iniziali delle attività di trattamento e, ancor prima, in quella dell'effettuazione della valutazione di impatto. È ancora in capo al titolare / responsabile l'onere di garantire che il DPO abbia a disposizione le risorse necessarie per assolvere i suoi compiti, per accedere ai dati e per garantire le sue conoscenze specialistiche.

Il DPO deve essere una figura dotata di:

- indipendenza: fa riferimento diretto al vertice gerarchico dell'azienda; non deve ricevere alcuna istruzione per l'esecuzione dei suoi compiti; nello svolgimento di altri compiti e funzioni non

devono sussistere conflitti di interesse; non può essere rimosso per aver adempiuto alle sue funzioni;

- autorevolezza: deve trattarsi di persona dotata di qualità professionali e conoscenza specialistica in materia di protezione dei dati; in particolare, dovrebbe essere a conoscenza della normativa e delle prassi nazionali ed europee in materia, avere familiarità con le operazioni di trattamento svolte, con le tecnologie informatiche e di sicurezza utilizzate; deve avere conoscenza dello specifico settore di attività del titolare / responsabile ed essere dotato di una capacità di diffondere una cultura della protezione dei dati all'interno dell'organizzazione.

Il DPO può essere un dipendente del titolare / responsabile del trattamento o un consulente esterno, nominato sulla base di un contratto di servizi. Quanto alla responsabilità, il DPO non risponde personalmente in caso di inosservanza del Regolamento; è infatti il titolare / responsabile a dover essere in grado di dimostrare che le operazioni del trattamento siano conformi alle disposizioni del Regolamento.

I principali compiti del DPO sono (art. 39):

- fornire consulenza e informazione al titolare, al responsabile e ai dipendenti che si occupano del trattamento dei dati in merito a obblighi derivanti dal Regolamento e dal generale quadro normativo in materia di protezione dei dati;

- sorvegliare sull'osservanza del Regolamento che implica la raccolta di informazioni per individuare i trattamenti, l'analisi e verifica della conformità di quest'ultimi, l'attività di informazione, consulenza e indirizzo al titolare / responsabile;

- fornire parere, se richiesto, sulla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

- cooperare con l'autorità di controllo e fare da punto di contatto con quest'ultima per questioni connesse al trattamento;
- fare da tramite tra interessato e titolare / responsabile del trattamento; ciò significa che può essere contattato dagli interessati per qualsiasi questione relativa al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal Regolamento.

L'elenco dei compiti spettanti al DPO non è da considerarsi esaustivo. Potrebbe, per esempio, rientrare tra le funzioni che il titolare / responsabile del trattamento affidano al DPO la tenuta del registro delle attività di trattamento.

Per provare la competenza, l'indipendenza e la professionalità del DPO sono in corso di definizione da parte dell'Unione e degli Stati membri dei meccanismi di certificazione. Si tratterà di una certificazione a valenza triennale che potrà essere rilasciata dall'autorità di controllo, dall'organismo nazionale di accreditamento a norma del Regolamento 765/2008 o da organismi di certificazione che sono in possesso di un livello adeguato di competenza in materia di protezione dei dati.

Trattamento dei dati

I principi applicabili al trattamento rimangono sostanzialmente invariati rispetto al Codice. Il trattamento dei dati deve essere effettuato in base ai princìpi di liceità, correttezza e trasparenza. I dati devono essere raccolti per finalità determinate, esplicite e legittime e successivamente trattati conformemente a tali finalità. I dati devono essere adeguati, pertinenti e limitati a quanto necessario alla luce delle finalità per le quali sono trattati; inoltre, devono essere esatti e aggiornati. La conservazione dei dati che consentono l'identificazione degli interessati deve essere limitata al tempo necessario al

conseguimento delle finalità del trattamento, salvo periodi più lunghi, richiesti da motivi di interesse pubblico, di ricerca scientifica o storica o a fini statistici; il trattamento deve garantire un'adeguata sicurezza dei dati e la protezione dell'integrità e della riservatezza (art. 5).

I fondamenti di liceità del trattamento coincidono, in linea di massima, con quanto previsto dal Codice, continuando a sostanziarsi nel consenso, nell'adempimento degli obblighi contrattuali, negli interessi vitali della persona interessata o di terzi, negli obblighi di legge cui è soggetto il titolare, nell'interesse pubblico o nell'esercizio di pubblici poteri, nell'interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Il consenso dell'interessato rimane il primo requisito di liceità del trattamento dei dati (art. 6). Deve essere libero, specifico, informato e inequivocabile; non è, invece, ammesso il consenso tacito o presunto. Deve, inoltre, essere manifestato attraverso "dichiarazione o azione positiva inequivocabile".

Il Regolamento introduce l'onere del titolare del trattamento di dimostrare che l'interessato abbia prestato il suo consenso per lo specifico trattamento. In caso di dichiarazione in forma scritta contenente più richieste rivolte all'interessato, il Regolamento prevede che la richiesta di consenso sia facilmente distinguibile dalle altre. Quanto alla forma, la richiesta deve essere comprensibile e facilmente accessibile, formulata con un linguaggio semplice e chiaro (art. 7).

Il consenso non deve essere necessariamente documentato per iscritto, né è richiesta la forma scritta, sebbene sia la modalità idonea ad assicurare che sia stato prestato in maniera inequivocabile ed esplicita. Il consenso dei minori con riferimento ai servizi della società dell'informazione, è valido a partire dai 16 anni; altrimenti è necessario ottenere il consenso del genitore o di chi ne fa le veci (art. 8). Per i trattamenti automatizzati il consenso deve essere esplicito.

Il Regolamento, come la Direttiva, dedica disposizioni specifiche per il trattamento di categorie particolari di dati personali, nella fattispecie, dati sensibili e dati relativi a condanne penali e reati (artt. 9-10).

Per i dati sensibili il consenso deve essere esplicito. Il fondamento di liceità del trattamento di tali categorie di dati rimane sostanzialmente analogo rispetto alla Direttiva, per cui in generale è vietato il trattamento di dati sensibili a meno che non ricorrano determinate condizioni, nello specifico nel caso in cui (art. 9):

- tali dati siano necessari per assolvere obblighi ed esercitare diritti specifici del titolare o dell'interessato in materia di diritto del lavoro, della sicurezza sociale e protezione sociale sempre che vi sia un fondamento legislativo o contrattuale;
- il trattamento sia necessario per tutelare interessi vitali dell'interessato;
- il trattamento sia svolto da un'associazione o da un organismo senza scopo di lucro a condizione che i dati riguardino i loro membri e non vengano comunicati all'esterno senza il consenso dell'interessato;
- i dati in questione siano stati resi manifestamente pubblici dall'interessato;
- il trattamento sia necessario per motivi di interesse pubblico, compresi quelli nel settore della sanità pubblica o è necessario per finalità di medicina preventiva o di medicina del lavoro;
- il trattamento sia necessario ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o ai fini statistici.

Per i dati relativi a condanne penali e reati, il fondamento di liceità del trattamento rimane una previsione esplicita in una disposizione di legge o il controllo da parte dell'autorità pubblica (art. 10).

Diritti dell'interessato

Il Regolamento stabilisce in via generale le modalità per l'esercizio di tutti i diritti da parte degli interessati (artt. 11 e 12). Il corretto esercizio dei diritti dell'interessato è basato sul principio di trasparenza. Esso impone che tutte le informazioni (artt. 13 e 14) e le comunicazioni (artt. 15-22 e all'art. 34) relative al trattamento non siano solo intellegibili ma anche concise, scritte con un linguaggio semplice e chiaro e facilmente accessibili. A tal fine, è possibile ricorrere all'uso di icone standardizzate (leggibili anche dai dispositivi mobili).

Il Regolamento introduce l'onere di fornire le informazioni relative al trattamento per iscritto e, ove possibile, in formato elettronico; possono essere fornite oralmente solo se richiesto dall'interessato (purché venga dimostrata la sua identità). Il compito di richiedere le informazioni necessarie a verificare e confermare l'identità dell'interessato rimane in capo al titolare del trattamento (in particolare nel contesto di servizi online); l'interessato ha il dovere di fornire dette informazioni secondo modalità idonee.

Quando il trattamento dei dati riguarda i minori, qualsiasi tipo di informazione e/o comunicazione deve essere fornita ricorrendo all'utilizzo di un linguaggio semplice e chiaro, tale da consentire una facile comprensione del testo al soggetto minorenne.

È opportuno prevedere modalità volte ad agevolare l'interessato nel richiedere ed ottenere gratuitamente l'accesso ai dati, la loro rettifica e la cancellazione e per esercitare il diritto di opposizione. Il titolare del trattamento deve facilitare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura tecnica e organizzativa a ciò idonea. L'onere di dare riscontro in caso di esercizio dei diritti (artt. 15-22) rimane in capo al titolare, il responsabile è tenuto a collaborare (art. 28, par. 3, lett. e).

Il Regolamento fissa i termini per dare riscontro alle richieste dell'interessato che devono essere evase senza ingiustificato ritardo entro al massimo 1 mese dal loro ricevimento ma, se necessario, il termine può essere prorogato di 2 mesi, in caso di particolare complessità e di ingente numero di domande pervenute. La proroga e il diniego devono comunque essere comunicati all'interessato entro 1 mese dalla richiesta con motivazione. A differenza di quanto previsto dal Codice, il riscontro alle richieste presentate dagli interessati deve avere per impostazione predefinita la forma scritta e può essere fornito anche attraverso strumenti elettronici. Solo qualora richiesto dall'interessato può essere dato oralmente. In caso di inadempimento da parte del responsabile, l'interessato può proporre ricorso al Garante o procedere in via giurisdizionale.

In linea di principio, come già previsto dal Codice, l'esercizio dei diritti, la richiesta di informazioni e le comunicazioni sono gratuite. Il Regolamento, tuttavia, introduce la possibilità di richiedere un contributo spese all'interessato nei casi in cui il titolare del trattamento accerti che le richieste siano manifestamente infondate, eccessive o ripetitive. L'ammontare dell'eventuale contributo per intraprendere l'azione è stabilito dallo stesso titolare che può tuttavia rifiutarsi di soddisfarla dimostrandone l'infondatezza o l'eccessività.

Informativa

Il Regolamento elenca tassativamente i contenuti dell'informativa (artt. 13, 14) che sono ampliati rispetto alle previsioni del Codice, mantenendo la distinzione tra le informazioni da fornire qualora i dati siano raccolti presso l'interessato e quelle da fornire qualora siano stati ottenuti da altra fonte.

Nello specifico, il titolare deve sempre indicare:

- i dati di contatto del titolare del trattamento (se presente anche del suo rappresentante) e del DPO;
- le finalità e la base giuridica del trattamento;
- l'interesse legittimo del titolare, se costituisce la base giuridica del trattamento (questa informazione è tra i contenuti ulteriori nei casi in cui i dati non siano ottenuti presso l'interessato);
- gli eventuali destinatari dei dati personali;
- l'intenzione di trasferire tali dati verso un Paese terzo/organizzazione internazionale. Se il trasferimento si basa su una decisione di adeguatezza della Commissione è necessario indicarla; negli altri casi (quando il trasferimento si basa su garanzie adeguate o eventuali deroghe, vedi par. 9.2 e ss.) è necessario indicare le garanzie e i mezzi per ottenere una copia dei dati o il luogo dove sono resi disponibili.

Il Regolamento prevede anche ulteriori informazioni da inserire nell'informativa per garantire un trattamento corretto e trasparente; in particolare, il titolare deve specificare:

- il periodo di conservazione dei dati o i criteri seguiti per stabilirlo;
- i diritti dell'interessato;
- la possibilità di revocare il consenso;
- il diritto di presentare un reclamo all'autorità di controllo;
- se il trattamento comporta processi decisionali automatizzati (tra cui la profilazione);
- se la comunicazione dei dati è un obbligo legale, contrattuale o un requisito necessario per la conclusione di un contratto e se l'interessato ha l'obbligo di fornire i dati e le relative conseguenze in caso di mancata comunicazione (qualora i dati vengano raccolti direttamente presso l'interessato).

L'interessato deve essere altresì informato dal titolare qualora i dati personali siano trattati per una finalità diversa da quella per cui essi sono stati originariamente raccolti; tutte le informazioni necessarie devono essere fornite prima del nuovo trattamento.

Tali informazioni devono essere fornite all'interessato nel momento della raccolta (qualora i dati siano ottenuti dallo stesso) o entro un termine ragionevole, ma al più tardi entro 1 mese (qualora i dati siano stati ottenuti da altra fonte).

Nel caso in cui i dati siano legittimamente comunicati ad altro destinatario, l'interessato deve esserne informato dal momento della comunicazione.

Se i dati sono raccolti presso l'interessato, non vi è l'obbligo di informare il soggetto quando dispone già di tali informazioni.

Se i dati sono ottenuti da fonte diversa dall'interessato, non vi è l'obbligo di informare il soggetto quando:

- la registrazione o la comunicazione dei dati sono previste per legge;
- informare l'interessato è impossibile o richiede sforzo sproporzionato;
- i dati devono rimanere riservati nel rispetto di un obbligo legale di segreto professionale.

Diritto di accesso

In materia di accesso, il Regolamento conserva l'impostazione prevista dal Codice, aggiungendo delle variazioni. L'interessato ha il diritto di ottenere l'accesso ai dati personali raccolti che lo riguardano e di esercitare tale diritto facilmente. Il Regolamento prevede che l'interessato riceva comunque una copia dei dati personali oggetto di

trattamento. Al fine di verificare la liceità del trattamento, l'interessato ha il diritto di ricevere dal titolare del trattamento le seguenti informazioni (artt. 14, 15-23 e 32):

- le finalità del trattamento;
- i destinatari a cui i dati personali sono stati o saranno comunicati;
- l'esistenza del diritto di rettifica, di cancellazione dei dati personali o la possibilità di limitare o opporsi al trattamento di dati che lo riguardano;
- il diritto di proporre reclamo a un'autorità di controllo;
- l'esistenza di qualsiasi trattamento automatizzato e le possibili conseguenze per l'interessato.

Il Regolamento non prevede più l'obbligo di comunicare all'interessato le modalità del trattamento, ma introduce quello di fornire due ulteriori informazioni:

- il periodo previsto per la conservazione dei dati personali trattati oppure, se non è possibile stabilirlo con certezza, i criteri utilizzati per determinare tale periodo;
- le garanzie applicate in caso di trasferimento dei dati a Paesi terzi.

Al fine di facilitare l'accesso, dev'essere consentito all'interessato di consultare direttamente i propri dati tramite l'accesso remoto ad un sistema sicuro. In ogni caso, il diritto di accesso non deve ledere i diritti e le libertà altrui, compreso il segreto industriale, aziendale e la proprietà intellettuale.

Diritto di rettifica e diritto alla cancellazione (diritto all'oblio)

L'interessato ha diritto di ottenere che il titolare del trattamento, senza ingiustificato ritardo, rettifichi o aggiorni i dati personali inesatti che lo riguardano e/o integri i dati personali incompleti.

Inoltre, il Regolamento introduce il diritto all'oblio, una forma rafforzata del diritto alla cancellazione dei propri dati personali (art. 17): l'interessato ha infatti diritto di richiedere la rimozione di essi e dunque di ottenere che non siano più sottoposti a trattamento. Tale diritto ha un campo di applicazione più esteso rispetto a quello previsto dal Codice (art.7, comma 3, lettera b); esso infatti non è più previsto solo nel caso in cui i dati non siano più necessari rispetto alle finalità per cui erano stati raccolti o trattati ma anche quando l'interessato revoca il proprio consenso o si oppone al trattamento e quando il trattamento è illecito e non conforme al Regolamento.

Al fine di rafforzare il diritto all'oblio nella rete, il titolare del trattamento che ha reso pubblici i dati per cui si richiede la cancellazione è obbligato a cancellarli e a richiedere ad altri titolari che trattano tali dati di rimuoverne qualsiasi link, copia o riproduzione.

Il diritto all'oblio non si applica nei casi in cui il trattamento dei dati sia necessario per esercitare il diritto alla libertà di espressione e di informazione; per adempiere un obbligo legale; per eseguire un compito di interesse pubblico o per l'esercizio di poteri pubblici; per motivi d'interesse pubblico nella sanità pubblica; per fini di archiviazione o statistici, di ricerca scientifica o storica; per accertare, esercitare o difendere un diritto in sede giudiziaria.

Diritto alla limitazione del trattamento

Tra i diritti dell'interessato, il Regolamento introduce il diritto alla limitazione del trattamento (art. 18). Rispetto al blocco del trattamento

previsto dal Codice (art.7, comma 3 lettera a), la limitazione del trattamento è un diritto più esteso, esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (alternativamente alla cancellazione) ma anche nei casi in cui:

- venga contestata l'esattezza dei dati personali ed è quindi necessario verificarla;
- i dati personali siano necessari per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- l'interessato si opponga al trattamento, in attesa della verifica della prevalenza degli interessi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Diritto alla portabilità dei dati

Il Regolamento introduce il diritto alla portabilità dei dati (art. 20). Al fine di rafforzare il controllo sui propri dati, l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune, leggibile da dispositivo automatico ed interoperabile, i propri dati personali che ha fornito ad un titolare del trattamento. In secondo luogo, l'interessato ha il diritto di trasmettere gli stessi dati senza impedimenti ad un altro titolare. Tale diritto è applicabile solo ai dati personali forniti dall'interessato mediante consenso o se il trattamento è necessario per l'esecuzione di un contratto. Il diritto alla portabilità, inoltre, sussiste esclusivamente se il trattamento è effettuato con mezzi automatizzati, non applicandosi quindi ad archivi o registri cartacei.

Il nuovo diritto, così come formulato, intende facilitare la circolazione, la copia o la trasmissione dei dati da un ambiente informatico all'altro. Ciò può avvenire su qualsiasi supporto personale o su un cloud privato, senza implicare necessariamente la trasmissione dei dati ad un altro titolare. I titolari che danno seguito a richieste di portabilità non sono

responsabili del trattamento effettuato dal singolo interessato o da un'altra società ricevente che accolga i dati in questione. Prima della trasmissione, i titolari che adempiono ad una richiesta di portabilità non hanno l'obbligo di verificare la qualità dei dati che dovrebbero già essere conformi ai requisiti di esattezza e di aggiornamento (art. 5).

L'esercizio del diritto alla portabilità dei dati (come di qualsiasi altro diritto) non compromette nessuno degli altri diritti. L'interessato può continuare a fruire e beneficiare del servizio offerto dal titolare anche dopo che sia avvenuta un'operazione di portabilità. Questa non comporta la cancellazione automatica dei dati conservati nei sistemi del titolare e non incide sul periodo di conservazione previsto originariamente per i dati oggetto di trasmissione.

Diritto di opposizione

Come già previsto dalla Direttiva, il Regolamento riconosce all'interessato il diritto di opporsi in qualsiasi momento al trattamento dei propri dati personali, anche attraverso strumenti automatizzati (art. 21). Tale diritto sussiste altresì nel caso in cui i dati siano legittimamente trattati per l'esecuzione di un compito svolto nel pubblico interesse, nell'esercizio di pubblici poteri da parte del titolare del trattamento o per i legittimi interessi di un titolare del trattamento o di terzi. L'interessato ha il diritto di opposizione anche qualora i dati personali siano trattati per fini di ricerca scientifica, storica o a fini statistici, salvo il caso in cui il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

Qualora l'interessato si opponga al trattamento, il titolare deve astenersi dal trattare ulteriormente i dati personali del soggetto, salvo dimostrare che i suoi interessi legittimi cogenti prevalgano sugli interessi, sui diritti e sulle libertà fondamentali dell'interessato.

Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento a tale trattamento, assicurandosi che i propri dati personali non siano più oggetto di trattamento per tali finalità.

Il Regolamento prevede che il soggetto interessato sia esplicitamente informato della possibilità di esercitare il diritto di opposizione, che deve essere inserito in modo chiaro e distinguibile dalle altre informazioni all'interno dell'informativa.

Diritto di opposizione a decisioni automatizzate

Il Regolamento, come già la Direttiva, riconosce all'interessato il diritto di non essere sottoposto a una decisione fondata unicamente sul trattamento automatizzato (tra cui la profilazione), che produca effetti giuridici che lo riguardano o che abbia effetti significativi sulla sua persona (art. 22).

Tale diritto non può essere esercitato nel caso in cui la decisione:

- sia autorizzata dal diritto dell'UE o dello Stato membro cui è soggetto il titolare del trattamento;
- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento;
- si basi sul consenso esplicito dell'interessato.

In questi ultimi due casi, è tuttavia necessario che il titolare del trattamento tuteli i diritti, le libertà e i legittimi interessi dell'interessato, riconoscendo allo stesso almeno il diritto di ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione.

Le limitazioni all'esercizio del diritto di opposizione non valgono se il trattamento riguarda i dati sensibili, a meno che l'interessato abbia prestato il proprio consenso esplicitamente, il trattamento sia

necessario per motivi di interesse pubblico e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Sicurezza e violazione dei dati (data breach)

Per garantire un livello di sicurezza adeguato e prevenire trattamenti in violazione del Regolamento, il titolare / responsabile del trattamento è tenuto ad adottare misure tecniche e organizzative per limitare i rischi inerenti al trattamento. In tal senso, il Regolamento fornisce un elenco aperto e non esaustivo di tali misure, annoverando tra queste il ricorso a meccanismi di cifratura o pseudonimizzazione e il ripristino tempestivo di disponibilità e accesso ai dati in caso di incidente fisico o tecnico.

Dopo il 25 maggio 2018, non saranno più sufficienti obblighi generalizzati di adozione di misure minime di sicurezza in quanto tale decisione sarà rimessa, caso per caso, al titolare / responsabile del trattamento in relazione ai rischi individuati dal Regolamento (art. 32). La conformità ai livelli e ai requisiti di sicurezza previsti (art. 32 par. 1) può essere dimostrata aderendo ad un codice di condotta (art. 40, vedi par. 8.1.) o a un meccanismo di certificazione (art. 42, vedi par. 8.2.). Inoltre, facendo riferimento a quanto previsto nel Codice (in particolare all'Allegato B), il Garante potrà decidere di elaborare linee guida o buone prassi sulla base dei risultati conseguiti negli anni. Le misure di sicurezza attualmente previste da disposizioni di legge potranno altresì restare in vigore nel caso in cui il trattamento sia necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento o per l'esecuzione di un compito d'interesse pubblico o comunque connesso all'esercizio di pubblici poteri (art. 6 par. 2 del Regolamento).

In caso di violazione dei dati personali che comporti un rischio elevato per i diritti e le libertà dell'interessato, il titolare del trattamento è tenuto a presentare una notifica al Garante e una comunicazione all'interessato.

Notifica al Garante

La violazione dei dati personali può provocare danni materiali o immateriali a persone fisiche se non affrontata in modo adeguato e tempestivo. Per questa ragione, non appena accertata una violazione dei dati personali, il titolare del trattamento è tenuto a notificarla al Garante senza ingiustificato ritardo, entro 72 ore dalla conoscenza della violazione stessa (art. 55). Qualora la notifica avvenga oltre le 72 ore, il titolare del trattamento deve motivare il ritardo. La notifica è facoltativa; il Regolamento infatti stabilisce che sia obbligatoria solo qualora venga accertato che la violazione comporti un rischio per i diritti e le libertà delle persone interessate.

Il Regolamento stabilisce che la notifica all'autorità di controllo deve comporsi di più elementi: la descrizione della violazione avvenuta; il numero approssimativo dei soggetti interessati; il nome e il contatto del DPO o di altro riferimento presso cui ottenere informazioni; la descrizione delle probabili conseguenze della violazione avvenuta e le misure adottate / adottabili dal titolare del trattamento per porre rimedio alla violazione e per contenere i possibili effetti negativi.

Anche nel caso in cui le violazioni dei dati personali non siano state comunicate al Garante e agli interessati, il titolare del trattamento è tenuto a documentarle, specificando le circostanze in cui sono avvenute, le conseguenze e i provvedimenti adottati in merito (art. 33, par. 5). Tale obbligo richiama quello attualmente previsto dal Codice (art. 32-bis, comma 7) per cui i titolari sono tenuti a fornire al Garante,

se richiesto, la documentazione raccolta per lo svolgimento di accertamenti.

Comunicazione all'interessato

Quando la violazione presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento è tenuto a comunicare senza ritardo all'interessato l'avvenuta violazione dei dati personali.

La comunicazione all'interessato deve essere redatta con un linguaggio semplice e chiaro e deve comporsi degli stessi elementi previsti per la notifica al Garante (vedi par. 7.1).

Essa non è richiesta nel caso in cui (art. 34, par. 3):

- il titolare del trattamento ha applicato ai dati oggetto di violazione adeguate misure di protezione tecniche ed organizzative, in particolare se ha utilizzato tecniche volte a rendere incomprensibili i dati ai non autorizzati (come già previsto dal Codice, art.32-bis);
- il titolare, a seguito della violazione, ha messo in atto tutte le misure adeguate a rimuovere i possibili rischi per i diritti e le libertà dell'interessato;
- la comunicazione in questione richiederebbe sforzi sproporzionati. In tal caso, è sufficiente predisporre una comunicazione pubblica mediante la quale gli interessati possano essere informati con equivalente efficacia.

Qualora il titolare del trattamento non comunichi la violazione all'interessato, il Garante - dopo aver valutato la probabilità che essa comporti rischi elevati per il soggetto interessato - può richiedere che avvenga la notifica o decidere che sia soddisfatta una delle condizioni per cui non è richiesta.

Sebbene il Regolamento non preveda un limite massimo di tempo entro il quale è necessario inoltrare all'interessato la comunicazione della violazione, per evitare ripercussioni, è sempre meglio trasmetterla contemporaneamente all'inoltro della notifica al Garante.

Codici di condotta e certificazione

Codici di condotta

Come già previsto dal Codice, è consigliata (quindi non obbligatoria) l'elaborazione di codici di condotta in modo da facilitare l'applicazione corretta del Regolamento (art. 40), tenendo conto delle caratteristiche specifiche dei trattamenti effettuati in alcuni settori particolari. Il ricorso a tali strumenti può risultare utile a calibrare gli obblighi dei titolari/responsabili del trattamento. Nell'elaborazione del codice, è raccomandabile consultare i soggetti coinvolti nelle attività di trattamento compresi, quando possibile, gli interessati. Se redatti, i codici di condotta devono essere sottoposti all'attenzione del Garante, che ha il compito di approvarli e sottoporli alla Commissione europea. Quest'ultima, una volta validati, deve darne adeguata pubblicità. Se l'attività dell'azienda è esercitata in più Stati membri, il controllo dev'essere effettuato rivolgendosi ad ogni autorità nazionale di controllo.

Il Regolamento prevede che, una volta adottato il codice di condotta, il titolare / responsabile del trattamento nomini un soggetto terzo (esterno all'azienda), indipendente ed in possesso del livello adeguato di competenze che vigili sul rispetto del codice. A questo soggetto, che necessita dell'accreditamento presso il Garante e presso il Comitato europeo per la protezione dei dati, è riconosciuta la possibilità di esercitare un controllo di conformità, di valutare la capacità dei titolari/responsabili del trattamento di applicare il codice, di controllare

periodicamente che esso venga rispettato e di istituire procedure per la gestione dei reclami relativi ad eventuali violazioni. In caso di violazione del codice da parte di un titolare / responsabile del trattamento, il soggetto accreditato per il controllo è chiamato ad adottare le misure adeguate, tra cui la sospensione o l'esclusione dal codice del titolare / responsabile del trattamento, comunicandole all'autorità di controllo. L'accreditamento del soggetto terzo può essere revocato dal Garante se le condizioni per l'accreditamento non sono più rispettate o se le misure adottate dallo stesso vìolino il Regolamento.

Certificazione

Il Regolamento incoraggia l'istituzione di meccanismi di certificazione, sigilli e marchi di protezione dei dati che dimostrino la conformità dei trattamenti effettuati al nuovo quadro giuridico e consentano agli interessati di valutare il livello di protezione dei dati garantito dall'azienda (art. 42). Tali certificazioni vengono raccolte, inserite in un registro e rese pubbliche dal Comitato europeo per la protezione dei dati.

La certificazione è volontaria e accessibile tramite procedura trasparente; non comporta la riduzione delle responsabilità dell'azienda (sia essa titolare o responsabile del trattamento) e non cambia i compiti delle autorità di controllo competenti. Meccanismi di certificazione possono essere adottati anche da parte di titolari/responsabili del trattamento non soggetti al Regolamento (art. 3) per agevolare trasferimenti di dati personali verso Paesi o organizzazioni internazionali; in questa maniera, tali soggetti assumono l'impegno di garantire le stesse condizioni previste dal Regolamento (anche per quanto riguarda i diritti degli interessati).

La certificazione è rilasciata da appositi organismi o dall'autorità di controllo competente (art. 43) cui il titolare / responsabile del trattamento fornisce tutte le informazioni necessarie per svolgere la procedura di certificazione, compreso l'accesso all'attività di trattamento. La certificazione viene rilasciata all'azienda per un periodo massimo di 3 anni e può essere rinnovata alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti, in caso contrario può anche essere revocata.

Gli organismi idonei a rilasciare e rinnovare la certificazione sono quelli in possesso di un livello adeguato di competenze in materia di protezione dei dati; essi, in ogni caso, operano in costante contatto con l'autorità di controllo. È necessario che tali organismi siano accreditati da uno o entrambi i seguenti enti:

- dal Garante *Privacy* (artt. 55-56);
- dall'organismo nazionale di accreditamento designato in virtù del Regolamento 765/2008/CE del Parlamento europeo e del Consiglio conformemente alla norma EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente (artt. 55-56).

L'azienda è tenuta a fornire all'ente certificatore tutte le informazioni necessarie per la valutazione; è quindi opportuno verificarne l'attendibilità presso il Garante prima di procedere con la richiesta della certificazione.

Trasferimento dei dati verso Paesi terzi e organismi internazionali

Il Regolamento affronta le sfide poste dall'aumento dei flussi di dati personali verso e da Paesi al di fuori dell'UE o verso e da organizzazioni

internazionali, con lo scopo di assicurare un livello di protezione adeguato a non causare il pregiudizio dei diritti fondamentali delle persone. L'approccio adottato è sostanzialmente conforme a quello previsto dalla Direttiva e dal Codice. Quando i dati vengono trasferiti da un Paese all'altro è necessario che il livello di tutela assicurato dal Regolamento non venga compromesso; ogni tipo di trasferimento può quindi essere effettuato solo nel pieno rispetto di esso. In generale, con il Regolamento viene meno il requisito dell'autorizzazione nazionale (art. 44 del Codice); il trasferimento verso un Paese terzo, salvo in alcune circostanze, potrà quindi avere inizio senza dover attendere l'autorizzazione del Garante. È tuttavia necessario che il trasferimento avvenga secondo una delle diverse modalità previste, sulla base di differenti presupposti.

Trasferimento sulla base di una decisione di adeguatezza

Come previsto dalla Direttiva, il trasferimento di dati personali verso un Paese terzo/organizzazione internazionale è ammesso se la Commissione ha deciso che il Paese / organizzazione in questione garantisce un livello di protezione adeguato; in tal caso il trasferimento non necessita di autorizzazioni specifiche (art. 45).

Nel valutare l'adeguatezza del livello di protezione, la Commissione prende in considerazione i seguenti elementi:

- lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale e la sua attuazione (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), le norme in materia di protezione dei dati, le norme professionali e le misure di sicurezza (comprese le norme per il trasferimento successivo dei dati personali verso un altro Paese terzo / organizzazione internazionale osservate nel Paese o

dall'organizzazione internazionale in questione), la giurisprudenza e i diritti effettivi e azionabili degli interessati;

- l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel Paese terzo o cui è soggetta un'organizzazione internazionale, con competenza a garantire e controllare il rispetto delle norme in materia di protezione dei dati;

- gli impegni internazionali assunti dal Paese terzo / organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti, in particolare in materia di protezione dei dati personali.

La Commissione decide dell'adeguatezza con un meccanismo di riesame periodico almeno ogni 4 anni. Se dalle informazioni disponibili risulta che un Paese terzo/organizzazione internazionale non garantisce più sufficienti livelli di protezione, la Commissione può revocare, modificare o sospendere la decisione di adeguatezza senza effetto retroattivo (art. 93). A seguito di tali decisioni, il trasferimento dei dati personali verso il Paese terzo/organizzazione è vietato a meno che non vengano nuovamente soddisfatti i requisiti espressi nel Regolamento.

L'elenco dei Paesi terzi / organizzazioni internazionali che la Commissione ritiene idonei a garantire un livello di protezione adeguato è pubblicato sulla Gazzetta ufficiale dell'UE e sul suo sito web. Le decisioni di adeguatezza adottate dalla Commissione e gli accordi internazionali in materia di trasferimento adottati dagli Stati membri prima del 24 maggio 2016 rimangono in vigore (fino ad eventuale revisione o modifica); restano quindi valide le autorizzazioni nazionali emesse fino ad ora dal Garante a seguito delle decisioni di adeguatezza della Commissione. Rimangono altresì valide le autorizzazioni rilasciate in questi anni dal Garante per i singoli casi specifici.

Trasferimento sulla base di garanzie adeguate

In mancanza di una decisione di adeguatezza, il titolare / responsabile del trattamento può trasferire comunque dati personali verso un Paese terzo/organizzazione internazionale solo assicurando agli interessati garanzie adeguate volte alla loro tutela (art. 46). Tali garanzie possono consistere in:

- accordi amministrativi tra autorità pubbliche (per cui è ancora necessaria l'autorizzazione del Garante);
- norme vincolanti d'impresa (art. 47, vedi par. 9.2.1);
- clausole adottate dalla Commissione o dal Garante e approvate dalla Commissione;
- adozione di codici di condotta o meccanismi di certificazione che disciplinano i trasferimenti (disposizione introdotta dal Regolamento);
- clausole contrattuali ad hoc tra parti interessate (non riconosciute come adeguate tramite decisione della Commissione, per cui è ancora necessaria l'autorizzazione del Garante).

Tali garanzie devono rispettare i requisiti in materia di protezione dei dati e assicurare agli interessati l'azionabilità dei diritti, l'effettività dei mezzi di ricorso (in sede amministrativa o giudiziale) e la possibilità di richiedere un risarcimento, nell'UE o in un Paese terzo.

Trasferimento sulla base di norme vincolanti d'impresa

Un gruppo imprenditoriale o un gruppo di imprese può applicare le norme vincolanti d'impresa (ossia norme interne vincolanti e riguardanti le modalità di trattamento dei dati) per i trasferimenti internazionali purché queste siano approvate dall'autorità Garante. L'approvazione delle norme vincolanti d'impresa deve avvenire

necessariamente attraverso il meccanismo di coerenza (artt. 63-65) prevedendo in ogni caso l'intervento del Comitato europeo per la protezione dei dati.

Il Regolamento fissa i requisiti per l'approvazione delle norme vincolanti d'impresa: essa, infatti, può avvenire se le norme sono giuridicamente vincolanti ed applicabili a tutte le parti, se contemplano tutti i princìpi fondamentali e se conferiscono diritti azionabili agli interessati in relazione al trattamento dei loro dati personali.

Inoltre, il Regolamento stabilisce i contenuti obbligatori delle norme vincolanti d'impresa; è necessario che esse specifichino almeno (art. 47):

- la struttura e le coordinate di contatto del gruppo imprenditoriale / gruppo di imprese e di ciascuno dei suoi membri;
- i trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e le relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del Paese terzo o dei Paesi terzi in questione;
- la loro natura giuridicamente vincolante, a livello sia interno che esterno;
- l'applicazione dei princìpi generali di protezione dei dati;
- i diritti dell'interessato in materia di trattamento, i mezzi per esercitarli e le procedure di reclamo;
- i profili di responsabilità del titolare / responsabile del trattamento stabilito nell'UE per qualunque violazione delle norme vincolanti d'impresa commessa da un membro del gruppo imprenditoriale non stabilito nell'UE. Il titolare / responsabile può essere esonerato da tale responsabilità (completamente o parzialmente) solo se dimostra la non imputabilità dell'evento dannoso al membro in questione;

- i compiti di qualunque DPO (o di ogni altro incaricato al controllo sul rispetto delle norme vincolanti d'impresa), i meccanismi adottati all'interno del gruppo imprenditoriale per garantire la verifica della conformità a tali norme e la formazione del personale che ha accesso i dati.

L'elenco, tuttavia, non è esaustivo; è dunque possibile che le autorità competenti, a seconda dei casi, prescrivano dei requisiti ulteriori.

Deroghe

Come già previsto dalla Direttiva, è possibile trasferire dati personali verso un Paese terzo / organizzazione internazionale, anche in caso di mancata decisione di adeguatezza o di garanzie adeguate (art. 49). Ciò è consentito se:

- l'interessato ha esplicitamente acconsentito al trasferimento proposto;
- il trasferimento è necessario all'esecuzione o alla conclusione di un contratto;
- il trasferimento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- il trasferimento è necessario per tutelare gli interessi vitali dell'interessato o di altre persone e l'interessato si trova nell'incapacità fisica o giuridica di prestare il proprio consenso;
- i dati sono trasferiti da pubblici registri; in questo caso, il trasferimento non può riguardare la totalità dei dati personali o intere categorie di dati. Quando il registro è destinato a essere consultato da persone aventi legittimo interesse, i dati possono essere trasmessi solo su loro richiesta o se ne sono i destinatari;

- il trasferimento è necessario per importanti motivi di interesse pubblico. In questo caso il Regolamento specifica che tali interessi devono essere riconosciuti dal diritto dell'UE o dal diritto dello Stato membro cui è soggetto il titolare del trattamento per cui non è più possibile far valere l'interesse pubblico dello Stato terzo ricevente. È opportuno tener presente che, in mancanza di una decisione di adeguatezza, il motivo d'interesse pubblico può essere altresì avanzato dall'UE o dagli Stati membri per fissare limiti al trasferimento di categorie specifiche di dati verso un paese terzo/organizzazione internazionale, previa comunicazione alla Commissione.

Se non fosse possibile basare il trasferimento sulle disposizioni indicate nei paragrafi precedenti e né applicare nessuna delle deroghe del presente paragrafo, il trasferimento di dati verso un Paese terzo / organizzazione internazionale potrebbe essere comunque autorizzato se è qualificabile come non ripetitivo e riguardante soltanto un numero limitato di interessati; se necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, sul quale non prevalgano gli interessi o i diritti e le libertà dell'interessato; qualora il titolare del trattamento abbia valutato tutte le circostanze relative al trasferimento (la natura dei dati personali, la finalità e la durata del trattamento o dei trattamenti proposti, la situazione nel Paese d'origine, nel Paese terzo e nel Paese di destinazione finale) e sulla base di tale valutazione abbia fornito garanzie adeguate per la protezione dati personali. In questo caso, il titolare del trattamento deve informare il Garante e l'interessato in merito al trasferimento.

Trasferimenti o comunicazioni non autorizzati

I trasferimenti di dati possono essere consentiti solo se ricorrono le condizioni espressamente previste dal Regolamento. Esso introduce il divieto di trasferimenti di dati effettuati sulla base di provvedimenti

come sentenze di un'autorità giurisdizionale o decisioni di un'autorità amministrativa di un Paese terzo, a meno che non siano in vigore accordi internazionali tra Paese terzo richiedente e UE o suo Stato membro (art. 48). In caso di trasferimenti non autorizzati, la protezione delle persone fisiche assicurata dall'UE potrebbe non essere garantita.

Mezzi di ricorso

Ogni qualvolta un interessato ritenga che il trattamento che lo riguarda sia stato effettuato in violazione del Regolamento ha il diritto di proporre reclamo all'autorità di controllo (al Garante italiano oppure all'autorità dello Stato in cui si è verificata la violazione) o all'autorità giurisdizionale.

Nel caso di reclamo all'autorità di controllo, l'autorità cui ci si appella ha il compito di informare il reclamante dello stato o dell'esito del reclamo nonché della possibilità di un ricorso giurisdizionale (art. 77).

Nel caso di ricorso all'autorità giurisdizionale, il ricorrente può avviare le azioni nei confronti del titolare / responsabile del trattamento dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare / responsabile del trattamento ha uno stabilimento o, in alternativa, in cui risiede l'interessato, salvo che il titolare / responsabile del trattamento sia un'autorità pubblica di uno Stato membro che agisce nell'esercizio dei suoi pubblici poteri (art. 79).

In ogni caso, qualsiasi persona fisica / giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo in merito ad una decisione giuridicamente vincolante che lo riguardi (art. 78) nei casi in cui l'autorità non dia seguito a un reclamo, lo respinga in tutto o in parte o lo archivi, non agisca quando è necessario intervenire per proteggere i diritti dell'interessato, non informi il soggetto entro 3 mesi dello stato o dell'esito del reclamo proposto.

Sanzioni

Il Regolamento uniforma ed inasprisce il regime sanzionatorio in tutti gli Stati membri; sono previste sanzioni amministrative pecuniarie sia in caso di violazione del Regolamento che in caso di data *breach*. Le sanzioni penali rimangono, invece, di competenza di ogni singolo Stato.

Il Garante assicura, in ogni specifico caso, che la sanzione stabilita sia effettiva, proporzionata e dissuasiva. Al momento di decidere se infliggere la sanzione amministrativa pecuniaria e fissarne l'ammontare, si tiene conto dei seguenti elementi (art. 83):

- la natura, la gravità e la durata della violazione anche in considerazione del numero degli interessati coinvolti e dei danni da essi subiti;
- il carattere doloso o colposo della violazione;
- le misure intraprese dal titolare / responsabile del trattamento per mitigare i danni subiti dagli interessati e il loro grado di responsabilità;
- eventuali rilevanti violazioni commesse precedentemente dal titolare / responsabile del trattamento;
- il livello di cooperazione con il Garante al fine di porre rimedio alla violazione ed attenuarne i possibili effetti negativi;
- le categorie di dati personali oggetto della violazione;
- la modalità in cui il Garante ha preso conoscenza della violazione e la modalità di notifica della stessa da parte del titolare / responsabile del trattamento;
- l'adesione ai codici di condotta o ai meccanismi di certificazione;
- altri eventuali fattori aggravanti o attenuanti.

Se il titolare / responsabile del trattamento commette una violazione di più disposizioni del Regolamento con dolo o colpa, l'importo totale della sanzione non dovrà superare l'importo indicato per la violazione più grave.

Sono soggette a sanzioni amministrative pecuniarie fino a 10 milioni di € o fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente se superiore, le violazioni delle norme circa:

- gli obblighi del titolare / responsabile del trattamento (artt. 8, 11, 25-39, 42 e 43);
- gli obblighi dell'organismo di certificazione (artt. 42 e 43);
- gli obblighi dell'organismo di controllo (art. 41, par. 4).

Sono soggette a sanzioni amministrative pecuniarie fino a 20 milioni di € o fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente se superiore, le violazioni delle norme circa:

- i princìpi di base del trattamento (artt. 5, 6, 7 e 9);
- i diritti degli interessati (artt. 12-22);
- i trasferimenti di dati personali a un destinatario in un Paese terzo / organizzazione internazionale (artt. 44-49);
- qualsiasi disposizione prevista dalle legislazioni degli Stati membri (capo IX);
- la mancata osservanza di un ordine, di una limitazione o di un provvedimento previsti dall'autorità di controllo (art. 58).

GDPR

Il nuovo regolamento privacy

Istruzioni per l'uso

Schede tecniche

CRTV LAB

LUISS

ROADMAP del GDPR nell'ordinamento italiano

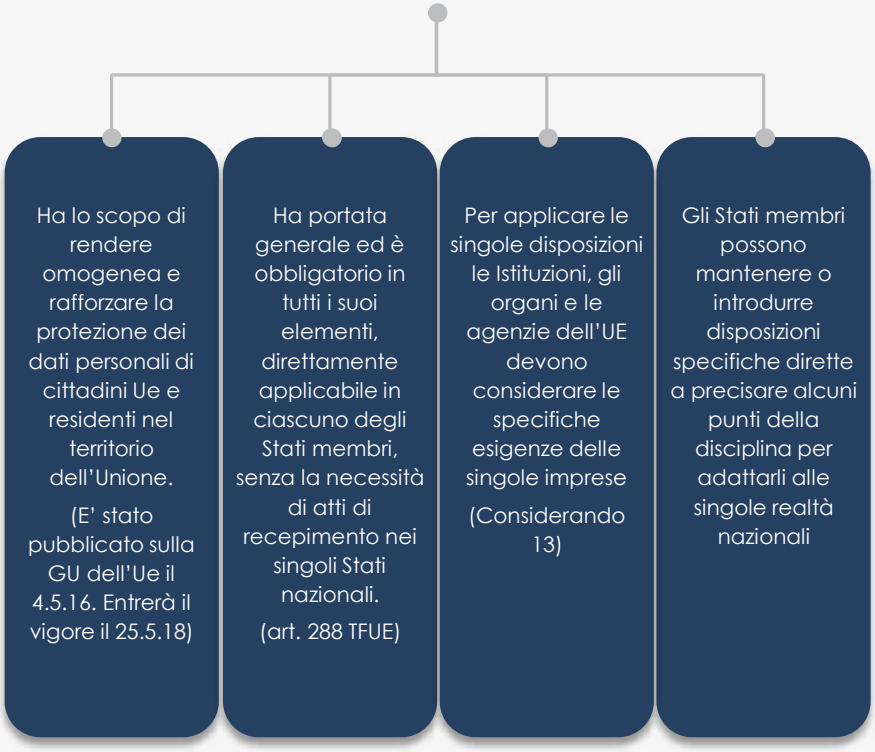
Avv. Annamaria La Cesa
(Normativa e Regolamentare, CRTV)

CRTV LAB

Le aree del GDPR

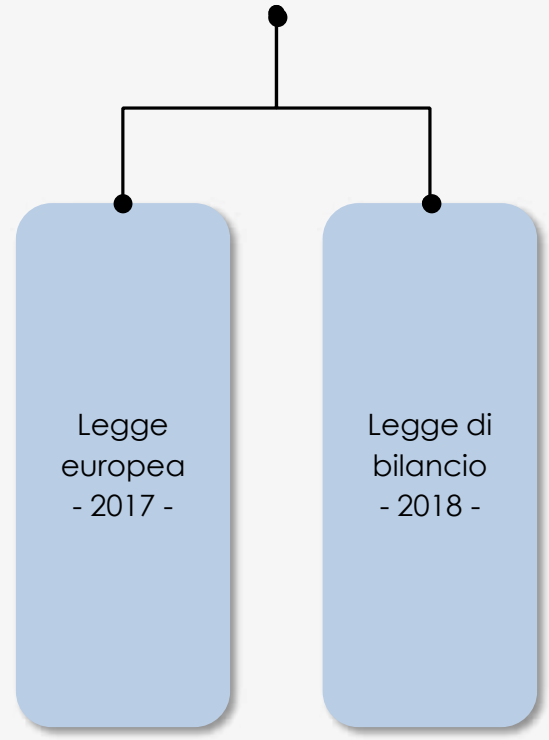
Obiettivi e portata

Regolamento sulla protezione dei dati

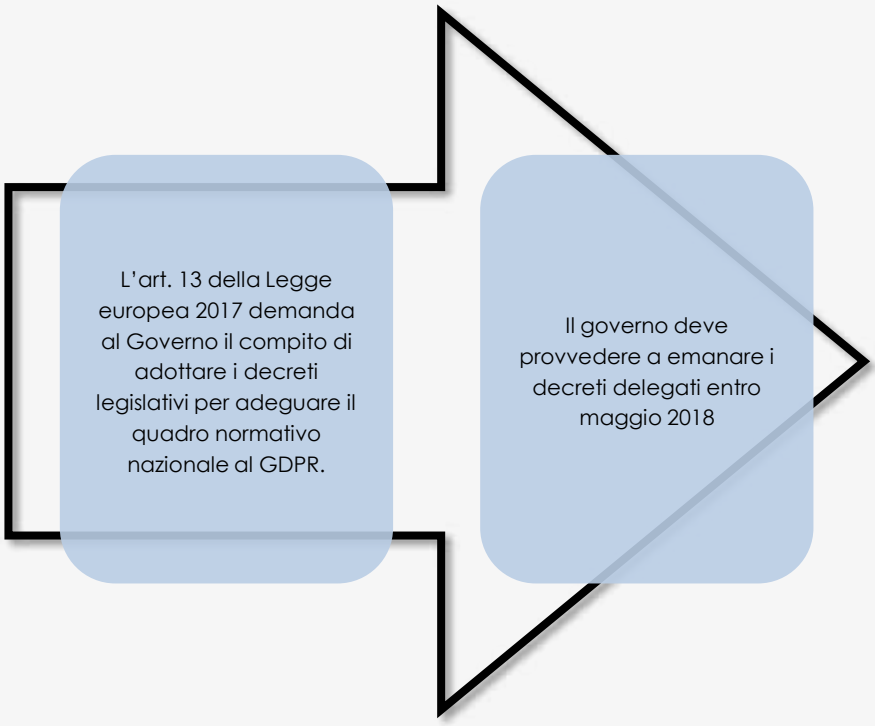


Attuazione

Norme italiane di attuazione



La legge europea 2017



I princìpi della delega

In base alla delega il Governo deve

- Abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, incompatibili con le disposizioni contenute nel Regolamento
- Modificare, se necessario, le norme del Codice Privacy non incompatibili con il regolamento
- Adeguare il sistema sanzionatorio penale e amministrativo vigente alle nuove disposizioni con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione
- Prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali

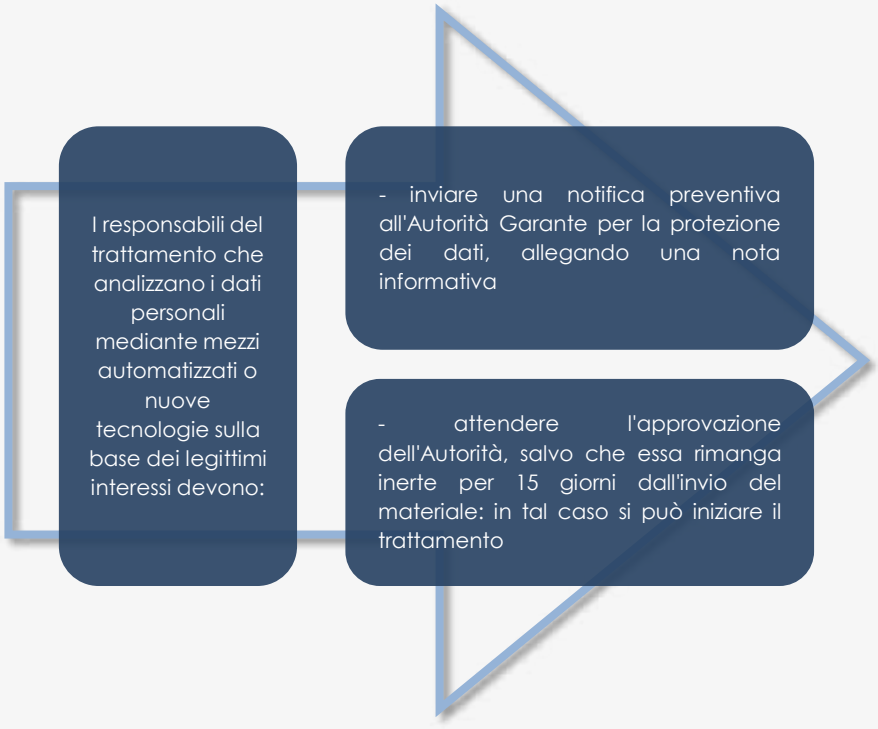
La legge di bilancio 2018

Legge di bilancio e Garante

Il Garante deve adottare un provvedimento per

- Disciplinare le modalità attraverso le quali il Garante stesso monitora l'applicazione del Regolamento GDPR e vigila sulla sua applicazione
- Predisporre un modello di informativa da compilare a cura dei titolari di dati personali che effettuano un trattamento fondato sull'interesse legittimo che prevede l'uso di nuove tecnologie o di strumenti automatizzati
- Disciplinare le modalità di verifica della presenza di adeguate infrastrutture per l'interoperabilità dei formati
- Definire linee-guida o buone prassi in materia di trattamento dei dati personali fondato sull' interesse legittimo del titolare

Legge di bilancio e interesse legittimo



Contenuti del Regolamento

Dott.ssa Michela Tresca
Dott.ssa Giulia Di Carlo
(@LawLAB LUISS)

LUISS

Titolare e responsabile del trattamento

Quando un'azienda è titolare del trattamento?

L'azienda è titolare del trattamento quando determina le finalità e i mezzi del trattamento dei dati personali. In questo caso, l'azienda deve prendere le misure adeguate a garantire la conformità del trattamento al Regolamento e deve essere in grado di dimostrarlo.

Quando un'azienda è responsabile del trattamento?

L'azienda è responsabile del trattamento quando tratta i dati per conto del titolare del trattamento.

Non è più espressamente prevista la figura dell'incaricato del trattamento, ma il titolare / responsabile può comunque autorizzare un altro soggetto al trattamento dei dati personali.

NOVITÁ

I titolari possono ricorrere alla **contitolarità del trattamento**, che richiede un accordo interno per definire in modo trasparente le rispettive responsabilità e funzioni dei contitolari, soprattutto con riferimento ai diritti degli interessati. Gli interessati possono rivolgersi indifferentemente a ognuno dei titolari.

L'**atto di designazione del responsabile** deve essere un contratto o altro atto giuridico conforme al diritto nazionale e deve contenere: la materia e la durata del trattamento, la natura e la finalità, il tipo di dati oggetto di trattamento, le categorie degli interessati, gli obblighi e i diritti del titolare del trattamento.

Sono previsti **obblighi specifici anche per il responsabile** (tra cui la redazione di un registro dei trattamenti; l'adozione di misure tecniche e organizzative di sicurezza; la designazione del DPO; la designazione di un rappresentante in Italia per titolari/responsabili non stabiliti nell'UE).

Il responsabile può nominare **sub-responsabili** per specifiche attività di trattamento rispondendo di eventuali inadempimenti.

Se il titolare/responsabile non è stabilito sul territorio dell'UE deve designare un **rappresentante** come interlocutore delle autorità di controllo e degli interessati. Se il trattamento è occasionale o effettuato da un'autorità/organismo pubblico questa figura non è necessaria.

Titolare e responsabile del trattamento

Quali sono le responsabilità dell'azienda titolare / responsabile?

Se l'azienda è titolare del trattamento risponde per danni causati da un trattamento effettuato in violazione del Regolamento.

Se l'azienda è responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto agli obblighi che il Regolamento le impone o se ha agito in modo differente o contrario rispetto alle istruzioni fornite dal titolare del trattamento.

L'azienda non è responsabile del danno se esso non le è imputabile in alcun modo.

Ogni azienda titolare / responsabile coinvolta nello stesso trattamento insieme ad altri titolari/responsabili, risponde in solido per l'intero ammontare del danno. Se un'azienda paga l'intero risarcimento, ha il diritto di reclamare dagli altri titolari/responsabili la parte di risarcimento corrispondente alla loro parte di responsabilità per il danno.

Ambito di applicazione

A quali aziende si applica il Regolamento?

All'azienda titolare/responsabile che ha uno stabilimento sul territorio dell'UE, anche se il trattamento è effettuato all'estero. All'azienda titolare/responsabile non stabilita sul territorio dell'UE ma stabilita in un luogo soggetto al diritto di uno Stato membro.

NOVITÁ

Il Regolamento si applica anche all'azienda titolare/responsabile non stabilita sul territorio dell'Ue che offre beni o servizi a soggetti presenti nell'UE o che monitora i loro comportamenti.
Se gli interessati non sono residenti nell'UE, il Regolamento si applica all'azienda titolare/responsabile del trattamento che ha uno stabilimento in UE e che effettua il trattamento nel territorio dell'UE.

Privacy by design, by default e valutazione d'impatto

Come garantire la privacy by default?

L'azienda deve trattare i dati solo se necessario per le finalità specifiche della loro raccolta. La raccolta e la conservazione dei dati deve limitarsi al raggiungimento delle finalità e al periodo di tempo necessario per fornire il bene o il servizio per cui il trattamento è stato effettuato.

NOVITÁ

Come garantire la privacy by design?

L'azienda deve garantire il rispetto della privacy sia nelle fasi di progettazione del sistema utilizzato per il trattamento che durante il trattamento. È l'azienda stessa a dover provare di aver adottato tutte le misure indispensabili per garantire la tutela della privacy dell'interessato.

Che cos'è la valutazione d'impatto sulla protezione dei dati?

È uno strumento introdotto dal Regolamento per valutare la necessità e la proporzionalità del trattamento, i rischi e le conseguenze che il trattamento potrebbe comportare.

In genere riguarda una singola operazione di trattamento, ma se più operazioni hanno rischi simili, questi possono essere valutati insieme.

L'azienda effettua la valutazione di impatto prima di procedere al trattamento; potrà quindi essere necessario aggiornarla una volta iniziato (ad esempio nel caso di variazione del rischio connesso al trattamento).

Privacy by design, by default e valutazione d'impatto

Quali sono i contenuti della valutazione d'impatto?

La valutazione deve contenere necessariamente almeno:

- la descrizione dei trattamenti e delle finalità;
- la valutazione della necessità e della proporzionalità del trattamento rispetto alle finalità;
- la valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste in caso di rischio;
- la prova della conformità del trattamento al Regolamento.

Quando è richiesta la valutazione d'impatto?

Quando il trattamento presenta elevati rischi per i diritti e le libertà degli interessati, ovvero in caso di:

- trattamento automatizzato che comporti una valutazione sistematica di aspetti personali degli interessati;
- trattamento su larga scala di dati sensibili e di dati relativi a condanne penali o a reati;
- sorveglianza sistematica e su larga scala di zona accessibile al pubblico.

Quando non è necessaria la valutazione d'impatto?

Quando i trattamenti sono imposti da un obbligo legale o dall'interesse pubblico (o comunque connessi all'esercizio di pubblici poteri).

Quando la valutazione è stata già effettuata per trattamenti simili e se ne possono riutilizzare i risultati.

Nell'eventualità in cui il Garante inserisca il trattamento in questione nella lista dei trattamenti che non richiedono valutazione d'impatto.

Privacy by design, by default e valutazione d'impatto

Cosa fare una volta effettuata la valutazione d'impatto?

Se dalla valutazione non emergono rischi connessi al trattamento:

L'azienda inizia il trattamento adottando tutte le misure necessarie per minimizzare i rischi.
L'azienda può consultare il Garante prima di iniziare il trattamento.

Se dalla valutazione emergono rischi elevati

L'azienda deve consultare il Garante

Se Consultazione preventiva

Con la consultazione preventiva il Garante indica le eventuali ed ulteriori misure che l'azienda deve adottare. In questo caso, l'azienda deve comunicare la valutazione d'impatto al Garante che, se necessario, può imporre misure correttive.

Se il Garante ritiene che il trattamento è in violazione del Regolamento, fornisce consulenza scritta entro 8 settimane, prorogabili fino a 6 in caso di trattamenti particolarmente complessi. In questo caso, l'azienda deve essere informata entro 1 mese dalla richiesta di consultazione.

La valutazione d'impatto riguarda i trattamenti di dati creati successivamente al mese di maggio 2018, o i casi in cui vi sia stato un cambiamento significativo nel trattamento.

Il Garante potrà redigere un elenco di trattamenti per cui è richiesta la valutazione d'impatto; si raccomanda quindi di tenersi aggiornati.

Anche quando la valutazione non è necessaria, è preferibile effettuarla.

Registro delle attività di trattamento

NOVITÁ

Che cos'è il registro delle attività di trattamento?

È uno strumento introdotto dal Regolamento indispensabile all'azienda per la valutazione e l'analisi dei rischi, per avere un quadro aggiornato dei trattamenti. Il registro è utile in caso di richieste da parte degli interessati (nell'esercizio dei loro diritti) e in caso di controlli da parte del Garante.

Il registro deve essere tenuto in forma scritta, su supporto cartaceo o elettronico.

Quando l'azienda è obbligata a tenere il registro?

Titolare / responsabile ha più di 250 dipendenti.

Al di là delle dimensioni dell'azienda:

- quando effettua trattamenti a rischio;
- quando tratta i dati in modo sistematico;
- quando tratta dati sensibili o dati relativi a condanne penali e a reati.

Registro delle attività di trattamento

Quali informazioni deve contenere il registro?

Se l'azienda è titolare del trattamento:

- nome e dati di contatto del titolare del trattamento e, se presenti, del contitolare del trattamento, del rappresentante del titolare e del DPO;
- finalità del trattamento;
- descrizione delle categorie di interessati e delle categorie dei dati personali;
- destinatari dei dati;
- trasferimenti di dati verso Paesi terzi / organizzazioni internazionali (se i dati sono presi da pubblici registri, allegare la documentazione delle garanzie adeguate per i trasferimenti);
- descrizione generale delle misure di sicurezza tecniche e organizzative adottate (eventuale).

Se l'azienda è responsabile del trattamento:

- nome e dati di contatto del responsabile del trattamento, di ogni titolare per conto del quale agisce il responsabile, del rappresentante del titolare o del responsabile e, se presente, del DPO;
- categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- trasferimenti di dati verso Paesi terzi / organizzazioni internazionali (se i dati sono presi da pubblici registri, allegare la documentazione delle garanzie adeguate per i trasferimenti);
- descrizione generale delle misure di sicurezza tecniche e organizzative adottate (eventuale).

Il Garante sta valutando l'opportunità di predisporre sul proprio sito un modello di registro dei trattamenti, che le aziende potranno integrare nei modi opportuni.

Responsabile della protezione dei dati (DPO)

NOVITÁ

Chi è il DPO?

È una nuova figura introdotta dal Regolamento per facilitare l'attuazione e il rispetto del nuovo quadro normativo. È un interlocutore all'interno della struttura aziendale, un punto di contatto per il Garante e per gli interessati.

Quando l'azienda deve nominare il DPO?

La nomina del DPO è obbligatoria quando l'azienda (titolare / responsabile) svolge come attività principale:

- un monitoraggio regolare e sistematico su larga scala;
- un trattamento su larga scala di dati sensibili o di dati relativi a condanne penali o a reati.

I gruppi di imprese possono nominare un solo DPO che deve essere raggiungibile da tutti gli stabilimenti.

I dati di contatto del DPO devono essere pubblicati e comunicati al Garante.

Deve essere **indipendente** (fa riferimento diretto al vertice dell'azienda), deve avere una conoscenza specialistica in materia di protezione dei dati e del settore di attività specifico dell'azienda.

Può essere un dipendente **interno** all'azienda o un consulente **esterno**, nominato sulla base di un contratto di servizi.

Non è responsabile per inosservanza del Regolamento, è sempre l'azienda a risponderne.

Responsabile della protezione dei dati (DPO)

Quali compiti ha il DPO?

- fornisce consulenza e informazioni all'azienda titolare/responsabile e ai dipendenti impegnati nel trattamento dei dati;
- controlla la conformità al Regolamento delle attività di trattamento;
- fornisce parere, se richiesto, sulla valutazione di impatto e ne segue lo svolgimento;
- coopera con il Garante;
- può essere contattato dagli interessati per qualsiasi questione relativa al trattamento e all'esercizio dei loro diritti.

Anche nei casi in cui la nomina del DPO non è obbligatoria, è sempre meglio nominare tale figura.
Sono in corso di definizione dei meccanismi di certificazione che consentiranno alle aziende di provare il livello di competenza, indipendenza e professionalità del DPO.

Consenso

Per poter trattare i dati personali, l'azienda deve ricevere il consenso dell'interessato. Il consenso deve essere libero, specifico, informato e inequivocabile; non è ammesso il consenso tacito o presunto.

NOVITÁ

La richiesta deve essere comprensibile e facilmente accessibile, deve essere utilizzato un linguaggio semplice e chiaro. Non è richiesta la forma scritta né la sua documentazione per iscritto.

La richiesta di consenso deve essere facilmente distinguibile se è inserita in un modello scritto insieme ad altre richieste.

Per i dati sensibili e i trattamenti automatizzati il consenso deve essere esplicito.

Se l'azienda è titolare del trattamento deve dimostrare che l'interessato ha prestato il suo consenso per lo specifico trattamento.

Nell'ambito dei servizi della società dell'informazione, il consenso dei minori è valido a partire dai 16 anni; prima di tale età è necessario il consenso del genitore o di chi ne fa le veci.

Anche se non è richiesta espressamente, la forma scritta è comunque la modalità più idonea a garantire che il consenso sia inequivocabile e, per i dati sensibili, esplicito.

Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche richieste dal Regolamento. In caso contrario, è opportuno che l'azienda provveda prima di tale data a raccogliere nuovamente il consenso.

Informazioni e comunicazioni all'interessato: Informativa

NOVITÁ

Tutte le informazioni e le comunicazioni all'interessato devono essere concise, trasparenti, facilmente comprensibili e accessibili, scritte con un linguaggio semplice e chiaro. Per facilitare la comprensione, si possono usare icone standardizzate.

Se il trattamento riguarda i minori, le informazioni devono essere date con un linguaggio adeguato.

Le informazioni sono date per iscritto e, se possibile, in formato elettronico. Solo se richiesto dall'interessato possono essere date oralmente, dopo che l'azienda titolare ha accertato la sua identità.

Esiste un termine per fornire l'informativa?

Se i dati sono ottenuti direttamente dall'interessato, l'informativa deve essere fornita prima di iniziare la raccolta dei dati.

Se i dati sono raccolti da altra fonte, l'informativa all'interessato deve comunque essere fornita entro un termine ragionevole (non oltre 1 mese dalla raccolta), oppure al momento della comunicazione dei dati (e non più al momento della loro registrazione).

In ogni caso, se i dati sono comunicati ad altro destinatario, l'interessato deve esserne informato dal momento della comunicazione.

Quando l'azienda non è tenuta a dare l'informativa?

Per i dati ottenuti direttamente dall'interessato, l'obbligo non sussiste quando l'interessato già dispone delle informazioni.

Per i dati raccolti da altra fonte, l'obbligo non sussiste quando:

- la registrazione o la comunicazione dei dati sono previste per legge;
- informare l'interessato è impossibile o richiede sforzo sproporzionato;
- i dati devono rimanere riservati nel rispetto di un obbligo legale di segreto professionale.

Informazioni e comunicazioni all'interessato: Informativa

Cosa deve contenere l'informativa?

Quando fornisce l'informativa, l'azienda titolare deve ***necessariamente*** indicare:

- i dati di contatto del titolare del trattamento (se presente anche del suo rappresentante) e del DPO;
- le finalità e la base giuridica del trattamento;
- l'interesse legittimo del titolare, se è la base giuridica del trattamento (informazione non obbligatoria se i dati non sono ottenuti dall'interessato);
- gli eventuali destinatari dei dati personali;
- l'eventuale intenzione di trasferire i dati all'estero insieme all'indicazione della decisione di adeguatezza (se questa è alla base del trasferimento) o all'indicazione delle garanzie / mezzi per avere una copia dei dati (se il trasferimento si basa su garanzie adeguate o deroghe).

In aggiunta, per garantire un trattamento corretto e trasparente l'azienda titolare deve indicare:

- il periodo di conservazione dei dati o i criteri seguiti per stabilirlo;
- i diritti dell'interessato;
- la possibilità di revocare il consenso;
- il diritto di presentare un reclamo al Garante;
- se il trattamento comporta processi decisionali automatizzati (ad es. la profilazione);
- se l'interessato ha l'obbligo di fornire i dati, la base di tale obbligo (legale / contrattuale) e le eventuali conseguenze in caso di mancata comunicazione.

È opportuno che le aziende titolari verifichino che le informative attualmente utilizzate rispondano ai criteri previsti dal Regolamento (in particolare per i contenuti obbligatori e le modalità di redazione) e se necessario, che le modifichino o integrino entro il 25 maggio 2018.

La Commissione europea sta definendo le caratteristiche delle icone che devono essere uguali in tutta l'UE. In attesa di esse, si consiglia di continuare o iniziare ad utilizzare quelle suggerite in questi anni dal Garante.

Diritti dell'interessato

L'azienda titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) idonea. È l'azienda titolare a dare riscontro in caso di esercizio dei diritti da parte dell'interessato, mentre l'azienda responsabile è tenuta a collaborare.

Anche se, in linea generale, l'esercizio dei diritti rimane gratuito, l'azienda titolare può richiedere e stabilire l'ammontare di un contributo spese all'interessato quando le richieste sono manifestamente infondate, eccessive o ripetitive.

NOVITÁ

Come dare riscontro all'interessato?

Qualsiasi riscontro all'interessato deve avere forma scritta, se possibile in formato elettronico. Solo se richiesto dall'interessato può essere dato oralmente, dopo che l'azienda titolare ha accertato la sua identità.

La risposta fornita all'interessato deve essere concisa, trasparente, facilmente comprensibile e accessibile, scritta con un linguaggio semplice e chiaro. Per facilitare la comprensione si possono usare icone standardizzate.

Quando dare riscontro all'interessato?

Il termine per la risposta alle richieste dell'interessato è di 1 mese, con possibile proroga di 2 mesi in caso di difficoltà nell'adempimento.

Il ritardo e il diniego devono comunque essere comunicati e motivati all'interessato entro un 1 mese dalla richiesta.

Diritti dell'interessato

Il Regolamento introduce nuovi diritti per l'interessato e novità per i diritti già riconosciuti

Diritto di accesso

L'interessato ha il diritto di richiedere all'azienda titolare del trattamento l'accesso ai dati personali che lo riguardano e le seguenti informazioni:

- le finalità del trattamento;
- eventuali destinatari dei dati;
- i diritti che può esercitare;
- il diritto di proporre reclamo al Garante;
- eventuali trattamenti automatizzati effettuati e le possibili conseguenze;
- *il periodo della conservazione dei dati o almeno i criteri usati per determinarlo;*
- *le garanzie in caso di trasferimento dei dati all'estero.*

Non c'è più l'obbligo di comunicare le modalità del trattamento.

L'azienda deve in ogni caso fornire all'interessato una copia dei dati personali oggetto di trattamento.

Per facilitare l'accesso, l'azienda deve consentire all'interessato di consultare direttamente i propri dati tramite l'accesso remoto a un sistema sicuro.

Diritto alla limitazione del trattamento

Il diritto alla limitazione del trattamento amplia il vecchio diritto al blocco del trattamento.

Quando l'interessato può richiedere all'azienda la

limitazione del trattamento?

- in caso di trattamento illecito (in alternativa alla cancellazione);
- *quando richiede la rettifica dei dati, come garanzia ulteriore durante il periodo necessario all'azienda per aggiornarli;*
- *quando i dati personali sono necessari per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.*

Diritti dell'interessato

NOVITÁ

Diritto alla portabilità dei dati

L'interessato ha il diritto di:

- **ricevere** i dati che ha fornito all'azienda titolare in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile;
- **trasmettere** i dati già forniti a un'azienda titolare ad altre aziende titolari. L'azienda titolare deve quindi essere in grado di trasferire direttamente i dati portabili ad altre aziende titolari indicate dall'interessato, se tecnicamente possibile.

Quali responsabilità ha l'azienda titolare che dà seguito a una richiesta di portabilità?

L'azienda non è responsabile del trattamento effettuato dall'interessato o da altra azienda che riceve i dati.

Attenzione! Prima della trasmissione, le aziende che danno seguito a una richiesta di portabilità non hanno l'obbligo di verificare la qualità dei dati perché questi dovrebbero già essere conservati in modo conforme al Regolamento.

Quando l'interessato può richiedere all'azienda la portabilità dei dati?

- quando i dati personali sono forniti con il consenso dell'interessato;
- quando il trattamento è necessario per l'esecuzione di un contratto;
- quando il trattamento è effettuato con mezzi automatizzati (non si applica quindi ad archivi o registri cartacei).

NOVITÁ

Diritto all'oblio

Il diritto alla cancellazione è ampliato nella forma del diritto all'oblio.

Quando l'interessato può richiedere all'azienda il diritto all'oblio?

- quando i dati non sono più necessari rispetto alle finalità della raccolta;
- quando l'interessato revoca il proprio consenso o si oppone al trattamento;
- quando il trattamento è illecito e non conforme al Regolamento.

Quando l'interessato non può richiedere all'azienda il diritto all'oblio?

Quando il trattamento dei dati è necessario:

- per esercitare il diritto alla libertà di espressione e di informazione;
- per adempiere un obbligo legale;
- per eseguire un compito di interesse pubblico o per l'esercizio di poteri pubblici;
- per motivi d'interesse pubblico nella sanità pubblica;
- per fini di archiviazione o statistici, di ricerca scientifica o storica;
- per accertare, esercitare o difendere un diritto in sede giudiziaria.

Attenzione! A seguito di una richiesta di oblio, l'azienda titolare non è solo obbligata a cancellare i dati ma è anche tenuta a richiedere agli altri titolari che li trattano di rimuoverne qualsiasi link, copia o riproduzione.

FOCUS: Diritto all'oblio sul materiale audiovisivo

Il Regolamento non specifica la tipologia di dati personali che possono essere rimossi in seguito a una richiesta di oblio da parte dell'interessato.

L'art. 85, tuttavia, prevede che per i dati personali utilizzati per scopi giornalistici, e in particolare per il settore audiovisivo, archivi stampa e emeroteche, siano ammesse deroghe alla disciplina con riferimento alle disposizioni riguardanti, tra le altre, i diritti dell'interessato (e quindi anche il diritto all'oblio).

Tale previsione è volta, in particolare, a conciliare le norme sulla libertà di espressione e di informazione con il diritto alla protezione dei dati personali.

Alla luce della normativa vigente, va riconosciuta, quindi, l'estensione del diritto all'oblio anche rispetto ai contenuti audiovisivi.

In questo caso tuttavia, data anche la peculiarità del mezzo radio-televisivo rispetto a quello telematico, bisognerà effettuare una verifica ancor più stringente sulla proporzionalità tra l'interesse sotteso all'esercizio del diritto all'oblio e il costo complessivo che l'azienda deve sostenere per la rimozione, ferma restando la ricorrenza delle condizioni previste dal Regolamento, vale a dire: i dati non sono più necessari rispetto alla finalità della raccolta; l'interessato revoca il consenso o si oppone al trattamento; il trattamento è illecito o non conforme al Regolamento; la cancellazione è necessaria per adempiere un obbligo previsto dal diritto dell'Unione o dello Stato membro; i dati sono stati raccolti relativamente all'offerta di servizi della società dell'informazione a seguito del consenso prestato dal minore (se di età pari o superiore a 16 anni) o dal titolare della responsabilità genitoriale (se di età inferiore).

Sicurezza e violazione dei dati

Cosa fare in caso di violazione dei dati?

L'azienda titolare del trattamento potrebbe dover presentare:

1) Notifica al Garante

È generalmente facoltativa. L'azienda titolare è obbligata a notificare la violazione al Garante solo se comporta un rischio elevato per i diritti e le libertà dell'interessato.

Deve avvenire entro 72 ore dalla conoscenza della violazione, altrimenti è necessario motivare il ritardo.

Deve contenere:

- la descrizione della violazione e delle probabili conseguenze;
- il numero approssimativo dei soggetti interessati;
- il nome e il contatto del DPO o di altro riferimento;
- le misure adottate / adottabili dall'azienda per fronteggiare la violazione.

In ogni caso, a prescindere dalla notifica al Garante, l'azienda titolare deve documentare le violazioni. Queste informazioni potranno essere necessarie in caso di accertamenti da parte dell'autorità.

2) Comunicazione all'interessato

L'azienda titolare è obbligata a comunicare la violazione all'interessato solo se comporta un rischio elevato per suoi i diritti e le sue libertà. Non è richiesta nel caso in cui:

- l'azienda titolare ha applicato misure di protezione tecniche ed organizzative adeguate;
- l'azienda titolare, dopo la violazione, ha applicato tutte le misure adeguate a rimuovere i rischi per i diritti e le libertà dell'interessato;
- la comunicazione richiede sforzi sproporzionati; in questo caso è sufficiente una comunicazione pubblica.

L'azienda titolare deve comunicare la violazione all'interessato con un linguaggio semplice e chiaro.
I contenuti sono gli stessi della notifica al Garante. In caso di mancata notifica all'interessato, il Garante, se necessario, può richiedere all'azienda titolare di effettuarla. Non sono stabiliti i tempi per la comunicazione all'interessato, ma si consiglia di effettuarla contemporaneamente alla notifica al Garante.

FOCUS: Profilazione

Quando si può procedere ad attività di profilazione?

In generale, l'utente ha diritto a non essere sottoposto ad attività che comprendono la profilazione basate esclusivamente su processi automatizzati e con effetti giuridici che lo riguardano (ad es. nel caso in cui sia compromesso il godimento di alcuni diritti) o con effetti che comunque incidano significativamente sulla sua persona. L'attività di profilazione è ammessa nel caso in cui:

- sia necessaria al fine della conclusione o esecuzione di un contratto tra titolare del trattamento e interessato;
- sia autorizzata dal diritto dell'Unione o dello Stato membro;
- si basi sul consenso esplicito dell'interessato.

Anche in questi casi, tuttavia, il titolare del trattamento deve comunque applicare tutte le misure per assicurare la tutela dei diritti dell'interessato e per garantire almeno il diritto ad ottenere l'intervento umano da parte del titolare del trattamento e il diritto ad esprimere la propria opinione o a contestare la decisione. Le decisioni automatizzate che includono particolari categorie di dati (sensibili e super-sensibili) sono ammesse solo a certe condizioni:

- consenso esplicito da parte dell'utente;
- il trattamento è necessario per ragioni di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri.

Quali princìpi si applicano?

Per le attività di profilazione valgono i princìpi applicabili al trattamento di dati personali (liceità, correttezza e trasparenza nel trattamento; finalità determinate, esplicite e legittime della raccolta; adeguatezza, pertinenza e principio della minimizzazione dei dati, conservazione in una forma che consenta l'identificazione dell'interessato per un tempo non superiore al conseguimento delle finalità; garanzie di sicurezza dei dati) e princìpi di liceità del trattamento (consenso; trattamento necessario per l'esecuzione di un contratto, per adempiere un obbligo legale, per la salvaguardia degli interessi dell'utente, per l'esecuzione di un compito di interesse pubblico, per il legittimo interesse dell'azienda titolare).

FOCUS: Profilazione

Quali sono gli oneri in capo all'azienda titolare del trattamento che effettua attività di profilazione?

L'azienda titolare del trattamento deve:

- utilizzare procedure matematiche o statistiche appropriate e mettere in atto misure tecniche e organizzative adeguate in modo da correggere fattori che comportano inesattezze dei dati e minimizzare il rischio di errori;
- indicare nell'informativa la sussistenza di un'attività di profilazione (a prescindere dal fatto che i dati siano stati ottenuti o meno presso l'interessato). In particolare, l'utente dovrebbe essere informato sulla logica utilizzata e sulla importanza e le conseguenza previste da tale trattamento;
- effettuare la valutazione di impatto sulla protezione dei dati prima dell'inizio del trattamento;
- specificare nelle norme vincolanti di impresa la sussistenza di attività di profilazione.

Quali diritti sono riconosciuti all'utente sottoposto a profilazione?

- diritto di accesso: diritto ad ottenere dall'azienda titolare la conferma che sia o meno in atto un trattamento dei suoi dati personali e ad essere informato se all'interno di questo vi sia un processo di profilazione;
- diritto di opposizione: diritto ad opporsi in qualsiasi momento alla profilazione, anche connessa a finalità di marketing diretto;

A prescindere dai diritti che si riferiscono espressamente anche alla profilazione, l'utente gode di tutti gli altri diritti riconosciuti in capo all'interessato (diritto di rettifica, diritto all'oblio, diritto di limitazione di trattamento).

Il Regolamento demanda al Comitato europeo per la protezione dei dati di provvedere alla pubblicazione di Linee Guida e di raccomandazioni per specificare i criteri e le condizioni delle decisioni basate sulla profilazione.

A tal proposito, il Gruppo art. 29 ha redatto delle Linee guida: WP 251, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.

Trasferimenti dei dati

Quando l'azienda può trasferire dati verso Paesi terzi o organismi internazionali?

A) Quando c'è una decisione di adeguatezza da parte della Commissione europea.
In questo caso non è necessaria alcuna autorizzazione specifica.

B) In presenza di garanzie adeguate, che possono essere:

- accordi amministrativi tra autorità pubbliche
- clausole contrattuali ad hoc tra parti interessate
- norme vincolanti d'impresa

→ è ancora necessaria l'autorizzazione del Garante

- clausole adottate dalla Commissione o dal Garante ed approvate dalla Commissione
- adozione di codici di condotta o meccanismi di certificazione che disciplinano i trasferimenti.

→ Non è più necessaria l'autorizzazione del Garante

È opportuno che le aziende titolari verifichino che le informative attualmente utilizzate rispondano ai criteri previsti dal Regolamento (in particolare per i contenuti obbligatori e le modalità di redazione) e se necessario, che le modifichino o integrino entro il 25 maggio 2018.

La Commissione europea sta definendo le caratteristiche delle icone che devono essere uguali in tutta l'UE. In attesa di esse, si consiglia di continuare o iniziare ad utilizzare quelle suggerite in questi anni dal Garante.

Trasferimenti dei dati

È possibile trasferire i dati anche in mancanza di decisione di adeguatezza o di garanzie adeguate?

Sì, nel caso in cui:

- l'interessato acconsente esplicitamente al trasferimento proposto;
- il trasferimento è necessario all'esecuzione/conclusione di un contratto;
- il trasferimento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- il trasferimento è necessario per tutelare gli interessi vitali dell'interessato/di altre persone e l'interessato si trova nell'incapacità fisica o giuridica di prestare il proprio consenso;
- il trasferimento riguarda dati presi da pubblici registri dai quali non è però possibile trasferire la totalità dei dati o intere categorie di dati. Se il registro è consultabile da persone aventi legittimo interesse, i dati possono essere trasmessi solo su loro richiesta o se ne sono destinatari;
- il trasferimento è necessario per importanti motivi di interesse pubblico.

Non è possibile far valere l'interesse pubblico dello Stato terzo ricevente.

Pur in assenza di questi requisiti, il trasferimento può comunque essere effettuato se:

- non è ripetitivo;
- riguarda un numero limitato di interessati;
- è necessario per il perseguimento di interessi legittimi dell'azienda titolare prevalenti su interessi, diritti o libertà dell'interessato;
- se l'azienda titolare, valutate le circostanze del trasferimento, ha dato garanzia adeguata per la protezione dei dati; in questo caso, l'azienda deve informare il Garante e l'interessato del trasferimento.

*Sono **vietati** i trasferimenti effettuati sulla base di decisioni di un Paese terzo (es. sentenze, provvedimenti), a meno che non siano in vigore accordi internazionali tra il Paese terzo e UE o suo Stato membro.*

FOCUS: Norme vincolanti d'impresa

Le norme vincolanti d'impresa devono essere approvate dal Garante.

NOVITÁ

Quali sono i requisiti per l'approvazione?

Esse devono:

- essere giuridicamente vincolanti ed applicabili a tutte le parti;
- riconoscere tutti i princìpi fondamentali;
- conferire diritti azionabili agli interessati.

Quali informazioni devono contenere?

Le norme vincolanti d'impresa devono necessariamente specificare:

- la struttura e le coordinate di contatto del gruppo imprenditoriale / gruppo di imprese e di ciascun membro;
- i trasferimenti di dati (categorie di dati personali, tipo di trattamento e finalità, interessati cui si riferiscono, identificazione del Paese terzo destinatario);
- la natura giuridicamente vincolante delle norme (a livello sia interno che esterno);
- l'applicazione dei princìpi generali di protezione dei dati;
- i diritti dell'interessato, i mezzi per esercitarli e le procedure di reclamo;
- le responsabilità dell'azienda titolare/responsabile del trattamento stabilita in UE per violazioni delle norme vincolanti d'impresa commesse da un'azienda parte del gruppo imprenditoriale non stabilita nell'UE. La responsabilità non sussiste solo se è dimostrata la non imputabilità dell'evento dannoso all'azienda estera;
- i compiti di ogni DPO (o altro incaricato al controllo sul rispetto delle norme vincolanti d'impresa), le garanzie di conformità alle norme e la formazione del personale che accede ai dati.

L'elenco non è esaustivo, potranno essere prescritti requisiti ulteriori.

Sanzioni

Il Regolamento specifica e inasprisce le sanzioni amministrative nei confronti delle aziende titolari/responsabili.

Quando l'azienda è soggetta a sanzioni?

L'azienda è soggetta a sanzioni amministrative pecuniarie fino a 10 milioni di Euro o fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore), per violazione delle norme su:

- obblighi del titolare/responsabile del trattamento;
- obblighi dell'organismo di certificazione;
- obblighi dell'organismo di controllo.

L'azienda è soggetta a sanzioni amministrative pecuniarie fino a 20 milioni di Euro o fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore), per violazione delle norme su:

- princìpi di base del trattamento;
- diritti degli interessati;
- trasferimenti di dati personali a un destinatario in un Paese terzo/organizzazione internazionale;
- qualsiasi disposizione prevista dalle legislazioni degli Stati membri;
- mancata osservanza di un ordine, di una limitazione o di un provvedimento previsti dal Garante.

Se l'azienda titolare / responsabile del trattamento vìola più disposizioni del Regolamento con dolo o colpa, l'importo totale della sanzione non supera l'importo indicato per la violazione più grave.

FOCUS: Trattamento dei dati del personale

In linea generale, al trattamento dei dati nell'ambito del rapporto di lavoro si applicano le disposizioni del Regolamento sul trattamento dei dati personali.

Che cosa prevede nello specifico il Regolamento?

Il Regolamento rinvia a leggi o contratti collettivi a livello nazionale (compresi gli accordi aziendali) per la previsione di norme specifiche sul trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro e, in particolare, sulla determinazione delle condizioni alle quali tali dati possono essere trattati con il consenso dei dipendenti.

Nel caso in cui lo Stato membro adotti tali norme è tenuto a notificarlo alla Commissione europea.

Quale disciplina è prevista in Italia?

Il **Codice privacy** contiene una disciplina sulla corretta gestione dei dati personali all'interno dell'azienda (art. 111 ss.).

Tra le previsioni:

- promozione da parte del Garante della sottoscrizione anche per i soggetti privati (oltre che pubblici) di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per la gestione del rapporto di lavoro;
- rinvio alle norme dello Statuto dei lavoratori (l. 300/1970) per la raccolta dei dati sui prestatori di lavoro e per il controllo a distanza del lavoratore.

FOCUS: Trattamento dei dati del personale

Lo **Statuto dei lavoratori**, così come da ultimo modificato (d.lgs. n. 151/2015 - Jobs Act), prevede:

- possibilità, da parte del datore di lavoro, per tutti i fini connessi al rapporto di lavoro (compresi motivi disciplinari) e purché venga rispettato il Codice privacy e venga informato il dipendente sulle modalità d'uso e di effettuazione dei controlli, di utilizzare:

  a) dati raccolti tramite impianti audiovisivi o di altri strumenti di controllo (impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e istallati previo accordo collettivo o, in assenza, previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro);

  b) dati raccolti tramite "strumenti di lavoro" (vale a dire strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa).

  Qualsiasi attività di controllo sui lavoratori deve quindi essere effettuata in conformità alla normativa in materia di privacy.

- divieto di indagini sulle opinioni dei lavoratori e su fatti non rilevanti per la valutazione dell'attitudine professionale del lavoratore (sia ai fini dell'assunzione che nel corso dello svolgimento del rapporto di lavoro).

Sulla nozione di "strumenti di lavoro" è intervenuto il Garante privacy (Provvedimento 13 luglio 2016); in essa si considerano rientranti solo strumenti strettamente funzionali alla prestazione lavorativa e, tra questi, sicuramente l'account e-mail in uso del dipendente e gli altri servizi della rete aziendale (tra cui il collegamento ai siti Internet). Sono, inoltre, ritenuti parte integrante di tali strumenti anche i sistemi e le misure che ne consentano il funzionamento e ne garantiscono la sicurezza (ad es. sistemi di logging per il servizio di posta elettronica; sistemi di filtraggio anti-virus).

Sull'accesso alla posta elettronica dei dipendenti è inoltre intervenuto il Garante con Provvedimento 22 dicembre 2016.

FOCUS: Trattamento dei dati del personale

Il **Garante privacy** ha dettato Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati (Deliberazione n. 53 del 23 novembre 2006). Principali previsioni:

- per i dati che l'azienda tratta (sia dati anagrafici, biometrici e sensibili del lavoratore che dati più strettamente connessi all'attività lavorativa) valgono tutti i princìpi alla base del trattamento dei dati personali (liceità, proporzionalità, minimizzazione ecc.);
- il trattamento dei dati personali riferibili a singoli lavoratori, anche sensibili, è lecito, se finalizzato ad assolvere obblighi derivanti dal contratto individuale; altri scopi possono essere previsti dalla contrattazione collettiva o dalla legge; in ogni caso deve essere rispettato il principio della compatibilità degli scopi perseguiti con quelli per i quali i dati sono stati raccolti;
- prima del trattamento, il datore di lavoro è tenuto a fornire al lavoratore dipendente un'informativa individualizzata e deve garantire tutte le misure di sicurezza volte a tutelare i dati di cui dispone;
- il lavoratore gode di una serie di diritti (tra cui: diritto di accesso, diritto di riscontro da parte del datore di lavoro, diritto all'aggiornamento dei dati);
- previsioni specifiche sono previste per i dati biometrici;
- il datore di lavoro per poter comunicare i dati dei dipendenti a terzi deve aver acquisito il consenso, a meno che non si tratti di dati in forma anonima (consenso necessario anche per pubblicare i dati nella intranet aziendale). La diffusione dei dati è ammessa solo se necessaria per dare esecuzione a obblighi che derivano dal contratto di lavoro. Il datore di lavoro deve, ove possibile, utilizzare forme di comunicazione individualizzata con il lavoratore. Per i dati sensibili (nello specifico i dati sanitari) devono essere utilizzate cautele particolari. A tal proposito, alle previsioni del Codice si aggiungono quelle di discipline di settore.

Giuseppe Colaiacomo

Avvocato, ammesso dal 2014 al patrocinio presso le Giurisdizioni superiori. Dal 2000 è componente dello Studio Legale Buzzelli, dove si occupa di diritto commerciale e del lavoro. Ha pubblicato numerosi articoli su varie riviste giuridiche e ha redatto il commento alle norme del Codice Civile sulla trascrizione nei registri immobiliari per il "Codice Civile Commentato" a cura di Alpa e Mariconda per i tipi dell'Ipsoa, sin dalla prima edizione.

Prof. Pietro Falletta

Invited Professor presso l'Université Paris 1 Panthéon-Sorbonne e Ricercatore in Diritto Amministrativo presso l'Università degli Studi del Molise. Titolare dei corsi di Diritto dell'informazione e della comunicazione e Diritto di Internet: social media e discriminazione presso la LUISS Guido Carli. È stato consulente esperto presso il Ministero per gli affari regionali e gli enti locali, il Ministero dell'Ambiente e della Tutela del Territorio e del Mare e l'Ufficio Nazionale Antidiscriminazioni Razziali della Presidenza del Consiglio dei Ministri. È autore di diverse pubblicazioni in materia di Diritto amministrativo, Diritto costituzionale e Diritto dell'informazione e della comunicazione.

Annamaria La Cesa

Avvocato dal 2009. Nel corso degli anni si è occupata, sia in qualità di procuratore che di membro del Collegio Arbitrale, di contenziosi tra privati e pubbliche amministrazioni. Si è interessata diffusamente anche di contenzioso in materia giuslavoristica, fallimentare e amministrativa. In Confindustria Radio Televisioni segue le attività dell'area normativa e regolamentare

Confindustria Radio Televisioni (CRTV) è l'associazione di categoria dei media televisivi e radiofonici italiani. Gli Associati ricomprendono i maggiori operatori radiotelevisivi nazionali: Discovery Italia, Elemedia (GEDI), Giglio Group, HSE24, La7, Mediaset, Persidera, Prima Tv, Qvc, Radio Italia, Rai, RDS – Radio Dimensione Suono, Rete Blu, RTL 102.5, Tivù, Viacom Media Network International Italia. Aderiscono a CRTV anche le maggiori emittenti locali, attraverso l'Associazione TV Locali, e l'Associazione Radio FRT. Tra i soci aggregati vi sono: Eutelsat Italia e DNG (Digital News Gathering).

In CRTV sono rappresentate tutte le principali componenti del settore: emittenti radiotelevisive pubbliche e private, nazionali e locali, operatori di rete e di piattaforma. Si tratta di un comparto che nel complesso esprime ricavi per oltre 9 miliardi di Euro e una forza lavoro di circa di circa 90.000 addetti, di cui circa 30.000 diretti (stime CRTV, dati bilancio 2015).

Obiettivo fondante di CRTV è la rappresentanza unitaria del settore radiotelevisivo sul piano istituzionale, legislativo e contrattuale. A tale riguardo CRTV sottoscrive con CGIL SLC, FISTel-CISL e UILCOM il contratto collettivo nazionale per i dipendenti delle imprese radiotelevisive private.

CRTV è socia di Auditel, è associata a IAP (Istituto di Autodisciplina Pubblicitaria), AER, Eurovisioni, ed è "sector member" dell'ITU-R. È presente con propri rappresentanti in diversi organismi, tra cui: Comitato Media e Minori (MISE), Comitato Consultivo Permanente per il Diritto d'Autore (MIBACT) e Comitato Sviluppo e Tutela dell'Offerta Legale di Opere Digitali (AGCom).

I membri del Consiglio di Presidenza di Confindustria Radio Televisioni sono:

FRANCESCO ANGELO SIDDI - Presidente CRTV
ALESSANDRO ARAIMO - Discovery Italia
ANDREA CASTELLARI - Viacom International Media Networks Italia
FRANCESCO DINI - Elemedia
FABRIZIO FERRAGNI - Rai
MARCO GHIGLIANI - La7
MAURIZIO GIUNCO - FRT
PIERO MANERA - FRT
GINA NIERI - Mediaset
PAOLO PENATI - Qvc Italia
PAOLO RUFFINI - Rete Blu
STEFANO SELLI - Mediaset
LORENZO SURACI - Rtl 102.5 Hit Radio

Il prossimo 25 maggio diverrà integralmente applicabile in Italia il Regolamento UE 2016/679 (GDPR) che innova profondamente la normativa sulla privacy in risposta all'accelerazione imposta dalla digitalizzazione dell'economia e al peso che le informazioni personali hanno assunto in essa.

Sono molti i nuovi adempimenti richiesti ai titolari e responsabili del trattamento dei dati e sono molte, a poche settimane dal 25 maggio, anche le aree "grigie" della nuova normativa. Il settore radiotelevisivo è ampiamente coinvolto dalle novità, con peculiarità che riguardano, tra l'altro, l'attività di informazione giornalistica e che richiedono attenta considerazione.

Il progetto di CRTV per accompagnare i propri associati - grandi, piccole e medie imprese del settore - nella delicata fase di adeguamento è un "work in progress", di cui questa pubblicazione è il primo tassello.

CONFINDUSTRIA RADIO TELEVISIONI

Palazzo Colonna
0187 Roma - Piazza dei SS. Apostoli, 66

tel. +39 06 93562121
fax: +39 06 69368541

www.confindustriaradiotv.it

info@confindustriaradiotv.it