

GDPR

Il Regolamento UE Generale sulla protezione dei dati personali n. 679/2016: analisi pratica del quadro generale di insieme e dei nuovi adempimenti privacy

Presentazione

1. Legge delega del Parlamento n.163 del 25 ottobre 2017 e abrogazione del d.lgs. 196/2003: profili d'incostituzionalità.
2. L'ambito di applicabilità soggettiva e territoriale del nuovo Regolamento privacy UE
2. Le nuove definizioni giuridiche dei concetti privacy
3. Dati personali comuni, sensibili e giudiziari: definizioni e regole per il trattamento
4. Le figure soggettive privacy: Titolare del trattamento, Responsabile del trattamento, persone autorizzate al trattamento, rappresentante designato del titolare trattamento
5. La nuova figura del Data Protection Officer
6. Il nuovo obbligo di redazione e detenzione del Registro generale delle attività di trattamento svolte
7. Il nuovo obbligo della valutazione preventiva d'impatto sulla protezione dei dati
8. I nuovi obblighi c.d. di privacy by design e privacy by default
9. La nuova Informativa privacy rafforzata
10. Il consenso al trattamento dei dati personali
11. Il consenso al trattamento dei minori di età nella fornitura di servizi della società dell'informazione
12. Il nuovo diritto alla portabilità dei dati
13. Le misure di sicurezza nel trattamento dei dati personali
14. La notifica della violazione dei dati personali ("Data Breach")
15. Trasferimento dei dati personali al di fuori dell'Unione Europea
16. La disciplina del c.d. diritto all'oblio
17. La disciplina dei trattamenti di profilazione

18. Il nuovo apparato sanzionatorio

19. Le Linee Guida attuative del Gruppo dei Garanti europei

Presentazione.

Il 4 Maggio 2016 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il “Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)”.

Il Regolamento sarà direttamente applicabile negli Stati Membri dal prossimo 25 Maggio 2018, senza necessità di recepimento con atti nazionali (anche se non poche disposizioni lasciano liberi gli Stati Membri - o richiedono agli stessi - di introdurre ulteriori regole e condizioni: si pensi ad esempio all'art. 88 del Regolamento che rinvia a norme nazionali specifiche per la disciplina del trattamento dei dati dei lavoratori). Attualmente, per quanto riguarda l'Italia, sono in corso i lavori parlamentari aventi ad oggetto lo schema di decreto legislativo (di 104 articoli) per il coordinamento della normativa privacy nazionale al Regolamento UE (sarà abrogato il Codice della privacy).

Il Regolamento mira a garantire una disciplina sulla protezione dei dati personali uniforme ed omogenea in tutta la UE, al fine di assicurare un livello coerente ed elevato di protezione e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione Europea.

Parecchie le novità. Dal momento che sono parecchie le novità introdotte che si traducono in obblighi organizzativi, documentali, tecnici e di personale che tutti i titolari del trattamento pubblici e privati dovranno aver implementato al 25 Maggio 2018, di seguito si riportano – in schede pratiche raggruppate in base alle più importanti tematiche del Regolamento - le principali novità introdotte (rispetto alla normativa vigente) e i temi che tutti i titolari del trattamento devono tenere presenti per garantire la totale *compliance* dei trattamenti entro la data di entrata in vigore del nuovo quadro normativo privacy.

1. Legge delega del Parlamento n.163 del 25 ottobre 2017 e abrogazione del d.lgs. 196/2003: profili d'incostituzionalità.

Non si sa ancora molto della bozza di decreto legislativo firmato dal Presidente del Consiglio uscente Gentiloni che abrogherebbe il d. lgs. 196/2003, la normativa che ha disciplinato la privacy in Italia negli ultimi 15 anni. Tuttavia dal comunicato stampa ufficiale diramato , 22 marzo 2018, pare di poter prevedere un testo incompleto e raffazzonato, magari molto lungo, anche più di 100 articoli, ipotizzo, ma con una incomprensione di fondo dello stratificarsi della disciplina in questi anni.

Potrebbe cominciare, nel caso in cui non venisse operato un cambiamento di rotta radicale, profilarsi all'orizzonte una possibile incostituzionalità dello stesso, proprio sul punto maggiormente discusso: l'abrogazione del d. lgs. 196/2003.

Ed infatti la legge delega del Parlamento n. 163 del 25 ottobre 2017 all'art. 13 prevedeva una delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679.

Più nello specifico, secondo il dettato dell'art 13 nell'esercizio della delega il Governo era tenuto a:

- abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679;

- modificare il codice 196/2003 limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679;

- coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679;

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 disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse.

Analizzando il testo della legge delega che menziona "modifica, coordinamento, adeguamento", tutte operazioni che si sarebbero dovute operare sul testo vigente del d. lgs. 196/2003, qualora non si operi un veloce revirement nel solco tracciato dalla delega, un atto così come descritto, di abrogazione totale del d. lgs. 196/2003, a mio modesto avviso, potrebbe incorrere, fin dai suoi primi mesi di applicazione, in una questione di legittimità costituzionale per eccesso di delega ai sensi dell'art. 76 Costituzione.

"Tutto dovrebbe essere reso il più semplice possibile, ma non più semplicistico": questa citazione di Albert Einstein racchiude un principio essenziale che il Legislatore, alle prese con l'adeguamento del quadro normativo nazionale in materia di protezione dei dati personali, avrebbe dovuto tener presente, al pari del principio di accountability, ossia della "responsabilizzazione", parola d'ordine del GDPR e l'unica, reale rivoluzione contenuta nello stesso.

A ben vedere è proprio la responsabilizzazione del nostro Legislatore ad essere venuta a mancare in un momento storico cruciale per la protezione dei dati personali sulla cui circolazione e aggregazione incessanti si fonda ogni moderna forma di interazione tecnologia e sociale. Il Regolamento dell'Unione europea 2016/679 (in seguito GDPR – General Data Protection Regulation), emanato oltre 20 anni dopo la "direttiva-madre" 95/46 (che viene abrogata) rivoluziona di fatto l'approccio alla protezione dei dati personali, introducendo un regime di accountability, cioè di responsabilizzazione, proprio in ragione del rinnovato paradigma relazionale che ormai ne permea ogni possibile ambito.

Ecco che per l'adeguamento della normativa nazionale al GDPR, la soluzione più semplicistica possibile è stata individuata nell'annunciata approvazione di uno schema di decreto legislativo che prevede espressamente l'abrogazione del Codice in materia di protezione dei dati personali. Un Codice, in realtà, autorevole, che vanta una sua storia e che ci ha reso pionieri, più di venti anni fa, in quella stessa Europa, di cui oggi siamo il fanalino di coda. Già, perché l'Italia, caso piuttosto singolare, ha intrapreso il suo percorso di adeguamento in netto ritardo rispetto alle tempistiche da record registrate in altri Paesi Europei, alle prese con questo lavoro già dal 2016. Si è "iniziato" così, solo nel gennaio di quest'anno e lo scorso 21 marzo è stata appunto annunciata dal Consiglio dei ministri l'approvazione di uno schema di decreto, condotta a luci spente e in posizione verosimilmente supina rispetto agli interessi delle multinazionali dei dati.

Mentre il mondo continua a confrontarsi con i dettagli sempre meno rassicuranti emersi della vicenda "Cambridge Analytica", l'Italia lascia così il fianco scoperto a una mossa potenzialmente incostituzionale, frutto di un palese eccesso di delega.

La delega al governo per far fronte al previsto adeguamento imponeva al governo di “abrogare” espressamente (solo e soltanto) le disposizioni del decreto legislativo 196/2003, incompatibili quelle introdotte dal GDPR, modificare il Codice 196/2003 “limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel GDPR”, coordinando, infine le disposizioni vigenti in materia con quelle introdotte dal Legislatore Europeo. Solitamente si cerca sempre di seguire (in modo più o meno rigoroso) la delega ricevuta per non incorrere nell'eccesso previsto dall'art. 76 Costituzione. Con questo schema incredibilmente si è scelto invece di andare proprio da un'altra parte – e in modo piuttosto schizofrenico – non ultimo alla luce dell'annunciata abrogazione anche delle sanzioni penali previste dal Codice che la legge delega aveva espressamente richiesto di mantenere.

Come si spiega tutto ciò? Maliziosamente non si può non sospettare che, a causa dei ritardi nell'affrontare la questione, la data del 25 maggio sembrava ormai a un Legislatore maldestro e svogliato troppo vicina per riuscire a coordinare i dettagli del Codice, operazione sicuramente difficile e dispendiosa. Più comodo gettare all'aria tutto il nostro sistema normativo preesistente, dando anche ai più la pericolosa sensazione che il Regolamento vada in qualche modo ulteriormente precisato e non sia direttamente applicabile nel nostro ordinamento giuridico, tanto da portare qualcuno a consigliare in questi giorni di sospendere qualsiasi adeguamento al GDPR.

Se è vero che l'approccio all'accountability non riguarda solo la parte tecnologica o strettamente organizzativa, ma anche e soprattutto l'assegnazione dei ruoli, sulla base della loro documentata competenza, è ora più che mai necessario comprendere e applicare questo principio, non solo all'interno di un'impresa o di una PA, ma anche e soprattutto nelle “alte sfere”, cioè nei riguardi di chi, *in primis*, ha il ruolo (anzi, il dovere) di decidere in materia. E' sempre più urgente che, infatti, la certezza del diritto ci aiuti a garantire la protezione della nostra esistenza (anche quella più intima), dal momento che siamo diventati tutti cittadini di vetro sempre visibili ai detentori del potere politico ed economico, con un rischio evidente per la libertà e la democrazia. Si chiede a gran voce quindi al legislatore di ritrovare una strada semplice, ma sorretta dal raziocinio.

Comunicato stampa del Consiglio dei Ministri n. 75

21 Marzo 2018

CODICE DELLA PRIVACY

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016,

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) (decreto legislativo – esame preliminare)

Il Consiglio dei Ministri, su proposta del Presidente Paolo Gentiloni e del Ministro della giustizia Andrea Orlando, ha approvato, in esame preliminare, un decreto legislativo che, in attuazione dell'art. 13 della legge di delegazione europea 2016-2017 (legge 25 ottobre 2017, n. 163), introduce disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

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

2..L'ambito di applicabilità soggettiva e territoriale del nuovo Regolamento privacy UE

Con riferimento all'ambito di applicazione materiale, il Regolamento conferma che la nuova disciplina si applica solo al trattamento dei dati personali di persone fisiche.

Riguardo invece all'ambito di applicazione territoriale, particolarmente innovativo il fatto che il Regolamento si applichi - oltre che al trattamento di dati personali effettuato da un titolare stabilito nella UE - anche ai trattamenti effettuati da titolari non stabiliti nell'Unione Europea se il trattamento ha ad oggetto dati personali di interessati che si trovano nella UE e riguarda (1) l'offerta di beni o servizi (anche non a pagamento) ai suddetti interessati (2) il monitoraggio del loro comportamento nel territorio dell'Unione Europea.

Ciò implica che – ad esempio – aziende estere non aventi sede legale nella UE o anche prive di sedi secondarie nella UE saranno soggette al Regolamento se i trattamenti specificati riguardano interessati che nella UE vivono, lavorano, sono residenti o hanno un domicilio. In tal caso sarà obbligatorio nominare un rappresentante del Titolare o del responsabile extra UE avente sede nella UE.

3. Le nuove definizioni giuridiche dei concetti privacy

Il Regolamento, rispetto alle definizioni oramai abituali della normativa privacy, introduce per la prima volta specifiche definizioni cui ricollega specifici adempimenti.

Novità... Sono una novità, ad esempio, le definizioni di “profilazione”, “pseudonimizzazione”, “dati genetici”, “dati biometrici”, “stabilimento principale”, “terzo” (definizione già presente nella abrogata Direttiva 95/46/CEE, ma assente nel Codice della privacy), “consenso dell’interessato” (definizione già presente nella abrogata Direttiva 95/46/CEE, ma assente nel Codice della privacy), etc.

... e aggiornamenti. Le altre definizioni usuali – come ad esempio quella di “dato personale” – sono aggiornate (ad esempio, la definizione di dato personale include ora anche “un identificativo online” oltre ai già noti “dati sulla ubicazione”) e innovative (sempre per quanto riguarda la definizione di

dato personale, è incluso nella stessa il riferimento a “uno o più elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale” della persona fisica interessata).

4.Dati personali comuni, sensibili e giudiziari: definizioni e regole per il trattamento

Con riferimento ai dati personali comuni, il Regolamento definisce il “dato personale” come «qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi

caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

Dati personali “sensibili” o dati personali “giudiziari”. Non esiste più una specifica definizione di dati personali “sensibili” o di dati personali “giudiziari”, ancorché la definizione sia ricavabile dagli articoli generali dedicati a queste categorie di informazioni. L’art. 9, difatti, individua in generale le «categorie particolari di dati personali» nelle informazioni «che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona fisica»; mentre il successivo art. 10 del Regolamento disciplina il trattamento dei «dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza».

Dati relativi alla salute. Il Regolamento introduce comunque una nuova definizione limitata ai «dati relativi alla salute» intesi quali i «dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute».

Interessante notare i nuovi principi a base del trattamento dei dati (ex) sensibili e giudiziari. Il trattamento di dati (ex) sensibili è addirittura vietato come regola generale, derogabile nei casi specifici elencati dall’art. 9 (consenso esplicito dell’interessato per una o più finalità specifiche; trattamento necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell’interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, trattamento necessario per tutelare un interesse vitale dell’interessato o di un’altra persona fisica qualora l’interessato si trovi nell’incapacità fisica o giuridica di prestare il proprio consenso; trattamento effettuato, nell’ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali; trattamento di dati personali resi manifestamente pubblici dall’interessato; trattamento necessario per accertare, esercitare o difendere un diritto in sede giudiziaria; trattamento necessario per motivi di interesse pubblico; trattamento necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali; trattamento necessario per motivi di interesse pubblico nel settore della sanità pubblica; trattamento necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici).

Gli Stati membri possono comunque mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute (lo schema di decreto legislativo italiano di coordinamento prevede difatti norme specifiche).

Per quanto riguarda il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, resta fermo il principio – già noto al Codice della privacy – per il quale il trattamento dei dati giudiziari deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

5. Le figure soggettive privacy: Titolare del trattamento, Responsabile del trattamento, persone autorizzate al trattamento, rappresentante designato del titolare trattamento

Le figure soggettive privacy tipiche restano sostanzialmente invariate, ma il Regolamento introduce degli obblighi organizzativi nuovi con riferimento ai loro ruoli e funzioni, come ad esempio i seguenti:

1. nel caso di contitolarità del trattamento, cioè allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, va redatto uno specifico accordo interno tra i contitolari che disciplini in modo trasparente le rispettive responsabilità e rifletta adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo va messo a disposizione dell'interessato;
2. con riferimento al Responsabile del trattamento, figura facoltativa nel Codice della privacy, la sua nomina diventa obbligatoria e va documentata con un «contratto o altro atto giuridico» - stipulato in forma scritta o anche in formato elettronico - che regoli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento; inoltre, novità rispetto al Codice della privacy, il Responsabile del trattamento può a sua volta designare altri responsabili del trattamento (sub-responsabili) ma previa autorizzazione scritta – specifica o generale – del titolare del trattamento e fermo restando che del loro operato risponderà esclusivamente il Responsabile che li nomina;
3. con riferimento agli incaricati del trattamento va segnalato che rispetto al Codice della privacy - che ne prevedeva la obbligatoria nomina scritta - la figura dell'incaricato del trattamento non è prevista dal Regolamento (come già sotto il vigore della abrogata Direttiva 46/95/CEE), se non indirettamente. Difatti il Regolamento individua (anche se non fornisce una definizione formale) le «persone autorizzate al trattamento» prevedendo che esse siano i soggetti che operano sotto la diretta responsabilità del titolare (che ai sensi del Considerando n. 29 ha l'obbligo di «indicare le persone autorizzate all'interno della struttura del titolare») o del responsabile (che deve garantire che «le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza»); infine, l'art. 29 del Regolamento dispone che chiunque agisca sotto la autorità del responsabile o sotto quella del titolare del trattamento e abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento (quindi sembrerebbero restare in vigore le obbligatorie istruzioni agli incaricati, anche

se nulla si dice riguardo alla forma scritta); l'art. 32 del Regolamento individua inoltre come misura di sicurezza la circostanza che «il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento»;

4. con riferimento alla figura del «rappresentante del titolare del trattamento» stabilito nella UE (già nota al Codice della privacy) esso va designato per iscritto in caso di trattamenti effettuati da titolari non stabiliti nell'Unione Europea se il trattamento ha ad oggetto dati personali di interessati che si trovano nella UE e riguarda (1) l'offerta di beni o servizi (anche non a pagamento) ai suddetti interessati (2) il monitoraggio del loro comportamento nel territorio dell'Unione Europea.

6. La nuova figura del Data Protection Officer

Del tutto nuova è la figura del Responsabile della protezione dei dati (Data Protection Officer) introdotta dall'art. 37 del Regolamento.

L'obbligo di designazione del Responsabile della protezione dei dati (da parte del titolare o del responsabile del trattamento) non è generale ma si applica solo se:

1. il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
2. 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;
3. le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, di dati genetici o biometrici, di dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona o di dati relativi a condanne penali e a reati.

Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati. Il Responsabile della protezione dei dati - che può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure un consulente esterno che assolve i suoi compiti in base a un contratto di servizi - va comunque designato in funzione delle elevate qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i delicati compiti assegnati. I dati di contatto del Responsabile della protezione dei dati vanno notificati al Garante e resi pubblici (può essere evitata la indicazione del nome e cognome, che vanno comunicati solo al Garante).

Il Responsabile della protezione dei dati è una figura apicale. Il Responsabile della protezione dei dati è una figura apicale (riferisce direttamente al vertice gerarchico del titolare del trattamento), assolutamente diversa quanto a ruolo e funzioni dal “semplice” responsabile del trattamento (con il quale non va confuso). Va tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. Deve avere le risorse necessarie e il potere di spesa per assolvere ai compiti assegnati, accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica (es: spese per il suo aggiornamento professionale). Il Responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, ma non deve ricevere dal titolare o dal responsabile alcuna istruzione per quanto riguarda l'esecuzione di tali compiti (è dunque figura del tutto autonoma) né è soggetto a potere disciplinare o sanzionatorio per l'adempimento dei propri compiti (ad esempio in ciò – tra l'altro - risiedono i caratteri distintivi tra Data Protection Officer e responsabile del trattamento, che al contrario deve ricevere istruzioni scritte ed è soggetto al controllo e all'autorità del titolare del trattamento, ivi compresi i profili sanzionatori).

L'art. 39 del Regolamento individua il nucleo minimo (che dunque può essere anche esteso) dei compiti assegnati al Responsabile della protezione dei dati.

7. Il nuovo obbligo di redazione e detenzione del Registro generale delle attività di trattamento svolte

Il Regolamento introduce un duplice obbligo documentale nuovo: quello del Registro delle attività di trattamento che – secondo le rispettive responsabilità e competenze - deve essere redatto (anche in formato elettronico) sia dal titolare che dal responsabile del trattamento e va esibito su richiesta al Garante.

Imprese o organizzazioni con più di 250 dipendenti. Il regolamento introduce - per le imprese o organizzazioni con più di 250 dipendenti - l'obbligo di elaborare un sistema documentale di gestione della privacy contenente tutti gli atti, regolarmente aggiornati, elaborati per soddisfare i requisiti di conformità al Regolamento. Tale obbligo di rendicontazione (o di “accountability”) impone a ciascun titolare del trattamento un duplice obbligo documentale nuovo: quello del Registro delle attività di trattamento svolte che – secondo le rispettive responsabilità e competenze - deve essere redatto (anche in formato elettronico) sia dal titolare che dal responsabile del trattamento e va esibito su richiesta al Garante.

Il titolare dovrà conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità, indicando obbligatoriamente - per ognuno di essi - una serie di dettagliate informazioni, tali da assicurare e comprovare la compliance privacy di ciascuna operazione alle disposizioni del Regolamento.

Ogni titolare del trattamento deve dunque redigere e detenere un Registro delle attività di trattamento svolte. Tale registro contiene tutte le seguenti informazioni:

1. il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
2. le finalità del trattamento;
3. una descrizione delle categorie di interessati e delle categorie di dati personali;
4. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
5. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;
6. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
7. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Ogni responsabile del trattamento deve poi redigere e detenere un Registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

1. il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
2. le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
3. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;
4. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Imprese o organizzazioni con meno di 250 dipendenti. Per le imprese o organizzazioni con meno di 250 dipendenti l'obbligo non si applica a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di dati (ex) sensibili o giudiziari.

8. Il nuovo obbligo della valutazione preventiva d'impatto sulla protezione dei dati

Tra i nuovi e più rilevanti oneri posti a carico del titolare del trattamento vi è quello della valutazione preventiva d'impatto sulla protezione dei dati (c.d. principio della *privacy impact assessment*).

Quando un trattamento prevede in particolare l'uso di nuove tecnologie oppure considerati la natura, l'oggetto, il contesto e le finalità del trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento, prima di procedere (e

consultandosi con il *Data Protection Officer*, ove nominato, e - se del caso – raccogliendo anche le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto) deve preventivamente effettuare una valutazione dell'impatto del trattamento previsto sulla protezione dei dati personali (una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi).

È comunque previsto che il Garante rediga e comunichi ai titolari un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati (e anche – al contrario - un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati, anche perché lo stesso Regolamento esclude tale obbligo in caso di trattamento necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento o di trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento).

L'obbligo di valutazione preventiva. Scatta tale obbligo, ad esempio, in caso di trattamenti automatizzati di profilazione sistematica degli interessati, di trattamento, su larga scala, di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, di dati genetici o biometrici, di dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona o di dati relativi a condanne penali e a reati, o nel caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La valutazione – soggetta a riesame periodico - contiene almeno una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; una valutazione dei rischi per i diritti e le libertà degli interessati e le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento.

Se la valutazione preventiva indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate per attenuare il rischio, il titolare, prima di procedere al trattamento, è tenuto a consultare il Garante (con una procedura analoga all'attuale interpello previsto dall'art. 17 del Codice della privacy, che verrà abrogato – unitamente all'obbligo di notificazione dei trattamenti – a partire dal 25 maggio 2018).

9. I nuovi obblighi c.d. di privacy by design e privacy by default

L'art. 25 del Regolamento ("Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita") impone vincoli che impattano sulle stesse fasi produttive e di operatività di apparati e/o servizi che implicano il trattamento di dati personali.

Privacy by design. Con riferimento al principio cosiddetto della privacy by design, il Regolamento prescrive che il titolare del trattamento - tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento - debba applicare misure tecniche e organizzative adeguate (es: anonimizzazione) volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie per tutelare i diritti degli interessati. E tale adempimento va effettuato sia al momento di determinare i mezzi del trattamento (es: progettazione di *device*) sia all'atto del trattamento stesso.

Privacy by default. Con riferimento al principio cosiddetto della privacy by default, il Regolamento stabilisce che il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita (cioè *by default*), solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure devono garantire che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica (che ad esempio consapevolmente disponga il settaggio dell'apparato o del servizio scegliendo di condividere con i terzi i dati personali oggetto di trattamento nell'ambito della operatività dell'apparato o del servizio).

Il titolare può ottenere una certificazione *ad hoc*, prevista dal Regolamento in base ad una specifica procedura, per dimostrare la conformità ai sopra citati principi.

10. La nuova Informativa privacy rafforzata

Il Regolamento sancisce a carico dei titolari del trattamento obblighi di informativa rafforzati rispetto a quanto avviene ora con l'art. 13 del Codice della privacy, prevedendosi numerose informazioni aggiuntive da fornire agli interessati - a meno che di tali informazioni gli interessati non siano comunque già in possesso. Ai sensi degli art. 13 - se le informazioni sono raccolte presso l'interessato - e 14 del Regolamento - nel caso di informazioni non raccolte presso l'interessato (e in questo caso all'interessato vanno fornite entro 30 giorni al massimo) il titolare del trattamento deve fornire gratuitamente all'interessato tutte le informazioni di seguito elencate, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Informazioni aggiuntive sul trattamento. Rispetto agli elementi obbligatori da indicare nell'informativa privacy che già siamo abituati a conoscere in applicazione dell'art. 13 del Codice della privacy italiano (e che ovviamente non vengono meno), i titolari del trattamento dovranno inserire obbligatoriamente anche le seguenti informazioni aggiuntive sul trattamento:

1. i dati di contatto della nuova figura del Data Protection Officer (Responsabile della protezione dei dati personali) ove prevista;
2. la base giuridica del trattamento a corredo della illustrazione delle finalità del trattamento;
3. qualora il trattamento si basi sulla necessità di perseguire un legittimo interesse del titolare del trattamento o di terzi, la specificazione di quali siano i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
4. l'ambito del trasferimento all'estero (ovviamente extra UE) o a un'organizzazione internazionale dei dati personali, ove applicabile, l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili;
5. il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
6. la specifica esistenza del diritto alla portabilità dei dati;

7. l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
8. il diritto di proporre reclamo al Garante privacy;
9. la eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato;
10. la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico (tale informazione è obbligatoria solo ove i dati non siano raccolti presso l'interessato);
11. le categorie di dati personali oggetto del trattamento (tale informazione è obbligatoria solo ove i dati non siano raccolti presso l'interessato).

Le informazioni da rendere agli interessati possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone devono essere leggibili da dispositivo automatico.

11. Il consenso al trattamento dei dati personali

Ovviamente, il Regolamento fonda sul «consenso dell'interessato» (definito formalmente come «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento») la principale condizione (salve le deroghe) di liceità del trattamento.

Consenso dell'interessato... L'art. 7 specifica inoltre le caratteristiche e le condizioni del consenso, stabilendo che il titolare del trattamento debba poter dimostrare che l'interessato ha prestato il consenso al trattamento dei propri dati personali. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro, pena l'invalidità del consenso prestato.

... che può essere revocato. L'interessato ha poi il diritto di revocare il proprio consenso (e tale informazione è uno dei nuovi elementi obbligatori dell'informativa privacy) in qualsiasi momento (anche se la revoca non pregiudica la liceità del trattamento fino a quel momento effettuato), con modalità di esecuzione della revoca del consenso facili come la sua prestazione originaria.

È specificatamente vietato che l'esecuzione di un contratto o la prestazione di un servizio siano condizionati alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione del contratto o servizio.

Alla specifica manifestazione del consenso è poi subordinata:

1. la liceità del trattamento (altrimenti vietato, a meno che non si applichino gli altri presupposti alternativi al consenso di cui all'art. 9 del Regolamento) dei dati personali che rivelano l'origine

razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dei dati genetici, dei dati biometrici, dei dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

2. la possibilità – altrimenti vietata – di procedere alla profilazione dell'interessato;

3. la possibilità di trasferire i dati personali dell'interessato verso un paese terzo extra UE o verso un'organizzazione internazionale.

12. Il consenso al trattamento dei minori di età nella fornitura di servizi della società dell'informazione

Se un trattamento di dati nell'ambito della fornitura ad un minore di un servizio della società dell'informazione (definito - come nella Direttiva (UE) 2015/1535 - come «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza senza la presenza simultanea delle parti, inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento, interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici o altri mezzi elettromagnetici e a richiesta individuale di un destinatario», ad esempio l'accesso a Internet, l'iscrizione a un social network, l'apertura di un account email, o il download di un'applicazione, etc.) prevede l'acquisizione del consenso preventivo, la raccolta del consenso e il trattamento dei dati del minore sono leciti se egli abbia compiuto almeno 16 anni (salvo il diritto degli Stati membri di stabilire anche un'età inferiore a tali fini - purché non inferiore ai 13 anni – e senza pregiudizio delle disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore).

Il titolare del trattamento è obbligato – sia pur con il criterio della “ragionevolezza” e tenendo presenti comunque le “tecnologie disponibili” - a verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della potestà genitoriale sul minore.

13. Il nuovo diritto alla portabilità dei dati

Inteso come corollario del diritto di accesso (rafforzato) dell'interessato ai propri dati personali («l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento») il nuovo «diritto alla portabilità dei dati personali» (non esercitabile se il trattamento «è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento») consiste nel diritto dell'interessato di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti. Tale diritto è esercitabile quando il trattamento: (1) è effettuato con mezzi automatizzati; (2) si basa sul consenso precedentemente prestato dall'interessato o (3) si basa su un contratto o su trattative precontrattuali.

In questi specifici casi l'interessato - fermo restando comunque il suo diritto alla cancellazione dei dati - ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, «se tecnicamente fattibile».

14. Le misure di sicurezza nel trattamento dei dati personali

La sicurezza nel trattamento dei dati è uno dei principi fondamentali del trattamento in base al nuovo articolo 5 del Regolamento («i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali – principio della “integrità e riservatezza”»).

L'art. 32 del Regolamento precisa le misure stabilendo che - tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche - il titolare del trattamento e il responsabile del trattamento debbano mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, “se del caso”:

1. la pseudonimizzazione e la cifratura dei dati personali;
2. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
3. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
4. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

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

Circa gli obblighi di documentazione delle misure di sicurezza (analoghi al vecchio e abrogato DPS previsto dalla normativa italiana), il Regolamento prescrive "ove possibile" di inserire nel nuovo Registro delle attività di trattamento svolte (applicabile però solo alle imprese con oltre 250 addetti, salvi casi eccezionali) «una descrizione generale delle misure di sicurezza tecniche e organizzative». Inoltre, nella documentazione della valutazione preventiva di impatto sulla protezione dei dati, il titolare deve descrivere anche – tra l'altro - le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone.

15. La notifica della violazione dei dati personali ("Data Breach")

Data Breach. La principale novità in materia è rappresentata dal fatto che l'obbligo di notifica al Garante di una avvenuta violazione di dati personali (c.d. "*data breach*" definita formalmente quale «violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati»;) - ora applicabile ai soli fornitori di servizi di comunicazione elettronica accessibili al pubblico - diventa obbligo generale per tutti i titolari del trattamento, indipendentemente dal fatto che siano o meno fornitori di servizi di comunicazione elettronica.

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

La notifica deve almeno:

1. descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
2. comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
3. descrivere le probabili conseguenze della violazione dei dati personali;
4. descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

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

Il titolare del trattamento deve documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio e mettere su richiesta a disposizione del garante la relativa documentazione.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione anche all'interessato, senza ingiustificato ritardo, descrivendola con un linguaggio semplice e chiaro, salve circostanze al verificarsi delle quali non è richiesta la comunicazione all'interessato.

16. Trasferimento dei dati personali al di fuori dell'Unione Europea

Qualunque trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale (compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione

internazionale) può avere luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni esplicitate dal Regolamento:

1. trasferimento sulla base di una decisione di adeguatezza (ove la Commissione UE abbia deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato; in tal caso il trasferimento non necessita di autorizzazioni specifiche);
2. trasferimento soggetto a garanzie adeguate (il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi; possono costituire garanzie adeguate senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo, tra le altre: le norme vincolanti d'impresa, le clausole contrattuali standard, clausole tipo elaborate dal Garante e approvate dalla Commissione, l'esistenza di un codice di condotta a norma dell'art. 40 del Regolamento, l'esistenza di un meccanismo di certificazione approvato a norma dell'articolo 42 del Regolamento, specifiche clausole contrattuali - dunque non standard - tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale).

Se non è applicabile nessuna delle condizioni sopra illustrate il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale sono ammessi soltanto se si verifica una delle seguenti condizioni:

- a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;
- b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;
- c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;
- d) il trasferimento sia necessario per importanti motivi di interesse pubblico;
- e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in

generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.

17. La disciplina del c.d. diritto all'oblio

Il Regolamento codifica compiutamente il diritto all'oblio (quale specifico esercizio del diritto alla cancellazione dei dati personali). L'interessato esercita il «diritto all'oblio» chiedendo al titolare del trattamento che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al Regolamento.

Tuttavia, rimane lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

Cancellare qualsiasi link. Per rafforzare il «diritto all'oblio» nell'ambiente online, il diritto di cancellazione è esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare altri titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati personali. Nel fare ciò, il titolare del trattamento adotta misure ragionevoli tenendo conto della tecnologia disponibile e dei mezzi a disposizione, comprese misure tecniche, per informare della richiesta dell'interessato gli altri titolari del trattamento che trattano i dati personali.

18. La disciplina dei trattamenti di profilazione

Il Regolamento introduce per la prima volta una definizione e una regolamentazione del particolare trattamento rappresentato dalla profilazione dell'interessato, giuridicamente definita come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

In linea generale la profilazione appare sostanzialmente vietata («L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona») a meno che non vi siano circostanze specifiche, tra le quali il chiaro consenso informato dell'interessato.

In secondo luogo, l'esistenza di trattamenti di profilazione diviene uno degli obblighi informativi fondamentali della nuova informativa privacy (che sul punto dovrà specificare tutte le «informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato» e dovrà menzionare il diritto di opporsi al trattamento esplicitamente portando tale informazione all'attenzione dell'interessato e presentandola chiaramente e separatamente da qualsiasi altra informazione). Correlativamente, il diritto di conoscere l'esistenza di trattamenti di profilazione (e di opporvisi) è uno dei nuovi diritti privacy dell'interessato: difatti, qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non possono più essere oggetto di trattamento per tali finalità.

Infine, va ricordato che i trattamenti di profilazione rappresentano uno dei presupposti che rendono obbligatoria la valutazione preventiva di impatto sulla protezione dei dati.

19. Il nuovo apparato sanzionatorio

Particolarmente rilevanti appaiono le disposizioni del Regolamento sulle sanzioni.

Dal punto di vista civilistico. Viene confermata la responsabilità risarcitoria per il c.d. “danno da trattamento”, che viene più precisamente codificato (rispetto, ad esempio, all’art. 15 del Codice della privacy): l’art. 82 prescrive difatti che «Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento». Sono inoltre meglio chiariti i meccanismi di ripartizione della responsabilità risarcitoria tra titolare e responsabile del trattamento, e tra contitolari del trattamento (con la previsione specifica di azioni di regresso reciproche) così come i meccanismi di esonero.

Per quanto riguarda l’applicazione delle sanzioni amministrative pecuniarie da parte delle autorità di controllo (il Garante), l’art. 83 del Regolamento, oltre a regolare le condizioni di determinazione delle sanzioni, fissa i seguenti importi:

1. sanzioni amministrative pecuniarie fino a 10.000.000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nel caso di violazione di determinati obblighi posti dal Regolamento;
2. sanzioni amministrative pecuniarie fino a 20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nel caso di violazione degli obblighi più stringenti posti dal Regolamento (anche nel semplice caso di inosservanza degli ordini del Garante).

Risarcimento del danno. Con riferimento al risarcimento del danno da trattamento dei dati personali, l'art. 82 del regolamento prevede ora una netta distinzione di responsabilità tra Titolare e Responsabile del trattamento (gli unici 2 soggetti cui il Regolamento imputa la responsabilità extracontrattuale diretta, mentre non sono responsabili in tale ottica il DPO, le persone autorizzate al trattamento o i sub responsabili del trattamento). Dispone l'art. 82 che chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il Regolamento, mentre un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno.

Dal punto di vista penalistico. Con riferimento alle sanzioni penali, come è noto il Diritto dell'Unione Europea non può prevederne, essendo la materia penale di stretta competenza nazionale. Occorrerà verificare cosa prevede in materia di sanzioni penali il futuro decreto legislativo di coordinamento.

20. attuative del Gruppo dei Garanti europei

Particolarmente rilevante ricordare a tutti i Titolari e Responsabili del trattamento, a conclusione di questo sintetico quadro riepilogativo delle novità che stanno per entrare in vigore, le fondamentali regole esecutive della nuova disciplina privacy europea così come contenute nelle numerose Linee Guida emanate fin dal 2016 dal Gruppo ex art. 29 che riunisce tutte le Autorità privacy UE (e che prenderà il nome di Comitato Europeo per la protezione dei dati personali, previsto dall'art. 68 del Regolamento).

Si riporta di seguito l'elenco delle Linee Guida definitive ad oggi applicabili:

- Linee-guida sul diritto alla portabilità dei dati personali WP242 del 13 dicembre 2016 (emendate il 5.4.2017)
- Linee-guida sui responsabili della protezione dei dati (RPD) WP243 del 13 dicembre 2016 (emendate il 5.4.2017)

- Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento WP244 del 13.12.2016 (emendate il 5.4.2017)
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679 WP248 del 5.4.2017 (emendate il 4.10.2017)
- Linee-guida sulla notificazione delle violazioni di dati personali ("data breach") applicazione e sulla definizione delle sanzioni amministrative ai sensi del Regolamento 2016/679 – WP 250 del 3 Ottobre 2017 (emendate il 6.2.2018)
- Linee-guida sui processi decisionali individuali automatizzati e sulla profilazione ai sensi del Regolamento 2016/679 – WP 251 del 3 Ottobre 2017
- Linee-guida sulla applicazione e sulla definizione delle sanzioni amministrative ai sensi del Regolamento 2016/679 – WP 253 del 3 Ottobre 2017
- Linee-guida sul consenso (RPD) WP259
- Linee-guida sulla trasparenza (RPD) WP260
- Linee-guida sull'accreditamento degli enti di certificazione (RPD) WP261