Giugno 2018

Le nuove regole in materia di privacy della GDPR e principali novità per le Banche*

Enea Franza, Responsabile Consumer Protection, Consob

Premessa

II Regolamento generale per la protezione dei dati personali n. 2016/679 (General Data Protection Regulation o, in breve, GDPR) è la normativa di riforma della legislazione europea in materia di protezione dei dati. Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016 è entrato in vigore il 24 maggio 2016, ma la sua attuazione è avvenuta a distanza di due anni, quindi dal 25 maggio 2018, e fin dalla sua applicazione ha determinato un cambiamento senz'altro profondo nella modalità di gestione dei dati personali. In quanto Regolamento europeo esso è direttamente applicabile e, quindi, non si prevede una normativa italiana di recepimento quanto, piuttosto, dei chiarimenti in relazione ad alcuni aspetti, ad esempio sui poteri del Garante Nazionale per la protezione dei dati personali (c.d. Garante Privacy). Analizziamo qui di seguito le più importanti novità e gli adempimenti da seguire per l'adeguamento alla nuova normativa. Centrale nella gestione della nuova disciplina è la definizione di dato personale, identificato, in senso ampio, in qualsiasi informazione come ad esempio nome, codice fiscale, immagine, voce, impronta digitale o traffico telefonico concernente una persona fisica identificata o identificabile anche indirettamente[1]. Il Regolamento generale si applica ad ogni trattamento, ovvero, a qualsiasi operazione o insieme di operazioni, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione che ha ad oggetto dati personali, ed a tutti i titolari (*controller*) e responsabili (*processor*) del trattamento stabiliti nel territorio dell'Unione, ma anche in generale a quelli che, offrendo beni e servizi a persone residenti nell'Unione, trattano dati di residenti nell'Unione europea (art.

---

* *Le opinioni sono espresse a titolo personale e non coinvolgono l'autorità presso cui lo scrivente lavora*.

[1] Prevede l'Articolo 4, Definizioni, del Regolamento europeo: "*Ai fini del presente regolamento s'intende per: 1) «dato personale»: 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*;".

3 del Regolamento). In tal modo la sua applicazione non è limitata alle sole aziende che si trovano in Europa, ma tutela tutti gli interessati che risiedono nel territorio dell'Unione, indipendentemente da dove si attua il trattamento dei loro dati[2]. La persona fisica identificata o identificabile in modo diretto o indiretto cui si riferiscono i dati personali oggetto di trattamento viene definito Interessato[3]. Categorie particolari di dati personali sono i dati sensibili, i dati sanitari, i dati biometrici, i dati genetici ed i dati personali che rivelano l'esistenza di reati o di condanne penali o connesse misure di sicurezza quali, ad esempio i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione[4]. Rilevano ai fini della normativa in esame le operazioni di trattamento dei dati, ovvero, le operazioni di raccolta o acquisizione, registrazione, organizzazione, strutturazione, conservazione, consultazione e visualizzazione, ma anche di elaborazione, selezione, estrazione, nonché utilizzo come la comunicazione (o cessione), il raffronto, l'interconnessione, il blocco e/o la diffusione. Hanno significato per la disciplina in esame, altresì, le operazioni di cancellazione, distruzione ed anonimizzazione (ovvero, il trattamento che ha lo scopo di impedire l'identificazione dell'interessato)[5].

A ben vedere - come rilevano i lavori preparatori ed i Considerando - l'intervento attuato con la normativa GDPR in materia di tutela dei dati personali, qualificati dalla stessa

[2] Il Regolamento, invece, non si applica nei seguenti casi: - trattamenti effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione; - trattamenti effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, del Trattato dell'UE (politica estera e sicurezza); - trattamenti effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse; - trattamenti effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico (vedi esenzione per uso personale).

[3] Il dato personale va sempre riferito al contesto: anche se un'informazione isolata non è in grado di portare all'identificazione di un individuo, il fatto che tale informazione possa essere utilizzata per l'identificazione tramite incrocio con altri dati ne determina la natura di dato personale (es. dati di navigazione on-line). Si pensi ad esempio, ad informazioni come il nome, un numero di identificazione, dati riguardanti l'ubicazione, un identificativo on-line oppure uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

[4] Secondo il Codice sulla protezione dei dati personali (D. Lgs. n. 196/2003, art. 4), sono considerati dati sensibili i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale. Tale elenco viene considerato chiuso, nel senso che non è lecito procedere per analogia. La raccolta ed il trattamento dei dati sensibili sono soggetti sia al consenso dell'interessato sia all'autorizzazione preventiva del Garante per la protezione dei dati personali

[5] Sulla esigenza di anomizzazione dei dati fa riflettere il seguente caso, tratto dalla cronaca. In California, una donna, anche prostituta si è vista consigliare da Facebook, come amici, sul suo profilo 'privato', alcuni clienti abituali, nonostante l'indirizzo email ed il telefono usato 'per lavoro' fossero differenti e non avesse un profilo Facebook nella vita 'parallela'; ciò è stato possibile perché al social network è stato concesso dagli utenti di usare informazioni estratte da altre app dello smartphone, tra cui la geolocalizzazione.

normativa come diritti fondamentali dell'uomo[6], si inserisce all'interno di una riforma assai più ampia attraverso la quale si persegue l'obiettivo di armonizzare le normative dei vari Stati Membri, garantendo una disciplina uniforme e omogenea in materia di tutela della *Privacy*, di rafforzare la protezione dei dati personali all'interno dell'Unione Europea, introducendo nuovi obblighi di trasparenza in capo ai Titolari del Trattamento e, di sviluppare il mercato unico digitale attraverso la creazione e la promozione di nuovi servizi, applicazioni, piattaforme e software. In ultima istanza, nelle intenzioni del legislatore europeo, come meglio vedremo di seguito, il regolamento costituisce con la direttiva (UE) 2016/680, lo strumento che consente di rimuovere gli ostacoli alla libera circolazione dei dati all'interno dell'Unione Europea, assicurare un livello omogeneo ed elevato di protezione delle persone fisiche in tutti gli Stati Membri e assicurare allo stesso tempo maggiori tutele, diritti e poteri di controllo ai Cittadini all'interno dell'Unione. [7]

1. Le fonti e le principali novità del GDPR

Il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali (c.d. "Codice della Privacy"), attuativo della Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, costituisce il principale *corpus normativo* di riferimento con riferimento ai diritti e delle libertà fondamentali dei cittadini in caso di trattamento dei dati personali da parte di soggetti pubblici e privati[8]. Il 24 maggio 2016, come premesso, è entrato ufficialmente in vigore il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, che abroga la citata direttiva 95/46/CE, che insieme alla Direttiva 2016/680[9] è parte del "Pacchetto protezione dati" adottato dal Parlamento europeo e dal Consiglio il 27 aprile 2016. In sintesi si possono individuare tre linee direttive: sanzioni ingenti e penalizzanti per le violazioni delle prescrizioni in materia di protezione dei dati e *privacy*; la garanzia agli operatori economici di una maggiore certezza del diritto e trasparenza; l'offerta agli interessati di nuovi diritti azionabili. Il GDPR ha previsto due anni per garantire l'allineamento fra la normativa nazionale e comunitaria ed adeguare i trattamenti già in corso ai nuovi principi e requisiti

[6] Prevede, l'Articolo 1, paragrafo 2, del Regolamento "*Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali*"

[7] Il Considerando (2) e (3) del Regolamento europeo recita *"… I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche. (3) La direttiva 95/46/CE del Parlamento europeo e del Consiglio (4) ha come obiettivo di armonizzare la tutela deidiritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri*".

[8] Decreto legislativo 30 giugno 2003, n. 196, codice in materia di protezione dei dati personali.

[9] La direttiva citata è indirizzata alla regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all'esecuzione delle sanzioni penali, in sostituzione e integrazione della decisione quadro 977/2008/CE sulla protezione dei dati personali scambiati dalle autorità di polizia e giustizia (che l'Italia al momento non ha, peraltro, ancora attuato).

introdotti. Con la legge 25 ottobre 2017, n. 163 (Delegazione Europea 2017/2017) si sono dettati i criteri direttivi per l'attuazione del Regolamento (art. 13) e per il recepimento della sopracitata direttiva (art. 11) nell'ordinamento nazionale. Rispetto alla Direttiva 45/96/CE e relativo Codice della Privacy i principali commentatori hanno rappresentato che il Regolamento "GDPR" supera nella sostanza l'approccio essenzialmente formalistico che ha caratterizzato la Direttiva abrogata (appunto la 45/96/CE), per il quale i titolari e responsabili sono chiamati ad adempiere ad obblighi e formalità ed adottare le misure minime di sicurezza previste per esimersi da responsabilità, ma si pretende che titolari e responsabili, invece, adottino soluzioni adeguate al proprio caso concreto ed allo specifico livello di rischio dei trattamenti svolti[10]. Le principali novità prevedono, dunque, oltre ad un rafforzamento dei diritti degli interessati, con un più facile accesso alle informazioni riguardanti i loro dati e le finalità e le modalità di trattamento degli stessi, l'introduzione del diritto alla cancellazione ed alla portabilità dei dati[11], che

[10] Il nuovo Regolamento europeo ha un approccio di tipo *risk based* (basato sulla valutazione del rischio), nel senso che tende a determinare la misura di responsabilità del titolare o del responsabile del trattamento, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti. A tal proposito il Considerando (75), con riferimento al concetto di rischio, dispone: "*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*".

[11] il Considerando (68) del Regolamento europeo, collegato all'Articolo 20, "Diritto alla portabilità dei dati", prevede *"... Per rafforzare ulteriormente il controllo sui propri dati è opportuno anche che l'interessato abbia il diritto, qualora i dati personali siano trattati con mezzi automatizzati, di ricevere in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile i dati personali che lo riguardano che abbia fornito a un titolare del trattamento e di trasmetterli a un altro titolare del trattamento. È opportuno incoraggiare i titolari del trattamento a sviluppare formati interoperabili che consentano la portabilità dei dati. Tale diritto dovrebbe applicarsi qualora l'interessato abbia fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l'esecuzione di un contratto. Non dovrebbe applicarsi qualora il trattamento si basi su un fondamento giuridico diverso dal consenso o contratto. Per sua stessa natura, tale diritto non dovrebbe essere esercitato nei confronti dei titolari del trattamento che trattano dati personali nell'esercizio delle loro funzioni pubbliche. Non dovrebbe pertanto applicarsi quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Il diritto dell'interessato di trasmettere o ricevere dati personali che lo riguardano non dovrebbe comportare l'obbligo per i titolari del trattamento di adottare o mantenere sistemi di trattamento tecnicamente*

consentirà di trasferire i dati personali tra i vari servizi *online*, ed il rafforzamento del diritto al reclamo. Sempre con riferimento ai diritti degli utenti, il Regolamento europeo identifica per i minori la necessità di una distinta protezione relativamente ai loro dati personali, in quanto meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali, specie nell'ambiente digitale come i *social network*[12].

In particolare, come cennato, la novità rafforzativa dei diritti individuali è costituita dall'istituzionalizzazione del diritto alla cancellazione dei dati, detto anche (impropriamente) diritto all'oblio[13], che consentirà di chiedere ed ottenere la rimozione dei dati quando viene meno l'interesse pubblico alla notizia, l'obbligo di notifica da parte delle aziende delle gravi violazione dei dati dei cittadini, nonché la previsione che le aziende dovranno rispondere alla sola autorità di vigilanza dello Stato nel quale hanno la sede principale (principio del "*one stop shop*" o sportello unico).

---

compatibili. Qualora un certo insieme di dati personali riguardi più di un interessato, il diritto di ricevere i dati personali non dovrebbe pregiudicare i diritti e le libertà degli altri interessati in ottemperanza del presente regolamento. Inoltre tale diritto non dovrebbe pregiudicare il diritto dell'interessato di ottenere la cancellazione dei dati personali e le limitazioni di tale diritto di cui al presente regolamento e non dovrebbe segnatamente implicare la cancellazione dei dati personali riguardanti l'interessato forniti da quest'ultimo per l'esecuzione di un contratto, nella misura in cui e fintantoché i dati personali siano necessari all'esecuzione di tale contratto. Ove tecnicamente fattibile, l'interessato dovrebbe avere il diritto di ottenere che i dati personali siano trasmessi direttamente da un titolare del trattamento a un altro".

[12] L'Articolo 8 del Regolamento europeo impone che chi si rivolge direttamente a una persona per offrire un servizio della società dell'informazione, e ne richiede il consenso informato per poter legittimamente trattare i suoi dati personali, abbia l'onere di accertarsi che l'interessato sia in grado di prestare validamente tale consenso. A questo scopo, e solo per questo, si fissa in sedici anni l'età necessaria affinché tale consenso sia valido ai fini della legittimità dei trattamenti, salvo appunto diversa decisione nazionale che, comunque, non può scendere sotto i tredici anni. In merito rileva il recente parere del Working Party art. 29 "*Guidelines on consent under Regulation 2016/679*", pubblicato in via definitiva il 10 aprile 2018 (Opinion n. 259), che precisare come il consenso di cui all'art. 8 non riguarda la validità di eventuali contratti che sia necessario stipulare fra provider e user ai fini della fornitura del servizio, il cui regime giuridico resta sempre disciplinato dalla legislazione nazionale o da quella del foro competente a decidere eventuali controversie relative al servizio.

[13] Il diritto all'oblio trova le sue origini nelle norme internazionali, per prima la Convenzione europea dei diritti dell'uomo (CEDU) del 1950, che all'art. 8 sancisce il diritto al rispetto della vita privata e familiare, inteso come diritto fondamentale. Prevede detto articolo:*"1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui. Anche denominato nel regolamento diritto alla cancellazione"*. Secondo la di Giustizia europea (13 maggio 2014, causa C-131/12, il cittadino ha il diritto di chiedere la rimozione dall'indice di Google delle informazioni *"inadeguate, non pertinenti o non più pertinenti ovvero eccessive in rapporto alle finalità per le quali sono stati trattati e al tempo trascorso". E Google "deve in tal caso procedere al debito esame della loro fondatezza e, eventualmente, porre fine al trattamento dei dati in questione*".

In particolare, l'art.17 del GDPR[14], che si intitola "Diritto alla cancellazione", pone il dovere specifico a carico del titolare che riceva una richiesta di cancellazione quando i dati che ne sono oggetto siano stati "resi pubblici" dal titolare stesso, di provvedere in tal senso l'art. 17, paragrafo 2, impone al titolare non solo di cancellare i dati (sempre ovviamente che lo stesso ritenga la richiesta legittima) ma anche, "*tenuto conto della tecnologia disponibile e dei costi di attuazione"*, di adottare *"misure ragionevoli, anche tecniche*" per informare della richiesta che gli è pervenuta anche gli altri eventuali titolari che stanno utilizzando i dati a lui resi pubblici[15]. In tal senso, dunque, la novità che consiste nel dovere del titolare, che abbia reso pubblici i dati, di diventare un "tramite obbligato" anche verso gli altri titolari che, a sua conoscenza, stiano trattando i dati oggetto della istanza di cancellazione, allorquando, naturalmente l'istante chieda anche la *delinkizzazione* o la cessazione di ogni copia o diffusione. Si consideri, su quest'ultimo aspetto, in particolare, l'articolo 77 del Regolamento, titolato, "Diritto di proporre reclamo all'autorità di controllo" che prevede che "… *Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione. 2. L'autorità di controllo a cui è stato*

[14] Articolo 17, Diritto alla cancellazione («diritto all'oblio»), *"1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:*
a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1. 2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. 3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: a) per l'esercizio del diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria".

[15] Questo obbligo, sussisterebbe, dunque, anche quando la richiesta dell'interessato abbia ad oggetto la cancellazione di "*qualsiasi link, copia o riproduzione dei suoi dati personali*"

proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78". Il Considerando (141), a tale norma collegato, chiarisce "… *Ciascun interessato dovrebbe avere il diritto di proporre reclamo a un'unica autorità di controllo, in particolare nello Stato membro in cui risiede abitualmente, e il diritto a un ricorso giurisdizionale effettivo a norma dell'articolo 47 della Carta qualora ritenga che siano stati violati i diritti di cui gode a norma del presente regolamento o se l'autorità di controllo non dà seguito a un reclamo, lo respinge in tutto o in parte o lo archivia o non agisce quando è necessario intervenire per proteggere i diritti dell'interessato. Successivamente al reclamo si dovrebbe condurre un'indagine, soggetta a controllo giurisdizionale, nella misura in cui ciò sia opportuno nel caso specifico. È opportuno che l'autorità di controllo informi gli interessati dello stato e dell'esito del reclamo entro un termine ragionevole. Se il caso richiede un'ulteriore indagine o il coordinamento con un'altra autorità di controllo, l'interessato dovrebbe ricevere informazioni interlocutorie. Per agevolare la proposizione di reclami, ogni autorità di controllo dovrebbe adottare misure quali la messa a disposizione di un modulo per la proposizione dei reclami compilabile anche elettronicamente, senza escludere altri mezzi di comunicazione".*

Altre principali novità riguardano:

- la ridefinizione dei ruoli di Titolare e del Co-titolare e nella istituzione della figura del Responsabile *Data Protection Officer* (DPO) e dell'onere del Titolare e del Responsabile di ridisegnare ed a ripensare le proprie *policy* in materia di *"data protection"* in base allo specifico livello di rischio, ispirate a principi di rendicontazione ed *accountability*[16], anche con riferimento agli obblighi di segnalazione all'autorità di controllo dei casi di avvenuta violazione di dati personali, ovvero, in definitiva di adottare politiche di *Privacy*

[16] La traduzione italiana di accountability vuol dire "dover rendere conto del proprio operato" , ma in realtà in termine andrebbe più correttamente riferito al principio di responsabilità-

by design e *by default*[17], *Privacy Impact Assessment (PIA)*, Procedure di *data breach*[18] e Registro delle attività di trattamento[19].

- l'obbligo per il Titolare e per il Responsabile del trattamento di designare un "Responsabile della protezione dati" ("RPD"), quando il trattamento è effettuato da un'autorità pubblica, o il trattamento abbia ad oggetto dati sensibili o giudiziari (cfr. articolo 37 del Regolamento) e nell'obbligo, per il titolare del trattamento, di effettuare, in presenza di determinati casi, di effettuare una "Valutazione di impatto" sulla protezione dei dati[20].

---

[17] Ovvero, il titolare del trattamento deve porre in essere misure tecniche e organizzative adeguate per garantire, sin dalla fase della progettazione, la tutela dei diritti dell'interessato (privacy by design). In particolare il Considerando (78) *"La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici"* e art. 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita.

[18] Considerando (85) *"Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica"* e Articolo 33

[19] Si rammenta che la nozione di trattamento è ampia, rientrandovi «qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati».

[20] In particolare l'articolo 35 evidenzia la necessità della valutazione di impatto nei seguenti casi: - il trattamento determina una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che

- il concetto di "legittimo interesse" del titolare quale base giuridica su cui valutare la liceità delle operazioni di trattamento di dati personali, e che consente di considerare legittimo il trattamento dei dati, oltre che nelle ipotesi già previste dal Codice per la protezione dei dati personali (d.l.vo n. 196/2003), anche qualora lo stesso sia effettuato per perseguire uno scopo legittimo del titolare sempre a condizione, tuttavia, che non siano prevalenti su tale scopo gli interessi o i diritti e le libertà fondamentali dell'interessato (art. 6, 1° comma, lett. f). In definitiva, il titolare che abbia un legittimo interesse può procedere al trattamento anche in assenza del consenso da parte dell'interessato, di un rapporto contrattuale (o di misure precontrattuali), di obblighi legali, di esigenze di salvaguardia di interessi vitali dell'interessato o di altra persona fisica, di esercizio di poteri pubblici[21]. Si tratta di un concetto nuovo per il nostro ordinamento che consente di considerare legittimo il trattamento dei dati oltre che nelle ipotesi già previste dal Codice per la protezione dei dati personali (d.l.vo n. 196/2003) anche qualora lo stesso sia effettuato per perseguire uno scopo legittimo del titolare a condizione che non siano prevalenti su tale scopo gli interessi o i diritti e le libertà fondamentali dell'interessato (art. 6, 1° comma, lett. f).

Più nel dettaglio, la valutazione d'impatto del trattamento (D.P.I.A., cioè del *Data Protection Impact Assessment*[22]) è un onere posto direttamente a carico del titolare del trattamento, col quale si assicura trasparenza e protezione nelle operazioni di trattamento dei dati personali, imponendo al titolare l'onere di una valutazione preventiva delle conseguenze del trattamento dei dati sulle libertà ed i diritti degli interessati. Il responsabile del trattamento deve assistere il titolare nella conduzione della DPIA

---

hanno effetti giuridici; - il trattamento riguarda dati sensibili o giudiziari su larga scala; - sorveglianza sistematica su larga scala di una zona accessibile al pubblico. Le Autorità di controllo hanno un ruolo importante, in quanto possono stabilire, con un elenco pubblico, quali tipologie di trattamenti richiedono comunque la valutazione di impatto. Allo stesso modo, possono redigere un elenco delle tipologie di trattamenti per i quali la valutazione non è necessaria.

[21] Il Considerando (47) del GDPR chiarisce che per la valutazione della sussistenza di un legittimo interesse del titolare deve innanzitutto tenersi conto delle "*ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento*". Tale valutazione, che nell'impostazione del Regolamento è svolta autonomamente dal titolare, deve quindi basarsi su ciò che l'interessato potrebbe ragionevolmente attendersi rispetto al trattamento dei propri dati da parte del titolare con cui abbia rapporti (o venga in contatto). Il Regolamento indica all'articolo 6 i presupposti perché il trattamento di dati possa dirsi lecito: a. l'interessato ha espresso il consenso al trattamento per una o più specifiche; b. il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c. il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d. il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e. 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; f. il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

[22] Il Garante italiano segnala il software messo a disposizione dalla CNIL (autorità di controllo francese) per la valutazione di impatto sia nella versione *standalone* (da scaricare sul computer) che in quella *online*, come tool per realizzare la valutazione.

fornendo ogni informazione necessaria[23]. Conformemente alla nuova disciplina la valutazione d'impatto deve contenere: (i) una descrizione dei trattamenti previsti e delle finalità del trattamento[24]; (ii) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; (iii) una valutazione per i rischi per i diritti e le libertà degli interessati e le misure previste per affrontare i rischi. In ogni caso il titolare dovrà giustificare le sue valutazione e rendicontarle nel registro dei trattamenti. Il titolare deve consultarsi col DPO (art. 35) quando svolge la valutazione di impatto, il quale DPO ha il compito di fornire, se richiesto, un parere in merito alla valutazione di impatto e sorvegliarne lo svolgimento. La norma prevede che, nel caso in cui il titolare non dovesse trovare misure idonee a eliminare o ridurre il rischio, il DPO dovrà motivare e documentare il suo dissenso e se il dissenso non si risolve occorrerà consultare l'Autorità di controllo, che interviene solo *ex post*, sulle valutazioni del titolare, indicando le misure ulteriori eventualmente da implementare, fino ad eventualmente ammonire il titolare o vietare il trattamento[25].

2. Approfondimento: titolare, co-titolare e DPO

Circa la figura del titolare, va evidenziato che esso è, nella normativa in esame, individuato nella persona fisica o giuridica, sia essa autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del

[23] Vedasi Considerando (78) *"La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici"* e Articolo 25.

[24] Più nel dettaglio la valutazione d'impatto del trattamento (D.P.I.A., cioè Data Protection Impact Assessment) è un onere posto direttamente a carico del titolare del trattamento, col quale si assicura trasparenza e protezione nelle operazioni di trattamento dei dati personali, imponendo al titolare l'onere di una valutazione preventiva delle conseguenze del trattamento dei dati sulle libertà e i diritti degli interessati. Il responsabile del trattamento deve assistere il titolare nella conduzione della DPIA fornendo ogni informazione necessaria.

[25] I compiti delle autorità, sul proprio territorio, sono indicati dall'artt. 57 e 58 del Regolamento e e sono ripartiti in poteri di indagine (art. 58, co.1), poteri correttivi (art. 58, co.2) e poteri autorizzativi e consultivi (art. 58, co.3). Ad introdurre la facoltà di infliggere sanzioni amministrative pecuniarie con il GDPR è, invece, l'art. 83.

trattamento di dati personali[26]; più esattamente, il titolare del trattamento (o anche *data controller*) è colui che *"da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali"* (direttiva 95/46, art. 2 lett. d) e decide quali categorie di dati personali devono essere registrate o, anche, è "*la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza*" (Codice in materia di protezione dei dati personali, art. 4). In sostanza, come si ricava dalle disposizioni ricordate, è colui che tratta i dati senza ricevere istruzioni da altri, ovvero il soggetto che decide "perché" e "come" devono essere trattati i dati. Invero, è stato rilevato come l'introduzione del nuovo regolamento generale ha creato qualche problema nella traduzione dei termini, in quanto il termine *data controller* va tradotto, come stabilito dal Garante italiano, con titolare del trattamento, cioè colui il quale è responsabile per il trattamento medesimo. Questo ha creato qualche confusione col responsabile del trattamento che, invece, più correttamente è la traduzione di *data processor*. In definitiva, il titolare del trattamento non è, quindi, chi gestisce i dati, ma chi decide il motivo e le modalità del trattamento, ed è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa, sia nazionale che internazionale, in materia di protezione dei dati personali, compreso l'obbligo di notifica al Garante nei casi previsti. E' pacifico che il titolare è sempre vincolato al dovere di riservatezza dei dati, inteso come dovere di non usare, comunicare o diffondere i dati al di fuori del trattamento. Quindi egli deve garantire che i dati non siano persi, alterati, distrutti o comunque trattati illecitamente. In tale prospettiva spetta a lui stabilire le misure adeguate di sicurezza.

A tale figura si affiancano il co-titolare, ovvero, quando il trattamento dei dati viene determinano da altro soggetto (appunto il co-titolare o *jointes controllers)* congiuntamente per le finalità ed i mezzi del trattamento ed il personale del titolare che effettua le operazioni di trattamento dei dati o parte del trattamento per conto di un titolare[27]. Il *Data Protection Officer* (DPO) o anche Responsabile per la Protezione dei Dati (RPD) è il soggetto che ha una funzione di informazione, consulenza e controllo della gestione del trattamento di dati e che può essere un soggetto interno

[26] Un privato che effettua un trattamento di dati a fini esclusivamente personali non rientra nell'ambito applicativo della direttiva europea in materia di protezione dei dati, e quindi non assume la qualifica di Titolare. Ma la Corte di Giustizia europea (CGUE) ha stabilito che comunque la pubblicazione di dati altrui su Internet costituisce trattamento, poiché la pubblicazione online determina l'accessibilità da parte di un numero enorme di individui, e quindi si può parlare di diffusione sistematica.

[27] Il co-titolare del Trattamento è una persona fisica o giuridica, che affianca il titolare ed a cui competono le responsabilità di cui all' accordo tra le parti (art.26), che, redatto in forma libera, deve riflettere in modo puntuale i ruoli reciproci (art.26.2), il riparto degli obblighi previsti dal Regolamento (art. 26.1), il rapporto reciproco nel confronto degli interessati (art. 26.2), come ad esempio in materia di riscontro e di fornitura dell'informativa (art. 26.1).

all'organizzazione o un consulente esterno[28]. Per tale nuova figura il Regolamento europeo richiede che essa venga individuata in funzione delle qualità professionali e della preparazione specialistica della normativa e della pratica in materia di protezione dati (ex art. 37 comma 5 e 6)[29]. La funzione di RPD può essere attribuita ad un soggetto interno, ovvero, esterno alla società ed in tal caso esercitata in base ad un contratto stipulato con una persona fisica o giuridica esterna all'organismo titolare (ovvero, responsabile) del trattamento[30]. Il RPD è coinvolto, con funzioni consultive, di sorveglianza e monitoraggio, in tutte le questioni interne che riguardano la protezione dei dati ed è tenuto a stringenti obblighi di riservatezza. In merito, ai fini della designazione rilevano le *"Linee Guida sui responsabili della protezione dei dati*" (in breve, Linee Guida), pubblicate sul sito del Garante [31].

---

[28] Il DPO in realtà è l'evoluzione del "privacy officer", figura prevista dalla direttiva europea 95/46 laddove, all'art. 18, consentiva agli Stati dell'Unione di prevedere semplificazioni o esenzioni nei casi di designazione di un soggetto indipendente che garantisca l'applicazione della normativa.

[29] Dalle "Nuove Faq sul Responsabile della Protezione dei Dati (RPD)" del Garante, si può leggere*:" in ambito privato Il responsabile della protezione dei dati personali, al quale non sono richieste specifiche attestazioni formali o l'iscrizione in appositi albi, deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento. Deve poter offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare. Deve inoltre agire in piena indipendenza (Considerando (97) del Regolamento UE 2016/679) e autonomia, senza ricevere istruzioni e riferendo direttamente ai vertici. Il responsabile della protezione dei dati personali deve poter disporre, infine, di risorse (personale, locali, attrezzature, ecc.) necessarie per l'espletamento dei propri compiti".*

[30] Considerando (81) *"Per garantire che siano rispettate le prescrizioni del presente regolamento riguardo al trattamento che il responsabile del trattamento deve eseguire per conto del tito lare del trattamento, quando affida delle attività di trattamento a un responsabile del trattamento il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento. L'applicazione da parte del responsabile del trattamento di un codice di condotta approvato o di un meccanismo di certificazione approvato può essere utilizzata come elemento per dimostrare il rispetto degli obblighi da parte del titolare del trattamento. L'esecuzione dei trattamenti da parte di un responsabile del trattamento dovrebbe essere disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri che vincoli il responsabile del trattamento al titolare del trattamento, in cui siano stipulati la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, tenendo conto dei compiti e responsabilità specifici del responsabile del trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'interessato. Il titolare del trattamento e il responsabile del trattamento possono scegliere di usare un contratto individuale o clausole contrattuali tipo che sono adottate direttamente dalla Commissione oppure da un'autorità di controllo in conformità del meccanismo di coerenza e successivamente dalla Commissione. Dopo il completamento del trattamento per conto del titolare del trattamento, il responsabile del trattamento dovrebbe, a scelta del titolare del trattamento, restituire o cancellare i dati personali salvo che il diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento prescriva la conservazione dei dati personali"* ed Articolo 28 Responsabile del trattamento.

[31] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/

Ai sensi dell'art. 38, par. 3, del Regolamento europeo, il RPD "*riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento"* e, in effetti, tale rapporto garantisce che il vertice amministrativo sia a conoscenza delle indicazioni e delle raccomandazioni fornite dal RPD nel quadro delle sue funzioni di informazione e consulenza a favore del titolare o del responsabile. Un esempio di tale rapporto diretto consiste nella redazione di una relazione annuale delle attività svolte dal RPD da sottoporre al vertice gerarchico. Tuttavia, il fatto di riferire non prevede alcun vincolo di subordinazione. In effetti, il RPD, nell'esecuzione dei compiti spettanti ai sensi dell'articolo 39 del Regolamento, non deve ricevere istruzioni sull'approccio da seguire, anche nel mero "*caso specifico*" che si dovesse presentare, né ricevere istruzioni sull'interpretazione da dare ad una specifica questione attinente alla normativa in materia di protezione dei dati. Tuttavia, l'autonomia del RPD non significa che quest'ultimo disponga di un margine decisionale superiore al perimetro dei compiti fissati nel medesimo articolo 39 del Regolamento[32]. Il titolare o il responsabile, infatti, mantenere la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati.

L'assenza di conflitti di interessi è strettamente connessa agli obblighi d'indipendenza, che non confligge neanche con l'eventuale svolgimento di altre diverse funzioni nella stessa azienda, diverse funzioni che sono tuttavia sottoposte al vincolo che, l'affidamento di tali ulteriori compiti e funzioni, non diano adito a conflitti di interessi; ciò significa, in particolare, che un RPD non può rivestire, all'interno dell'organizzazione del titolare o del responsabile, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali. Si tratta dunque di un elemento da tenere in considerazione caso per caso guardando alla specifica struttura organizzativa del singolo titolare o responsabile. Peraltro, secondo quanto previsto dalle citate Linee Guida, possono sussistere situazioni di conflitto all'interno dell'organizzazione del titolare o del responsabile riguardo a ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT), ma anche rispetto a posizioni

[32] Articolo 39 Regolamento *" Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; d) cooperare con l'autorità di controllo; e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione".* 2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

gerarchicamente inferiori, se queste ultime comportano la determinazione di finalità o mezzi del trattamento.

L'articolo 38, secondo paragrafo, del Regolamento, obbliga il titolare o il responsabile a sostenere il RPD "*fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica"*. Ciò secondo le "Linee Guida" si traduce in un'adeguata disponibilità di tempo (se il RPD è adibito ad altre mansioni), sia di risorse finanziarie che di infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, di personale.

Il DPD ed è obbligatorio in alcuni specifici casi, come quando: il titolare è un'autorità o un organismo pubblico (salvo il caso di autorità giurisdizionali), se le attività principali del titolare o del responsabile consistono in trattamenti che, per loro natura, ambito di applicazione e finalità, richiedono un monitoraggio regolare e sistematico dei soggetti interessati su larga scala; oppure, se le attività principali del titolare o del responsabile comprendono il trattamento, su larga scala, di dati particolari e di dati relativi a condanne penali e a reati. Al DPD compete l'istituzione del Registro delle attività di trattamento (l'articolo 30 del Regolamento)[33], della cui tenuta egli stesso è responsabile. Per avviare il registro è essenziale avviare la ricognizione dei trattamenti svolti e delle loro principali caratteristiche, ovvero, le finalità del trattamento, la descrizione delle categorie di dati e interessati, le categorie di destinatari cui è prevista la comunicazione, le misure di sicurezza adottate, da adottare e suggerite, i tempi di conservazione, ed ogni altra informazione che il titolare ritenga opportuna al fine di documentare le attività di trattamento svolte[34].

3. La notifica delle violazioni dei dati personali

[33] Art. 30 Regolamento "*1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni: a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati; b) le finalità del trattamento; c) una descrizione delle categorie di interessati e delle categorie di dati personali; d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1. 2. ...*", e Considerando (82).

[34] In dettaglio, si necessita comunque almeno la predisposizione e l'aggiornamento della documentazione attestante i trattamenti svolti (registro dei trattamenti; valutazione di impatto, trasferimento dati extra UE), della documentazione attestante il rispetto dei diritti degli interessati (informative, moduli raccolta consenso) di quella di ripartizione ruoli e responsabilità (contratti e nomine dei responsabili esterni e incaricati; procedure interne, ecc...), nonché della documentazione attestante le misure di sicurezza implementate.

Un'ulteriore novità introdotta dal nuovo Regolamento UE sulla Protezione dei dati (GDPR) nella gestione del fenomeno del *data breach.* Esso si sostanzia nelle ipotesi di incidenti di sicurezza in cui dati sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato e si realizza con una divulgazione di dati riservati o confidenziali all'interno di un ambiente privo di misure di sicurezze (da esempio, su web) in maniera involontaria o volontaria. In pratica, tale divulgazione può avvenire in seguito ad una perdita accidentale come, ad esempio, lo smarrimento di una chiavetta USB contenente dati riservati, un furto di un *notebook* contenente dati confidenziali, o addirittura quando una persona interna (all'azienda o alla P.A.) che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico, ovvero, da accesso abusivo, che si realizza da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite. Tale evento è previsto all'art. 4, c. 12 del Regolamento europeo, che definisce il data breach *"... la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati"* e sancisce l'obbligo, con modalità e tempistiche differenti a seconda dei settori d'attività, di comunicare le citate eventuali violazioni di dati personali al Garante ed, in alcuni casi, anche ai soggetti interessati[35]. L'art. 33 del GDPR dispone, infatti, che in caso di violazione dei dati personali, il titolare del trattamento notifichi la violazione all'autorità di controllo competente ai sensi dell'articolo 55 del Regolamento europeo senza ingiustificato ritardo, 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 non sia effettuata entro 72 ore, la notifica all'autorità di controllo è corredata di una giustificazione motivata[36]. Ai sensi della norma richiamata, tale notifica deve come minimo*:" ... a) descrivere la natura della violazione dei dati*

[35] Il Garante, con il provvedimento del 4 aprile 2013, pubblicato sulla Gazzetta Ufficiale n. 97 del 4 aprile 2013, ha dato attuazione alla direttiva europea 2009/136/CE – che ha modificato, in parte, la direttiva 2002/58/CE – sulla privacy nel settore delle comunicazioni elettroniche. Nel provvedimento si prevede che le società telefoniche e Internet Service Provider hanno l'obbligo di comunicazione entro 24 ore dalla scoperta dell'evento, e di fornire al Garante le informazioni necessarie a consentire una prima valutazione dell'entità della violazione. Inoltre è previsto l'obbligo di informare ciascun utente coinvolto entro 3 giorni dalla scoperta. Per i casi di Data breach su sistemi biometrici c'è l'obbligo di comunicare entro 24 ore dalla conoscenza del fatto, con comunicazione tramite apposito modello di tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi. Quanto ai Data breach su dossier sanitario elettronico vige l'obbligo di comunicare entro 48 ore dalla conoscenza del fatto, con comunicazione tramite apposito modello tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario. Infine, per i Data breach per le amministrazioni pubbliche c'è l' obbligo di comunicare entro 48 ore dalla conoscenza del fatto, con comunicazione tramite apposito modello tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati.

[36] Al fine del rispetto del termine di 72 ore deve essere definita una procedura ad hoc che stabilisca i controlli da effettuare e le modalità di realizzazione degli stessi al fine di offrire una segnalazione precisa e coerente al Garante che permetta, al tempo stesso, di intervenire tempestivamente per bloccare la perdita di dati

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

L'art. 34 prevede inoltre, la comunicazione di una violazione dei dati personali all'interessato, quando la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, senza ingiustificato ritardo. La predetta comunicazione deve descrive "*con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le raccomandazioni di cui all'art. 33 paragrafo 3, lettere b), c) e d)".* Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità Garante può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che non ve ne sia bisogno in quanto una delle condizioni richieste dalla normativa sia da ritenere soddisfatta. Il Regolamento europeo si premura anche di stabilire le possibili ipotesi di esenzione dall'onere di comunicazione. Infatti, detta comunicazione non è dovuta quando: *"a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1; c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia*".

Infine va rilevato che il titolare del trattamento ha l'onere di documentare qualsiasi violazione dei dati personali, incluse le circostanze in cui si è verificata, le sue conseguenze ed i provvedimenti adottati per porvi rimedio e che la documentazione in discorso deve, oltre ad essere a disposizione, consentire all'autorità di controllo di verificare il rispetto dell'art. 33 (del Regolamento).

Va osservato, peraltro, che il Regolamento disegna un quadro normativo di principio che lascia spazio a norme di dettaglio ed a semplificazioni differenziate per settore e attività. In particolare, l'articolo 40 GDPR favorisce l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del Regolamento. Prevede, infatti, la citata norma *"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". I soggetti deputati sono le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento che, alla bisogna, possono *"… elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente regolamento*". In particolare, ai sensi del citato articolo 40, comma 2, le materie oggetto di elaborazione di codici di condotta, possono riguardare il *"… trattamento corretto e trasparente dei dati, gli legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici, la raccolta dei dati personali, la pseudonimizzazione dei dati personali, l'informazione fornita al pubblico e agli interessati, l'esercizio dei diritti degli interessati, l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore, le misure e le procedure di cui agli articoli 24 e 25 e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32*[37]*, la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato, il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, o le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli articoli 77 e 79"*.

4. Principali riflessi nella disciplina per banche e intermediari

La protezione dei dati personali è un tema di cruciale importanza per gli istituti bancari atteso che assicurare la riservatezza e la sicurezza dei dati bancari, inclusi i dati personali, oltre ad evitare di incorrere nelle sanzioni previste dalla passata e dalla nuova disciplina, è certamente elemento di capacità concorrenziale. La questione relativa alla circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie già affrontata con provvedimenti del Garante n. 192/2011 e n. 357/2013[38], dovrà essere aggiornata con le modifiche previste nel Regolamento. In merito, di prezioso aiuto è la su richiamata "Guida all'applicazione del Regolamento UE 2016/679 in materia di protezione dei dati personali". Il Garante individua sei questioni principali, specificandone gli elementi di novità e di continuità rispetto agli elementi del Codice

[37] Il Considerando (77) prevede: *"Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti in particolare mediante codici di condotta approvati, certificazioni approvate, linee guida fornite dal comitato o indicazioni fornite da un responsabile della protezione dei dati. Il comitato può inoltre pubblicare linee guida sui trattamenti che si ritiene improbabile possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e indicare quali misure possono essere sufficienti in tali casi per far fronte a tale rischio*", e Articolo 32

[38] "Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie" - 12 maggio 2011 (Pubblicato sulla Gazzetta Ufficiale n. 127 del 3 giugno 2011) e "Chiarimenti in ordine alla delibera n. 192/2011 in tema di circolazione delle informazioni riferite a clienti all'interno dei gruppi bancari e 'tracciabilità' delle operazioni bancarie; proroga del termine per completare l'attuazione delle misure originariamente prescritte" - 18 luglio 2013

Privacy ed offrendo consigli pratici sui possibili approcci da adottare in vista della piena applicazione del GDPR**.** Al fine di chiarire alcune delle ambiguità contenute nel Regolamento europeo, un ulteriore supporto certamente verrà dal Gruppo dei Garanti Europei[39], che già si è attivato per realizzare delle linee guida all'applicazione pratica del nuovo dettato normativo[40].

L'analisi condotta nei precedenti paragrafi ha messo in evidenzia come, rispetto all'attuale disciplina di riferimento, il Regolamento si incardina sugli obblighi e sulla responsabilizzazione del titolare (e del co-titolare) e del responsabile del trattamento[41]. Tale principio di *accountability*, come già più sopra rilevato, si traduce nell'adozione di misure tecniche e di modelli organizzativi atti a garantire che la gestione e la conservazione dei dati avvenga in maniera conforme ai principi di protezione dei dati personali. In adempimento, dunque, il titolare del trattamento sarà tenuto a svolgere un'analisi preventiva dell'impatto del trattamento (*Data Privacy Impact Assessment*) che consenta d'individuare ed applicare, sin dalla progettazione del servizio o prodotto, i correttivi opportuni per la prevenzione del rischio[42]. Quanto alle misure di sicurezza, il GDPR richiede che le stesse siano in grado di garantire un livello di sicurezza "*adeguato al rischio*", offrendo una lista aperta di misure applicabili. Gli istituti bancari, nell'implementare il sistema, non potranno non tener conto sia delle singolarità previste dalle varie disposizioni di vigilanza della Banca d'Italia, che delle disposizioni contenute nelle prescrizioni in materia di tracciamento degli accessi ai dati bancari dei clienti, tempi di conservazione dei relativi file di log e implementazione di *alert* di rilevazione di intrusioni o accessi anomali ai dati bancari. Al *Data Protection Officer*, dunque, è demandato il compito di valutare, organizzare e governare la gestione del trattamento dei dati nel rispetto della nuova normativa. Più nello specifico, circa il trattamento di dati personali in rispetto alla normativa precedente, il GDPR non richiede né la forma scritta né la documentazione per iscritto del consenso al trattamento, ma prevede che il titolare

[39] L'art. 29 della Direttiva 95/46/CE prevede l'istituzione del Gruppo quale organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione.

[40] Sono state approvate le linee guida: *"sul diritto alla portabilità dei dati"* Wp 242, sul "RDP" Wp 243, *"sull'autorità capofila*" Wp 244 e "*sulla valutazione d'impatto privacy e sulla determinazione dei casi nei quali il trattamento deve essere considerato ad alto rischio*" Wp 248, mentre hanno concluso la consultazione "*sulla Notificazione dei data breach*" Wp 250 e "*sul processo decisionale automatizzato relativo alle persone fisiche compresa la profilazione*" Wp 251

[41] Il Considerando (74) prevede: *"È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare 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".* Vedasi anche Articolo 5, paragrafo 2, e Articolo. 24.

[42] Se dal DPIA risulti impossibile individuare delle *misure "opportune in termini di tecnologia disponibile e costi di attuazione"* atte ad attenuare sufficientemente il rischio del trattamento dovrà di questo rendersi edotto il Garante.

del trattamento sia "*in grado di dimostrare che l'interessato ha acconsentito a tale trattamento*[43]. Sarà, dunque, necessario - in relazione ad uno specifico trattamento - tenere idonea traccia del consenso accordato. Quanto al legittimo interesse, modalità in un certo senso alternativa al consenso per il trattamento dei dati, la novità del GDPR consiste di rimuovere il limite ai casi indicati dal Garante[44], con il che, tuttavia, resta rimessa al titolare del trattamento la valutazione circa la prevalenza del legittimo interesse del titolare (o del terzo rispetto) ai diritti ed alle libertà dell'interessato.

I contenuti dell'informativa da fornire al trattato elencati nel GDPR sono più estesi rispetto al Codice Privacy[45] e vanno forniti per iscritto; tuttavia, per i servizi resi tramite sito *web*, l'informativa può essere anche provvista in formato elettronico, anche con "icone", che richiamino, tuttavia, per esteso gli elementi informativi necessari. Circa, inoltre, il diritto dell'interessato di ottenere la cancellazione dei dati personali senza ingiustificato ritardo, si tratterà certamente d'implementare quelle possibili soluzioni tecniche che siano in grado di assicurare la cancellazione automatica dei dati e, si badi bene, non solo sul singolo sistema aziendale tramite il quale i dati sono stati raccolti, ma anche su tutti gli altri sistemi all'interno dei quali tali dati sono eventualmente transitati. L'anzidetta innovazione si accompagna al diritto alla portabilità; in effetti, l'onere di dar corso alle richieste di cancellazione, come a quelle di portabilità, impone sia l'adeguamento delle politiche interne quanto la mappatura dei dati e dei flussi di dati trattati da parte del titolare del trattamento, in modo tale che si rispetti sia la norma che la volontà dell'interessato richiedente, ma anche che sia garantito una maggior controllo dei dati di modo da limitare o evitare la divulgazione di notizie ulteriori, come informazioni confidenziali o segreti industriali, ad altri titolari eventualmente concorrenti. Peraltro, nel caso in cui la banca elabori essa stessa i dati dei clienti, cioè, risulti unico titolare del trattamento, si dovrà procedere a nominare formalmente il responsabile del trattamento con specifica indicazione della natura, durata e finalità del trattamento o dei trattamenti assegnati, nonché delle categorie di dati oggetto di trattamento, delle misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento, anche ai fini dell'adempimento degli obblighi in caso di *data breach* e della cancellazione dei dati al termine della fornitura dei servizi. Per altro verso, qualora la banca sia co-titolare del trattamento dei dati assieme alla società di gestione dei sistemi informativi, dovrà essere definito specificamente il rispettivo ambito di responsabilità ed i rispettivi compiti con riferimento all'esercizio dei diritti degli interessati, fatta salva, naturalmente, la

[43] Come già previsto dal Codice Privacy, il consenso deve essere libero, specifico, informato e manifestato mediante "*dichiarazione o azione positiva inequivocabile*". In questo senso, non possono essere intesi come volti a prestare il consenso il silenzio, l'inattività o la preselezione di caselle.

[44] Il Codice Privacy prevedeva la possibilità di trattamento senza consenso: *"nei casi individuati dal Garante sulla base dei princìpi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato"*

[45] Tra le altre, una novità rilevante riguarda l'esigenza di riportare in informativa l'indicazione del periodo per il quale i dati raccolti e trattati verranno conservati.

responsabilità solidale dei contitolari nei confronti degli interessati, e ciò indipendentemente da tale ripartizione di compiti e obblighi.

Si segnala che il GDPR ha confermato l'approccio attualmente vigente in materia di flussi di dati al di fuori dell'Unione europea, prevedendo, in linea di principio, che tali flussi sono vietati, a meno di specifiche garanzie, quali ad esempio una decisione di adeguatezza del Paese terzo coinvolto riconosciuta tramite decisione della Commissione europea, ovvero, l'esistenza di garanzie adeguate di natura contrattuale o pattizia. Su punto, l'allineamento fra la normativa nazionale e le disposizioni del Regolamento richiederà evidentemente un grande sforzo, sia per le banche italiane che per quelle europee. In effetti, ed in particolare, come hanno già evidenziato attenti commentatori[46], il venir meno del requisito dell'"autorizzazione nazionale", nel senso che il trasferimento verso un Paese terzo "adeguato" in base alla decisione assunta dalla Commissione europea, ovvero, a delle clausole contrattuali modello o di norme vincolanti d'impresa potrà avere inizio già a partire dall'entrata in vigore del Regolamento e senza attendere l'autorizzazione Garante[47].

Infine, a parere di chi scrive, novità degna di segnalazione è la possibilità per i gruppi bancari di individuazione di un'unica autorità di controllo di rifermento a livello comunitario, che funge da "sportello unico" per i trattamenti transnazionali, laddove, il titolare o il responsabile tratti dati personali in più stabilimenti nell'UE offra prodotti o servizi in più Paesi Ue[48].

5. Regime sanzionatorio

Il mancato o ritardato adempimento della comunicazione espone, naturalmente, alla possibilità di sanzioni amministrative.

Nel caso di trattamento in violazione delle norme del regolamento europeo, il titolare risponde per il danno cagionato all'interessato, secondo quanto previsto dall'articolo 82 e dal Considerando (146). Il titolare risponde in caso di violazione delle disposizioni del GDPR, ma anche delle norme attuative, degli atti delegati, delle norme esecutive e di tutte le altre disposizione degli Stati membri. Se più titolari o responsabili sono coinvolti nello stesso trattamento e sono responsabili del danno causato, ne rispondono in solido per l'intero danno, al fine di garantire l'intero risarcimento. Ovviamente chi paga l'intera

[46] "Gli istituti bancari al test del Regolamento privacy europeo" di Giangiacomo Olivi e Laura Borelli, Rivista Bancaria del 30/05/2017

[47] Considerando (36) *"... Se il trattamento è effettuato da un gruppo imprenditoriale, lo stabilimento principale dell'impresa controllante dovrebbe essere considerato lo stabilimento principale del gruppo di imprese, tranne nei casi in cui le finalità e i mezzi del trattamento sono stabiliti da un'altra impresa*". Va da sé che, tuttavia, tale autorizzazione sarà ancora necessaria se un titolare desidera utilizzare clausole contrattuali *ad-hoc* (cioè non riconosciute come adeguate tramite decisione della Commissione europea) oppure accordi amministrativi stipulati tra autorità pubbliche.

[48] Vedasi linee guida del 13 dicembre 2016, come aggiornate lo scorso 5 aprile per comprendere nel dettaglio le modalità di individuare dell'autorità capofila.

somma avrà diritto di regresso nei confronti degli altri responsabili per la quota. Il titolare ed il responsabile saranno esonerati da responsabilità se dimostrano che l'evento dannoso non è imputabile alla loro condotta, o se dimostrano di aver adottato tutte le misure idonee per evitare il danno stesso. La previsione di un apposito regime sanzionatorio per le violazioni delle disposizioni del Regolamento che recano obblighi in capo al titolare del trattamento ed al responsabile del trattamento sono previste all'art. 83, par. 4 e 5, del Regolamento. La violazione prevede regime che immagina due livelli di infrazione, che considerano come sanzioni multe fino a 20 milioni di Euro (o al 4% fatturato di gruppo) per il primo livello di infrazioni e fino a 10 milioni di Euro o al 2% fatturato per il secondo livello d'infrazioni. Il primo livello d'infrazioni, soggette a sanzioni più pensanti, riguardano i principi di base del trattamento, comprese le condizioni relative al consenso, i diritti degli interessati, gli ordini o limitazioni del Garante, la Normativa speciale nazionale e il Trasferimento dati extra UE. Il secondo livello d'infrazioni, riguarda, invece, la sicurezza e *data breach*, i principi di *privacy by design* e *by default*, il consenso dei minori (16 anni), il registro delle attività e PIA, la cooperazione con il Garante e la *governance* interna.

6. Conclusioni. Cosa si deve fare ?

Ciò premesso, nell'attuale contesto caratterizzato da una crescente minaccia alla sicurezza dei sistemi informativi, appare fondamentale la pronta attuazione delle nuove misure relative alle violazioni dei dati personali, tenendo in particolare considerazione i criteri di attenuazione del rischio indicati dalla disciplina europea e individuando quanto prima idonee procedure organizzative per dare attuazione alle nuove disposizioni (art. 33 – 34 del Regolamento). Risulta, dunque, da quando cennato che uno dei punti centrali della nuova disciplina europea è rappresentato dalla necessità di garantire che i dati personali siano trattati in modo da garantirne l'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato degli stessi dati. Infatti, presupposto essenziale del principio di *accountabilty* (responsabilizzazione) del titolare del trattamento è rappresentato dal dovere di adottare "*misure tecniche e organizzative adeguate*" al fine di evitare il rischio che si verifichino trattamenti non autorizzati o illeciti, nonché la perdita o la distruzione dei dati personali e delle attrezzature impiegate per il trattamento. Con riguardo a queste misure "*di sicurezza*", il Regolamento richiama, con valore esemplificativo e non esclusivo (l'art. 30), la pseudonimizzazione e la cifratura, chiaramente ispirate a un tipo di trattamento realizzato con l'ausilio di strumenti elettronici[49]. Risulta dunque opportuno che le soluzioni di sicurezza (tecnologica,

[49] Tra le tecniche di anonimizzazione più utilizzate, si possono segnalare, il c.d. data masking che consiste nella mera cancellazione dei principali identificativi personali (nome, data di nascita, etc.: è quella usata, ad esempio, per la pubblicazione delle sentenze nelle banche dati giuridiche), la pseudoniminizzazione, ovvero, la tecnica con la quale si attribuisce un attributo univoco di un dato con un altro; la persona potrebbe, comunque, essere identificata in maniera indiretta e, infine, l'aggregazione, che resta una delle tecniche ritenute più sicure e che consiste nel pubblicare i dati personali di molti in modo aggregato; come sommatoria di dati di molti individui, la possibilità di una re-identificazione, diviene molto remota (benché non impossibile).

organizzativa e logistica) in tema di strutture informative risultino quanto più armoniche ed omogenee possibile con quelle da assumere in materia di protezione dei dati personali al fine di rendere il sistema flessibile ed idoneo per gli scopi assegnati.

Nella sostanza, in sequenza logico temporale, dovranno essere compiuti vari adempimenti ed attività di verifica da svolgersi a cominciare dall'attività di *assessment* (ovvero valutazione) per verificare appunto lo stato dell'arte in materia di trattamento dei dati (che devono essere auditati tutte le aree preposte al trattamento). Va dunque verificato si per l'azienda corre l'obbligo o meno di nomina del DPO (o consulente di supporto per transizione GDPR) e vanno di conseguenza, eventualmente, ridefiniti i ruoli interni e predisposti gli atti conseguenti alle nomine. Vanno da se, la riscrittura degli organigrammi di privacy, la verifica di "compliance" al GDPR del sistema aziendale di videosorveglianza, e dei rapporti contrattuali con fornitori esterni nominati responsabili del trattamento nonché la verifica delle competenze (eventuale ricollocazione dei server). Va, quindi, redatto il registro dei trattamenti effettuati in qualità di titolare (anche se in *outsourcing*) del registro dei trattamenti effettuati in qualità di responsabile (per conto terzi) e si dovrà verificare la conformità delle informative e dei consensi già acquisiti rispetto al GDPR, la redazione nuove informative e consensi per la compliance al GDPR, nonché la verifica di compliance rispetto al GDPR del sito internet.

Altre questioni riguardano la definizione o l'adeguamento delle procedure per gestire le richieste degli interessati di modificare, cancellare, accedere, portare i dati, implementate politiche *privacy by design* e *privacy by default*, la definizione o l'adeguamento delle procedure di monitoraggio dei sistemi ICT e di notifica dei data breach, nonché la conformità rispetto al GDPR delle misure di sicurezza informatiche. La definizione della procedura di svolgimento del Data Protection Impact Assessment e del fabbisogno formativo di ciascuna "tipologia" di ruolo e, inoltre, della Programmazione audit di mantenimento di raccolta di tutte le procedure interne e del registro dei trattamenti (Sistema Gestione Privacy), costituisco ulteriore elemento d'implementazione.

Dunque, da quanto sopra osservato, ne consegue che il Regolamento europeo impone di necessità la nomina di un consulente in grado di adeguare il "sistema azienda" alle nuove modalità di gestione del dato ed al principio di accountability, capace di valutare l'adeguatezza o meno dei propri processi di compliance. Per tale incarico, che non può essere assegnato solo ad un professionista del settore legale, ma neanche esclusivamente ad una società informatica, si pone il problema di individuare un soggetto che possegga ambedue le professionalità. Inoltre, si pone il problema di nominare, per le società che devono avere tale figura professionale, un DPO, che può anche essere individuato all'interno dell'azienda, salvo che non vi sia un soggetto con una competenza specifica in materia, nonché di dare corso ad un investimento in infrastrutture IT. Le osservazioni

fatte lasciano intendere che il GDPR rappresenta un costo (di non poco conto) per le aziende ma anche un'opportunità per i consulenti in materia[50].

Fino ad ora abbiamo evidenziato e sommariamente trattato gli elementi di novità del Regolamento europeo, cioè, in definitiva, quello che cambia. Trovano, invece, conferma nel GDPR i principi generali già delineati dal previgente quadro normativo che sommariamente potremmo definire di rispetto delle norme (liceità) e rispetto delle reciproche esigenze dell'interessato e del titolare (correttezza), nonché di trasparenza verso l'interessato affinché possa legittimamente fondare il proprio consenso al trattamento dei dati personali. Inoltre, trova conferma il principio che i dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione e devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. In particolare, il principio secondo il quale i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità o con il legittimo interesse del titolare. Per ogni diversa finalità deve essere richiesto uno specifico consenso. I dati raccolti devono essere esatti e, se necessario, aggiornati anche prevedendo misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati. Permane, infine, il principio della limitazione della conservazione; i dati personali, infatti, continuano a dover essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati[51].

[50] L'IAPP (International Association of Privacy Professionals) ed Ernst & Young hanno recentemente pubblicato una ricerca su un campione di 600 esperti di privacy provenienti da tutto il mondo dalla quale emergono i seguenti dati: Il 75% delle multinazionali Europee (ossia società con più di 75.000 dipendenti nel mondo) hanno previsto un investimento di almeno 5 milioni di euro per l'adeguamento al GDPR con l'assunzione di almeno 2 o 3 dipendenti dedicati a tempo pieno al tema privacy. Interessante notare che gli stessi tipi di investimenti vengono effettuati dal 50% delle grandi multinazionali statunitensi. Delle circa 30.000 aziende seguite dai 600 esperti coinvolti in tale tipo di ricerca, solo il 60% sarà "fully compliant" ossia pienamente conforme al GPDR entro maggio 2018. A distanza quindi di 7 mesi dall'entrata in vigore della normativa, molte società (soprattutto le PMI) si stanno rendendo conto di non riuscire ad arrivare in tempo alla scadenza prevista dal Regolamento Europeo. Il valore medio di investimento per l'adeguamento al GDPR per le aziende nel 2016 era di 349.000 euro, mentre nel 2017 è salito a 480.000 euro. Tale importo è rappresentato sia dai costi HR derivanti dal ruolo del DPO, dai costi dei consulenti e dagli investimenti in IT derivanti dalla necessità di essere compliant alla normativa. L'investimento complessivo nel 2017 è stato di 6,5 miliardi di Euro su 30.000 aziende.

[51] Ricordiamo che i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici