

Giuseppe Nucci

Protezione dei dati personali e GDPR: dai precetti giuridici ai processi organizzativi

DPO e altri profili professionali – Processi e prassi –
Modello operativo efficace e compliant rispetto
al General Data Protection Regulation

Prefazione: avvocato Giulia Adotti
Presentazione: avvocato Christiane Colinet

QUESTO VOLUME È ANCHE ONLINE

Consultalo gratuitamente ne "LA MIA BIBLIOTECA", la prima biblioteca professionale in the cloud con le pubblicazioni di **CEDAM, UTET Giuridica, IPSOA, ALTALEX**.

Grazie ad un evoluto sistema di ricerca, puoi accedere ai tuoi scaffali virtuali e trovare la soluzione che cerchi da PC o tablet. Ovunque tu sia.

Per conoscere le modalità di accesso al servizio e consultare il volume online, collegati al sito www.lamiabiblioteca.com

La consultazione online viene offerta all'acquirente del presente volume a titolo completamente gratuito ed a fini promozionali del servizio "La Mia Biblioteca" e potrebbe essere soggetta a revoca da parte dell'Editore.

PROPRIETÀ LETTERARIA RISERVATA

© 2018 Wolters Kluwer Italia S.r.l. Via Dei Missaglia, 97, Edificio B3, 20142 - Milano

ISBN: 978-88-217-6666-4

Il presente file può essere usato esclusivamente per finalità di carattere personale. I diritti di commercializzazione, traduzione, di memorizzazione elettronica, di adattamento e di riproduzione totale o parziale con qualsiasi mezzo sono riservati per tutti i Paesi.

La presente pubblicazione è protetta da sistemi di DRM. La manomissione dei DRM è vietata per legge e penalmente sanzionata.

L'elaborazione dei testi è curata con scrupolosa attenzione, l'editore declina tuttavia ogni responsabilità per eventuali errori o inesattezze.

*Dedico questo libro a coloro che hanno intenzione di leggerlo,
ai quali - per onestà - devo però precisare
che mi sono ispirato a questo aforisma
di Nicolás Gómez Dávila:
«I libri seri non istruiscono, interrogano».
Sulla serietà del libro non garantisco ma sul resto...*

L'Autore

PROFILO AUTORE

Giuseppe Nucci

Giuseppe Nucci ha ricoperto incarichi di responsabilità in diverse pubbliche amministrazioni (per ultimo è stato Direttore della sicurezza dell'Agencia delle Entrate e Direttore dell'*Internal Audit* dei Monopoli dello Stato e del Comune di Roma), acquisendo competenze sia specialistiche che trasversali.

Ha maturato una ventennale esperienza come docente presso istituti universitari e scuole di formazione manageriale, approfondendo tematiche relative all'*internal audit*, al *risk management*, ai modelli organizzativi, alla gestione del capitale umano e alla comunicazione organizzativa, anche in relazione alle necessarie connessioni con il *data protection*. Attualmente collabora con la *Luiss Business School*, la *Business School 24*, l'*Università di Pisa* (Dipartimento di Economia e Management) ed il *CEIDA* di Roma.

Giornalista pubblicista, collabora con il *Quotidiano degli Enti locali e della pubblica amministrazione* del Sole24ore e con il sito www.riskcompliance.it. Ha pubblicato circa 50 pubblicazioni (recentemente gli e-book *L'internal audit nelle amministrazioni pubbliche* (2016) e *Controlli interni e risk management nelle amministrazioni pubbliche*. Dalla cultura dell'adempimento alla gestione manageriale (2018), entrambi editi dal Sole24ore).

È Presidente dell'Organismo indipendente di valutazione e della performance (OIV) del Comune di Reggio Emilia, Presidente dell'Organismo di Vigilanza di Napoli Servizi S.p.A. e Componente dell'Organismo di Vigilanza dell'ente pubblico economico ATER di Roma.

PREFAZIONE

Il *diritto alla Privacy* come delineato nel Nuovo Regolamento Europeo per la Protezione dei Dati 679/2016, corrisponde ad un sistema molto più complesso ed articolato rispetto alle normative nazionali dei singoli Stati membri, un sistema volto alla protezione dei dati personali e basato essenzialmente - a parere della scrivente - su tre principi cardine: primo fra tutti l’**“awareness”** ossia il principio di **“consapevolezza”** per cui i dati che rendono una persona identificata od identificabile sono un patrimonio da tutelare e di cui essere responsabili innanzitutto per il soggetto interessato. Da quanto detto discende il secondo principio, ovvero quello dell’**“accountability”**; si rafforza, infatti, nella disciplina regolamentare europea il concetto di **“responsabilizzazione”** anche per i soggetti che determinano finalità e mezzi del trattamento o che trattano i dati per conto di questi con un approccio proattivo e non solo reattivo, a fronte di una eventuale ipotesi di violazione del dato personale. Ciò che viene preteso dai Titolari e Responsabili del Trattamento è che mettano in campo azioni e comportamenti che prevengano in modo effettivo l’eventuale evento dannoso che potenzialmente possa ledere i diritti e le libertà delle persone.

Quanto negli anni è stato espresso dai massimi interlocutori internazionali della materia (si veda fra le altre l’Opinion 3/2010 del WP art. 29) è stato chiaramente tradotto nell’art. 24 del GDPR 679/2016, norma che per l’appunto porta il titolo **“Responsabilità del Trattamento”** e che in sostanza contiene l’obbligo da parte del Titolare del Trattamento di essere *compliant* alle previsioni del Regolamento garantendo e conseguentemente dimostrando la conformità delle misure adottate, sulla base dell’analisi dei rischi, anche in termini probabilistici e di valutazione della gravità degli stessi.

Di fatto, quindi, le misure organizzative e di sicurezza sono impostate su scelte operate dal Titolare e dal Responsabile del trattamento sulla base della valutazione iniziale del rischio. Il terzo principio, quindi, si incardina su un approccio metodologico di **“privacy by design”** ossia di progettazione del trattamento dei dati che preveda una pianificazione della protezione del dato ancor prima dell’avvio del trattamento.

Intorno alla realizzazione della c.d. *“governance”* della *data protection* ruotano attori, processi, metodologie ed analisi in applicazione delle norme e delle prassi già consolidate a livello internazionale, anche sulla base di standard riconosciuti in altri ambiti, per costruire un modello organizzativo conforme alla nuova normativa europea.

Insomma, siamo di fronte alla *“modernizzazione”* del diritto della *privacy* e la forma (e la sostanza) del Regolamento (basta vedere come sono normate le sanzioni e come sono delineate le attività delle *“Autorità”*) denuncia l’assimilazione del *drafting* normativo e dell’istituto con modelli ben consolidati

e di sicuro rilievo (il paragone con il sistema del diritto della Concorrenza pare calzante, almeno per gli aspetti sopra citati).

Il testo di Giuseppe Nucci ha quindi il merito di inserirsi in questa fase di avvio dell'applicazione del GDPR e di contribuire inizialmente a chiarire aspetti articolati e complessi che solo successive regolamentazioni ed interpretazioni potranno meglio definire.

Giulia Adotti

Avvocato - Partner Studio Legale Adotti - Adotti & Associati

PRESENTAZIONE

L'entrata in vigore, il 25 maggio scorso, del regolamento europeo 2016/679/UE, Regolamento generale sulla protezione dei dati personali (*RGDP* o *GRDP* -secondo l'acronimo inglese-) segna una pietra miliare nello sviluppo di un quadro regolatore armonizzato a livello europeo in uno dei settori più sensibili della tutela dei diritti umani, quella dei dati personali, diventati, con lo sviluppo sfrenato delle tecnologie oggetto di business sregolato e di ogni genere di manipolazioni. Basti pensare al recente scandalo della raccolta dati di *Facebook* da parte della società *Cambridge Analytica* per creare programmi in grado di prevedere e orientare scelte elettorali.

Nella società moderna, si è, infatti, enucleata una gestione del dato separata dal fenomeno cui il dato si riferisce. L'automazione sempre più spinta dei processi di raccolta e memorizzazione delle informazioni e la loro digitalizzazione ha facilitato l'accumulazione, il trattamento e la circolazione dei dati, circolazione facilitata da Internet. I dati personali, una volta forniti, fuoriescono dalla sfera di controllo dei loro titolari per diventare oggetto di mercato, fonte di valore economico, *core business* di alcune imprese. Si assiste al diffondersi di sistemi che vivono sulla circolazione di dati. Lo sviluppo delle tecnologie ha anche permesso una sempre maggiore precisazione dei dati rilevabili: geolocalizzazione, genetica, biometria etc. I processi automatizzati di intelligenza artificiale facilitano, inoltre, l'estrazione, le interrelazioni e la manipolazione degli stessi dati personali. Si è arrivati a profilare gusti, preferenze, comportamenti sulla base di informazioni sparse, fornite consapevolmente o inconsapevolmente sulle piattaforme sociali, sui vari siti consultati dagli utenti, nelle comunicazioni sociali. La mole di dati personali che circolano nel web non è facilmente quantificabile¹, ma secondo i dati dell'Unione Europea, attualmente il 71% dei cittadini europei condivide i propri dati personali online, mentre solo il 15% ritiene di averne il controllo². Si arriva all'assoggettamento ad un potere incontrollato ed incontrollabile³ in cambio di servizi ed applicazioni sempre più sofisticate ed utili a risolvere ogni problema⁴.

Il regolamento europeo stabilisce una serie di principi giuridici fondamentali

¹ Secondo il rapporto McKinsey del 2016 (*The Age of Analytics: Competing in a Data-Driven World*), il flusso di dati che vengono scambiati a livello transfrontaliero è diventato 45 volte più importante di 20 anni fa e il volume di dati circolanti raddoppia ogni tre anni.

² Cfr. In <https://www.ecc-netitalia.it/it/news-e-pubblicazioni/news/716-privacy-maggiori-tutele-con-il-gdpr-il-regolamento-europeo-sulla-protezione-dei-dati-personali>.

³ "L'eurodeputato che ha messo in crisi Zuckerberg nel corso dell'udienza davanti al Parlamento Europeo", <https://www.tpi.it/2018/05/28/verhofstadt-zuckerberg-parlamento-europeo>.

⁴ F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, Giappichelli, 2016, p. 394.

in materia di tutela dei dati personali, che l'autore ricorda nella prima parte dell'opera. Da sottolineare il linguaggio preciso e concreto, con numerosi esempi pratici, come quello dei *cookies* (par. 3.3.). Tali principi erano in gran parte già stati enucleati nelle norme fondatrici sviluppate a livello tanto del Consiglio d'Europa che dell'Unione europea, di cui l'autore ricorda bene il lungo percorso storico (par. 1.1.), norme che sono via via anche state meglio precisate nella giurisprudenza sia dalla Corte europea dei diritti dell'uomo di Strasburgo che dalla Corte di giustizia dell'Unione europea⁵. Si assiste infatti qui ad una delle caratteristiche del processo di integrazione europea, questa "comunità di valori", sviluppatasi attraverso la progressiva definizione di *standards comuni*, tecnici, economici o giuridici, chiamati a diventare punti di riferimento per la regolazione delle attività che si svolgono nel mercato unico europeo, e che finiscono per imporsi anche a livello globale⁶, dal momento che il mercato unico europeo rappresenta il più grande mercato del mondo. Del resto, l'ambito territoriale del regolamento va ben oltre i confini dell'Unione. Interessante qui l'analisi fatta sul "perimetro del sistema protezione dati personali" (par. 1.3.). Incidentalmente, merita essere sottolineato che in coincidenza con l'entrata in vigore dell'RGPD, dopo un lungo iter iniziato nel 2011, è stato portato a termine dal Comitato dei Ministri del Consiglio d'Europa il 18 maggio scorso il processo di modernizzazione della Convenzione 108 del 1981, tuttora unico strumento sulla protezione dei dati vincolante a livello internazionale⁷.

Come ha ben colto l'autore di questo libro, il cui titolo è chiarissimo, la nuova disciplina europea sulla protezione dei dati personali va ben al di là dei precetti giuridici che stabilisce: il regolamento prescrive infatti tutta una serie di attività e misure come il monitoraggio degli accessi ai dati, la gestione della sicurezza dei dati lungo tutto il loro ciclo di vita, la cifratura dei dati e la pseudonimizzazione, la valutazione d'impatto, tutte attività che devono essere incardinate nel funzionamento delle organizzazioni, siano esse pubbliche o private, economiche o non profit, dal momento che si trattano dati personali. Il pregio del lavoro di Giuseppe Nucci è proprio di offrire una guida pratica per integrare i precetti del regolamento nei processi organizzativi in modo da fare di un obbligo di *compliance* un'occasione di rinnovo e modernizzazione delle strutture organizzative. È l'oggetto della seconda parte dell'opera, in cui l'autore analizza, passo per passo, il ruolo dei vari attori (cap. 4), fa una mappatura dei processi (par. 5.3.2.), si sofferma sui vari registri (par. 5.3.3.) e sviluppa un modello

⁵ *Manuale sul diritto europeo in materia di protezione dei dati*, a cura dell'Agenzia dell'Unione europea per i diritti fondamentali e della Cancelleria della Corte europea dei diritti dell'uomo del Consiglio d'Europa, Luxembourg, Ufficio delle pubblicazioni dell'Unione Europea, 2014.

⁶ I politologi parlano di "normative power" dell'Unione europea, cfr. Ian Manners, "The Normative Ethics of the European Union", *International Affairs*, vol. 84, Issue 1, Jan. 2008, pp. 45-60.

⁷ "Migliorare la protezione dei dati a livello mondiale: il Consiglio d'Europa aggiorna la sua storica Convenzione", https://www.coe.int/portal/tutte_le_notizie.

di integrazione della protezione dei dati con gli altri controlli nella più larga funzione di prevenzione e gestione dei rischi (cap. 5). L'autore utilizza qui la sua esperienza in materia di audit interno per mettere in evidenza gli stretti legami che esistono tra precetti del regolamento in materia di responsabilizzazione delle figure apicali (*accountability* del titolare e del responsabile del trattamento) e la necessaria integrazione della protezione dei dati nella più larga attività di prevenzione e gestione dei rischi, attività che costituisce un elemento essenziale della *corporate governance* (par. 5.3). Del resto, i concetti di *privacy by design* e *privacy by default* come quello di *data protection impact assessment* (cap. 6) previsti dal regolamento rispondono a questi obiettivi di massimizzazione della tutela e di minimizzazione dei rischi che si ritrovano nel *risk management*. Il grande pregio dell'analisi di Giuseppe Nucci è di aver saputo illustrare ogni aspetto del cambiamento organizzativo indotto da questo regolamento con tabelle e figure che illustrano in maniera chiara e sintetica i vari passi da compiere. L'autore mette anche a disposizione del lettore chiavi di lettura e metodologie per trovare le soluzioni organizzative più adeguate, facendo anche sempre un riferimento distinto al contesto delle amministrazioni pubbliche, che peraltro conosce anche molto bene. Infine, con l'occasione, l'autore fa anche vedere un'altra opportunità offerta dal regolamento europeo e, cioè, quella dello sviluppo di nuove figure o profili professionali, che sono chiamati ad intervenire per la corretta applicazione del regolamento, come il *Data Protection Officer* (par. 4.5)

Christiane Colinet

Avvocato al Foro di Bruxelles e al Foro di Firenze

INTRODUZIONE

Questo libro non è, né vuole essere, un testo giuridico.

Poiché l'argomento trattato trova il suo fondamento in un provvedimento di natura normativa - il Regolamento Europeo 27 aprile 2016, n. 679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, ormai noto come GDPR (*General Data Protection Regulation*) - le norme, ovviamente, costituiscono la base di partenza e la loro esegesi è quindi indispensabile (e, per certi versi, anche stimolante), ma ciò che più mi ha interessato nell'affrontare questo impegno sono state le ricadute organizzative.

Le riflessioni che ne sono seguite, di conseguenza, si sono ispirate ad un concetto che mi ha sempre accompagnato nell'approccio con le materie di cui mi occupo (*internal audit, risk management, anticorruzione, sistema "231"*) nel contesto dei modelli organizzativi: la *compliance* non basta se si perde di vista la performance!

La cattiva applicazione di normative e discipline, infatti, prima ancora di probabili conseguenze sanzionatorie, provoca gravi esternalità negative in termini di perdita di efficacia, efficienza ed economicità.

So benissimo che l'applicazione dipende non solo dall'interessato ma anche da elementi che sfuggono al suo controllo, imputabili al sistema di regolazione, primo tra tutti i contenuti e la forma delle norme.

Questo aspetto, per gli obiettivi che mi sono proposto, non sarà trattato ma ritengo significativo riportare alcune affermazioni che comunque danno un'idea sulla portata di queste criticità.

Secondo uno studio di qualche anno fa - citato dall'ex commissario straordinario per la revisione della spesa, dott. Carlo Cottarelli - il costo degli adempimenti burocratici gravanti sulle piccole e medie imprese era stimato nel 2% del PIL di cui quasi la metà riguardante oneri relativi a lavoro e previdenza: della rimanente parte, circa 15 miliardi, la tutela della *privacy* ne assorbiva ben 2,6 miliardi!

*"Il grado di intensità burocratica di un paese può secondo me essere meglio misurato dal numero di leggi, regolamenti, procedure varie con cui il cittadino si deve scontrare, nonché dalla loro complessità. E qui non siamo messi bene. [...] Le nostre leggi sono scritte, sono tante, lunghe e scritte male. E cambiano anche troppo rapidamente. Infine, c'è un problema di efficienza nell'amministrare le leggi e nell'applicare i regolamenti"*⁸.

È vero che nella normativa sulla protezione dei dati personali il testo base è rappresentato da un regolamento europeo, ma spesso sono le disposizioni attuative - nazionali - a fare la differenza (oltre alla qualità delle traduzioni ...).

⁸ Cfr. Carlo Cottarelli, *I sette peccati capitali dell'economia italiana*, Feltrinelli, 2018, pagg. 66, 68 e 74.

Ma torniamo ad occuparci di quanto un'amministrazione, un'azienda o un libero professionista deve sapere e deve fare per conoscere ed attuare le disposizioni relative al *data protection*.

Per la verità, nel passato (neanche troppo remoto), in nome della "privacy" sono state frequentemente sollevate - senza fondamento - difficoltà con forti impatti sia sulla nostra vita privata che sulla dimensione collettiva (sociale, politica, produttiva, ecc.), coinvolgendo singoli individui e organizzazioni, sia pubbliche che private.

La casistica è incredibilmente estesa e variegata (mi limito ad un caso che mi ha colpito per il richiamo a ormai antichi e nostalgici ricordi, e cioè alla classe della scuola elementare a cui è stato inibito farsi la foto ricordo⁹).

Talvolta, al contrario, la *privacy* (o meglio, la sua violazione) è stata alla base di veri e propri disastri: pensiamo al recente scandalo Cambridge Analytica che ha coinvolto Facebook per la violazione di 87milioni di profili di utenti.

La risposta deve ricercarsi soprattutto nelle soluzioni organizzative: l'individuazione dei principi e dei diritti dipende dalle norme giuridiche ma il grado della loro effettività dipende dall'attuazione, e cioè dai modelli, dai processi, dagli assetti organizzativi.

Ad esempio, ormai i *social network*, piattaforme web e motori di ricerca sono soggetti alla normativa europea anche se gestiti da società con sede fuori dall'Unione Europea - e ciò significa che il perimetro di protezione si è allargato, adeguandosi alle attuali esigenze - ma se le misure "organizzative e tecnologiche", richiamate dal GDPR, non saranno evolute, le nuove tutele rimarranno lettera morta.

Il *data protection* sarà sempre di più un fattore abilitante e favorirà le organizzazioni che capiranno che non si tratta più solo di una serie di adempimenti da gestire ma di un processo organizzativo aziendale che ha natura produttiva e non solo normativa.

Le aziende, per rimanere competitive, devono gestire e sfruttare i dati per creare, ad esempio, marketing diretto personalizzato, sviluppo di nuovi prodotti e servizi, migliorare la relazione con il cliente. Ma la fidelizzazione del cliente deve passare innanzitutto attraverso una strategia che poggi sul rispetto dei suoi diritti, sulla trasparenza e sulla *accountability*.

Il 25 maggio 2018, giorno di entrata in vigore del GDPR, è stato pubblicato un articolo di stampa¹⁰ secondo il quale si poteva quantificare in un miliardo di euro il costo per l'adeguamento alle disposizioni posto a carico di artigiani, liberi professionisti, micro e piccole imprese italiane.

Al di là dell'entità elevatissima dell'onere finanziario, la domanda più

⁹ Cfr. l'arguto articolo di Massimo Gramellini "Foto senza classe", *Corriere della Sera*, 16 marzo 2018, pag. 1.

¹⁰ Cfr. l'articolo "Privacy, la nuova normativa costa 1 miliardo a Pmi e professionisti" di Isidoro Trovato, *Corriere della Sera*, 25 maggio 2018, pagina 31.

significativa è se questa spesa servirà semplicemente a rispettare asetticamente delle regole oppure riuscirà a concorrere concretamente allo sviluppo sociale ed economico della collettività, coniugando le garanzie della persona con le esigenze organizzative e produttive.

Con queste premesse è stato costruito il percorso del libro che si suddivide in due parti, una generale, "di sistema", e l'altra incentrata sulla dimensione organizzativa.

Nella prima parte, costituita da tre capitoli, dopo un breve *excursus* storico, vengono presi in considerazione gli elementi costitutivi del "Sistema GDPR": i principi, le nozioni fondamentali, l'ambito di applicazione del trattamento dei dati personali e gli strumenti per garantirne la qualità (codici, accreditamenti e certificazioni), le categorie e le tipologie dei dati personali, il data breach - e cioè la gestione delle irregolarità - e, infine, le autorità e gli organismi nazionali e comunitari.

Il capitolo 2 contiene invece un quadro sistematico dei diritti dell'interessato, con una descrizione dei mezzi di tutela.

Il capitolo 3 approfondisce gli strumenti che, per antonomasia, sono posti a disposizione dell'interessato per esercitare i propri diritti: l'informativa ed il consenso.

Nella seconda parte, con il capitolo 4, vengono analizzati i ruoli ed i soggetti che operano nel sistema GDPR - con tutte le innovazioni apportate dalla nuova disciplina, tra le quali spicca la nuova figura del *Data protection officer* - con riferimento ai compiti, le caratteristiche, le competenze ed i requisiti professionali, per ultimo fissati in parte con la norma UNI:11697:2017.

Il capitolo 5 è dedicato al *Data protection by design*, uno degli elementi qualificanti il nuovo sistema GDPR, finalizzato a conseguire tre obiettivi: attuare i principi di protezione dei dati, garantire i requisiti del GDPR, tutelare i diritti degli interessati. In questo lavoro esso è interpretato come un modello costituito da tre elementi che sono stati analizzati dettagliatamente: il *framework*, il processo di risk management e, a valle, le politiche con le misure organizzative e tecnologiche.

Lo sviluppo di tale analisi è preceduta dall'approfondimento della nozione di rischio da trattamento e dai presupposti organizzativi - governance, mappatura dei processi e registri dei trattamenti - e si conclude con una disamina delle metodologie e degli standard internazionali e nazionali applicabili a tale sistema.

L'ultimo capitolo è dedicato al *Data protection impact assessment* (DPIA) che, nel modello proposto, viene identificato nel processo di risk management, richiamato nel capitolo precedente come uno dei tre elementi del *Data protection by design*. Il DPIA si propone di raggiungere quattro obiettivi: la conformità con le normative, determinare i rischi e gli effetti che ne conseguono, gestire i rischi, assicurare l'accountability su quanto fatto.

Un approfondimento sui *data audit* conclude il capitolo.

Prima di terminare questa introduzione, desidero soddisfare quella che è per

me una doverosa, e al contempo piacevole, prassi: ringraziare tutti coloro che, seppure con modalità ed intensità diverse, mi hanno aiutato in questo lavoro fornendomi utilissimi spunti di riflessione e consigli preziosi e sostenendomi con generosi incoraggiamenti.

Non posso certo menzionarli tutti ma un particolare segno di riconoscenza desidero rivolgerlo a coloro che sono risultati determinanti nelle fasi di realizzazione di questo libro.

L'avv. Giulia Adotti è una professionista che si contraddistingue per stile, serietà e capacità. Ho avuto modo di apprezzarne il garbo, la disponibilità e la profonda competenza nell'ambito di interessanti attività di ricerca promosse dal prestigioso Studio legale Adotti & Associati di Roma di cui, insieme al fratello, avv. Alessandro Adotti, è partner.

Desidero ringraziare Giulia perché, in effetti, è stata lei ad avviarmi nel complesso mondo del *data protection* e, anche per la realizzazione di questo libro, i suoi stimoli sono stati di indubbio interesse.

Anche Christiane Colinet è un avvocato. Nel libro ho talvolta espresso le mie riserve per le situazioni in cui il sapere giuridico "puro" - applicato al *data protection* - non si coniuga con visioni, saperi e contaminazioni di altra natura, soprattutto nell'ambito delle scienze organizzative e sociali.

L'avv. Christiane Colinet, invece, fin dai primi scambi di vedute, si caratterizza immediatamente per un approccio multidisciplinare, impreziosito dal fatto di esercitare la propria attività, oltre che in Italia, anche in Belgio - paese di origine - e nelle istituzioni comunitarie. Nonostante le occasioni di confronto non siano state numerose, ciò ha comunque contribuito ad aprire la mia visione anche rispetto alle tematiche affrontate nel libro e di questo le sono particolarmente grato.

Un ulteriore ringraziamento lo devo alla dottoressa Antonella Baroli, responsabile della redazione di Wolters Kluwer (tra i cui componenti ho avuto il piacere di conoscere la dottoressa Rossella Magnelli), editore del volume.

In realtà se questo libro è stato pubblicato, lo si deve alla fiducia che la dottoressa Baroli ha avuto fin dall'inizio in questo progetto, alla costante e discreta attenzione con cui ha curato tutti i dettagli, agli incoraggiamenti nei momenti di difficoltà. Il tutto con generosità, innata signorilità e rara professionalità!

L'ultima citazione è rivolta al mio fraterno amico Silvano Sereni Lucarelli, un generale della Guardia di Finanza ora "a riposo" che, a dispetto del doppio cognome, non è nobile di nascita ma lo è sicuramente di animo ...

Appartiene a quella categoria, molto ristretta, di persone che manifestano la loro vicinanza attraverso una generosità disinteressata e con autentica partecipazione, stando al tuo fianco e sostenendoti nei momenti critici e esaltando i traguardi, seppur modesti, che riesci a raggiungere, talvolta anche alimentando la componente "narcisistica" che è in ognuno di noi ...

Anche di questo importantissimo contributo ha potuto beneficiare questo libro, e cioè di un fondamentale supporto “ideale” ma anche concreto (dal confronto di idee ad una revisione delle bozze che potrei senz’altro definire “maniacale!”).

Non posso citare le altre persone di cui sono debitore, l’elenco sarebbe troppo lungo. Le ringrazio tutte con sincera gratitudine.

SOMMARIO

Profilo Autore	I
Prefazione	II
Presentazione	IV
Introduzione	VII

Parte I

Il General Data Protection Regulation (GDPR)

Capitolo 1 – Il sistema GDPR

1.1. Un lungo percorso	3
1.2. Le categorie dei dati personali.....	8
1.3. Il perimetro del sistema “protezione dei dati personali”	9
1.4. Il trattamento dei dati: principi e tipologie.....	13
1.5. Trasferimenti di dati personali verso paesi terzi od organizzazioni internazionali	18
1.6. Strumenti per la qualità del data protection.....	21
1.6.1. Il codice di condotta e l’organismo di controllo	21
1.6.2. La certificazione.....	23
1.6.3. L’accreditamento.....	24
1.7. Data breach: notifiche, comunicazioni e responsabilità. Il sistema sanzionatorio.....	25
1.8. Le autorità di controllo indipendenti.....	29
1.9. Dal Gruppo “articolo 29” al Comitato Europeo per la protezione dei dati	31

Capitolo 2 – I diritti tutelati

2.1. Diritto alla protezione dei dati personali (data protection), diritto alla riservatezza (privacy) e diritti derivati.....	35
2.2. Limitazioni all’esercizio dei diritti dell’interessato	37
2.3. Diritto all’informativa e diritto di accesso.....	38
2.4. Diritto di rettifica.....	40
2.5. Diritto alla cancellazione o diritto all’oblio.....	40
2.6. Diritto alla limitazione del trattamento	42
2.7. Diritto alla portabilità dei dati	43
2.8. Diritto di opposizione.....	43
2.9. Diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato	44
2.10 Reclami e ricorsi giurisdizionali.....	45

Capitolo 3 – Conoscere e decidere: l’informativa e il consenso

3.1. L’informativa.....	48
3.1.1. I contenuti.....	48
3.1.2. I tempi	49
3.1.3. La forma	50
3.1.4. I costi	51
3.2. Il consenso	51
3.3. Segue: l’esempio dei <i>cookies</i>	52

Parte II

La dimensione organizzativa

Capitolo 4 – I soggetti e i ruoli

4.1. La distribuzione delle competenze e delle responsabilità. Un’ipotesi di organigramma.....	57
4.2. Il Titolare del trattamento	59
4.3. Il Responsabile del trattamento	62
4.4. L’Incaricato del trattamento).....	64
4.5. Il Responsabile della protezione dei dati (Il Data Protection Officer) ...	65
4.5.1. Obbligatorietà e facoltatività della nomina del DPO.....	65
4.5.2. Compiti e requisiti professionali	66
4.5.3. Prerogative e doveri del DPO	69
4.6. I profili professionali previsti dalla norma UNI 11697:2017	70

Capitolo 5 – Il Data protection by design: progettare il trattamento dei dati

5.1. Il rischio da trattamento dei dati personali.....	74
5.2. Il Data protection by design.....	76
5.3. I presupposti organizzativi.....	79
5.3.1. Corporate governance e integrazione del data protection con gli altri controlli: la necessità di un approccio sistemico.....	79
5.3.2. La mappatura dei processi	82
5.3.3. I registri delle attività di trattamento	88
5.4. Il framework per la gestione del rischio	92
5.4.1. Il mandato.....	93
5.4.2. Progettazione del framework.....	94
5.4.3. Attuazione della gestione del rischio.....	95
5.4.4. Monitoraggio e riesame del framework.....	96
5.4.5. Miglioramento continuo del framework	96
5.5. Le attività critiche: la progettazione e l’informatizzazione.....	96
5.5.1. Come gestire i progetti: il masterplan e il diagramma di Gantt...	96
5.5.2. Il supporto informatico.....	99
5.6. Metodologie, standard internazionali e norme UNI	103

5.6.1. Standard specifici per il Data Protection	103
5.6.2. Standard per la sicurezza delle informazioni	104
5.6.3. Standard per il risk management	105
5.6.4. Standard per l'internal auditing	107
5.6.5. Standard per la prevenzione della corruzione	107
Capitolo 6 – Il Data protection impact assessment (DPIA)	
6.1. Il DPIA come modello giuridico	108
6.2. Il DPIA come processo "ordinario" di risk management	112
6.3. Definizione del contesto	115
6.3.1. Il contesto esterno ed interno	115
6.3.2. I documenti	116
6.3.3. I risk criteria	117
6.3.4. segue: i criteri per la misurazione del livello del rischio	117
6.4. La valutazione del rischio	118
6.5. Il trattamento del rischio: l'opzione della "mitigazione del rischio"	121
6.5.1. Le opzioni del risk treatment	121
6.5.2. La mitigazione del rischio	122
6.5.3. I presidi di controllo. Misure "organizzative" vs misure "tecno- logiche"	123
6.5.4. Consultazione preventiva	125
6.6. Consultazioni, reportistica e comunicazione	127
6.7. Il monitoraggio e il riesame	132
6.8. I data audit	132
6.8.1. A chi compete la responsabilità dei data audit	133
6.8.2. Come si svolgono i data audit	136
6.8.3. I metodi applicabili ai data audit	141
Glossario, acronimi e abbreviazioni	144

Indice delle tavole e delle figure

Capitolo 1 – Il sistema GDPR

Tavola 1 – Primi principi in materia di privacy	4
Figura 1 – Sintesi dell'evoluzione storica	6
Tavola 2 – Atti giuridici dell'Unione Europea	7
Figura 2 – Le categorie dei dati personali	9
Figura 3 – Adeguamento del quadro normativo nazionale alle disposi- zioni del Regolamento (UE) 2016/679	10
Figura 4 – Nozione di trattamento di dati	12
Figura 5 – Ambito di applicazione del GDPR	13
Figura 6 – I principi del trattamento dei dati (art. 5 GDPR)	14

Figura 7 – Il trattamento dei dati sensibili e giudiziari	18
Figura 8 – Condizioni per il trasferimento di dati a Paesi terzi	19
Figura 9 – Il codice di condotta	23
Figura 10 – Gli elementi del Data Breach	27
Figura 11 – Il sistema sanzionatorio	29
Figura 12 – Le linee guida del Gruppo “articolo 29”	33

Capitolo 2 – I diritti tutelati

Tavola 3 – Diritto alla protezione dei dati e diritto alla riservatezza.....	36
Figura 13 – Diritti degli interessati	37
Figura 14 – Limitazioni ai diritti degli interessati	38

Capitolo 3 – Conoscere e decidere

Figura 15 – Esempio di icone utilizzabili nell’informativa	51
Tavola 4 – Cookie Policy	53

Capitolo 4 – I soggetti e i ruoli

Figura 16 – Esempio di organigramma “data protection”	57
Figura 17 – Il Titolare del trattamento.....	59
Figura 18 – Proporzionalità delle misure tecniche ed organizzative.....	60
Tavola 5 – Il Responsabile del trattamento.....	62
Figura 19 – Nomina del Responsabile del trattamento.....	64
Tavola 6 – Compiti del DPO	66
Tavola 7 – Competenze e conoscenze del DPO.....	67
Figura 20 – Prerogative e doveri del DPO	69
Tavola 8 – Profili professionali: compiti principali	70
Figura 21 – I profili professionali della norma UNI 11697:2017	72
Tavola 9 – Requisiti per l’accesso ai profili professionali.....	72

Capitolo 5 – Il Data protection by design: progettare il trattamento dei dati

Tavola 10 – Categorie dei rischi da trattamento	74
Figura 22 – Mappatura dei rischi vs processi e strutture.....	76
Figura 23 – Ipotesi di sistema “data protection by design”	78
Figura 24 – Il Data protection by design.....	79
Figura 25 – Attività di controllo ed attori.....	82
Figura 26 – Processi, procedure e procedimenti amministrativi.....	85
Figura 27 – Grado di rischiosità rispetto all’adeguatezza del processo.....	86
Tavola 11 – Informazioni contenute nei registri delle attività di trattamento.....	88
Tavola 12 – Esempio di modello di registro delle attività di trattamento.....	90
Figura 28 – Il Framework.....	93
Tavola 13 – Le aree di progettazione del framework.....	94

Figura 29 – Il masterplan	97
Figura 30 – Gli step del masterplan.....	98
Tavola 14 – Esempio di funzionalità di un applicativo dedicato al data protection	100
Figura 31 – Cruscotti SSD: esempi di monitoraggio delle attività.....	100
Figura 32 – Esempio di gestione del registro dei trattamenti	101
Figura 33 – Il CoSO ERM	106

Capitolo 6 – Il Data protection impact assessment (DPIA)

Tavola 15 – Criteri per individuare trattamenti di dati ad alto rischio.....	109
Figura 34 – Il modello giuridico del DPIA	111
Figura 35 – Una concezione “operativa” del DPIA.....	114
Figura 36 – Criteri per la validità di un DPIA.....	115
Figura 37 – Gli output documentali del GDPR.....	116
Figura 38 – Matrice probabilità/impatto	118
Figura 39 – Rischi più comuni.....	119
Figura 40 – La fase della valutazione del rischio	121
Figura 41 – Misure organizzative e misure tecnologiche	125
Figura 42 – Le riunioni: fasi e ruoli.....	130
Figura 43 – Fasi dell’intervista.....	131
Figura 44 – Condizioni per lo sviluppo ed il riesame della DPIA.....	132
Tavola 16 – Specifiche del valutatore privacy.....	133
Tavola 17 – Raffronto tra DPO e Responsabile Internal audit	134
Figura 45 – Processo per la gestione di un programma di audit	137
Figura 46 – Processo di audit.....	138
Figura 47 – Il rapporto di audit	140
Tavola 18 – Metodi di audit.....	141

Parte I

**IL GENERAL DATA PROTECTION
REGULATION (GDPR)**

Affermare che non si è interessati al diritto alla privacy perché non si ha nulla da nascondere è come dire che non si è interessati alla libertà di parola perché non si ha nulla da dire.
Edward Snowden. Informatico statunitense, ex tecnico della CIA

Le indiscrezioni si fanno raccomandando la massima discrezione!
Roberto Gervaso, giornalista e scrittore

1. Il sistema GDPR¹

1.1. Un lungo percorso ...

Iniziamo con una nota di colore. Nella ricerca delle origini di questa materia, tralasciando (presunte) testimonianze che alcuni studiosi collocano addirittura nelle origini delle prime civiltà, mi è piaciuta la tesi suggestiva secondo la quale tutto è iniziato nel 1890 negli Stati Uniti quando l'avvocato Samuel Warren, stanco di leggere indiscrezioni sulla propria vita matrimoniale sul quotidiano *Evening Gazette di Boston*, insieme al suo collega Louis Brandeis diede alle stampe un saggio intitolato "The Right to Privacy. The Implicit Made Explicit".

Si tratterebbe dell'ennesima conferma di come questioni molto serie possano scaturire anche da episodi piuttosto ... pruriginosi.

Facendo un salto a piè pari su tutta l'evoluzione dottrina e giurisprudenziale, giungiamo al 7 maggio 1997, e cioè alla data in cui sul sito del Garante per la protezione dei dati personali veniva pubblicato un comunicato stampa (tuttora *on line*):

"Domani 8 maggio 1997 entrerà in vigore un'importante legge che attiene alla raccolta e all'elaborazione delle informazioni di carattere personale (Legge 31 dicembre 1996, n. 675).

La legge reca una disciplina organica per la tutela dei diritti della personalità, e protegge in modo particolare il diritto alla riservatezza e il diritto all'identità personale.

La trasparenza e il controllo sulla circolazione delle informazioni diventano anche uno strumento essenziale per il corretto funzionamento del mercato e per lo sviluppo degli scambi.

Le garanzie previste riguardano sia i dati attinenti agli individui, sia le informazioni riferite alle associazioni, agli enti, alle imprese.

Il quadro normativo è complesso, e merita particolare attenzione nella sua applicazione. [...]

Al cittadino sono riconosciuti alcuni diritti significativi, quale quello di:

a) accedere ai dati che lo riguardano, contenuti nelle banche dati pubbliche e private. Per alcuni archivi finalizzati alla cura di particolari interessi pubblici, si potrà chiedere a questa autorità di effettuare una verifica;

b) ottenere la rettifica, l'integrazione e la cancellazione dei dati erronei, incompleti o elaborati illecitamente;

c) opporsi al trattamento delle informazioni, qualora ricorrano "motivi legittimi" ovvero quando i dati siano utilizzati per determinate attività pubblicitarie o di informazione commerciale.

Questi ed altri diritti potranno essere fatti valere dinanzi all'autorità giudiziaria, oppure dinanzi a questa autorità indipendente e di garanzia, i cui membri sono stati eletti dalle assemblee parlamentari."

¹ L'acronimo inglese indica il Regolamento CE 27 aprile 2016, n. 2016/679/UE, "Regolamento generale sulla protezione dei dati", pubblicato nella G.U.U.E. 4 maggio 2016, n. L 119.

Si tratta di una sintesi che rappresenta una curiosità di valore quasi storico, considerato che negli oltre vent'anni trascorsi, in questo campo in così rapida evoluzione, si sono registrati mutamenti radicali.

Questa prima legge, in realtà, segna l'approdo di un *iter* che ha avuto origine il 28 gennaio 1981.

A tale data, infatti, risale il testo della "Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale" n. 108 del Consiglio d'Europa, uno dei più importanti strumenti normativi per la protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, che l'Italia ha recepito nel proprio ordinamento dopo circa otto anni².

Il provvedimento - ispirato alla *Convenzione europea dei diritti dell'uomo*³ e aperto anche all'adesione di Stati non membri del Consiglio d'Europa⁴ - riguarda tutti i trattamenti di dati personali effettuati sia nel settore privato che pubblico (ad esempio, anche quelli della polizia e dell'autorità giudiziaria).

Tavola 1 – Primi principi in materia di privacy

Convenzione europea dei diritti dell'uomo	Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale
<p>Articolo 8 - Diritto al rispetto della vita privata e familiare</p> <p>1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.</p> <p>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.</p>	<p>Articolo 1 – Oggetto e scopo</p> <p>Scopo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano («protezione dei dati»).</p>

In effetti con i suoi 27 articoli, la *Convenzione europea dei diritti dell'uomo* ha costituito la prima risposta di rilievo all'esigenza di tutela per le persone a seguito

² Legge 21 febbraio 1989, n. 98, "Ratifica ed esecuzione della convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981".

³ "Convenzione per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali" del Consiglio d'Europa del 4 novembre 1950, così come modificato dalle disposizioni del Protocollo n. 14 a partire dalla sua entrata in vigore il 1° giugno 2010.

⁴ Tutti gli Stati UE hanno aderito.

del proliferare di tecnologie dell'informazione e comunicazione, mirando a proteggere gli individui da abusi e a regolamentare i flussi transnazionali dei dati. In virtù della *Convenzione*, inoltre, è stata istituita a Strasburgo, nel 1959, la *Corte europea dei diritti dell'uomo* (CEDU) che, al fine di garantire che gli Stati contraenti adempiano ai propri obblighi, decide sulle denunce presentate dai singoli individui, oppure da associazioni o persone giuridiche, ma sempre dopo che siano stati esperiti i rimedi giurisdizionali interni.

Tuttavia, il 24 ottobre 1995, per le pressanti maggiori esigenze di protezione, il Parlamento e il Consiglio dell'Unione Europea hanno adottato la Direttiva 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali ed alla libera circolazione di tali dati.

Questa direttiva si proponeva soprattutto di armonizzare il livello di tutela, prevedendo in ogni Stato membro l'istituzione di autorità di controllo indipendenti, dotate di poteri di regolazione, ispettivi e sanzionatori.

Per tutto ciò che riguarda l'applicazione della Direttiva 95/46/CE, come di tutto il diritto dell'Unione Europea, la competenza è attribuita alla Corte di giustizia dell'Unione europea (CGUE)⁵.

Questa direttiva è stata attuata in Italia con la Legge 31 dicembre 1996, n. 675, "*Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*", menzionata all'inizio del paragrafo, che costituisce la prima legge organica sulla cosiddetta "privacy". Deve peraltro essere evidenziato che l'adozione di questo fondamentale provvedimento legislativo non derivò da un'autentica apertura rispetto una concezione più rispettosa della persona ma fu sostanzialmente un obbligo: l'Europa avrebbe permesso ad uno Stato di godere dei benefici dell'Accordo di Schengen solo se avesse adeguato la propria normativa sul trattamento dei dati personali.

Successivamente, per affrontare adeguatamente l'evoluzione tecnologica, i servizi *on line*, ecc., è stata adottata la direttiva 2002/58/CE del Parlamento Europeo e del Consiglio del 12 luglio 2002⁶ relativa al "*trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche* (direttiva relativa alla vita privata e alle comunicazioni elettroniche) – denominata *e-privacy* – le cui disposizioni, come recita l'art. 2, "*... precisano e integrano la direttiva 95/46/CE*".

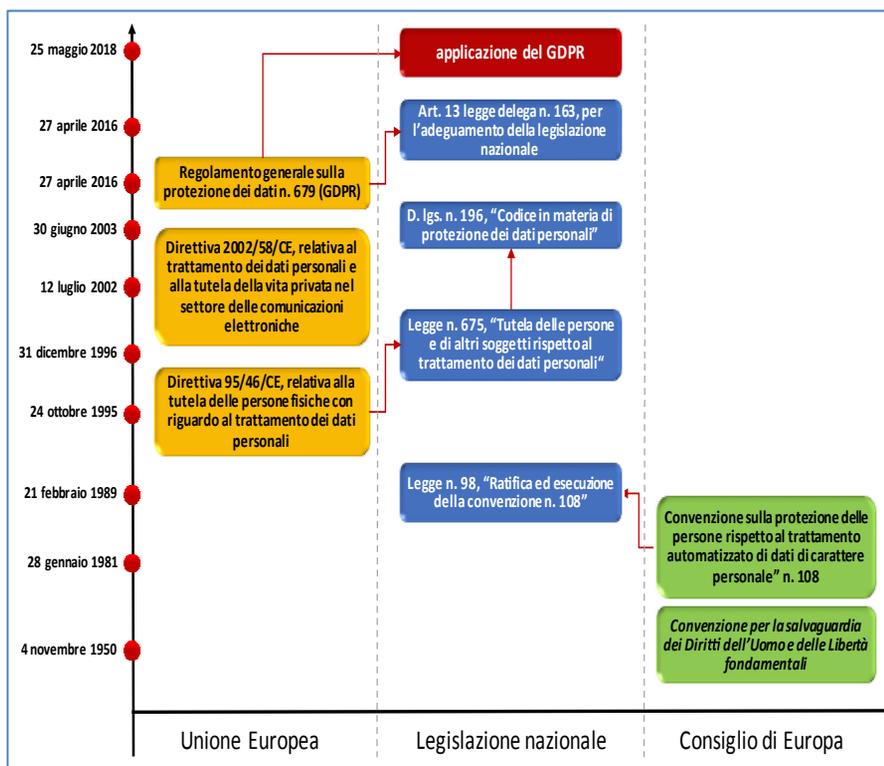
Nel frattempo, alla Legge n. 675/1996 si erano affiancate ulteriori testi normativi riguardanti specifici aspetti del trattamento dei dati e ciò aveva determinato una stratificazione che ne aveva reso complicata l'attività di coordinamento.

⁵ La Corte di giustizia dell'Unione Europea (CGUE), istituita nel 1952 in Lussemburgo, interpreta il diritto dell'UE per garantire che sia applicato allo stesso modo in tutti gli Stati membri e dirime le controversie giuridiche tra governi nazionali e istituzioni dell'UE. Può essere adita, in talune circostanze, anche da singoli cittadini, imprese o organizzazioni allo scopo di intraprendere un'azione legale contro un'istituzione dell'UE qualora ritengano che abbia in qualche modo violato i loro diritti.

⁶ La direttiva è stata modificata dalla Direttiva 2009/136/CE del Parlamento Europeo e del Consiglio del 25 novembre 2009.

Per superare la sopravvenuta complessità normativa è stato emanato il D.Lgs. 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", che ha riordinato interamente la materia, abrogando la Legge n. 675/1996, introducendo nuove garanzie per i cittadini, razionalizzando le norme esistenti e semplificando gli adempimenti⁷.

Figura 1 - Sintesi dell'evoluzione storica



E a questo punto – ritenendo di poter rinunciare a richiamare tutte le ulteriori fonti normative internazionali e comunitarie nel frattempo intervenute⁸ – siamo arrivati all'attualità!

⁷ Anche a questo testo sono state apportate delle modifiche nel tempo (ad esempio, il Documento programmatico sulla sicurezza è stato reso facoltativo).

⁸ Per motivi di sintesi, non sono stati menzionati altri significativi provvedimenti, come, ad esempio, la Carta dei diritti fondamentali dell'Unione Europea (Carta di Nizza) proclamata il 7 dicembre 2000 che, nel titolo dedicato alla libertà (gli altri diritti sono riferiti alla dignità, eguaglianza, solidarietà, cittadinanza e giustizia), riserva l'art. 8 alla "protezione dei dati di carattere personale". Il Trattato di Lisbona, entrato in vigore il 1° dicembre 2009, ha incluso la Carta di Nizza sotto forma di allegato, conferendole così carattere giuridicamente vincolante all'interno dell'ordinamento dell'Unione Europea, secondo quanto disposto dall'art. 6.

Si tratta del Regolamento europeo per la protezione dei dati personali n. 2016/679⁹, che è direttamente e integralmente applicabile dal 25 maggio 2018 in tutti gli Stati dell'Unione Europea, realizzando così una definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione europea.

Questo Regolamento UE (che nel prosieguo del testo chiameremo anche con l'acronimo inglese GDPR), insieme alla Direttiva 2016/680¹⁰ - che a differenza del primo necessita di un atto nazionale di recepimento¹¹ - costituisce il c.d. "Pacchetto europeo della protezione dei dati" che, come vedremo meglio nel paragrafo 1.3, è integrato con il "*diritto dello Stato membro cui è soggetto il Titolare del trattamento*".

La Tavola 2 riporta l'art. 288 del Trattato, in cui sono descritte le fonti giuridiche dell'Unione Europea.

Tavola 2 – Atti giuridici dell'Unione Europea

Trattato sul funzionamento dell'Unione Europea (versione consolidata) - Art. 288

Per esercitare le competenze dell'Unione, le istituzioni adottano regolamenti, direttive, decisioni, raccomandazioni e pareri.

Il regolamento ha portata generale. Esso è obbligatorio in tutti i suoi elementi e **direttamente applicabile in ciascuno degli Stati membri**.

La direttiva vincola lo Stato membro cui è rivolta per quanto riguarda il risultato da raggiungere, salva restando la competenza degli organi nazionali in merito alla forma e ai mezzi.

La decisione è obbligatoria in tutti i suoi elementi. Se designa i destinatari è obbligatoria soltanto nei confronti di questi.

Le raccomandazioni e i pareri non sono vincolanti.

Il GDPR è articolato in 11 Capi e 99 articoli nonché in 173 "considerando" che costituiscono un preambolo particolarmente utile per comprendere le premesse, le esigenze da soddisfare, i percorsi logici e giuridici, gli obiettivi, le modalità attuative e i collegamenti con gli altri provvedimenti dell'Unione (il Garante per

⁹ Si tratta del Regolamento UE "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", del Parlamento europeo e del Consiglio n. 679 del 27 aprile 2016 (pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016), in vigore dal 24 maggio 2016 e applicabile dal 25 maggio 2018. Il regolamento è anche denominato "Regolamento generale sulla protezione dei dati" ed è spesso indicato con l'acronimo inglese GDPR (*General Data Protection Regulation*).

¹⁰ Si tratta della Direttiva (UE) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

¹¹ La direttiva è stata recepita attraverso l'art. 11 della legge di delegazione europea (2016-2017) del 25 ottobre 2017, n. 163, a seguito della quale è stato emanato il D.Lgs. 18 maggio 2018, n. 51.

La protezione dei dati personali ha pubblicato sul proprio sito un testo del Regolamento UE in cui per ogni articolo sono indicati i "considerando" di riferimento). Il tutto – secondo il contatore di *word* – è contenuto in 132 pagine, 56.010 parole e 334.409 caratteri!

1.2. Le categorie dei dati personali

In generale i «dati personali» sono qualificabili come "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)"¹².

Com'è noto, i dati personali sono suddivisi in specifiche tipologie che rilevano fondamentalmente in relazione alla disciplina del loro trattamento, che sarà esaminato in dettaglio nel paragrafo 1.4.

Il GDPR¹³ - attraverso l'art. 4, paragrafo 1, numeri 13, 14 e 15 - innanzitutto definisce tre categorie, distinguendo:

- «dati genetici»: dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- «dati biometrici»: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- «dati relativi alla salute»: 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.

Tuttavia, il successivo art. 9 individua un'altra categoria generale – che può essere indicata con la previgente denominazione di "dati sensibili" - che, oltre a ricomprendere le tre categorie descritte, inserisce anche dati di altra natura come, ad esempio, quelli relativi alle opinioni politiche, alle convinzioni religiose o filosofiche, o all'appartenenza sindacale.

Infine l'art. 10 determina un'ulteriore tipologia di dati, che potremmo definire "giudiziari", riferiti esclusivamente all'ambito penalistico e riguardanti condanne e procedimenti connessi a reati e a misure di sicurezza.

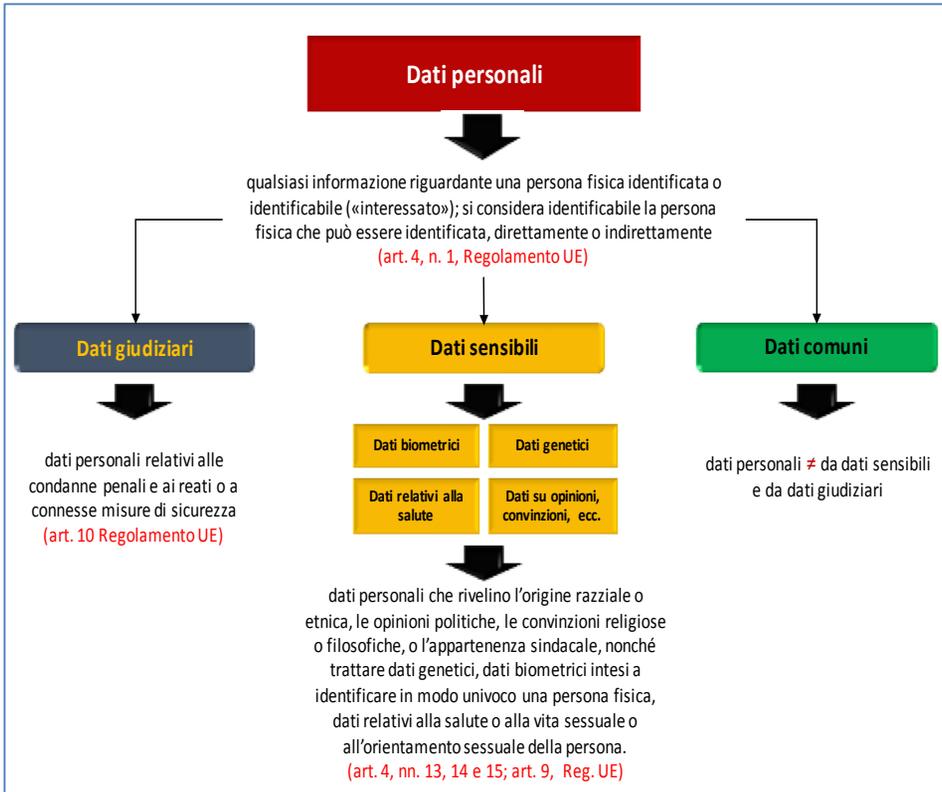
Per il trattamento di tali dati non è più previsto l'obbligo di notificazione all'Autorità Garante, a seguito dell'abolizione generale di tale prescrizione in vigore nella precedente normativa

Riassumendo, a seconda della disciplina del trattamento, possiamo distinguere i dati personali in *comuni*, *sensibili* e *giudiziari*, come sintetizzato nella Figura 2.

¹² Cfr. l'art. 4, n. 1, del Regolamento UE.

¹³ Cfr. i considerando 34, 35 e 51 del Regolamento UE.

Figura 2 – Le categorie dei dati personali



1.3. Il perimetro del sistema “protezione dei dati personali”

Abbiamo visto come tutto il sistema ruoti intorno al "diritto alla protezione dei dati di carattere personale", diritto distinto ed autonomo rispetto al diritto alla riservatezza.

In tale ambito si sono da tempo intrecciate varie tematiche: le relazioni tra posizioni giuridiche soggettive e sviluppo delle tecnologie; la necessità di realizzare una disciplina sovranazionale e, in particolare, modalità comuni di trattamento dei dati personali a prescindere dalla nazionalità o dalla residenza delle persona fisiche; la vulnerabilità dell'individuo rispetto ad una società in continua mutazione sotto il profilo etico, sociale ed economico; l'invasività delle tecniche di circolazione delle informazioni commerciali e non; la gestione delle banche dati; le profilazioni.

Il GDPR affronta queste ed altre sfide accogliendo importanti principi come il principio di trasparenza, il diritto all'oblio, il principio di *accountability*, il principio della *privacy by design*.

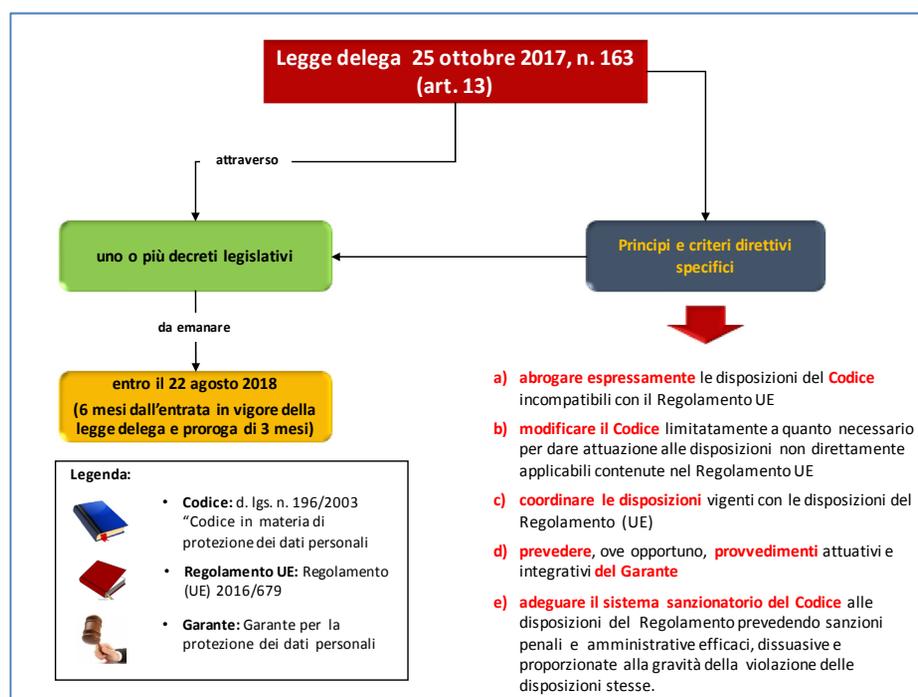
Si tratta di un Regolamento che, in quanto tale, non ha bisogno di un provvedimento nazionale di recepimento¹⁴ e che ha previsto un termine piuttosto realistico, due anni, per la sua applicabilità in modo da consentire i necessari interventi organizzativi di adeguamento.

Soffermiamoci ora su tre aspetti fondamentali di sistema: il quadro normativo di riferimento, la nozione di "trattamento dei dati" e l'ambito di applicazione del GDPR.

Il **quadro normativo** è definito dalle disposizioni del GDPR e da quelle nazionali ad esso compatibili.

Questa operazione di armonizzazione non appare semplicissima e, per porre rimedio a questa difficoltà, si è provveduto con l'art. 13 della legge di delegazione europea (2016 – 2017) del 25 ottobre 2017, n. 163¹⁵, e cioè con una delle leggi con cui periodicamente il Parlamento delega il Governo a recepire la legislazione comunitaria (in precedenza tali leggi erano denominate "leggi comunitarie").

Figura 3 – Adeguamento del quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679



¹⁴ Vedasi la Tavola 2 – Atti giuridici dell'Unione Europea.

¹⁵ La rubrica è "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017".

Dai contenuti della delega, sintetizzati nella Figura 3, si può rilevare che il quadro di riferimento legislativo poggia su due pilastri: il Regolamento UE e la legislazione nazionale.

Quest'ultima è costituita fundamentalmente dal D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" che deve essere reso compatibile al Regolamento UE con abrogazioni espresse, modifiche e con l'adeguamento del sistema sanzionatorio. Tuttavia è anche prevista l'adozione di *"disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del Titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto"*.¹⁶

Purtroppo la delega, che prevedeva l'adozione di un decreto legislativo entro sei mesi dalla pubblicazione della legge, non è stata esercitata per cui, in virtù dell'art. 13, comma 3, il Governo dovrà emanare il decreto entro il 22 agosto 2018¹⁷.

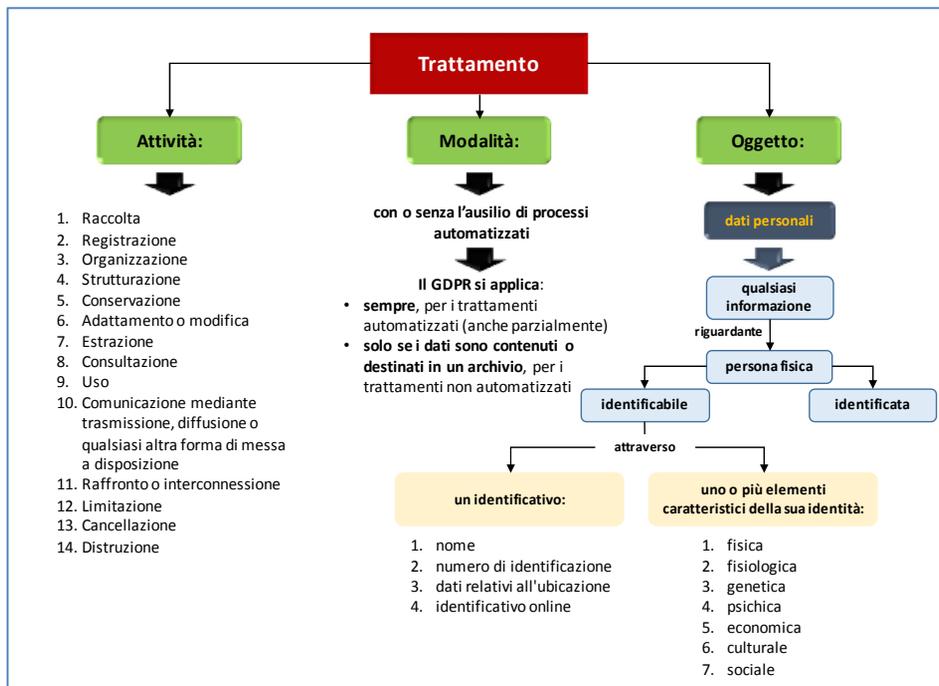
Un ulteriore elemento di rilievo – in questa opera di armonizzazione – è rappresentato dai provvedimenti del Garante per la protezione dei dati personali e dalla giurisprudenza in quanto è evidente che, laddove tale coordinamento non dovesse aver luogo, determinando dubbi interpretativi, occorre supplire con gli interventi dell'autorità Garante e, soprattutto, con l'attività ermeneutica della giurisprudenza tenendo conto che, com'è noto, il giudice nazionale è tenuto a disapplicare la norma statale che si ponga in contrasto con quella comunitaria.

Il secondo elemento che concorre a definire il perimetro in cui opera il GDPR è la **nozione di trattamento dei dati**, concetto prodromico a qualsiasi analisi e valutazione e ora definito dall'art. 4, nn. 1) e 2) del GDPR, come sintetizzato nella Figura 4.

¹⁶ Cfr. l'art. 6, paragrafo 3, del Regolamento UE.

¹⁷ L'art. 13, comma 3, della Legge n. 163/2017, prevede che il Governo eserciti la delega secondo le procedure previste dall'art. 32 della legge 24 dicembre 2012, n. 234. Quest'ultima norma, a sua volta, specifica che quando gli schemi dei decreti delegati vengano inviati alle Commissioni parlamentari per il previsto parere e manchino meno di 30 giorni alla scadenza della delega, tale scadenza è automaticamente prorogata di tre mesi.

Figura 4 – Nozione di trattamento di dati



Veniamo ora al terzo elemento di sistema: ***l'ambito di applicazione del GDPR***¹⁸.

Secondo un *criterio oggettivo*, il Regolamento UE si applica ai dati personali:

- se il trattamento è automatizzato, anche parzialmente: sempre;
- se il trattamento non è automatizzato: solo se i dati sono contenuti o destinati ad un archivio.

In ogni caso la disciplina non si applica se il trattamento dei dati è riferito ad attività che: i) non rientrano nel diritto dell'Unione; ii) rientrano nella politica estera e di sicurezza comune; iii) sono svolte a "titolo domestico"; iv) sono effettuate dalle autorità competenti a fini della prevenzione e repressione dei reati; v) riguardano le istituzioni dell'Unione¹⁹.

Secondo un *criterio soggettivo*, la nuova normativa si applica quando nell'Unione Europea è "stabilito" il Titolare o il Responsabile del trattamento oppure, se questi sono all'esterno, ai soggetti interessati all'interno dell'Unione Europea quando il trattamento riguardi (i) l'offerta di beni o la prestazione di servizi o (ii)

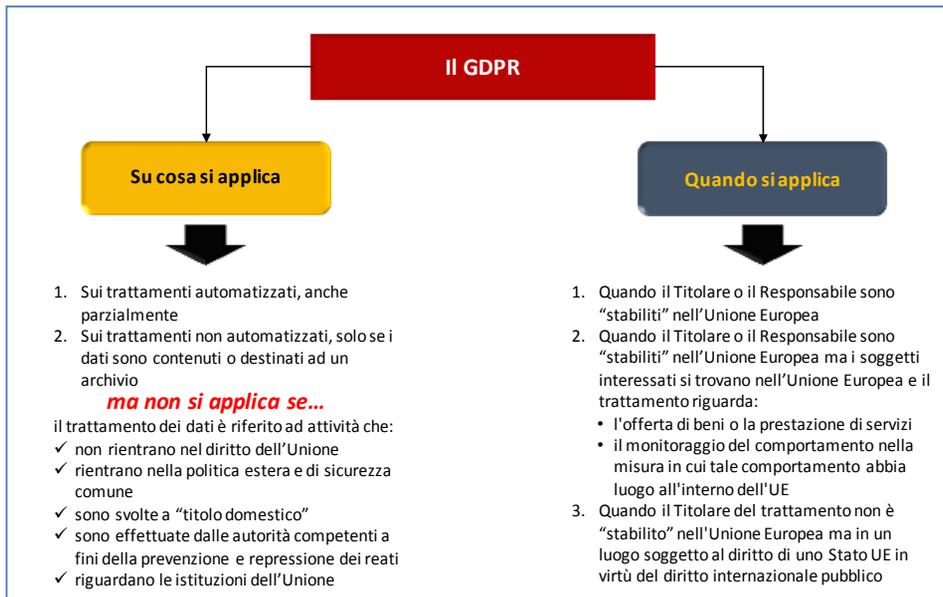
¹⁸ Cfr. gli artt. 2 e 3 del Regolamento UE.

¹⁹ Tali attività sono svolte nel rispetto del regolamento (CE) n. 45/2001 che, comunque, deve essere adeguato al GDPR. Inoltre, il paragrafo 4 dell'art. 2 stabilisce che "l'applicazione della Direttiva 2000/31/CE, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva" non è pregiudicata dal GDPR.

il monitoraggio del comportamento nella misura in cui tale comportamento abbia luogo all'interno dell'UE²⁰. Inoltre se il Titolare del trattamento non è "stabilito" nell'Unione Europea, il regolamento si applica qualora si trovi in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

La figura 5 schematizza i criteri esposti.

Figura 5 – Ambito di applicazione del GDPR



1.4. Il trattamento dei dati: principi e tipologie

Ogni sistema poggia su specifici principi che, tra gli scopi perseguiti, annoverano quello di fissare ed esplicitare con chiarezza le direttrici, i requisiti ed i vincoli che caratterizzano il sistema stesso.

Non si tratta di una dimensione "filosofica" ma di una guida strategica indispensabile per passare da un modello teorico alla sua concreta implementazione.

Spesso, infatti, davanti alle problematiche che sorgono nell'interpretazione delle norme, o nella fase operativa in cui viene definito ed attuato un modello, è necessario adottare un approccio "sistematico" che vede, appunto, i principi tra i propri elementi essenziali.

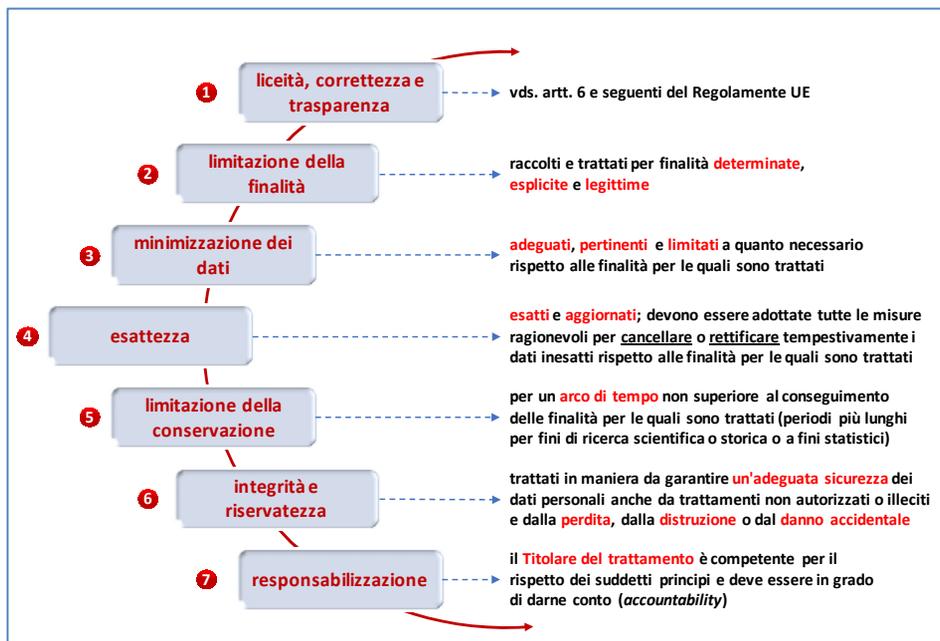
I principi, insomma, devono costituire una sorta di *benchmark*, un parametro di riferimento che, da un lato, rileva sotto il profilo della *compliance* e, dall'altro, in relazione agli obiettivi strategici da conseguire.

²⁰ Alle Istituzioni dell'UE si applica il regolamento (CE) n. 45/2001 ed altri atti giuridici che devono però essere adeguati ai principi e alle norme del GDPR conformemente all'art. 98.

Il GDPR dedica il Capo II, costituito da 7 articoli (dal 5 all'11), all'indicazione e alla descrizione dei principi relativi al trattamento dei dati²¹.

In totale sono individuati 7 principi - rappresentati nella Figura 6.

Figura 6 – I principi del trattamento dei dati (art. 5 GDPR)



Al primo principio, quello della *liceità*, il GDPR dedica un ampio spazio, stabilendone le condizioni. In sintesi, esse riguardano la necessità:

- del consenso dell'interessato al trattamento dei dati espresso con riferimento alle specifiche finalità che si devono perseguire;
- di eseguire un contratto;
- di adempiere un obbligo legale del Titolare del trattamento;
- di salvaguardare interessi vitali dell'interessato o di un'altra persona;
- di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri attribuiti al Titolare del trattamento;
- di perseguire il legittimo interesse del Titolare del trattamento o di terzi, a meno che prevalgano i diritti fondamentali dell'interessato, soprattutto se minore (questa condizione non si applica se il trattamento di dati è effettuato dalle autorità pubbliche).

A tali condizioni, di cui almeno una deve sussistere per rendere lecito il trattamento dei dati, gli Stati membri possono aggiungere disposizioni più specifiche

²¹ Cfr., anche, i considerando n. 39 e 74 del Regolamento UE.

in relazione ai trattamenti connessi ad obblighi legali, ai pubblici poteri²² e alle situazioni specifiche indicate nel capo IX²³ del GDPR.

E se i dati sono trattati per una finalità diversa da quella per la quale sono stati inizialmente raccolti, cosa succede? Nel caso di trattamenti che si basano sul consenso, la regola generale è che sono necessarie richieste di consenso distinte a fronte di una pluralità di finalità²⁴. Tuttavia il Titolare del trattamento deve comunque valutare se le due finalità sono compatibili, tenendo conto di vari elementi, tra cui:

- il nesso tra le due finalità;
- il contesto in cui i dati personali sono stati raccolti, con riferimento alla relazione tra l'interessato e il Titolare del trattamento;
- la natura dei dati personali;
- le possibili conseguenze per gli interessati;
- l'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione²⁵.

Riassumendo, per essere lecito il trattamento di dati deve basarsi sul consenso o su un atto legislativo dell'Unione o degli Stati membri.

Soffermandoci sul **consenso**²⁶ - che, come abbiamo visto, è una condizione riconducibile al principio di *liceità* - possiamo considerarlo come una manifestazione di volontà dell'interessato indispensabile se il trattamento dei dati non sia autorizzato da precetti normativi.

Il consenso²⁷ deve innanzitutto essere richiesto dal Titolare del trattamento. Se viene espresso per iscritto, la richiesta deve essere presentata "in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro".

Sono **sei le caratteristiche essenziali del consenso**, nel senso che esso deve essere:

- 1) provato, in relazione alla sua esistenza, dal Titolare del trattamento (onere della prova);
- 2) libero (ad esempio, l'esecuzione di un contratto non può essere condizionata al consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto né sono ammessi consensi raccolti con caselle pre-barrate);

²² Inoltre per tali trattamenti, di cui all'art. 6, paragrafo 1, lett. c) ed e), è stabilito che essi si debbano fondare sul diritto dell'Unione o di uno Stato membro.

²³ Si tratta di situazioni collegate a: libertà di espressione e di informazione; accesso del pubblico a documenti ufficiali; numero di identificazione personale; rapporti di lavoro; pubblico interesse e ricerca scientifica o storica o a fini statistici; obblighi di segretezza; chiese e associazioni religiose.

²⁴ Cfr. il considerando n. 32 del Regolamento UE.

²⁵ Cfr. l'art. 6, paragrafo 4 del Regolamento UE.

²⁶ Sul consenso si vedano anche i paragrafi 3.2 e 3.3.

²⁷ Cfr. l'art. 4, n. 11), l'art. 7 e l'art. 8 del Regolamento UE. Si vedano anche i considerando nn. 32 (ambiente web), 42 (consenso informato) e 43 (trattamenti per finalità plurime ed esecuzione dei contratti).

- 3) specifico;
- 4) informato;
- 5) inequivocabile, mediante dichiarazione o comportamento "concludente" (deve trattarsi, cioè, di un'*azione positiva inequivocabile*);
- 6) dal contenuto inderogabile rispetto alle prescrizioni del Regolamento UE e, pertanto, in caso di violazione (dichiarazione non disgiunta da altri aspetti o clausole del contratto, linguaggio oscuro, ecc.), le parti viziate del consenso non sono vincolanti.

Per l'offerta diretta di servizi della *società dell'informazione* ai minori, il consenso è valido se il minore ha almeno 16 anni²⁸ mentre, se di età inferiore, è necessario che il consenso sia prestato dal titolare della responsabilità genitoriale della cui validità deve accertarsi il Titolare del trattamento.

Non è più richiesto il requisito del consenso espresso se non per i dati "sensibili"²⁹ e per decisioni basate su trattamenti automatizzati (compresa la profilazione)³⁰.

Tornando ai principi generali del trattamento (riepilogati nella precedente Figura 6), si ritiene utile sottolineare come l'ultimo, quello della responsabilizzazione, costituisca un fondamentale adeguamento al concetto di *accountability*: per il responsabile del trattamento non è sufficiente adempiere ai doveri che scaturiscono dalle proprie competenze, ma occorre anche ... darne conto!

Inoltre, a corollario del principio di "responsabilizzazione" troviamo l'attribuzione al Titolare del trattamento – e non ad altre autorità – della competenza sulla valutazione sul bilanciamento fra il proprio (o di un terzo) legittimo interesse e i diritti e le libertà dell'interessato³¹.

Veniamo ora al trattamento di due categorie particolari di dati personali, già definiti nel paragrafo 1.2: i **dati sensibili** e quelli **giudiziari**.

In realtà questi termini non sono adottati dal GDPR ma, comunque, corrispondono alle definizioni finora usate nella legislazione nazionale.

I dati sensibili, in sostanza, sono richiamati nell'art. 9 nel quale viene precisato che, in generale, non possono essere trattati. Tuttavia, nel paragrafo 2 del medesimo articolo sono indicate una serie di deroghe³² riferite alle seguenti ipotesi:

- a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati (salvo nei casi in cui ciò non sia consentito);

²⁸ Gli Stati membri possono abbassare il limite di età fino a 13 anni (art. 8, paragrafo 1, ultimo periodo, del Regolamento UE Vds. anche il considerando 38).

²⁹ Cfr. l'art. 9 del Regolamento UE.

³⁰ Cfr. l'art. 22 del Regolamento UE. Al riguardo si vedano le linee guida in materia di profilazione e decisioni automatizzate del Gruppo "Articolo 29" (WP 251) del 3 ottobre 2017.

³¹ Cfr. il considerando n. 74 del Regolamento UE.

³² Gli Stati membri possono introdurre condizioni aggiuntive per l'applicazione delle deroghe se si tratta di dati genetici, biometrici e relativi alla salute.

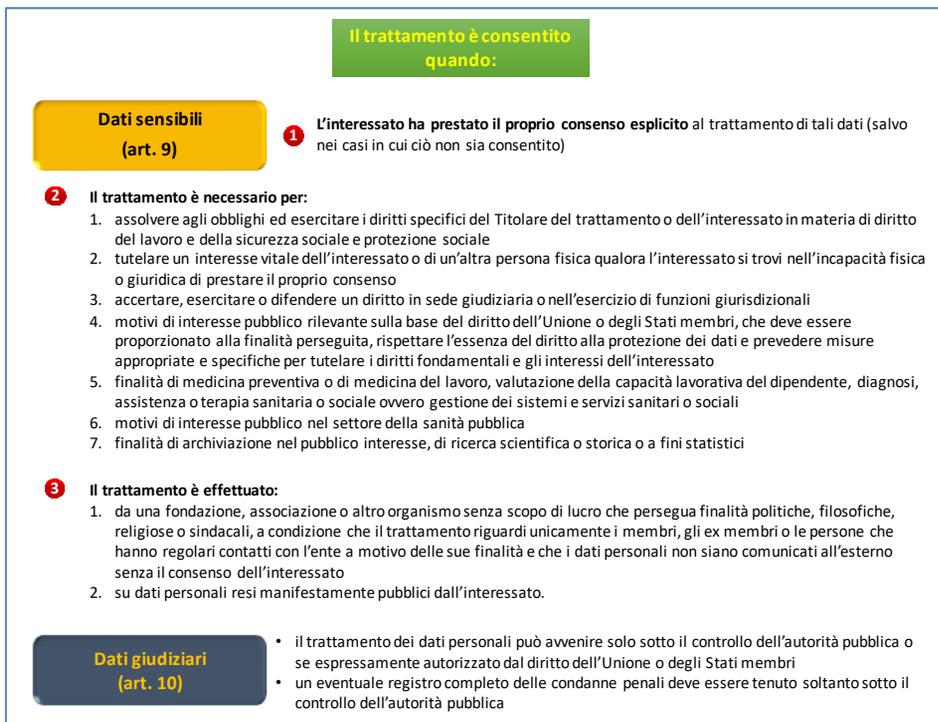
- b) il trattamento è necessario per:
- 1) assolvere agli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
 - 2) tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
 - 3) accertare, esercitare o difendere un diritto in sede giudiziaria o nell'esercizio di funzioni giurisdizionali;
 - 4) motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
 - 5) 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;
 - 6) motivi di interesse pubblico nel settore della sanità pubblica;
 - 7) finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;
- c) il trattamento è effettuato:
- 1) da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con l'ente a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
 - 2) su dati personali resi manifestamente pubblici dall'interessato.

A fattor comune, i dati devono essere trattati sotto la responsabilità di un professionista soggetto al segreto professionale.

Per quanto attiene ai dati giudiziari, invece, secondo l'art. 10, il trattamento dei dati personali può avvenire solo sotto il controllo dell'autorità pubblica (*... "un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica"*) o se espressamente autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

La Figura 7 riassume le condizioni per il trattamento dei dati sensibili e giudiziari.

Figura 7 – Il trattamento dei dati sensibili e giudiziari



Come norma di chiusura sul trattamento, l'art. 11 stabilisce che quando le finalità del trattamento non richiedono più l'identificazione dell'interessato, il Titolare del trattamento non è tenuto a conservare dati personali al solo scopo di poter rispondere a potenziali richieste da parte di quest'ultimo, tranne quando questi, al fine di esercitare i propri diritti³³, fornisce ulteriori informazioni che ne consentano l'identificazione.

1.5. Trasferimenti di dati personali verso paesi terzi od organizzazioni internazionali

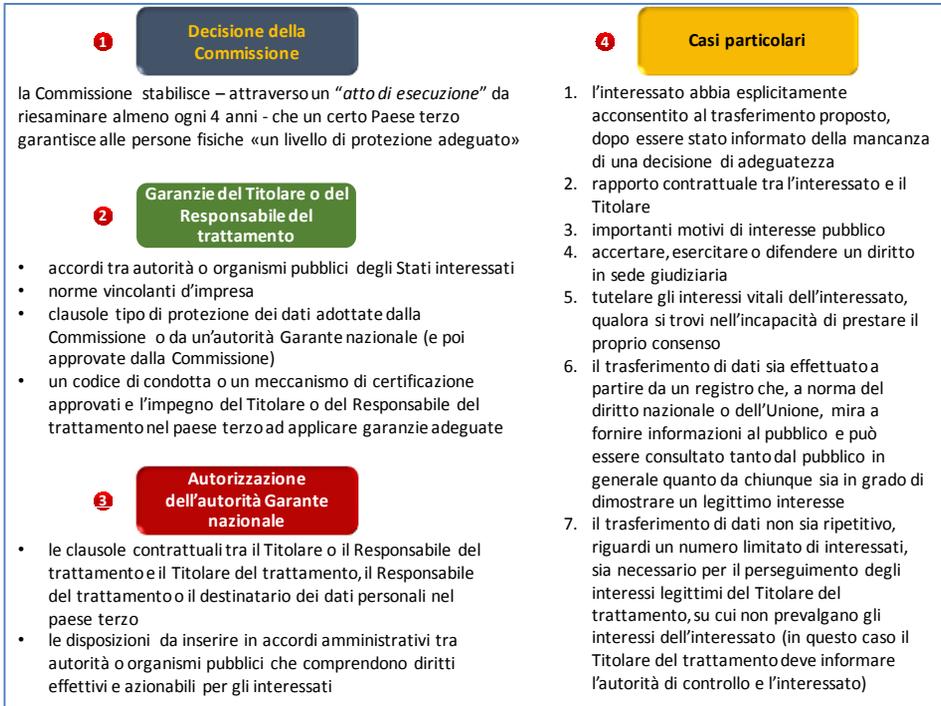
Il trasferimento dei dati in Paesi o organizzazioni extra UE³⁴ deve necessariamente garantire agli interessati un adeguato livello di garanzie che non può essere derogato neanche con accordi internazionali.

Esso può avvenire solo in quattro casi.

³³ Si veda il capitolo 2, dedicato ai diritti dell'interessato.

³⁴ Cfr. gli artt. 44 – 50 ed i considerando 101 - 103, 107 - 110, 114-115, 167-169 del Regolamento UE.

Figura 8 – Condizioni per il trasferimento di dati a Paesi terzi



Il primo si verifica quando la Commissione stabilisce – attraverso un “atto di esecuzione” da riesaminare almeno ogni 4 anni - che un certo Paese terzo garantisce alle persone fisiche “un livello di protezione adeguato”³⁵.

Se il Paese terzo non garantisce più il precedente livello di protezione, a seconda dei casi la Commissione provvede a revocare, modificare o sospendere, senza effetto retroattivo, la decisione di adeguatezza.

L'elenco dei paesi terzi per i quali la Commissione ha deciso che è o non è più garantito un livello di protezione adeguato è pubblicato nella Gazzetta ufficiale dell'Unione europea e sul suo sito *web*.

In ogni modo il trasferimento dei dati a tali Paesi è comunque possibile attraverso le ulteriori modalità che esamineremo, se ne sussistono gli specifici requisiti.

La seconda ipotesi prevede la possibilità di trasferire dati solo se il Titolare o il Responsabile del trattamento ha fornito garanzie adeguate e gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Tali garanzie possono essere costituite da:

- accordi tra autorità o organismi pubblici degli Stati interessati;

³⁵ I criteri rilevanti per la decisione della Commissione sono fissati nell'art. 45, paragrafo 2, del Regolamento UE.

- norme vincolanti d'impresa³⁶;
- clausole tipo di protezione dei dati adottate dalla Commissione o da un'autorità Garante nazionale (e poi approvate dalla Commissione);
- un codice di condotta o un meccanismo di certificazione approvati³⁷ e l'impegno del Titolare o del Responsabile del trattamento nel paese terzo ad applicare garanzie adeguate.

La terza ipotesi si riferisce all'autorizzazione dell'autorità Garante nazionale con riferimento a:

- clausole contrattuali 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;
- disposizioni da inserire in accordi amministrativi tra autorità o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati.

L'ultima ipotesi – che può verificarsi solo in assenza delle condizioni già esaminate – è rappresentata da una serie di casi particolari. In primo luogo il trasferimento è consentito quando il trattamento è necessario per:

- l'esecuzione di un contratto concluso tra l'interessato e il Titolare del trattamento ovvero l'esecuzione di misure precontrattuali adottate su istanza dell'interessato;
- 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;
- importanti motivi di interesse pubblico che, è bene precisarlo, devono essere affermati dal diritto dello Stato membro del Titolare o dal diritto dell'UE e non possono essere fatti valere dallo Stato terzo;
- accertare, esercitare o difendere un diritto in sede giudiziaria;
- 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.

Inoltre, il trasferimento di dati personali è possibile se:

- l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato della mancanza di una decisione di adeguatezza e di garanzie adeguate;
- il trasferimento di dati sia effettuato a partire da un registro che, a norma del diritto nazionale o dell'Unione, mira a fornire informazioni al pubblico e può essere consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse;

³⁶ Si veda l'art. 47 del Regolamento UE secondo il quale le norme contrattuali d'impresa devono essere preventivamente validate dall'autorità Garante nazionale (in particolare è richiesto il rispetto di almeno 14 prescrizioni oltre a quelle che dovessero rendersi necessarie in relazione al caso concreto).

³⁷ Si vedano gli artt. 40 e 42 del Regolamento UE. Cfr. anche il paragrafo 1.6.1. del volume.

- il trasferimento di dati non sia ripetitivo, riguardi un numero limitato di interessati, sia necessario per il perseguimento degli interessi legittimi cogenti del Titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il Titolare del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali (in questo caso il Titolare del trattamento deve informare l'autorità di controllo e l'interessato)³⁸.

Per la PA

Alcuni dei casi sopra elencati non si applicano alle autorità pubbliche.

È in ogni caso vietato il trasferimento di dati verso Titolari o Responsabili in un Paese terzo sulla base di decisioni giudiziarie o ordinanze amministrative emesse da autorità di tale Paese terzo, a meno dell'esistenza di accordi internazionali. Diverse informazioni sui trattamenti – e relative garanzie – vanno riportate nel registro dei trattamenti³⁹.

1.6. Strumenti per la qualità del data protection

1.6.1. Il codice di condotta e l'organismo di controllo

Il GDPR prevede⁴⁰ che le associazioni e gli altri organismi rappresentanti le categorie di Titolari e Responsabili del trattamento possano elaborare, se lo ritengono, un proprio Codice di condotta, «destinato a contribuire alla corretta applicazione del presente Regolamento, in funzione delle specificità settoriali e delle esigenze specifiche delle micro, piccole e medie imprese».

Gli scopi dell'adesione ad un codice di condotta da parte dei Titolari e dei Responsabili dei trattamenti di dati personali - che, sottolineiamo, è facoltativa - sono essenzialmente tre:

- facilitare il rispetto del GDPR da parte dei soggetti aderenti, anche in funzione della specificità dei vari settori del trattamento e delle specifiche esigenze delle micro, piccole e medie imprese;
- concorrere a dimostrare la conformità da parte del Titolare del trattamento o dal Responsabile del trattamento ai requisiti previsti per un trattamento legittimo ed il rispetto degli obblighi posti a loro carico;

³⁸ Alcune fattispecie non si applicano alle pubbliche amministrazioni nell'esercizio di pubblici poteri (si veda l'art. 49, paragrafo 3, del Regolamento UE).

³⁹ Cfr. l'art. 49, paragrafo 6, del Regolamento UE. Si veda anche la Tavola 11.

⁴⁰ Cfr. gli artt. 40 e 41 ed i considerando 98, 99, 167 e 168 del Regolamento UE.

- acquisire garanzie richieste per trasferire dati personali verso paesi terzi o organizzazioni internazionali – questa finalità è riferita ai Titolari o Responsabili non soggetti al GDPR – in quanto il Regolamento UE le equipara all'adesione al codice di condotta.

I contenuti del codice di condotta riguardano fundamentalmente un'autodisciplina riferita a vari ambiti, tra cui:

- 1) il trattamento corretto e trasparente dei dati;
- 2) i legittimi interessi perseguiti dal Responsabile del trattamento in contesti specifici;
- 3) la raccolta dei dati personali;
- 4) la pseudonimizzazione dei dati personali;
- 5) l'informazione fornita al pubblico e agli interessati;
- 6) l'esercizio dei diritti degli interessati;
- 7) l'informazione fornita e la protezione del minore;
- 8) il *data protection by design e by default* nonché le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32;
- 9) la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni all'interessato;
- 10) il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali;
- 11) le procedure stragiudiziali e di altro tipo per comporre le controversie tra Titolari del trattamento e interessati.

Inoltre il codice di condotta comprende le modalità con cui l'apposito organismo richiamato dall'art. 41 del GDPR – accreditato dall'autorità Garante nazionale - controlla il rispetto del codice stesso da parte dei Titolari e dei Responsabili del trattamento che hanno aderito.

Per la PA

Non è previsto tale organismo per i trattamenti effettuati da autorità pubbliche e da organismi pubblici.

Questo organismo adotta specifiche misure in caso di violazione del codice da parte di un Titolare o di un Responsabile del trattamento, tra cui la sospensione o la revoca dell'adesione al codice, informandone l'autorità Garante nazionale. In ogni caso, rimangono fermi i poteri di controllo dell'autorità Garante nazionale. Il processo di formazione di un codice di condotta è piuttosto articolato. In primo luogo, il progetto di codice deve essere sottoposto all'autorità Garante nazionale che, nel caso lo approvi, provvede alla sua registrazione e pubblicazione.

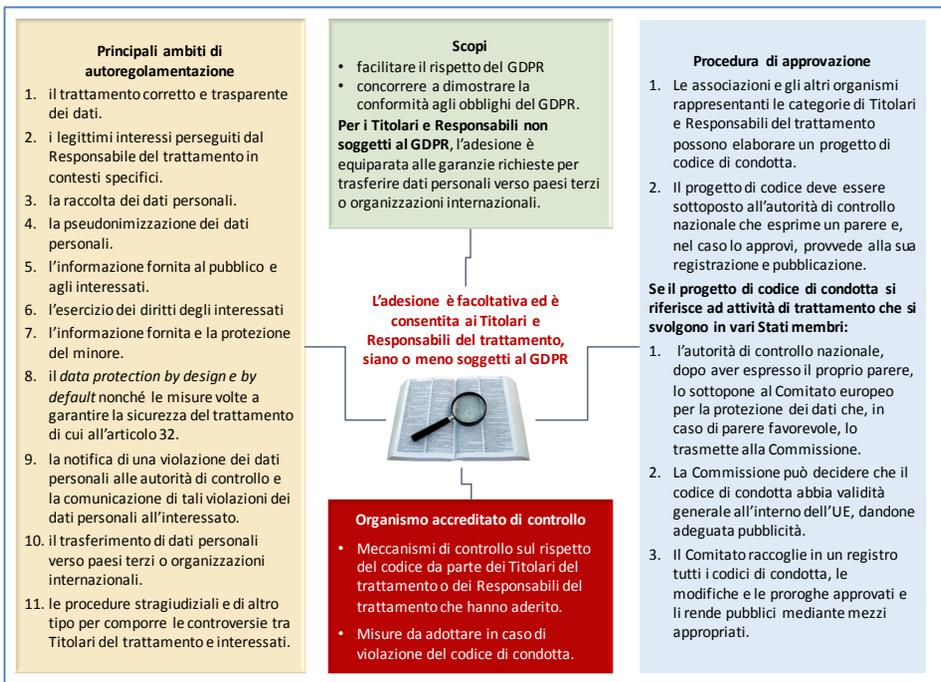
Se il progetto di codice di condotta si riferisce ad attività di trattamento che si svolgono in vari Stati membri, l'autorità Garante nazionale, dopo aver espresso il proprio parere, lo sottopone al Comitato europeo per la protezione dei dati che, in caso di parere favorevole, lo trasmette alla Commissione.

La Commissione, in questo caso, può decidere che il codice di condotta abbia validità generale all'interno dell'UE, dandone adeguata pubblicità.

Il Comitato, infine, raccoglie in un registro tutti i codici di condotta, le modifiche e le proroghe approvati e li rende pubblici mediante mezzi appropriati.

La Figura 9 sintetizza gli aspetti descritti.

Figura 9 – Il codice di condotta



1.6.2. La certificazione

Per dimostrare la conformità dei trattamenti effettuati dai Titolari e dai Responsabili del trattamento al GDPR, sono previsti anche meccanismi di certificazione, sigilli e marchi di protezione dei dati, che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi⁴¹.

Alcune caratteristiche sono analoghe a quelle dei codici di condotta in quanto, come questi ultimi, le certificazioni:

- sono volontarie;

⁴¹ Cfr. gli artt. 42 e 43 ed i considerando 100, 166, 167 e 168 del Regolamento UE.

- tengono in considerazione le esigenze specifiche delle micro, piccole e medie imprese;
- concorrono a dimostrare la conformità da parte del Titolare o del Responsabile del trattamento al GDPR, anche se tale accertamento deve avvenire in concreto e salvo i poteri dell'autorità Garante;
- per i Titolari o Responsabili non soggetti al GDPR, l'adesione ai meccanismi di certificazione, ai sigilli ed ai marchi è equiparata alle garanzie richieste per trasferire dati personali verso paesi terzi o organizzazioni internazionali.

Tra tali caratteristiche deve peraltro sottolinearsi quella che attribuisce valore di mera presunzione semplice alla certificazione: l'art. 42, infatti, prevede che la certificazione "non riduce" le responsabilità del Titolare o del Responsabile che l'abbia ottenuta.

La procedura di certificazione – che deve essere *trasparente* e consentire una certificazione *accessibile* – si basa su criteri approvati dall'autorità Garante nazionale o dal Comitato⁴² e prevede che il Titolare del trattamento (o il Responsabile) fornisca all'organismo di certificazione (o, ove applicabile, all'autorità di controllo) tutte le informazioni e l'accesso alle attività di trattamento.

La certificazione è rilasciata al Titolare o al Responsabile del trattamento per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti mentre, in caso contrario, è revocata.

L'organismo di certificazione comunica i motivi del rilascio, del diniego o della revoca della certificazione all'autorità Garante che può, se lo ritiene, modificare la decisione.

Gli organismi di certificazione sono responsabili della corretta valutazione che comporta il rilascio o il diniego della certificazione o la revoca di quest'ultima, ferma restando la responsabilità del Titolare o del Responsabile del trattamento riguardo alla conformità al Regolamento UE.

Il Comitato rende pubblici tutti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati, provvedendo a raccogliergli in un registro.

1.6.3. L'accreditamento

Innanzitutto, per dirimere eventuali dubbi, indichiamo la differenza tra accreditamento e certificazione.

L'accreditamento serve a riconoscere la competenza tecnica e organizzativa di un organismo di valutazione della conformità mentre la certificazione è la procedura attraverso la quale una terza parte conferma per iscritto che prodotti, processi, sistemi o persone sono conformi a determinati requisiti⁴³.

⁴² Cfr., rispettivamente, gli artt. 58 e 63 del Regolamento UE.

⁴³ Cfr. la norma ISO/IEC 17000, par. 5.5 e par. 5.6.

La differenza tra le due procedure, in apparenza simili, consiste nel fatto che, nel caso dell'accreditamento, si pone in primo piano il riconoscimento formale delle competenze mentre nel caso della certificazione si tratta innanzitutto di accertare la conformità a una norma o a un quadro normativo.

Ad esempio, abbiamo appena visto il caso dell'organismo di controllo del rispetto dei codici di condotta, da parte del Titolare e del Responsabile del trattamento.

Questo organismo può essere accreditato dall'autorità Garante nazionale se ha:

- dimostrato di essere indipendente e competente riguardo al contenuto del codice;
- istituito apposite procedure per stabilire se i Titolari e i Responsabili del trattamento applicano e rispettano il codice e ne riesaminano periodicamente il funzionamento;
- istituito procedure trasparenti e strutture atte a gestire i reclami relativi a violazioni del codice o al modo in cui è attuato;
- dimostrato che i compiti e le funzioni svolti non danno adito a conflitto di interessi.

In generale gli organismi di certificazione sono accreditati dall'autorità Garante nazionale oppure dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio conformemente alla norma EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo.

Se le condizioni ed i requisiti previsti vengono meno, l'autorità Garante revoca l'accreditamento dell'organismo.

L'accreditamento è rilasciato per un periodo massimo di cinque anni e può essere rinnovato alle stesse condizioni purché l'organismo di certificazione confermi il possesso dei requisiti.

1.7. Data breach: notifiche, comunicazioni e responsabilità. Il sistema sanzionatorio

Cosa accade in caso di violazione dei dati personali (c.d. "*personal data breaches*")?

Innanzitutto dobbiamo stabilire cosa si intende per "violazione dei dati personali". La definizione è fissata dallo stesso GDPR, al n. 12 dell'art. 4, secondo cui si tratta della "*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*".

Al riguardo, è stato opportunamente evidenziato che tali violazioni possono essere ricondotti ai seguenti principi di sicurezza delle informazioni⁴⁴, su cui ci soffer-

⁴⁴ Si veda la norma ISO/IEC 27000:2016 Information technology – Security techniques – Information security management system – Overview and vocabulary. Si rinvia anche alle *Guidelines on Personal*

fermeremo nel paragrafo 5.1: riservatezza, disponibilità, integrità, autenticità, non ripudio.

Il considerando 85 indica anche alcune delle conseguenze che possono discendere da tali violazioni: *"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, decifrazione 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"*.

Constatata l'avvenuta violazione dei dati personali, il Responsabile del trattamento informa immediatamente il Titolare del trattamento che⁴⁵:

- invia una notifica all'autorità Garante nazionale, senza ingiustificato ritardo e, ove possibile, entro 72 ore⁴⁶, a meno che non sia in grado di dimostrare che *"è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche"*;
- se la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, informa l'interessato non appena possibile per consentirgli di prendere le precauzioni necessarie, formulando anche raccomandazioni finalizzate ad attenuare i potenziali effetti negativi.

Risulta quindi necessario predisporre un sistema che segnali tempestivamente al Titolare ogni violazione attraverso, ad esempio, la progettazione e l'utilizzo dei c.d. *software sentinella*.

Ma quando un *data breach* comporta delle responsabilità? Al riguardo è necessario verificare se i dati personali fossero o meno protetti con adeguate misure tecnologiche e organizzative atte a limitare efficacemente le violazioni (il rischio di furto d'identità o altre forme di abuso).

In particolare occorre dare una valutazione sull'*adeguatezza* delle misure di sicurezza che, secondo l'art. 32 del GDPR⁴⁷, deve tener conto:

- dello stato dell'arte e dei costi di attuazione;
- della natura, dell'oggetto, del contesto e delle finalità del trattamento;
- della probabilità e gravità del rischio "privacy" per i diritti e le libertà delle persone fisiche;

data breach notification under Regulation 2016/679, elaborate dal Gruppo di lavoro "Articolo 29" per la protezione dei dati, del 3 ottobre 2017.

⁴⁵ Cfr. gli artt. 33 e 34 ed i considerando 85, 86, 87 e 88 del Regolamento UE.

⁴⁶ Oltre il termine di 72 ore, la notifica dovrebbe essere corredata dalle ragioni del ritardo.

⁴⁷ Cfr. anche il considerando 83.

- dalle conseguenze che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali comunque trattati.

In concreto, le misure di sicurezza messe in atto dal Titolare e dal Responsabile del trattamento, possono includere:

- 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 adottate.

È infine previsto che l'adesione a un codice di condotta approvato dall'autorità Garante nazionale o a un meccanismo di certificazione accreditato possano essere utilizzati per dimostrare la conformità ai requisiti di sicurezza.

La Figura 10 sintetizza i concetti esposti.

Figura 10 – Gli elementi del Data Breach



L'ultimo aspetto da esaminare, una volta accertata un'eventuale responsabilità, è quello delle conseguenze, con riferimento a due distinte procedure.

La prima, azionabile dinanzi all'autorità giudiziaria nazionale, consiste nel garantire il diritto al risarcimento del danno⁴⁸, materiale o immateriale, da parte del:

- Titolare del trattamento, per il danno cagionato a seguito delle violazioni del GDPR;
- Responsabile del trattamento, solo se non ha adempiuto ai suoi obblighi specifici previsti dal GDPR o se ha agito in modo difforme rispetto alle istruzioni del Titolare del trattamento.

In caso di concorso, la responsabilità è solidale, al fine di garantire il risarcimento effettivo dell'interessato.

La seconda procedura si riferisce all'applicazione delle sanzioni amministrative pecuniarie previste dall'art. 83 del GDPR, che possono essere integrate con altre sanzioni – di natura penale o amministrativa - stabilite da ciascun Stato membro, nel rispetto del principio del *ne bis in idem*⁴⁹: in entrambi i casi le sanzioni devono avere i caratteri dell'*effettività*, della *proporzionalità* e della *dissuasività*.

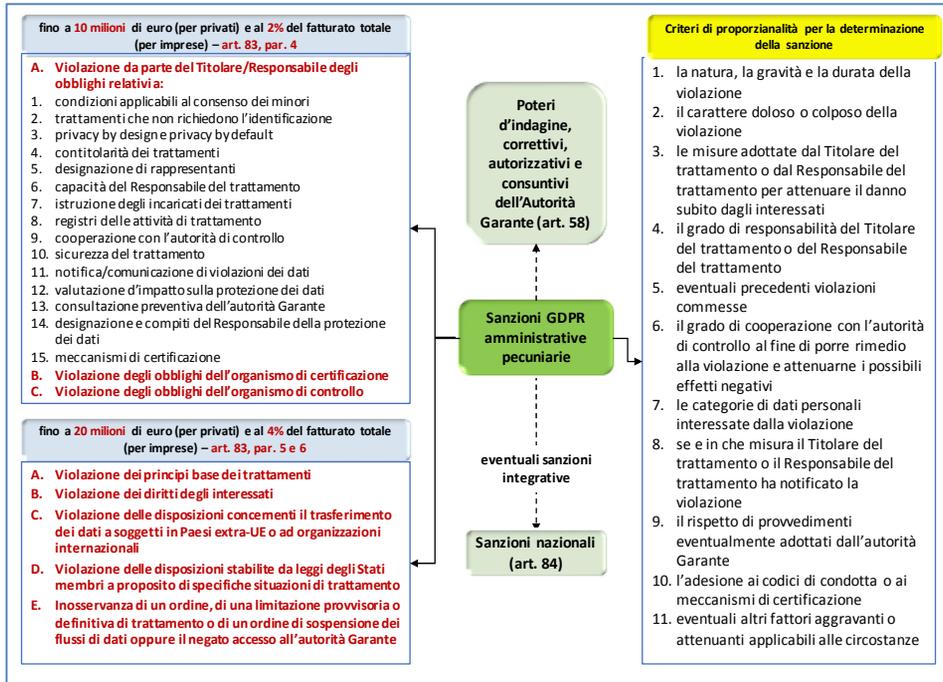
Le sanzioni previste dal GDPR sono particolarmente severe in quanto prevedono la misura massima di € 20.000.000 per i privati o del 4% del fatturato complessivo (consolidato), se superiore, per le imprese. In concreto la loro entità è graduata in base ad una serie di ipotesi (carattere doloso o colposo della violazione, entità del danno, ecc.).

La Figura 11 riassume i componenti del sistema sanzionatorio.

⁴⁸ Cfr. l'art. 82 ed i considerando 142, 146 e 147 del Regolamento UE.

⁴⁹ Cfr. anche l'art. 84 ed i considerando 148, 149, 150 e 152 del Regolamento UE.

Figura 11 – Il sistema sanzionatorio



1.8. Le autorità di controllo indipendenti

L'autorità di controllo italiana è denominata *Garante per la protezione dei dati personali* ed è un'autorità amministrativa indipendente istituita dalla *legge 31 dicembre 1996, n. 675* (poi abrogata e sostituita dal D.Lgs. 30 giugno 2003 n. 196, Codice in materia di protezione dei dati personali).

Il Regolamento UE⁵⁰ prevede l'istituzione di una o più autorità di controllo per ciascun Stato membro incaricate di sorvegliarne l'applicazione al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento, nonché di agevolare la libera circolazione dei dati personali all'interno dell'Unione.

Ovviamente è riconosciuta espressamente l'indipendenza dell'autorità di controllo - anche attraverso l'attribuzione delle risorse umane, tecniche e finanziarie necessarie - che si sostanzia, ad esempio, con la previsione di un bilancio separato da quello generale dello Stato, della selezione diretta del proprio personale, dell'astensione per tutta la durata del mandato dall'esercizio di qualunque altra attività incompatibile, remunerata o meno, e del divieto di sollecitare o accettare istruzioni.

⁵⁰ Cfr. gli artt. 51 - 59 ed i considerando 117 - 125, 127 - 129, 131-132 del Regolamento UE.

Il Regolamento UE, attesa la rilevanza strategica di questo soggetto, entra nel dettaglio anche per le modalità di scelta dei componenti e prevede specifiche riserve di legge.

Innanzitutto stabilisce che i componenti dell'autorità Garante possano essere nominati solo dal Parlamento, dal Governo, dal capo dello Stato o da un organismo indipendente a ciò deputato e che posseggano le qualifiche, l'esperienza e le competenze, in particolare nel settore della protezione dei dati personali, necessarie per lo svolgimento dei loro compiti.

Passando alle riserve di legge, è previsto che i seguenti ambiti siano disciplinati con provvedimento legislativo:

- l'istituzione dell'autorità di controllo;
- le qualifiche, le condizioni di idoneità e le procedure per la nomina del membro dell'autorità di controllo;
- la durata del mandato del membro, che comunque non può essere inferiore a quattro anni⁵¹;
- l'eventuale rinnovabilità del mandato del membro e, in caso positivo, il numero di rinnovi;
- le condizioni riferite agli obblighi dei membri e del personale dell'autorità di controllo; i divieti relativi ad attività, professioni e benefici incompatibili con tali obblighi durante e dopo il mandato; le regole che disciplinano la cessazione del rapporto di lavoro.

Inoltre, è stabilito che ogni Stato membro abbia notificato alla Commissione le disposizioni di legge adottate al più tardi entro il 25 maggio 2018 (si tratta senz'altro di un termine ordinatorio, coerente con i ritardi che purtroppo continuano a registrarsi!), comunicando senza ritardo ogni successiva modifica.

I compiti demandati all'autorità di controllo sono indicati in un elenco di 22 punti che, sostanzialmente, comprendono ambiti di intervento riguardanti:

- il rispetto del GDPR;
- la promozione della cultura del *data protection*;
- attività di consulenza ai vari *stakeholders*;
- tutela e supporto all'interessato;
- collaborazione con le altre autorità di controllo;
- aspetti specialistici quali, ad esempio, le clausole contrattuali tipo, valutazione d'impatto sulla protezione dei dati, codici di condotta, meccanismi di certificazione, accreditamento degli organismi di certificazione, norme vincolanti di impresa.

Per quanto concerne i poteri, si distinguono quelli di indagine, correttivi, autorizzativi e consultivi. I primi tendono all'acquisizione di informazioni dai Titolari/Responsabili ovvero alla contestazione ai medesimi di presunte violazioni; i secondi concernono per lo più avvertimenti, ammonimenti, ingiunzioni, ordini e

⁵¹ Salvo per le prime nomine dopo il 24 maggio 2016.

sanzioni ai Titolari/Responsabili; i terzi e gli ultimi sono finalizzati al rilascio di pareri, autorizzazioni e accreditamenti.

Tali poteri devono essere esercitati "in modo imparziale ed equo ed entro un termine ragionevole" e, in particolare, "ogni misura dovrebbe essere appropriata, necessaria e proporzionata al fine di assicurare la conformità al presente regolamento". Inoltre ogni misura giuridicamente vincolante dell'autorità di controllo deve prevedere almeno i seguenti requisiti:

- avere forma scritta;
- essere chiara e univoca;
- riportare la denominazione dell'autorità di controllo che ha adottato la misura e la relativa data di adozione;
- recare la firma del Garante o di un membro dell'autorità di controllo da lui autorizzato;
- precisare i motivi della misura;
- fare riferimento al diritto di esperire un ricorso effettivo;
- essere soggetta al controllo giurisdizionale dello Stato membro dell'autorità di controllo che ha adottato la decisione.

All'autorità di controllo è, inoltre, riconosciuta una legittimazione attiva processuale in quanto ogni Stato membro deve disporre, con legge, che la propria Autorità abbia il potere di intentare un'azione o di agire in sede giudiziale o stragiudiziale in caso di violazione del regolamento, al fine di farne rispettare le disposizioni.

L'autorità di controllo deve infine redigere e trasmettere al Parlamento, al Governo e alle altre autorità designate dallo Stato membro una relazione annuale sulla propria attività.

Il documento - che deve essere messo a disposizione del pubblico, della Commissione e del Comitato europeo per la protezione dei dati - deve contenere, tra l'altro, un elenco delle tipologie di violazioni notificate e dei poteri correttivi esercitati.

1.9. Dal Gruppo "articolo 29" al Comitato Europeo per la protezione dei dati

Con l'art. 29 della direttiva 95/46 - da cui ha preso il nome - è stato istituito un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designato da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati) e da un rappresentante della Commissione.

Il Gruppo, articolato in sottogruppi, approva all'inizio dell'anno un programma di lavoro in cui vengono indicate le priorità operative e si riunisce in seduta plenaria in media ogni due mesi.

Il successivo art. 30 ne fissa i compiti tra i quali ricordiamo l'emanazione di linee guida e la formulazione di pareri e raccomandazioni - trasmessi di regola alla Commissione che a sua volta fornisce riscontro sulle determinazioni assunte - su

qualsiasi questione riguardante la protezione dei dati personali nell'Unione Europea nonché in caso di divergenze tra le legislazioni degli Stati membri.

Inoltre il Gruppo redige una Relazione Annuale – che viene pubblicata e trasmessa alla Commissione, al Parlamento ed al Consiglio – in cui sono illustrate le attività svolte e le linee evolutive, anche in relazione all'attività condotta dalle autorità Garanti nazionali⁵².

La Figura 12 indica le linee guida emanate dal Gruppo "articolo 29"⁵³.

Il Regolamento UE ha previsto la trasformazione del Gruppo "articolo 29" nel neo costituito organismo Comitato europeo per la protezione dei dati - come si evince dall'art. 94 secondo il quale *"I riferimenti al gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE si intendono fatti al comitato europeo per la protezione dei dati istituito dal presente regolamento"* – potenziandolo ulteriormente.

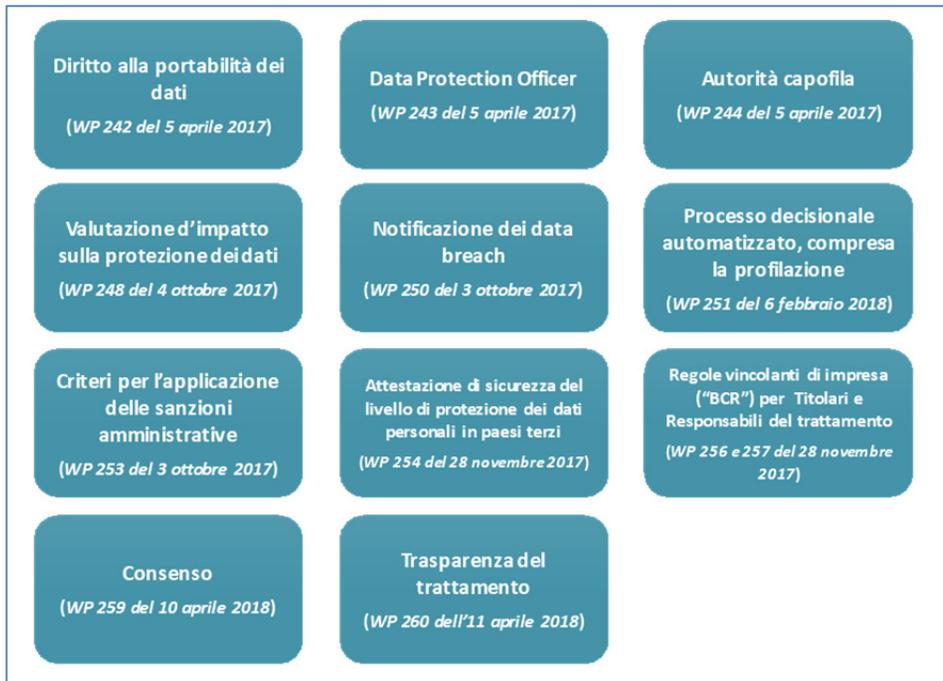
Il Comitato europeo per la protezione dei dati⁵⁴ - la cui indipendenza è espressamente richiamata dall'art. 69 e garantita dal potere di autorganizzazione - è composto dall'autorità Garante di ciascuno Stato e dal Garante europeo della protezione dei dati (o dai rispettivi rappresentanti) nonché dal rappresentante della Commissione che partecipa alle attività senza diritto di voto e, in definitiva, concorre ad attuare il principio sancito dall'art. 63 del Regolamento UE secondo il quale *"Al fine di contribuire all'applicazione coerente del presente regolamento in tutta l'Unione, le autorità di controllo cooperano tra loro[...]"*, in quanto contribuisce a garantire che la legislazione sulla protezione dei dati sia applicata in modo coerente in tutta l'UE e assicura una cooperazione efficace tra le autorità per la protezione dei dati.

⁵² I provvedimenti adottati dal Gruppo sono ordinati cronologicamente, a partire dal 1997, e reperibili sia sul link http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358 che sul sito del Garante per la protezione dei dati personale (home>attività internazionali>Gruppo di lavoro ex articolo 29) con una scheda esplicativa di accompagnamento.

⁵³ Le date delle linee guida si riferiscono alla loro emanazione o all'ultima rettifica.

⁵⁴ Cfr. gli artt. 63 - 76 ed i considerando 139 e 140 del Regolamento UE.

Figura 12 – Le linee guida del Gruppo “articolo 29”



Deve, infatti, evidenziarsi che questo organismo non si limita a pubblicare linee guida sull’interpretazione dei concetti fondamentali del GDPR, ma è chiamato anche a pronunciarsi mediante decisioni vincolanti sulle controversie relative al trattamento transfrontaliero, garantendo in tal modo un’applicazione uniforme delle norme unionali per evitare che lo stesso caso possa essere trattato in modo diverso.

Al riguardo possono ricordarsi le seguenti competenze:

- il controllo sul GDPR per assicurarne l’applicazione corretta, fatti salvi i compiti delle autorità nazionali di controllo;
- il potere di comporre le controversie che si instaurano con e tra le Autorità di controllo;
- l’emanazione di linee guida, raccomandazioni e migliori prassi;
- l’emanazione di pareri e lo scambio informativo con le autorità di controllo;
- l’attività di consulenza alla Commissione;
- l’accreditamento di organismi di certificazione;
- la promozione di programmi comuni di formazione;
- la tenuta di un registro elettronico, accessibile al pubblico, delle decisioni adottate dalle autorità di controllo e dalle autorità giurisdizionali su questioni trattate nell’ambito del “meccanismo di coerenza”.

Infine, il Comitato deve redigere una relazione annuale sulla protezione delle persone fisiche – che, tra l’altro, deve includere la valutazione dell’applicazione pratica delle linee guida, raccomandazioni e migliori prassi nonché delle decisioni vincolanti delle controversie che si instaurano con e tra le Autorità di controllo – che viene poi pubblicata e trasmessa al Parlamento europeo, al Consiglio e alla Commissione.

2. I diritti tutelati

2.1. Diritto alla protezione dei dati personali (data protection), diritto alla riservatezza (privacy) e diritti derivati

Molte analisi, anche approfondite, risultano inconcludenti in quanto, anche in presenza di persone competenti, non si riescono a definire correttamente gli elementi “di base” delle questioni e ciò condiziona negativamente le attività rivolte ad inquadrare i problemi e ad individuare adeguate soluzioni.

A mio avviso, ciò accade perché molte cose che diamo per scontate – spesso anche quelle fondamentali – in realtà, non lo sono! Per questa ragione, innanzitutto, vorrei soffermarmi a riflettere brevemente sulle situazioni che la normativa intende tutelare.

In sostanza, ciò che le disposizioni intendono proteggere è inteso come un diritto plurifunzionale, destinato a rispondere a molteplici finalità e ad offrire una sorta di tutela globale alla persona che nella società in cui viviamo – non a caso da molti denominata *dell'informazione* – si risolve sempre più spesso nella protezione dei dati che la riguardano. Semplificando, possiamo distinguere due ipotesi, a seconda che il *focus* sia indirizzato al diritto alla protezione dei dati personali oppure al diritto alla riservatezza.

Nella prima ipotesi, il c.d. *data protection*, l'oggetto del diritto sono i dati personali e quindi la tutela è riferita ad ogni uso improprio di essi.

L'altra ipotesi riguarda il diritto alla riservatezza il cui corrispondente termine inglese “privacy” – di facile richiamo semantico – ha denominato l'intera normativa. L'uso di tale termine risulta però fuorviante, o quantomeno limitativo, rispetto alla realtà in quanto la *privacy* costituisce un ambito più ristretto rispetto a quello relativo alla concezione precedente.

Essa, infatti, **si configura sul modello del diritto di proprietà e, in particolare, nei suoi riflessi oppositivi ai terzi** (*ius excludendi alios* dalla propria vita privata) poiché sostanzialmente rappresenta un (giusto?) **limite alla libertà di espressione e al diritto all'informazione**, inibendo la diffusione di informazioni personali nel caso in cui la persona interessata non abbia dato il suo consenso, salvo deroghe eccezionali (ad esempio se la notizia sia di pubblico interesse o per la notorietà della persona interessata).

Salomonicamente l'art. 1 del GDPR precisa che le sue disposizioni proteggono “in particolare il diritto alla protezione dei dati personali” **ma anche** “i diritti e

le libertà fondamentali delle persone fisiche”, qual è appunto il diritto alla riservatezza (qualche giurista preciserebbe che rientra nei diritti della personalità che, a loro volta, fanno capo ai diritti soggettivi assoluti¹).

Non può, tuttavia, sfuggire come il GDPR, rispetto al passato, si focalizzi più sulla protezione dei dati che sul diritto alla riservatezza, come può rilevarsi dalla Tavola 3.

Tavola 3 – Diritto alla protezione dei dati e diritto alla riservatezza

D.Lgs. 30 giugno 2003, n. 196, “Codice in materia di protezione dei dati personali”	Regolamento UE 2016/679 in materia di protezione dei dati personali
Articolo 2 - Finalità Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza , all'identità personale e al diritto alla protezione dei dati personali .	Articolo 1 - Oggetto e finalità 1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali , nonché norme relative alla libera circolazione di tali dati. 2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali . 3. (<i>omissis</i>)

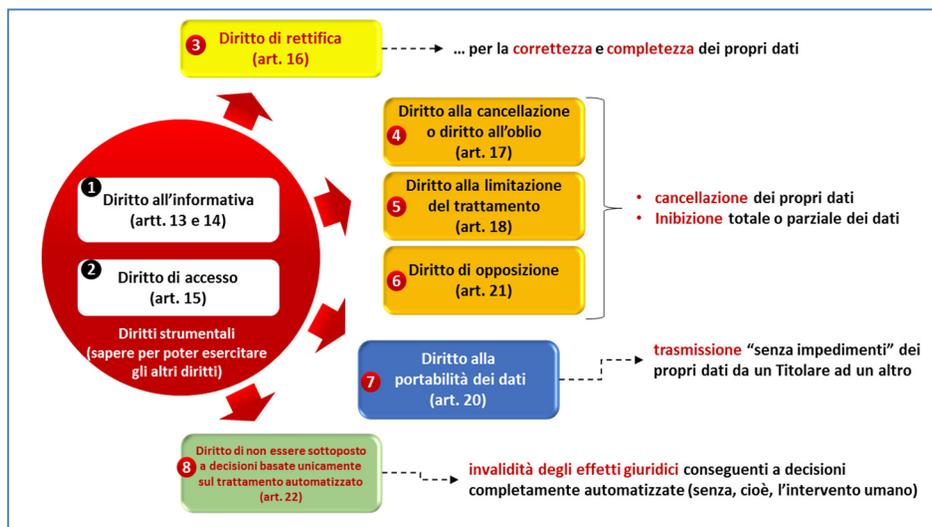
In definitiva appare evidente come le due nozioni abbiano punti di contatto e aree di sovrapposizione ma può senz'altro affermarsi che l'attuale disciplina pone il *focus* sulla tutela del diritto alla protezione dei dati coerentemente con la linea di tendenza registrata nella precedente normativa ma, sicuramente, in maniera più netta rispetto al passato. La prospettiva è quella di proteggere il dato non in quanto tale ma perché, attraverso la protezione del dato, possa tutelarsi la persona.

Queste riflessioni – che possono apparire come sterili disquisizioni di natura giuridica – si propongono di consolidare un punto di vista privo di ambiguità, una base concettuale chiara, indispensabile per costruire un sistema coerente. E ciò soprattutto sulla base del fatto che i fallimenti che si registrano nelle *performance* dei modelli complessi, trovano frequentemente la loro causa principale nella fase di progettazione e nell'ambito del *problem solving* e, in particolare, nella mancata definizione degli elementi base della questione (obiettivi, strumenti, attori, ecc.).

¹ Il diritto alla riservatezza può essere collocato nell'ambito di quei diritti di nuova formazione, non presenti all'epoca della codificazione costituzionale. Nel nostro ordinamento, il riconoscimento del diritto alla riservatezza è stato riconosciuto per la prima volta in via giurisprudenziale, con la sentenza della Corte di Cassazione 27 maggio 1975, n. 2129.

Ma veniamo ora ad esaminare gli specifici diritti che il sistema GDPR riconosce agli interessati – sintetizzati nella Figura 13 – le cui modalità di esercizio devono essere caratterizzate da trasparenza, chiarezza, semplicità, tempestività e, in genere, senza oneri economici, come in dettaglio stabilito dall'art. 12 del GDPR.

Figura 13 – Diritti degli interessati



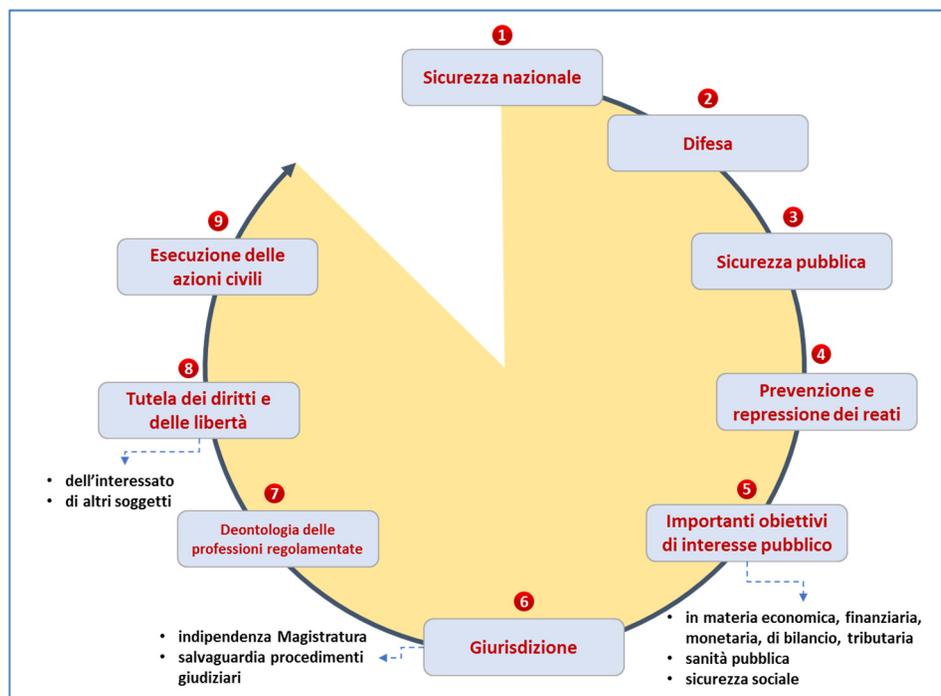
Prima di procedere con una loro puntuale disamina, tuttavia, nel prossimo paragrafo ci soffermeremo preliminarmente sulle limitazioni a cui possono essere soggetti, a factor comune, tutti i diritti degli interessati.

2.2. Limitazioni all'esercizio dei diritti dell'interessato

Il diritto comunitario e quello nazionale (del Titolare o del Responsabile del trattamento) possono limitare, mediante misure legislative, i diritti dell'interessato ed i principi applicabili al trattamento dei dati personali che impattano su tali diritti, "qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare" determinati interessi², riportati nella Figura 14.

² Cfr. l'art. 23 ed il considerando 73 del Regolamento UE.

Figura 14 – Limitazioni ai diritti degli interessati



Tuttavia, stabilisce il GDPR, i provvedimenti legislativi che limitano i diritti dell'interessato devono precisare:

- le finalità del trattamento o le categorie di trattamento;
- le categorie di dati personali;
- la portata delle limitazioni introdotte;
- le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti;
- l'indicazione del Titolare del trattamento;
- i periodi di conservazione e le garanzie applicabili;
- i rischi per i diritti e le libertà degli interessati;
- il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

2.3. Diritto all'informativa e diritto di accesso

Questi due diritti sono strettamente connessi in quanto entrambi correlati alle informazioni e comunicazioni destinate all'interessato.

Il primo diritto riguarda le informazioni che il Titolare del trattamento ha l'obbligo di fornire all'interessato *"nel momento in cui i dati personali sono ottenuti"*, sia direttamente sia presso altri soggetti. Si tratta del diritto all'informativa, che sarà trattato specificamente nel capitolo 3 al paragrafo 3.1.

Il diritto di accesso³, invece, consiste nella potestà, da parte dell'interessato, di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano.

In caso positivo, l'interessato può ottenere l'accesso gratuito ai propri dati personali attraverso una copia di essi ma, se sono richieste più copie, il Titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se la richiesta è presentata attraverso mezzi elettronici, salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

L'interessato, inoltre, può ottenere diverse informazioni quali, ad esempio, quelle relative:

- alla finalità del trattamento;
- alle categorie dei dati personali trattati;
- ai destinatari dei dati personali;
- al periodo di conservazione dei dati personali previsto oppure, se non è possibile, ai criteri utilizzati per determinare tale periodo;
- al diritto di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- al diritto di proporre reclamo a un'autorità di controllo;
- a tutte le informazioni disponibili sull'origine dei dati trattati, qualora non siano stati raccolti presso l'interessato;
- all'esistenza di un processo decisionale automatizzato, compresa la profilazione, con la specificazione della logica utilizzata, nonché dell'importanza e delle conseguenze previste per l'interessato;
- alle garanzie applicate in caso di trasferimento dei dati verso Paesi terzi.

In sintesi si tratta di un diritto di contenuto informativo, strumentale per l'esercizio di diritti ulteriori - indicati dagli articoli dal 13 al 22 - quali la rettifica, la cancellazione e l'opposizione al trattamento.

Risulta interessante il riferimento del GDPR al modo con cui l'interessato può esercitare il diritto di accesso: "facilmente" e "a intervalli ragionevoli".

Nel primo caso, si deve pensare alle soluzioni che il Titolare del trattamento ha l'obbligo di adottare, da un lato, per eliminare tutti gli oneri inutili a carico dell'interessato e, dall'altro, per individuare tutte le misure che lo possano aiutare come, ad esempio, la consultazione diretta ai propri dati personali attraverso l'accesso remoto. Si tratta quindi di intervenire nel sistema di gestione e, cioè, sia nell'ambito dell'organizzazione che dei processi.

Gli "intervalli ragionevoli", invece, consistono in una garanzia posta a favore del Titolare del trattamento a difesa dell'*abuso del diritto*, e cioè di richieste di accesso reiterate, senza soluzione di continuità, che potrebbero costituire veri e propri atti emulativi, concepiti sul modello di cui all'art. 833 del Codice civile.

³ Cfr. l'art. 15 ed i considerando 63 e 64 del Regolamento UE.

Altrettanto significativa appare la precisazione del considerando 64: "Il Titolare del trattamento non dovrebbe conservare dati personali al solo scopo di poter rispondere a potenziali richieste"⁴.

2.4. Diritto di rettifica

A seguito dell'accesso, l'interessato può, quindi, verificare la correttezza e la completezza dei propri dati personali utilizzati nel trattamento.

Conseguentemente, in caso di irregolarità può:

- nella prima ipotesi, esercitare il diritto di ottenere dal Titolare del trattamento la rettifica, senza ritardo, dei dati personali inesatti che lo riguardano;
- nella seconda ipotesi, ottenere l'integrazione dei dati, anche fornendo una dichiarazione integrativa.

In entrambi i casi, vanno informati i destinatari ai quali erano stati trasmessi i dati.

2.5. Diritto alla cancellazione o diritto all'oblio

Tra i diritti dell'interessato il GDPR cita il diritto alla cancellazione, indicandolo anche come "diritto all'oblio".

Preliminarmente va però osservato che sul concetto di diritto all'oblio si registrano opinioni contraddittorie.

Sintetizzando. Per alcuni studiosi il diritto all'oblio ha una sua netta autonomia e corrisponde al diritto all'identità personale attuale, poggiando su una dimensione connotata dall'elemento temporale (vetustà dei fatti e decorso del tempo) e dall'*inutilità* sociale dell'informazione. Ed in questo senso, il diritto all'oblio si caratterizzerebbe perché potrebbe essere violato solo da un mezzo di informazione che abbia dato grande rilevanza ad una notizia datata, in mancanza di un interesse sociale attuale.

A questo orientamento si contrappone chi invece considera il diritto all'oblio come un prolungamento del diritto alla riservatezza inteso come il diritto a cancellare, ovvero a contestualizzare, i dati personali per vietare un travisamento dell'immagine sociale di un soggetto, per evitare che la vita passata possa costituire un ostacolo per la vita presente e possa ledere la propria dignità umana. Inoltre, per molto tempo, ci si è chiesto se il diritto all'oblio (noto con le espressioni *right to be forgotten* o *right to erasure*) riguarda la riservatezza dei dati – e quindi afferisce alla tutela del trattamento dei dati personali – o altri diritti.

La questione, ai nostri fini, ha perso gran parte del proprio rilievo, se non per il fatto che il concetto di oblio risulta più ampio di quello di cancellazione: esso, infatti, si può considerare come il diritto di un soggetto a vedersi "dimenticato" dalle banche dati e dai motori di ricerca. Ciò comporta attività particolarmente

⁴ Tale affermazione è stata però criticata da alcuni commentatori che hanno evidenziato l'inopportunità della modalità verbale usata (il condizionale, **dovrebbe**, anziché l'indicativo, **deve**).

complesse in relazione all'immane quantità di dati che ognuno di noi rilascia quotidianamente, a volte inconsapevolmente, nella rete (*social networks*, ecc.). Venendo al diritto positivo⁵, l'art. 17 del Regolamento UE stabilisce che è possibile ottenere dal Titolare di un trattamento, "senza ingiustificato ritardo", la cancellazione dei propri dati personali in presenza di determinati requisiti (assenza di attualità/necessità dei dati, l'illiceità *ab origine* del trattamento, ecc.). La cancellazione dei dati, in particolare, è condizionata sotto un duplice profilo: da un lato, tecnologicamente, poiché è previsto che l'obbligo di cancellazione per il Titolare del trattamento sia adempiuto tenuto conto della tecnologia disponibile e dei costi di attuazione; dall'altro, in quanto impone il rispetto di altri diritti e interessi ritenuti meritevoli di tutela, quale, *in primis*, l'esercizio del diritto alla libertà di espressione e di informazione.

In dettaglio, l'interessato può decidere che siano cancellati e non sottoposti ulteriormente a trattamento i propri dati personali:

- 1) quando non siano più necessari per le finalità per le quali sono stati raccolti;
- 2) nel caso di opposizione al trattamento nonché di revoca del consenso e non sussiste alcun fondamento giuridico al trattamento;
- 3) quando il trattamento non sia altrimenti conforme al Regolamento;
- 4) nel caso di trattamento illecito;
- 5) se devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento;
- 6) se sono stati raccolti relativamente all'offerta di servizi della società dell'informazione ai minori.

Tuttavia, nonostante la ricorrenza delle precedenti ipotesi, l'ulteriore conservazione dei dati personali risulta legittima:

- qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione;
- per adempiere a un obbligo legale;
- per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri dei quali è investito il Titolare del trattamento;
- per accertare, esercitare o difendere un diritto in sede giudiziaria;
- se sussiste una ragione di pubblico interesse, nel settore della sanità pubblica e ai fini di archiviazione nell'ambito della ricerca scientifica e storica e per fini statistici.

⁵ Cfr. gli artt. 17 e 19 e i considerando 31, 65 e 66 del Regolamento UE.

Ma cosa succede se i dati che si chiede di cancellare sono già stati pubblicati?

Si prevede l'obbligo per i Titolari che hanno reso pubblici i dati personali dell'interessato (ad esempio, pubblicandoli su un sito *web*) di informare della richiesta di cancellazione gli altri Titolari che trattano i dati personali da cancellare (compresi "qualsiasi link, copia o riproduzione"). Il tutto "adottando le misure necessarie, in considerazione della tecnologia disponibile e dei costi di attuazione".

2.6. Diritto alla limitazione del trattamento

Questo diritto⁶ consiste nell'inibire al Titolare - permanentemente o per un periodo di tempo limitato, del tutto o in parte - il trattamento di specifici dati personali o determinate operazioni.

La limitazione *temporanea* del trattamento può essere ottenuta se l'interessato:

- 1) contesta l'esattezza dei dati personali (la limitazione opera per il periodo necessario per le verifiche sull'esattezza dei dati);
- 2) si è opposto al trattamento (la limitazione opera fin quando il Titolare del trattamento non dimostri l'esistenza di motivi "cogenti" prevalenti rispetto a quelli dell'interessato).

Altri casi di limitazione del trattamento sono previsti nelle ipotesi in cui il trattamento:

- 1) è illecito ma l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- 2) non è più necessario per il Titolare ma l'interessato sostenga che i dati gli sono necessari per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Ma la limitazione del trattamento è assoluta?

No, perché i dati, innanzitutto, continuano ad essere conservati e, inoltre, possono continuare ad essere trattati non solo, ovviamente, con il consenso dell'interessato, ma anche per:

- l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- tutelare i diritti di un'altra persona fisica o giuridica;
- rilevanti motivi di interesse pubblico dell'Unione o di uno Stato membro.

La limitazione del trattamento va comunicata all'interessato e ad eventuali soggetti cui i dati sono stati trasmessi e, in ogni caso, una volta ottenuta la limitazione, l'eventuale revoca va preventivamente comunicata all'interessato.

Il GDPR indica alcuni esempi in relazione a come attuare il diritto di limitazione: trasferimento temporaneo dei dati verso un altro sistema di trattamento, rimozione temporanea dai siti web dei dati pubblicati, apposite procedure automatizzate che impediscano ulteriori trattamenti dei dati e la loro modifica, ecc.

⁶ Cfr. l'art. 18 ed il considerando 67 del Regolamento UE.

2.7. Diritto alla portabilità dei dati

Con il nuovo diritto alla "portabilità dei dati"⁷, l'interessato ha il diritto di:

- ricevere in un formato strutturato, di uso comune e leggibile da un dispositivo, i dati personali che lo riguardano forniti a un Titolare del trattamento⁸;
- trasmettere tali dati a un altro Titolare del trattamento senza impedimenti (se tecnicamente possibile, direttamente da un Titolare all'altro).

L'esercizio di questo diritto, tuttavia, incontra alcuni limiti. Sono infatti portabili solo i dati:

- oggetto di trattamento automatizzato;
- trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato;
- che siano stati "forniti" dall'interessato al Titolare.

Per agevolare la piena attuazione di questo diritto, risulta necessario che i Titolari del trattamento sviluppino formati interoperabili dei dati personali e realizzino apposite funzionalità e strumenti come, per esempio, *tools* per il *download* dei dati.

2.8. Diritto di opposizione

Il diritto dell'interessato ad opporsi al trattamento di dati che lo riguardano⁹ è ricondotto a tre ipotesi¹⁰.

La prima riguarda il caso in cui il trattamento dei dati si basi sui seguenti presupposti¹¹:

- esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
- perseguimento del legittimo interesse del Titolare del trattamento o di terzi.

Il diritto di opposizione può essere esercitato tranne se il Titolare dimostri l'esistenza di "motivi legittimi cogenti" che prevalgono "sugli interessi, sui diritti e

⁷ Cfr. l'art. 20 ed il considerando 68 del Regolamento UE. Si vedano anche le Linee guida WP 242 sul diritto alla portabilità dei dati, elaborate dal Gruppo di lavoro "Articolo 29" per la protezione dei dati, aggiornato al 5 aprile 2017.

⁸ In questo senso, il diritto alla portabilità costituisce un'integrazione del diritto di accesso. Per esempio, un interessato potrebbe voler recuperare l'elenco dei brani musicali preferiti (o ascoltati) detenuto da un servizio di musica in *streaming*, per scoprire quante volte ha ascoltato determinati brani o stabilire cosa acquistare o ascoltare su un'altra piattaforma di musica digitale.

⁹ Cfr. l'art. 21 ed i considerando 69 e 70 del Regolamento UE.

¹⁰ Nelle prime due ipotesi è espressamente previsto che il diritto di opposizione debba essere portato all'attenzione dell'interessato al più tardi al momento della prima comunicazione, con chiarezza e separatamente da qualsiasi altra informazione.

¹¹ Cfr. l'art. 6, paragrafo 1, lettere e) ed f) del Regolamento UE.

sulle libertà dell'interessato" oppure se il trattamento sia necessario "per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria" (come abbiamo visto, nelle more di tale dimostrazione l'interessato ha il diritto di ottenere la limitazione del trattamento).

La seconda ipotesi si riferisce ai trattamenti per finalità di *marketing* diretto: l'interessato può sempre opporsi al trattamento, compresa la profilazione¹². Al riguardo deve evidenziarsi l'esplicito riferimento alla Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, che disciplina le comunicazioni commerciali e il *marketing* diretto, nel senso che sono mantenute in vigore le specifiche modalità per esercitare il diritto di opposizione stabilite nell'ambito telefonico, della posta elettronica e dei messaggi SMS. In tale contesto, inoltre, l'interessato deve poter esercitare il proprio diritto di opposizione con mezzi automatizzati.

La terza ed ultima ipotesi attiene al trattamento a fini di ricerca scientifica o storica o a fini statistici: l'interessato, per motivi connessi alla sua "situazione particolare", ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

2.9. Diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato

Si tratta del diritto¹³ che garantisce l'interessato rispetto alle eventuali decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione¹⁴, che producano effetti giuridici che lo riguardano (il Regolamento UE cita, come esempi di effetti giuridici, il rifiuto automatico di una domanda di credito *on line* o pratiche di assunzione elettronica senza interventi umani): in tali casi gli effetti giuridici non si realizzano.

Tuttavia, il diritto non può essere esercitato se la decisione:

- è necessaria per la conclusione o l'esecuzione di un contratto;
- è autorizzata dal diritto nazionale o comunitario;
- si basa sul consenso esplicito dell'interessato.

¹² Il Regolamento UE, all'art. 4, definisce la profilazione 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". Si raccomanda di soffermarsi anche sui considerando 24, 30, 71 e 72.

¹³ Cfr. l'art. 22 ed i considerando 71 e 72 del Regolamento UE. Si vedano anche le Linee guida su profilazione e processi decisionali automatizzati, elaborate dal Gruppo di lavoro "Articolo 29" per la protezione dei dati, del 23 ottobre 2017.

¹⁴ Per la nozione di profilazione si rinvia alla precedente nota 12.

Se il trattamento, invece, riguarda i c.d. dati sensibili¹⁵ - di cui all'art. 9, par. 1, del GDPR - il processo decisionale automatizzato è consentito solo in presenza del consenso esplicito dell'interessato o per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri.

In ogni caso, se la decisione automatizzata è lecita, l'art. 13, par. 2, lett. f) e l'art. 15, par. 1, lett. h) stabiliscono il diritto dell'interessato di conoscere l'esistenza del processo decisionale automatizzato e, in particolare, di ottenere informazioni significative sulla logica utilizzata e sulle conseguenze previste di tale trattamento.

Inoltre, l'interessato ha il diritto di ottenere l'intervento umano da parte del Titolare, di esprimere la propria opinione e di contestare la decisione, nei casi in cui essa sia prevista per contratto o conseguente al suo consenso.

2.10. Reclami e ricorsi giurisdizionali

Dopo aver analizzato i diritti degli interessati, possiamo all'individuazione dei mezzi di tutela esperibili nel caso in cui vengano violati tali diritti o il GDPR in generale¹⁶.

Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, sono previsti due specifici rimedi: il **reclamo** e il **ricorso giurisdizionale**. Quest'ultimo, poi, può essere presentato avverso l'autorità di controllo o nei confronti del Titolare e/o del Responsabile del trattamento.

Il reclamo. Esso va presentato all'autorità di controllo dello Stato in cui l'interessato risiede abitualmente, oppure lavora o, infine, in cui la presunta violazione ha avuto luogo.

È altresì previsto che¹⁷:

- l'autorità di controllo debba agevolare la proposizione dei reclami, tramite misure quali la predisposizione di un apposito modulo, compilabile anche elettronicamente, senza peraltro escludere altri mezzi di comunicazione;
- l'interessato non debba sopportare alcuna spesa, ma se le richieste sono manifestamente infondate o eccessive, in particolare per il carattere ripetitivo, l'autorità di controllo può addebitare un contributo spese ragionevole basato sui costi amministrativi o rifiutarsi di soddisfare la richiesta.

Il ricorso giurisdizionale. Con quello esperibile avverso l'autorità di controllo potrà essere impugnata qualsiasi sua "decisione giuridicamente vincolante". Rientrano nella casistica la decisione su un reclamo (ma anche la non trattazione di un reclamo) oppure la mancata informazione entro 3 mesi dello stato o dell'esito del relativo procedimento.

¹⁵ Per un rapido riepilogo sulle categorie di dati, si rinvia alla Figura 2 del capitolo 1.

¹⁶ Cfr. gli artt. 77 - 84 ed i considerando 141 - 150 e 152 del Regolamento UE.

¹⁷ Cfr. l'art. 54 del Regolamento UE.

Sono quindi esclusi da questo gravame gli atti dotati di carattere non vincolante come, ad esempio, i pareri e le consulenze.

Il ricorso contro il Titolare e/o il Responsabile del trattamento ha invece come oggetto la violazione – a causa o a seguito di un trattamento di dati – di un diritto dell'interessato e la giurisdizione è del giudice dello Stato membro in cui:

- il Titolare o il Responsabile ha uno stabilimento, oppure,
- l'interessato risiede abitualmente (sempre che il Titolare/Responsabile non sia un'autorità pubblica di uno Stato membro "nell'esercizio dei pubblici poteri", nel qual caso il giudice competente è quello dello Stato membro in cui ha sede l'autorità pubblica).

Per la PA

Se il Titolare/Responsabile del trattamento è un'autorità pubblica, il Giudice competente è quello dello Stato in cui ha sede l'autorità.

Il Regolamento UE disciplina anche l'istituto della **litispendenza**¹⁸ presso autorità giurisdizionali operanti in diversi Stati membri disponendo che il giudice adito successivamente possa sospendere l'azione o, su richiesta di una delle parti, dichiarare la propria incompetenza qualora la causa sia pendente in primo grado e l'autorità giudiziaria preventivamente adita sia "*competente a conoscere delle domande proposte e la sua legge consenta la riunione dei procedimenti*".

Oltre al reclamo e al ricorso giurisdizionale, è in ogni caso prevista - presso l'autorità giudiziaria dello Stato membro - l'azione del **risarcimento del danno** materiale o immateriale causato da una violazione del Regolamento UE.

Il Titolare del trattamento risponde di tali danni se non dimostra che l'evento dannoso non gli è in alcun modo imputabile mentre il Responsabile del trattamento solo se non ha adempiuto ai propri obblighi previsti dal regolamento o se ha agito in modo difforme rispetto alle istruzioni del Titolare del trattamento. In caso di concorso, il Titolare e il Responsabile sono responsabili in solido.

Particolare interesse riveste la previsione del diritto dell'interessato di dare mandato a un organismo, a un'organizzazione o a un'associazione senza scopo di lucro, debitamente costituiti secondo il diritto di uno Stato membro, i cui obiet-

¹⁸ Tuttavia, anche se l'art. 81 parla di "azioni riguardanti lo stesso oggetto", il considerando 144 utilizza il concetto di "azioni connesse" precisando che sono considerate tali "quando hanno tra loro un **legame così stretto** (sic!) da rendere opportuno trattarle e decidere in merito contestualmente, per evitare il rischio di sentenze incompatibili risultanti da azioni separate".

tivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e della libertà degli interessati in materia di protezione dei dati personali.

Al riguardo appare singolare la previsione secondo la quale tali soggetti possono proporre reclamo e presentare ricorsi giurisdizionali *"indipendentemente dal mandato ricevuto dall'interessato"*.

3. **Conoscere e decidere: l'informativa e il consenso**

3.1. L'informativa

L'informativa¹ - a cui si è fatto cenno nel precedente capitolo 2, paragrafo 2.3 - è uno dei documenti fondamentali del sistema di trattamento dei dati personali e assume una valenza determinante per il relativo **sistema di gestione**.

Essa può riguardare le informazioni da fornire all'interessato in caso di raccolta dei suoi dati personali oppure le comunicazioni all'interessato che intenda esercitare i diritti che gli sono riconosciuti in relazione al trattamento dei suoi dati.²

Questo documento è fornito dal Titolare del trattamento ed è obbligatorio per qualsiasi trattamento, tranne quando l'interessato dispone già delle informazioni oppure, nel caso in cui i dati non siano stati ottenuti direttamente dall'interessato, per:

- motivi giuridici, e cioè quando ciò sia previsto dal diritto dell'Unione o dello Stato membro unitamente a misure appropriate per tutelare gli interessi legittimi dell'interessato oppure se i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale o di segretezza previsto per legge;
- motivi organizzativi, e cioè se comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato.

Per le informative connesse all'esercizio dei diritti che sono riconosciuti all'interessato in relazione al trattamento dei dati, le relative richieste possono essere rigettate se sono manifestamente infondate o eccessive (in particolare per il loro carattere ripetitivo).

3.1.1. I contenuti

L'informativa deve specificare:

- 1) identità e i dati di contatto del Titolare del trattamento e quella dell'eventuale rappresentante nel territorio italiano;
- 2) i dati di contatto del Responsabile della protezione dei dati, ove applicabile;
- 3) le finalità del trattamento;
- 4) la base giuridica del trattamento;
- 5) nel caso in cui il trattamento si basi sul perseguimento di un legittimo interesse, quali siano i legittimi interessi perseguiti dal Titolare del trattamento o dai terzi;

¹ Cfr. gli artt. 12, 13 e 14 ed i considerando 58-62 e 64 del Regolamento UE.

² I diritti sono stabiliti negli articoli 15 – 22 del Regolamento UE. Si veda anche il capitolo 2.

- 6) i destinatari dei dati personali;
- 7) se i dati personali sono trasferiti in Paesi terzi e, in caso positivo, attraverso quali strumenti.

Inoltre, quando i dati personali sono raccolti, il Titolare del trattamento deve fornire anche le seguenti ulteriori informazioni:

- 1) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- 2) l'esistenza dei diritti riconosciuti all'interessato (diritto all'accesso ai dati personali, alla rettifica, alla cancellazione, alla limitazione del trattamento, all'opposizione al loro trattamento, alla portabilità dei dati);
- 3) il diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento avvenuto prima della revoca;
- 4) il diritto di proporre reclamo a un'autorità di controllo;
- 5) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- 6) l'esistenza o meno di un processo decisionale automatizzato, compresa la profilazione (con informazioni significative sulla logica utilizzata nonché sulle conseguenze per l'interessato).

3.1.2. I tempi

Per la tempistica dobbiamo considerare varie ipotesi.

Nel caso dell'interessato che intenda esercitare i diritti che gli sono riconosciuti in relazione al trattamento dei dati il Titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa **senza ingiustificato ritardo** e, comunque entro un mese dal ricevimento della richiesta stessa.

Se il Titolare non ottempera, entro tale termine deve alternativamente:

- prorogare il periodo entro il quale fornire le informazioni al massimo di ulteriori due mesi - se risulta necessario in relazione alla complessità e al numero delle richieste - ed informare l'interessato di tale proroga e dei motivi che l'hanno determinata;
- informare l'interessato di non voler ottemperare alla richiesta, precisandone i motivi, nonché della possibilità di proporre sia un reclamo a un'autorità di controllo che un ricorso giurisdizionale.

Nel caso di dati personali raccolti presso l'interessato l'informativa è immediata e cioè va fornita nel momento in cui i dati sono ottenuti.

Infine, se i dati personali non sono raccolti direttamente presso l'interessato, l'informativa deve essere fornita **entro un termine ragionevole che non può superare 1 mese** dalla raccolta, oppure:

- nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato;

- nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

Viene anche disciplinata l'ipotesi dell'informativa nei casi di ulteriore trattamento dei dati per finalità diverse da quelle per cui sono stati già ottenuti: in questo caso il Titolare deve fornire l'informativa prima di tale ulteriore trattamento.

3.1.3. *La forma*

L'informativa deve:

- essere concisa, trasparente, intelligibile per l'interessato e facilmente accessibile;
- avere un linguaggio chiaro e semplice;
- per i minori, prevedere modalità specifiche;
- essere fornita per iscritto, in formato elettronico³ o con altri mezzi; se richiesto dall'interessato, le informazioni possono essergli fornite oralmente, previo accertamento dell'identità.

In relazione agli "altri mezzi" è ammesso l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa. Queste icone saranno identiche in tutta l'Ue e saranno definite dalla Commissione europea su proposta del Comitato europeo per la protezione dei dati⁴.

Di seguito si riportano le icone allegate alla bozza di Regolamento UE, poi espunte dal testo all'atto della sua definitiva approvazione.

³ L'informativa è fornita, se possibile, con mezzi elettronici quando l'interessato presenta la richiesta in tale modo, salvo diversa indicazione di quest'ultimo (art. 12, paragrafo 3, del Regolamento UE).

⁴ Cfr. art. 70, lett. r), del Regolamento UE.

Figura 15 – Esempio di icone utilizzabili nell’informativa

ICONA	INFORMAZIONI ESSENZIALI	SI/NO
	La raccolta di dati personali è limitata al minimo necessario per ogni specifica finalità del trattamento	
	La memorizzazione di dati personali è limitata al minimo necessario per ogni specifica finalità del trattamento	
	Il trattamento di dati personali è limitato alle finalità per le quali sono stati raccolti	
	Non sono forniti dati personali a terze parti commerciali	
	Non sono effettuati la vendita o l' affitto di dati personali	
	I dati personali non sono memorizzati in forma non cifrata	

3.1.4. I costi

Circa i costi, è stabilito che, in generale, le informative sono gratuite. Per le informative connesse all’esercizio dei diritti connessi al trattamento dei dati, qualora le richieste dell’interessato siano ritenute manifestamente infondate o eccessive (in particolare per il loro carattere ripetitivo) dal Titolare del trattamento, questi, se non dovesse ritenere di rigettare la richiesta, può addebitare un contributo spese tenendo conto dei costi amministrativi sostenuti.

3.2. Il consenso

Talvolta, essere informato sul trattamento dei propri dati personali non è sufficiente ma occorre anche esprimere il proprio consenso.

Il consenso dell’interessato – che abbiamo già incontrato nel paragrafo 1.4, tra le condizioni riconducibili al principio di liceità del trattamento - è “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”⁵.

Come abbiamo già visto il consenso espresso è previsto per i dati “sensibili” e in relazione alle decisioni basate su trattamenti automatizzati (compresa la profilazione)⁶.

⁵ Cfr. nota 27. Per un approfondimento si rinvia al capitolo 1, paragrafo 1.4.

⁶ Cfr. gli artt. 9 e 22 del Regolamento UE.

Va peraltro evidenziato che, per l'art. 7 del GDPR, è il Titolare del trattamento che deve provare la prestazione del consenso da parte dell'interessato e di averlo richiesto rispettando determinati canoni: appare, dunque, opportuna la forma scritta *ad probationem*.

Ogni consenso fa riferimento ad uno specifico trattamento e, comunque, l'interessato ha il diritto di revocarlo e di essere informato, se esercita questo diritto, dal Titolare del trattamento, ferma restando la validità di tutti i trattamenti compiuti prima della revoca.

3.3. Segue: l'esempio dei cookies

Un esempio significativo delle novità introdotte dal Regolamento europeo con riferimento al consenso è quello che riguarda i *cookies*.

Ma cosa sono esattamente i *cookies*? Si tratta di stringhe di testo di piccole dimensioni che i siti visitati dall'utente inviano al suo terminale (solitamente al browser), dove vengono memorizzati per essere poi ritrasmessi agli stessi siti alla successiva visita del medesimo utente.

Le funzioni principali di un cookie sono:

- permettere di effettuare il *login* su un sito *web* (registrando *username* e *password*, senza che ci vengano chiesti a ogni accesso);
- personalizzare la pagina sulla base delle preferenze dell'utente (un motore di ricerca, per esempio, permette di decidere quanti risultati visualizzare per pagina, una volta avviata la ricerca);
- seguire i percorsi dell'utente: si tratta della funzione più importante per le compagnie pubblicitarie, che riescono così a ottenere informazioni e a usarle per presentargli, sui siti che visita o via mail, solo i banner pubblicitari che potrebbero interessarlo;
- consentire di condividere le informazioni sui *social network* con altri utenti (ad esempio, il "mi piace" di Facebook).

I *cookies* si distinguono per durata, finalità e provenienza.

La durata dei *cookies* può essere di sessione o persistente. Il primo tipo di cookie viene automaticamente cancellato dopo la chiusura del *browser*, mentre il secondo tipo permane sul dispositivo dell'utente fino ad una scadenza prestabilita. In relazione alle finalità distinguiamo i *cookies* tecnici ed i *cookies* di profilazione. I *cookies* tecnici sono quelli necessari al funzionamento del sito ed alla erogazione dei servizi; questi vengono utilizzati al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica.

I ***cookies* di profilazione**, invece, sono volti a creare profili relativi all'utente e vengono spesso utilizzati al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dallo stesso nell'ambito della navigazione in rete.

Alcuni esempi di *cookies* di profilazione sono:

- i *cookies* di profilazione pubblicitaria, utilizzati per proporre pubblicità basata sugli interessi che gli utenti manifestano durante la navigazione;

- i *cookies* di *retargeting*, utilizzati per proporre pubblicità agli utenti che hanno visitato il sito in precedenza;
- i *cookies* di *social network*, utilizzati per la condivisione di contenuti sui *social network*;
- i *cookies* di statistica, utilizzati per la gestione delle statistiche di navigazione.

Questi tipi di *cookies* possono essere di *prime parti* (quando è installato dal gestore del sito che l'utente sta visitando) e di *terze parti* (quando viene inviato da un sito diverso da quello che viene visualizzato dall'utente).

In precedenza⁷, i gestori dei siti avevano l'obbligo di mostrare al primo accesso di un utente, con un *banner*, informazioni sui *cookies* e per i *cookies* di profilazione si doveva avvisare l'utente che sarebbe stato profilato per ragioni pubblicitarie (c'era la possibilità di negare il consenso, ma così facendo spesso non veniva consentito di visitare il sito).

Con l'entrata in vigore del Regolamento europeo, invece:

- serve un consenso esplicito dell'utente;
- il gestore del portale deve descrivere precisamente l'uso che farà dei *cookies*;
- deve esserci la possibilità di revocare il consenso in modo semplice.

A titolo esemplificativo, la Tavola 4 riporta uno stralcio dell'*Informativa e richiesta di consenso per il trattamento dei dati personali – Cookie Policy* di un gruppo editoriale che opera anche *online*.

Tavola 4 – Cookie Policy

Tipologia dei dati trattati
<p>Il sito web offre contenuti di tipo informativo e, talvolta, interattivo. Durante la navigazione del sito xxx potrà, quindi, acquisire informazioni sul visitatore. nei seguenti modi:</p> <p>Dati di navigazione: i sistemi informatici e le procedure software preposte al funzionamento di questo sito web acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet. In questa categoria di dati rientrano: gli indirizzi IP, il tipo di browser utilizzato, il sistema operativo, il nome di dominio e gli indirizzi di siti web dai quali è stato effettuato l'accesso, le informazioni sulle pagine visitate dagli utenti all'interno del sito, l'orario d'accesso, la permanenza sulla singola pagina, l'analisi di percorso interno ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente.</p> <p>Ulteriori categorie di dati: si tratta di tutti quei dati personali forniti dal visitatore attraverso il sito, ad esempio, registrandosi e/o accedendo ad una area riservata e/o ad un servizio e/o partecipando a una delle iniziative lanciate da XXX S.r.l. da sola o in partnership con soggetti terzi, scrivendo ad un indirizzo di posta elettronica di XXX S.r.l. per richiedere informazioni</p>

⁷ Cfr. le Direttive Comunitarie 2002/58/CE e 2009/136/UE relative al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, che avevano introdotto alcune precisazioni specifiche rispetto alla Direttiva 95/46 (ora abrogata) con riferimento alla raccolta di dati personali effettuata on line e in particolare all'uso dei *cookies*.

oppure telefonando ad un nostro numero verde per avere un contatto diretto con il servizio clienti.	
Finalità del trattamento	
Finalità	Base giuridica
Fornire il bene e/o il servizio richiesto dall'utente, gestire i contratti perfezionati dall'utente, espletare i relativi adempimenti amministrativi, contabili, fiscali e legali, nonché evadere le richieste inoltrate dall'utente.	I trattamenti posti in essere per queste finalità sono necessari per l'adempimento di obblighi contrattuali e non necessitano di uno specifico consenso da parte dell'interessato.
Rilevare la sua esperienza d'uso delle nostre piattaforme, dei prodotti e servizi che offriamo e assicurare il corretto funzionamento delle pagine web e dei loro contenuti.	I trattamenti posti in essere per queste finalità si basano su un legittimo interesse del Titolare.
Inviarle comunicazioni commerciali relative a promozioni e/o offerte per le quali potrebbe aver diritto a beneficiare, nell'interesse del Titolare o delle altre società del Gruppo XXX.	I trattamenti posti in essere per queste finalità vengono effettuati con lo specifico consenso fornito dall'utente, fatta eccezione per le comunicazioni commerciali relative a prodotti e/o servizi analoghi a quelli già acquistati e/o sottoscritti dall'utente per le quali il trattamento si basa su un legittimo interesse del Titolare.
Svolgere attività di profilazione ossia di analisi e elaborazione di informazioni relative all'utente, alle sue preferenze, abitudini, scelte di consumo e/o esperienze di navigazione. Tale attività viene effettuata anche mediante l'utilizzo di tecnologie quali i cookie (per maggiori informazioni si rimanda al paragrafo 14 della presente Informativa "Cookie Policy").	I trattamenti posti in essere per queste finalità vengono effettuati con lo specifico consenso fornito dall'utente, fatta eccezione per un'attività di analisi di informazioni elementari relative alle sue preferenze di consumo.

Parte II

LA DIMENSIONE ORGANIZZATIVA

*I fantastici progressi nel campo della comunicazione elettronica
costituiscono il peggiore pericolo per la privacy dell'individuo.
Earl Warren (1871 – 1974).
Politico statunitense.*

*Sono andato ad un corso sulla privacy e hanno preso le firme. Potevano
farlo?
Il Titolare di un trattamento
di dati personali.*

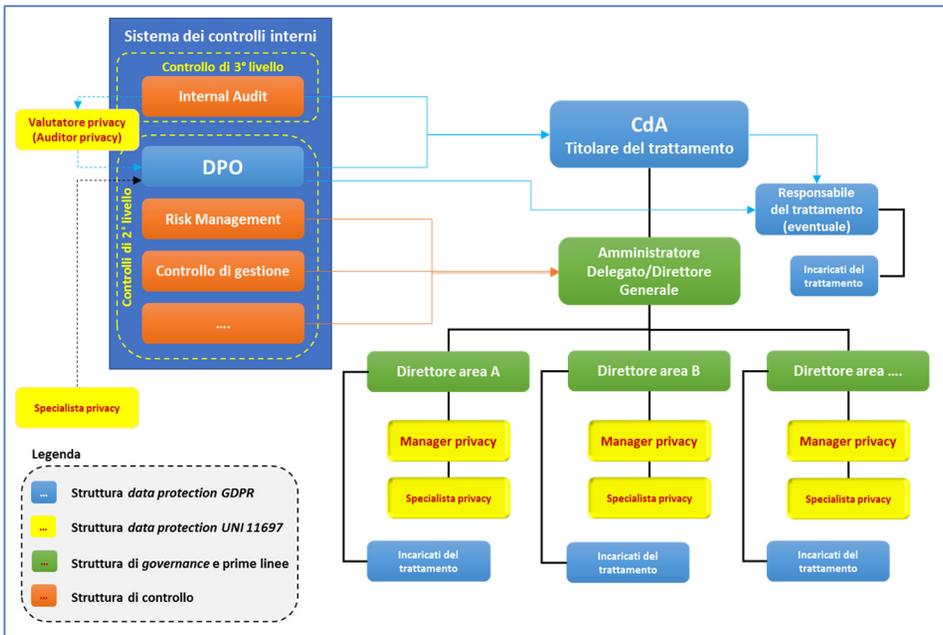
*Se è riservato verrà dimenticato nella fotocopiatrice.
Un Data Protection Officer*

4. I soggetti e i ruoli

4.1. La distribuzione delle competenze e delle responsabilità. Un'ipotesi di organigramma

Come in tutti i modelli organizzativi, anche in quello riferito al *data protection* risulta indispensabile una chiara ripartizione delle competenze e delle responsabilità dei soggetti coinvolti¹.

Figura 16 – Esempio di organigramma “data protection”



Come può rilevarsi dalla Figura 16, armonizzare l'organizzazione dedicata al *data protection*, con quella aziendale generale, appare piuttosto complesso.

Proviamo a fornire una visione d'insieme, rimandando ai paragrafi successivi l'analisi di dettaglio dei vari aspetti.

L'organizzazione di *data protection* è costituita innanzitutto dai ruoli previsti dal Regolamento UE: Titolare del trattamento (*Data controller*), Responsabile del trattamento (*Data processor*), Responsabile della protezione dei dati (*Data Protection Officer – DPO*) e Incaricati del trattamento.

¹ Fra i numerosi riferimenti a questo concetto, si veda il considerando 79 del Regolamento UE.

Ad essi si aggiungono i profili professionali indicati dalla norma nazionale UNI 11697 del novembre 2017, che oltre al già citato DPO, introduce le figure del “manager privacy”, dello “specialista privacy” e del “valutatore privacy”.

In sostanza il Titolare, supportato dal DPO, opera attraverso il Responsabile del trattamento (se nominato) e gli Incaricati. Nel contempo può avvalersi del *manager privacy* – con riferimento a specifici contesti organizzativi dell’azienda, particolarmente complessi – e dello *specialista privacy* per l’implementazione delle misure tecniche ed organizzative da adottare e gestire.

Un’esigenza rilevante è quella di verificare se “il sistema privacy” è adeguato e, al riguardo, la UNI 11697 prevede la figura del valutatore privacy (la logica sottesa richiama il sistema delineato dal D.Lgs. n. 231/2001, in cui ad un soggetto – l’organismo di vigilanza – è attribuito il compito di valutare se il modello organizzativo è adeguato e se viene correttamente attuato).

In termini di funzioni e competenze, secondo l’ipotesi formulata nella Figura 16, la responsabilità della verifica “indipendente” sul funzionamento del sistema ricade sul DPO.

Quest’ultimo, per esercitare tale attività, normalmente si avvale del valutatore privacy che sostanzialmente è un *auditor* esperto in materia di *data protection*.

Il valutatore *privacy* dovrebbe essere incardinato nella struttura aziendale di *internal audit*, il cui responsabile lo mette a disposizione, di volta in volta, del DPO. È chiaro che in assenza di una struttura di *internal audit*, o della specifica competenza richiesta, tale figura deve essere presa dall’esterno.

Uno dei problemi più diffusi delle organizzazioni è quello delle ridondanze e delle sovrapposizioni delle funzioni organizzative.

Con riferimento all’ambito dei controlli interni, rifacendoci alla concezione ormai tradizionale, possiamo prevedere un perimetro in cui agisce l’*internal audit* come controllo di terzo livello, in quanto rivolto a valutare l’adeguatezza del sistema di controllo interno aziendale nella sua interezza.

Il sistema di *data protection*, in quanto controllo specialistico, rientra nei controlli di secondo livello (insieme, ad esempio, al *risk management* e al controllo di gestione) ma, diversamente da questi, riporta direttamente al vertice, analogamente all’*internal audit*.

In sostanza, quest’ultima funzione, svolge nei confronti del sistema “*data protection*” la verifica della sua adeguatezza secondo due modalità: o direttamente, attraverso la sua tipica funzione di *assurance*² svolta nei confronti del Sistema di

² Secondo il glossario degli standard IIA, i servizi di *assurance* “consistono in un esame obiettivo delle evidenze allo scopo di ottenere una valutazione indipendente dei processi di *governance*, di gestione del rischio e di controllo dell’organizzazione. Tra gli esempi si possono citare incarichi di tipo finanziario, di tipo operativo, di conformità, di sicurezza informatica e di *due diligence*”. Lo standard, inoltre, precisa che “i servizi di *assurance* comportano un’obiettiva valutazione delle evidenze da parte degli *internal auditor* finalizzata alla formulazione di giudizi o conclusioni riferiti a un’organizzazione, attività, funzione, processo, sistema o altro. L’*internal auditor* definisce la natura e

Controllo Interno (e quindi anche dei controlli di secondo livello) o indirettamente, fornendo al DPO le risorse necessarie (*auditor* esperti in *data protection*) per effettuare verifiche autonome.

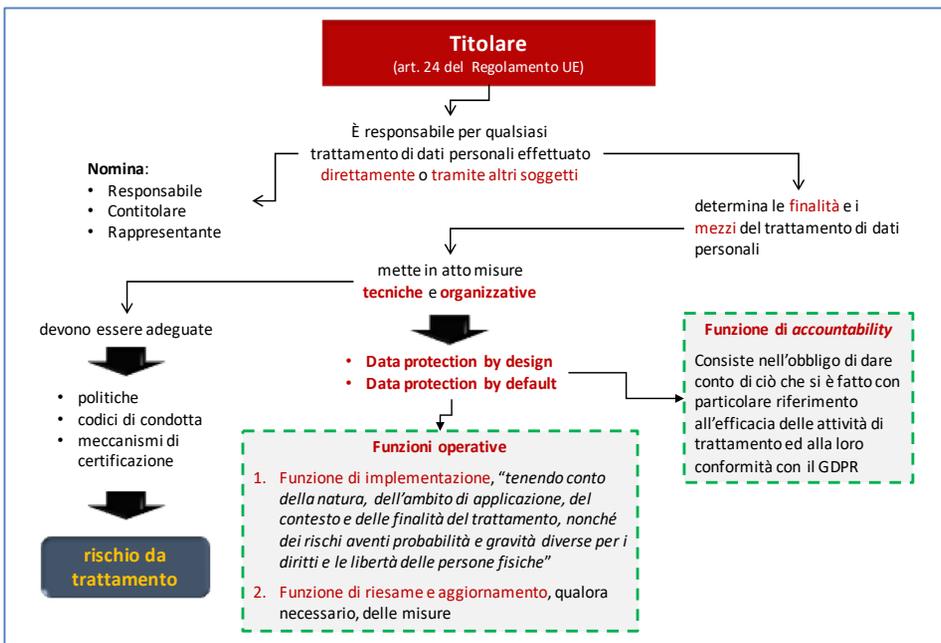
Per concludere, mi pare che sia emerso un dato incontrovertibile: il sistema GDPR richiede capacità professionali sempre più trasversali.

Un effetto di ciò è che la protezione dei dati è destinata a trasformarsi in una materia in cui gli avvocati saranno un po' meno protagonisti – continueranno ad occuparsi, ad esempio, della stesura di contratti che regolamentano i rapporti fra clienti e fornitori anche in materia di trattamento dati personali – a beneficio di esperti di *audit* e *risk management*, analisti di organizzazione, di specialisti in sicurezza delle informazioni, ecc.

4.2. Il Titolare del trattamento

Il Titolare del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

Figura 17 – Il Titolare del trattamento



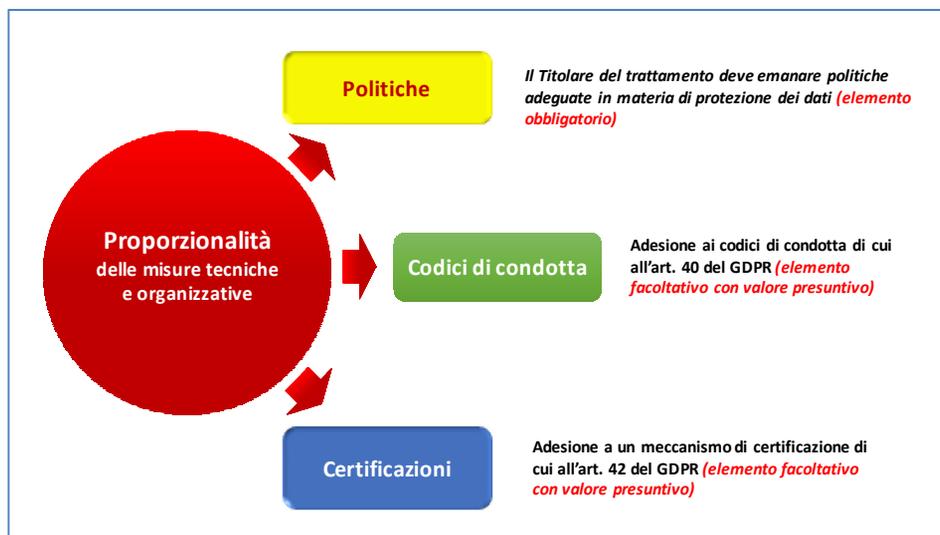
l'ampiezza dell'incarico di *assurance*. Tre sono le parti generalmente coinvolte nei servizi di *assurance*: (1) il *process owner*, cioè la persona o il gruppo direttamente coinvolti nell'organizzazione, attività, funzione, processo, sistema o altro, (2) l'*internal auditor*, cioè la persona o il gruppo che effettua la valutazione e (3) l'utente, cioè la persona o il gruppo che utilizzerà tale valutazione".

A questo soggetto è quindi attribuita la responsabilità generale per qualsiasi trattamento di dati personali effettuato direttamente o tramite altri soggetti. Egli svolge tre funzioni fondamentali – in cui si fondono esigenze operative e di *accountability* - in relazione alle misure tecniche e organizzative necessarie per adeguare il trattamento dei dati al GDPR³:

- funzione implementativa, “tenendo conto della natura, dell’ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche”;
- funzione di riesame e aggiornamento, qualora necessario, delle misure tecniche ed organizzative;
- funzione di *accountability*, sancita dall’obbligo di dare conto di ciò che si è fatto con particolare riferimento all’efficacia delle attività di trattamento ed alla loro conformità con il GDPR.

L’elemento di riferimento, comune a tali funzioni, è quello della *proporzionalità* delle misure tecniche e organizzative che, per la sua valutazione, deve tenere presente i tre elementi – politiche, codici di condotta e meccanismi di certificazione⁴ - riportati nella Figura 18.

Figura 18 – Proporzionalità delle misure tecniche ed organizzative



Tuttavia, deve evidenziarsi che il primo elemento fattuale da prendere in considerazione per analizzare il concetto di proporzionalità delle misure tecniche e

³ Cfr. l'art. 4, n. 7) e l'art. 24 ed i considerando 74-78 del Regolamento UE.

⁴ Per i codici di condotta e le certificazioni si rinvia ai paragrafi 1.6.1 e 1.6.2.

organizzative è quello che potremmo definire come il "*rischio da trattamento di dati personali*", per il cui approfondimento si rinvia al capitolo 5, paragrafo 5.1.

Un altro compito fondamentale del Titolare è quello della nomina del Responsabile del trattamento, a cui è dedicato il paragrafo successivo, attraverso un contratto che disciplini i reciproci rapporti conformemente a quanto previsto, in particolare, dall'art. 28, paragrafo 3, del GDPR.

Il GDPR contempla anche il caso in cui vi siano dei contitolari del trattamento⁵, che si verifica quando due o più Titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento. In questa ipotesi, per la parte che non sia fissata dal diritto dell'Unione o dello Stato membro cui i Titolari del trattamento sono soggetti, è previsto un *accordo interno* – il cui contenuto essenziale deve essere messo a disposizione dell'interessato – che stabilisca le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR con particolare riguardo:

- all'esercizio dei diritti dell'interessato;
- alle comunicazioni delle informazioni da fornire all'interessato.
- ad un eventuale punto di contatto per gli interessati.

L'accordo, dunque, è un elemento fondamentale nell'ambito del rapporto interno tra i vari Titolari anche ai fini delle conseguenze derivanti da eventuali danni che, tuttavia, non vincola l'interessato che rimane libero di rivolgersi, indipendentemente dall'accordo, a qualsiasi contitolare, salva l'eventuale azione di rivalsa di quest'ultimo nei confronti degli altri contitolari.

Un'ultima previsione è quella del Rappresentante⁶ e cioè della persona fisica o giuridica stabilita nell'Unione che è designata per iscritto dal Titolare del trattamento (e come vedremo anche dal Responsabile del trattamento) quando questi non è stabilito, a differenza degli interessati, nell'Unione, allorché le attività di trattamento riguardino:

- l'offerta di beni o la prestazione di servizi, anche gratuiti;
- il monitoraggio del comportamento degli interessati.

L'obbligo di nomina del rappresentante non opera se il trattamento:

- è occasionale;
- non include dati sensibili e giudiziari;
- è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche;
- è svolto da autorità e organismi pubblici.

⁵ Cfr. l'art. 26 ed il considerando 79 del Regolamento UE.

⁶ Cfr. l'art. 4, n. 17, l'art. 27 ed il considerando 80 del Regolamento UE.

Per la PA

Non è previsto l'obbligo della nomina del rappresentante del Titolare del trattamento.

Il rappresentante, in ogni caso, funge da interlocutore delle autorità di controllo e degli interessati, per tutte le questioni riguardanti il trattamento, ferma restando la responsabilità generale del Titolare del trattamento e la possibilità di proporre comunque azioni legali contro quest'ultimo.

4.3. Il Responsabile del trattamento

Come abbiamo in precedenza accennato, il Titolare del trattamento nomina il Responsabile del trattamento che è definito come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento"⁷.

La Tavola 5 riassume le prescrizioni contenute nel GDPR⁸.

Tavola 5 - Il Responsabile del trattamento

N.	Prescrizione	Descrizione
1	Competenza	La scelta del Responsabile del trattamento richiede idonee garanzie sulla capacità di mettere in atto misure tecniche e organizzative adeguate che possono essere dimostrate: <ul style="list-style-type: none">• dall'adesione a un codice di condotta approvato ex art. 40;• da un meccanismo di certificazione ex art. 42. Tali garanzie devono riguardare, in particolare, <i>la conoscenza specialistica, l'affidabilità e le risorse</i> .
2	Atto di nomina	Contratto o altro atto giuridico scritto (anche in formato elettronico) individuale o basato su clausole contrattuali tipo stabilite dalla Commissione o dell'autorità Garante nazionale. Per un inquadramento generale si rinvia alla Figura 19.
3	Sub Responsabile	Il Responsabile del trattamento può ricorrere a un altro Responsabile, in possesso delle medesime garanzie di competenza, per specifiche attività di trattamento solo previa autorizzazione scritta del Titolare del trattamento. L'ulteriore Responsabile è incaricato con le stesse modalità e contenuti del Responsabile iniziale che, peraltro, conserva, nei confronti del Titolare del trattamento, l'intera responsabilità per le attività dell'altro Responsabile.

⁷ Cfr. l'art. 4, n. 8 del Regolamento UE.

⁸ Cfr. l'art. 28 ed il considerando 81 del Regolamento UE.

N.	Prescrizione	Descrizione
4	Inottemperanze	Il Responsabile del trattamento: <ul style="list-style-type: none"> • se determina le finalità e i mezzi del trattamento viene considerato Titolare del trattamento; • è tenuto al risarcimento del danno causato se non ha adempiuto agli obblighi del GDPR o ha agito in modo difforme o contrario rispetto alle istruzioni del Titolare del trattamento; • risponde al Titolare dell'inadempimento dell'eventuale Sub-Responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento; • è esente da responsabilità se dimostra che "l'evento dannoso non gli è in alcun modo imputabile".

Una questione di rilievo riguarda se il Responsabile deve provenire dall'interno dell'organizzazione o dall'esterno.

La risposta non è univoca.

In assenza di una specifica indicazione, si ritiene di dover accogliere l'interpretazione che consente la duplice provenienza del Responsabile nel rispetto delle prescrizioni indicate dal GDPR⁹.

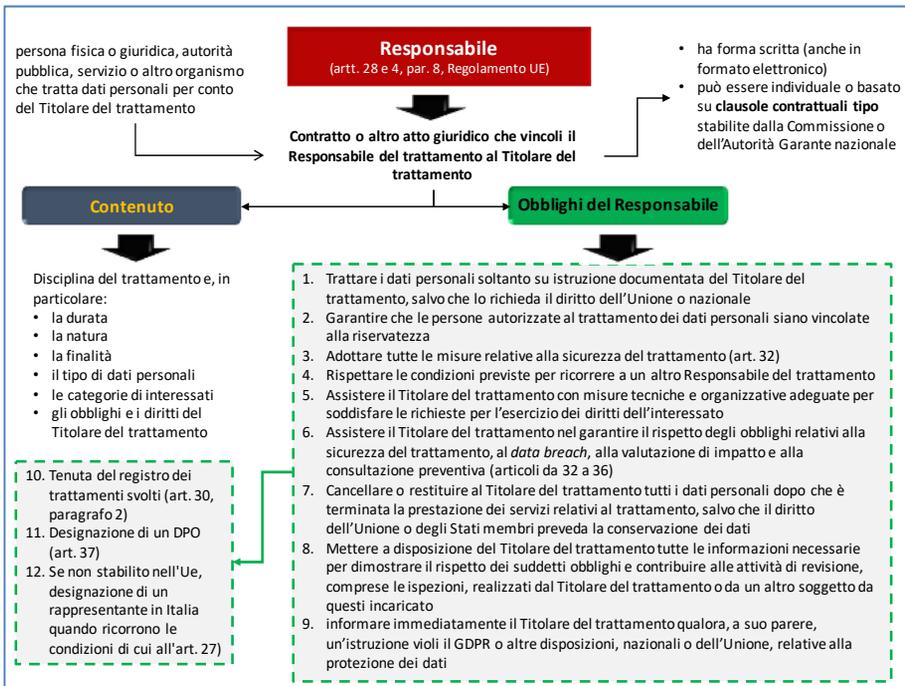
È comunque evidente che in caso di esternalizzazione dei trattamenti la società esterna opera quale Responsabile¹⁰.

La Figura 19 schematizza un inquadramento generale sulla nomina del Responsabile del trattamento e, in particolare, sulla formalizzazione dell'atto di nomina, sul contenuto riferito sia al trattamento dei dati che agli obblighi a cui tale figura è soggetta.

⁹ Nel senso favorevole all'ipotesi della nomina di Responsabili provenienti dall'interno dell'organizzazione, si veda la pubblicazione "L'attuazione negli enti locali del nuovo Regolamento UE n. 679/2016 sulla protezione dei dati personali – Istruzioni tecniche, linee guida, note e modulistica", edita nel gennaio 2018, nella serie "I quaderni" dell'ANCI (Associazione Nazionale dei Comuni Italiani).

¹⁰ Nella prassi ci sono moltissime situazioni di Responsabili esterni (i cui rapporti con i Titolari devono adesso essere regolati in maniera precisa) e numerosi casi – che riguardano piccolissime imprese o professionisti – in cui i Titolari non si sono avvalsi della possibilità di affidare il trattamento ad un Responsabile.

Figura 19 – Nomina del Responsabile del trattamento



4.4. L'Incaricato del trattamento

Il GDPR non prevede espressamente la figura dell'*Incaricato del trattamento* ma fa riferimento a "persone autorizzate al trattamento dei dati personali" (art. 28, paragrafo 3, lett. b) e a "chiunque" agisca sotto l'autorità del Titolare o del Responsabile del trattamento (art. 29)¹¹.

In sostanza, quindi, continua ad essere contemplato l'Incaricato che deve essere:

- autorizzato a trattare i dati personali dal Titolare o dal Responsabile del trattamento, attraverso un atto formale;
- istruito dal Titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri¹²;
- vincolato alla riservatezza o ne sia obbligato in virtù di un obbligo legale (questo requisito, se l'Incaricato è autorizzato dal Responsabile, deve essere garantito da quest'ultimo nei confronti del Titolare del trattamento attraverso specifica menzione nel contratto - o altro atto giuridico scritto - di nomina).

¹¹ Si noti che l'art. 4, n. 10, nel definire - per esclusione - il "terzo", cita tra coloro che non rientrano in tale nozione "le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile".

¹² Si veda anche l'art. 32, paragrafo 4, del Regolamento UE.

4.5. Il Responsabile della protezione dei dati (Il Data Protection Officer)

4.5.1. Obbligatorietà e facoltatività della nomina del DPO

Il GDPR introduce, nella platea degli attori "tradizionali" – costituita dal "Titolare", dal "Responsabile" e dall'"Incaricato" - la figura del Responsabile della protezione dei dati¹³, ormai noto con l'acronimo DPO (*Data Protection Officer*).

Si tratta di un nuovo ruolo che è facoltativo ad eccezione dei seguenti casi, in cui invece è obbligatorio, raggruppabili secondo:

- 1) *un criterio soggettivo*, e cioè quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico¹⁴, eccettuata l'autorità giudiziaria nell'esercizio delle proprie funzioni giurisdizionali;
- 2) *un criterio oggettivo*, e cioè quando le attività principali del Titolare o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono *il monitoraggio regolare e sistematico su larga scala*¹⁵:
 - degli interessati;
 - di categorie particolari di dati personali sensibili o giudiziari;
- 3) *un criterio legale*, e cioè quando la nomina è obbligatoria in base alla normativa comunitaria o nazionale.

È opportuno ricordare che la mancata nomina del DPO, quando obbligatoria, è soggetta alla sanzione amministrativa pecuniaria fino a 10 milioni di euro, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore)¹⁶.

Il DPO è nominato dal Titolare o dal Responsabile del trattamento e può essere un dipendente oppure un soggetto esterno all'organizzazione, assunto in base a un contratto di servizi, i cui dati di contatto sono pubblicati e comunicati all'autorità Garante nazionale.

¹³ Cfr. gli artt. 37, 38 e 39 ed il considerando 97 del Regolamento UE.

¹⁴ La nozione di "autorità pubblica e organismo pubblico" non è univocamente definita. Al riguardo potrebbe farsi riferimento al concetto di Amministrazione Pubblica, definito dall'art. 1, comma 2, del D.Lgs. 30 marzo 2001, n. 165, oppure all'elenco delle amministrazioni pubbliche inserite nel conto economico consolidato, individuate dall'ISTAT ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196.

¹⁵ Il GDPR non fornisce le definizioni di "monitoraggio regolare e sistematico" e di "larga scala" che invece sono chiarite dalle linee guida n. 243 del Gruppo "articolo 29". In sintesi, il primo concetto fa riferimento a trattamenti che avvengono in modo continuo ovvero a intervalli definiti per un arco di tempo prestabilito e che hanno luogo nell'ambito di progetti complessivi di raccolta di dati; il secondo concetto è invece riconducibile al numero di soggetti interessati dal trattamento (in termini assoluti ovvero in percentuale), al volume dei dati, alla persistenza e alla portata geografica dell'attività di trattamento.

¹⁶ Cfr. l'art. 83, paragrafo 4, del Regolamento UE.

Particolare attenzione va posta nel caso di nomina di un dipendente, in quanto il ruolo che ricopre nell'organizzazione deve escludere ogni forma di conflitto di interesse ed essere compatibile con l'esercizio autonomo ed indipendente delle sue funzioni.

Per la PA

La nomina del DPO è obbligatoria (tranne che nell'esercizio di funzioni giurisdizionali). È consigliata la nomina di un dirigente o un funzionario di elevata professionalità, la previsione di specifici "referenti" del DPO in relazione alla complessità dei trattamenti e dell'organizzazione mentre si sconsiglia la nomina del RPCT (perché già gravato da onerosi impegni) e di figure in potenziale conflitto d'interesse (es. Responsabile IT).

Può essere nominato un unico DPO nel caso di un gruppo imprenditoriale (a condizione che sia facilmente raggiungibile da ciascun stabilimento) o di più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

4.5.2. *Compiti e requisiti professionali*

Il DPO deve possedere, in particolare, una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati nonché la capacità di svolgere i compiti di cui all'art. 39, riassunti nella Tavola 6.

Tavola 6 – Compiti del DPO

N.	Descrizione
1	Informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che trattano i dati personali.
2	Sorvegliare l'osservanza della normativa comunitaria e nazionale nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento riguardanti anche "l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo".
3	Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento.
4	Cooperare con l'autorità Garante nazionale.
5	Fungere da punto di contatto per l'autorità Garante nazionale 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.

In relazione ai compiti va peraltro precisato che l'elenco di cui all'art. 39 costituisce una base minimale in quanto rappresenta quelli che il DPO deve svolgere "comunque", con ciò presupponendo la possibilità, per il Titolare o il Responsabile del trattamento, di aggiungerne altri.

Anche interessante risulta la precisazione, contenuta nel medesimo articolo, che il DPO, nello svolgimento dei propri compiti, non deve perdere mai di vista il "rischio da trattamento", tenendo conto dei seguenti parametri del trattamento stesso:

- natura;
- ambito di applicazione;
- contesto;
- finalità.

Dall'esame dei compiti emerge la necessità che il DPO abbia adeguate competenze sia manageriali che in ambito giuridico, informatico nonché nei settori del *risk management* e dell'analisi processuale.

La norma UNI 11697:2017 stabilisce nel dettaglio le competenze e le conoscenze del DPO, riportate nella Tavola 7.

Tavola 7 – Competenze e conoscenze del DPO

Competenze
<ul style="list-style-type: none"> • Pianificazione di Prodotto o di Servizio • Sviluppo della Strategia per la Sicurezza Informatica • Gestione del Contratto • Sviluppo del Personale • Gestione del Rischio • Gestione delle Relazioni • Gestione della Sicurezza dell'Informazione • Governance dei sistemi informativi
Conoscenze
<ul style="list-style-type: none"> • I principi di privacy e protezione dei dati by design e by default • I diritti degli interessati previsti da leggi e regolamenti vigenti • Le responsabilità connesse al trattamento dei dati personali • Norme di legge italiane ed europee in materia di trattamento e di protezione dei dati personali • Norme di legge in materia di trasferimento di dati personali all'estero e circolazione dei dati personali extra UE/SEE • Le metodologie di valutazione d'impatto sulla protezione dei dati e PIA • Le possibili minacce alla protezione dei dati personali • Le norme tecniche ISO/IEC per la gestione dei dati personali • I codici di condotta e le certificazioni applicabili in materia di trattamento e protezione dei dati personali • Tecniche e strumenti di comunicazione (relazione con Istituzioni, autorità, Forze dell'ordine, enti locali e stampa) • Le tecniche crittografiche

- Le tecniche di anonimizzazione
- Le tecniche di pseudonimizzazione
- I sistemi e le tecniche di monitoraggio e "reporting"
- Gli strumenti di controllo della versione per la produzione di documentazione
- I metodi di sviluppo delle competenze
- I processi dell'organizzazione ivi inclusi le strutture decisionali, di budget e di gestione.
- I rischi critici per la gestione della sicurezza
- I tipici KPI (*key performance indicators*)
- Il potenziale e le opportunità offerte dagli standard e dalle best practices più rilevanti
- Il ritorno dell'investimento comparato all'annullamento del rischio
- L'impatto dei requisiti legali sulla sicurezza dell'informazione
- La *computer forensics* (analisi criminologica di sistemi informativi)
- La politica di gestione della sicurezza nelle aziende e delle sue implicazioni con gli impegni verso i clienti, i fornitori e i sub-contraenti
- La strategia dell'informazione nell'organizzazione
- Le *best practice* (metodologie) e gli standard nella analisi del rischio
- Le *best practice* e gli standard nella gestione della sicurezza delle informazioni
- Le metodologie di analisi dei fabbisogni di competenze e *skill*
- Le norme legali applicabili ai contratti
- Le nuove tecnologie emergenti (per esempio sistemi distribuiti, modelli di virtualizzazione, sistemi di mobilità, *data sets*)
- Le possibili minacce alla sicurezza
- Le problematiche legate alla dimensione dei data sets (per esempio *big data*)
- Le problematiche relative ai dati non strutturati (per esempio *data analytics*)
- Le tecniche di attacco informatico e le contromisure per evitarli

Come si può vedere, nell'enumerare i requisiti del DPO, la norma nazionale appare un tantino sovrabbondante!

Per dare maggiore tranquillità a chi deve scegliere il DPO, possiamo riportare quanto indicato nelle specifiche FAQ del sito dell'autorità Garante nazionale:

"[Il DPO] deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento. Deve 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".

In effetti si tratta di una descrizione decisamente meno "ansio-gena"!

In pratica sono sicuramente più importanti competenze di base consolidate negli ambiti legale, informatico e gestionale ma non necessariamente particolarmente approfondite, piuttosto che essere esperti di una materia e non conosce-

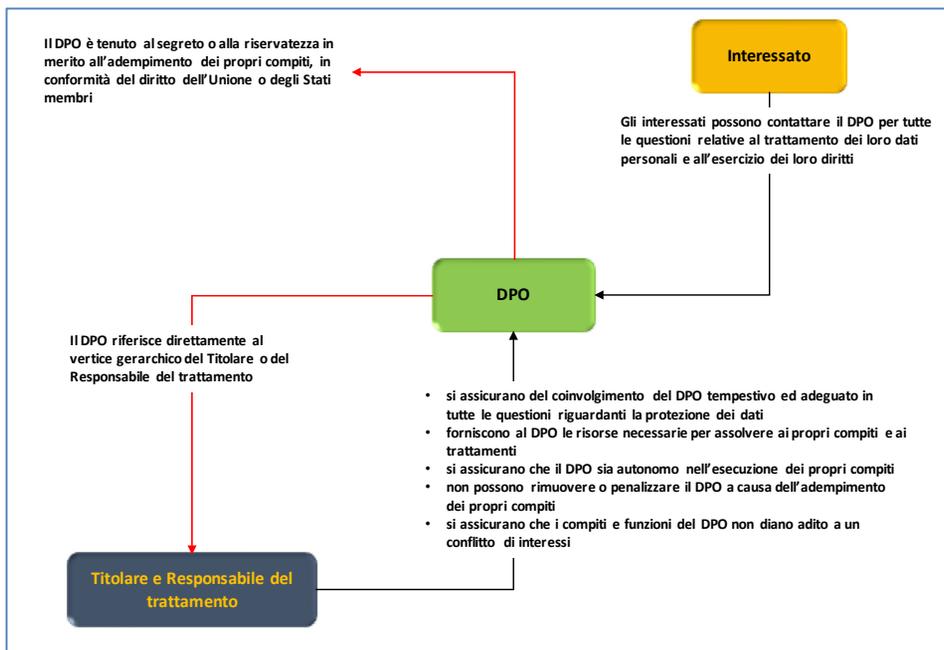
re nulla delle altre, tanto più che il DPO potrà essere supportato da un team di specialisti, interni o esterni all'organizzazione.

Per il DPO non sono previste le certificazioni di cui all'art. 42 del GDPR anche se si stanno diffondendo alcune certificazioni "proprietarie", legate a specifici percorsi formativi, che costituiscono una presunzione "semplice" di idoneità professionale il cui valore è rimesso al "prudente apprezzamento" dei Titolari che, pertanto, non sono esonerati dal valutare in concreto i requisiti del DPO.

4.5.3. Prerogative e doveri del DPO

Al DPO, per l'efficace svolgimento delle proprie attività, sono riconosciuti specifiche prerogative e attribuiti determinati doveri, come riportato nella Figura 20.

Figura 20 – Prerogative e doveri del DPO



Particolare rilievo rivestono il requisito dell'indipendenza del DPO (il considerando 97 riporta testualmente che il DPO deve "*poter adempiere alle funzioni e ai compiti in maniera indipendente*"), a prescindere che sia un dipendente o meno del Titolare del trattamento, ed il requisito dell'autonomia intesa nel senso che devono essergli attribuite le risorse necessarie per assolvere ai propri compiti.

È utile, comunque, ricordare che i DPO non rispondono direttamente in caso di inosservanza del GDPR, in quanto tale responsabilità ricade sul Titolare o sul Responsabile del trattamento

Sul DPO il Gruppo "articolo 29" ha emanato le linee guida WP 243 rev. 01 (versione aggiornata del 5 aprile 2017).

4.6. I profili professionali previsti dalla norma UNI 11697:2017

Nell'ambito delle attività di *data protection*, la norma nazionale UNI 11697:2017, "Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza" individua i seguenti profili professionali, definendone i compiti (punto 4) e le conoscenze, abilità e competenze (punto 5):

- *responsabile della protezione dei dati* (c.d. DPO, *Data Protection Officer*): profilo corrispondente a quanto previsto dall'art. 39 del GDPR 679/16;
- *manager privacy*: profilo congruo a soggetti di elevatissimo livello di competenze funzionale alla garanzia dell'adozione delle misure idonee di sicurezza per il trattamento dei dati;
- *specialista privacy*: profilo indicato per i soggetti che supportano il D.P.O. o il *manager privacy* nel mettere a punto le idonee misure di sicurezza;
- *valutatore privacy*: profilo pertinente a soggetti indipendenti con conoscenze e competenze in diversi settori che impattano con la protezione dei dati e che possono avvalersi di specialisti per la conduzione di *Audit*.

Si riportano, nella Tavola 8, i compiti principali dei profili professionali, previsti dalla norma UNI 11697:2017¹⁷.

Tavola 8 – Profili professionali: compiti principali

Manager privacy
<ul style="list-style-type: none">• Assistere il Titolare nel dare seguito alle richieste di esercizio dei diritti degli interessati.• Assistere il Titolare nel disporre la cancellazione o la restituzione dei dati personali alla conclusione del trattamento.• Informare periodicamente il Titolare sullo stato del trattamento e della protezione dei dati personali.• Gestire il budget per la protezione dei dati personali.• Controllare con continuità il livello complessivo di protezione dei dati personali.• Organizzare e attribuire le Responsabilità relative al trattamento e alla protezione dei dati personali.• Approvare le politiche e le procedure per il trattamento e la protezione dei dati personali.• Assistere il Titolare nell'approvazione delle misure da adottare per gestire i rischi relativi alla protezione dei dati personali.• Partecipare alle attività di valutazione del rischio relativo alla sicurezza delle informazioni.• Adoperarsi per garantire il rispetto dei requisiti in materia di trattamento e protezione dei dati personali anche nelle attività progettuali.• Comunicare, se appropriato, le violazioni di dati personali agli interessati. Gestire i registri delle attività di trattamento.

¹⁷ Si omettono i compiti del DPO in quanto già indicati nel paragrafo 4.5.2.

- Definire e valutare gli SLA e i PLA che devono essere garantiti da terzi eventualmente coinvolti nel trattamento dati personali.
- Integrare le attività per la conformità al trattamento dei dati personali con le attività relative ad altri tipi di conformità ove possibile.

Specialista privacy

- Condurre le attività di valutazione d'impatto sulla protezione dei dati personali. Fornire supporto specialistico relativamente a questioni specifiche.
- Proporre le misure da adottare per gestire i rischi relativi al trattamento e alla protezione dei dati personali.
- Redigere e aggiornare le politiche e le procedure per il trattamento la protezione dei dati personali.
- Attuare processi relativi alla protezione dei dati personali. Attuare soluzioni tecniche per la protezione dei dati personali.
- Documentare i processi relativi al trattamento e alla protezione dei dati personali affinché venga riscontrata l'evidenza della conformità del trattamento effettuato.
- Documentare la gestione delle soluzioni tecniche per il trattamento e la protezione dei dati personali.
- Documentare le violazioni dei dati personali.

Valutatore privacy

- Programmare, pianificare e svolgere le attività di audit.
- Riesaminare la documentazione relativa al trattamento e alla protezione dei dati personali ed effettuare interviste al personale ad ogni livello dell'organizzazione.
- Descrivere gli scostamenti rilevati rispetto a leggi e regolamenti applicabili.

Tranne il DPO (già esaminato nel precedente paragrafo 4.5), le altre figure non sono espressamente richiamate dal GDPR mettendo in discussione, secondo alcuni studiosi, l'opportunità della scelta di individuare un numero così elevato di attori.

Ciò, infatti, potrebbe facilmente generare una notevole confusione considerando che il GDPR ha scelto di affiancare al Titolare ed al Responsabile del trattamento una sola figura, quella del DPO.

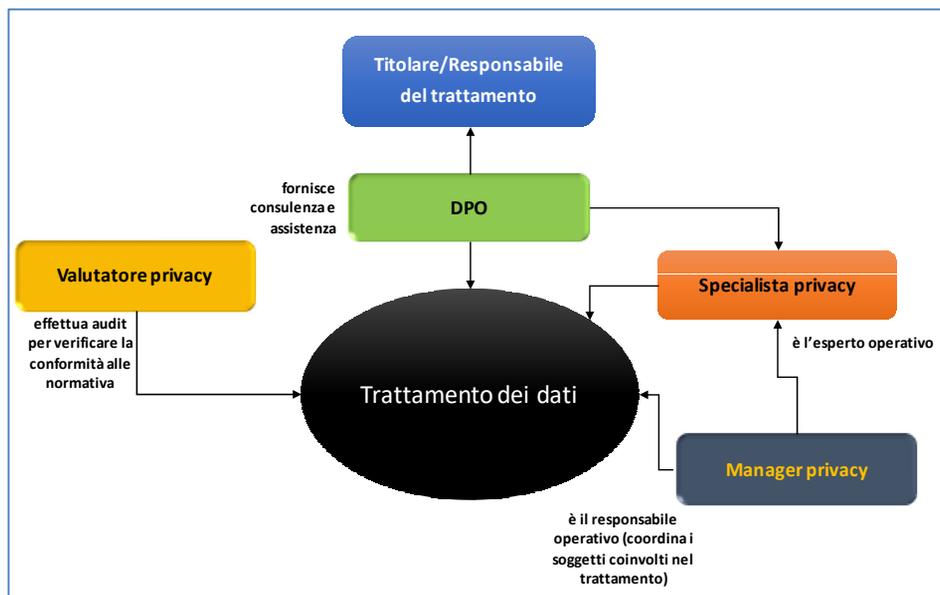
Di converso, i fautori dell'utilità della norma in esame sostengono addirittura la necessità di includere, tra i protagonisti del *data protection*, una figura manageriale, una operativa e un valutatore esterno, ritenendoli indispensabili per fornire – con un approccio sinergico - tutto il supporto necessario ai Titolari e ai Responsabili del trattamento.

In ogni caso, appare comunque opportuno approfondire la norma UNI 11697:2017 rilevando, in primis, che l'affermazione contenuta nel punto 1, secondo la quale *"i profili definiti nella presente norma non sono da intendersi come esaustivi ..."*!

La norma, inoltre, precisa che *"il professionista operante nell'ambito del trattamento e della protezione dei dati personali svolge un'ampia gamma di attività aventi frequentemente natura trasversale rispetto agli altri processi aziendali, sia*

rispetto al ciclo di vita del trattamento - dalla progettazione fino alla cessazione - sia rispetto ai temi trattati, tecnologici, legali e di altro tipo [... e...] contribuisce alla gestione o alla verifica di un insieme più o meno ampio di processi e sistemi informativi coinvolti nel trattamento di dati personali per conto di persone fisiche o giuridiche quali per esempio enti, istituzioni, associazioni, soggetti pubblici o privati". La Figura 21 rappresenta le interazioni tra i profili professionali esaminati.

Figura 21 – I profili professionali della norma UNI 11697:2017



Un ulteriore elemento da evidenziare sono i requisiti per l'accesso ai profili professionali - legati a titoli di studio, formazione specifica ed esperienze lavorative - riportati in dettaglio nella Tavola 9.

Tavola 9 – Requisiti per l'accesso ai profili professionali

Titolo di studio	Formazione specifica	Esperienza lavorativa	Equipollenza
Responsabile protezione dati			
Laurea che includa discipline almeno in parte afferenti alle conoscenze del professionista privacy,	Corso di almeno 80 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni (2).	Minimo 6 anni di esperienza lavorativa legata alla privacy di cui almeno 4 anni in incarichi di livello	Se in possesso di laurea magistrale l'esperienza lavorativa si riduce a 4 anni di cui 3 in incarichi di livello manageriale. Se in possesso di diploma di scuola media superiore mini-

Titolo di studio	Formazione specifica	Esperienza lavorativa	Equipollenza
legali o tecnico / informatiche (1).		lo manageriale (3).	mo 8 anni di esperienza lavorativa di privacy di cui almeno 5 anni in incarichi di livello manageriale.
Manager privacy			
Laurea che include discipline almeno in parte afferenti alle conoscenze del professionista privacy, legali o tecnico / informatiche (1).	Corso di almeno 60 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni (2).	Minimo 6 anni di esperienza lavorativa legata alla privacy di cui almeno 3 anni in incarichi di livello manageriale (3).	Se in possesso di laurea magistrale l'esperienza lavorativa si riduce a 4 anni di cui 2 in incarichi di livello manageriale. Se in possesso di diploma di scuola media superiore minimo 8 anni di esperienza lavorativa di privacy di cui almeno 4 anni in incarichi di livello manageriale
Specialista privacy			
Diploma di scuola media superiore.	Corso di almeno 24 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni (2).	Minimo 4 anni di esperienza lavorativa legata alla privacy.	Se in possesso di laurea l'esperienza lavorativa si riduce a 2 anni.
Valutatore privacy			
Diploma di scuola media superiore.	Corso di almeno 40 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni (2).	Minimo 6 anni di esperienza lavorativa continuativa legata alla privacy di cui almeno 3 anni in incarichi di audit.	Se in possesso di laurea l'esperienza lavorativa si riduce a 4 anni di cui 2 in incarichi di audit. Se in possesso di Laurea Magistrale minimo 3 anni di esperienza lavorativa di cui 2 in incarichi di audit.
<p>(2) Un laureato con laurea non afferente alle conoscenze del professionista <i>privacy</i>, legali o tecnico/informatiche è da considerarsi equiparato a un diplomato di scuola media superiore.</p> <p>(2) È ammissibile la riduzione delle ore di formazione richieste fino a un massimo del 10% (30% per il Valutatore Privacy) in caso di possesso di certificazioni professionali riconosciute come attinenti alle conoscenze richieste al professionista <i>privacy</i> in questione.</p> <p>(3) Gli incarichi di livello manageriale possono includere anche attività rilevante svolta nell'ambito di attività di consulenza o di prestazione d'opera condotta nell'ambito dell'esecuzione di ingaggi professionali.</p> <p>(Fonte: <i>appendice B della norma UNI 11697:2017, pag. 32</i>)</p>			

La disciplina dei profili professionali – è utile precisarlo – non va confusa con quella relativa alle certificazioni previste dal GDPR, disciplinate dall'art. 42, per le quali si rinvia al capitolo 1, paragrafo 1.6.2.



5. Il Data protection by design: progettare il trattamento dei dati

5.1. Il rischio da trattamento dei dati personali

L'applicazione del GDPR ruota intorno alla nozione di rischio da trattamento di dati personali.

In generale il rischio può essere definito come l'effetto dell'*incertezza sugli obiettivi*¹ o, in termini più accessibili, alla *possibilità di accadimento di qualcosa che avrà un impatto sugli obiettivi*².

Con riferimento al trattamento di dati personali, il considerando 75 specifica che tale tipologia di rischio:

- ha come oggetto i diritti e le libertà delle persone fisiche;
- ha una rilevanza (probabilità e gravità) variabile;
- può determinare danni fisici, materiali o immateriali che, nel dettaglio, vengono individuati nelle categorie descritte nella Tavola 10.

Tavola 10 - Categorie dei rischi da trattamento

N.	Categoria del rischio	Descrizione
1	Rischio da danno sociale ed economico	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, decifrazione non autorizzata della pseudonimizzazione o qualsiasi altro danno economico o sociale significativo;
2	Rischio da lesione dei diritti personali	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;
3	Rischio da dati sensibili e giudiziari	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;
4	Rischio da profilazione	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 sposta-

¹ Si veda la definizione di rischio nella norma ISO/IEC 27000:2016 "Information technology - Security techniques - Information security management system - Overview and vocabulary".

² Definizione contenuta nello standard AS/NZS 4360 del 1995.

5. Il Data protection by design: progettare il trattamento dei dati

N.	Categoria del rischio	Descrizione
		menti, al fine di creare o utilizzare profili personali;
5	Rischio da trattamento su persone vulnerabili	se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;
6	Rischio da trattamento massivo	se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Oltre all'elenco riportato nella tavola 10 - associato alla tipologia di danno - occorre sottolineare le tipologie tipiche di "rischio relativo alle informazioni"³:

- violazione della riservatezza: solo i soggetti autorizzati possono avere accesso ad un'informazione;
- disponibilità: un'informazione deve essere accessibile ai soggetti autorizzati al momento appropriato;
- integrità: un'informazione può essere modificata solo dai soggetti autorizzati e nei modi autorizzati;
- autenticità: il destinatario dell'informazione deve poter verificare l'identità del mittente;
- non ripudio: il mittente di un'informazione non può negare di averlo inviato.

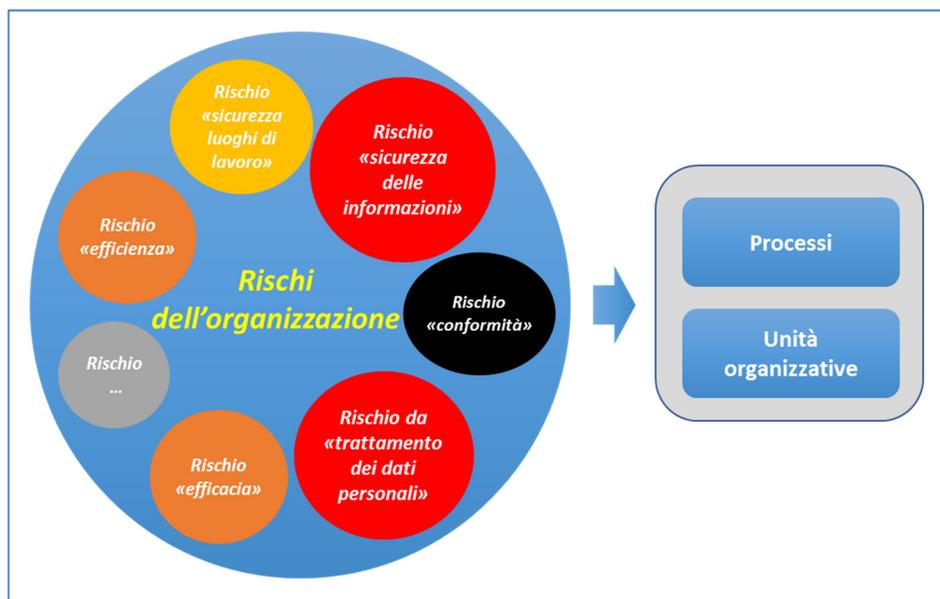
Occorre infine precisare due aspetti fondamentali che riguardano i rischi da trattamento di dati personali.

Il primo è che tali rischi non devono essere presi in considerazione autonomamente bensì all'interno del sistema di gestione generale dei rischi dell'organizzazione in cui confluiscono tutti i rischi - indipendentemente dalla loro natura - ed i relativi presidi di controllo.

Il secondo aspetto si riferisce agli ambiti da analizzare per l'identificazione - e cioè per la mappatura - dei rischi: si tratta di due contesti che derivano dalle *best practice* relative al *risk management* e si identificano nei processi - a cui è dedicato il paragrafo 5.3.2 - e nelle unità organizzative. Ciò, in definitiva, consente di porre correttamente il *focus*, rispettivamente, sulle attività e sulle strutture (ed i loro responsabili) in cui le attività si svolgono.

³ Cfr. il considerando 83 del Regolamento UE e la nota 44 del capitolo 1.

Figura 22 - Mappatura dei rischi vs processi e strutture



Appare evidente che questi ambiti, schematizzati nella Figura 22, devono essere considerati complementari.

5.2. Il Data protection by design

La progettazione di un'attività di *risk management* costituisce un'attività indispensabile per chiunque tratti dati personali, al fine di evitare conseguenze negative in termini di:

- danni di immagine e patrimoniali per la non conformità alle norme;
- mancato o insufficiente conseguimento degli obiettivi;
- inefficienza e inefficacia dei processi operativi, con conseguenti costi gestionali.

Il GDPR addirittura sposta questa attività dalla dimensione delle "buone pratiche" organizzative a quella delle prescrizioni giuridiche, secondo una ormai consolidata tendenza - consolidatasi soprattutto nell'ambito delle organizzazioni pubbliche ma riscontrabile ormai anche in molte normative di "regolamentazione" applicabili anche alle aziende private - a "normare" processi, prassi e procedure di *governance* e di gestione⁴.

⁴ Ad esempio si pensi alla disciplina sulla prevenzione della corruzione (legge n. 190/2012 e provvedimenti discendenti) e sulla performance (D.Lgs. n. 150/2009).

Per la PA

Anche le pratiche manageriali sono spesso contenute in norme di legge ...

L'art. 25 del Regolamento UE, infatti, introduce il *data protection by design*, e cioè un sistema in grado di produrre una serie di attività specifiche e dimostrabili finalizzate a prevedere, *ex ante*, le misure tecniche e organizzative per:

- attuare i principi di protezione dei dati;
- garantire il rispetto delle prescrizioni contenute nel GDPR;
- tutelare i diritti degli interessati.

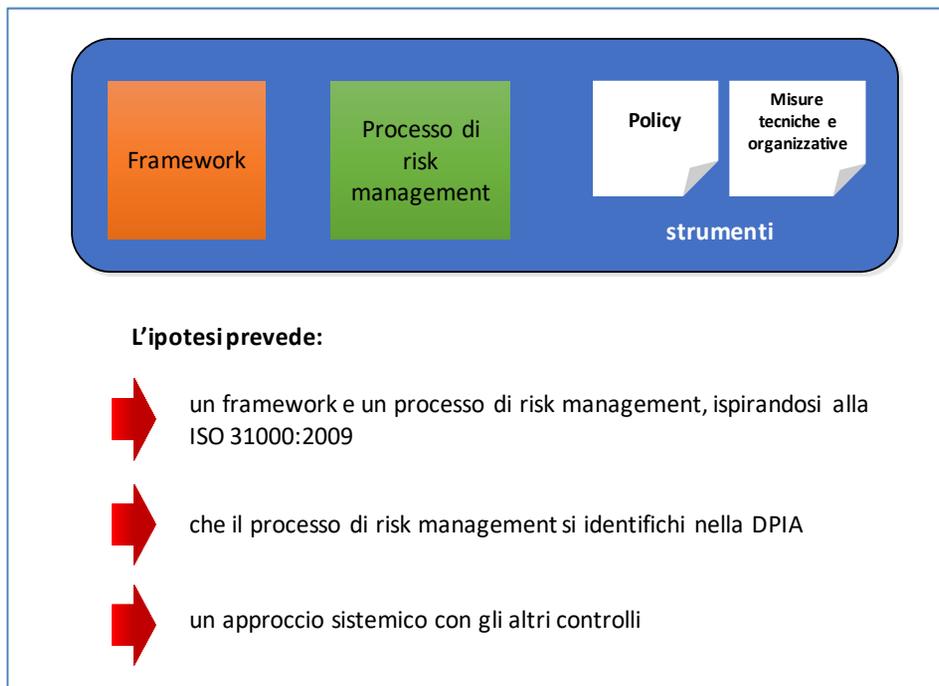
Si tratta, in definitiva, di una progettazione per la quale formuleremo un'ipotesi applicativa che sarà approfondita nel prosieguo del capitolo.

Essa si basa su un sistema - ispirato allo standard internazionale ISO 31000:2009 - che prevede i seguenti tre elementi:

- 1) un *framework*, e cioè un modello per la gestione del rischio, su cui ci si soffermerà nel paragrafo 5.4;
- 2) un processo di *risk management*, che può identificarsi nel *data protection impact assessment* (DPIA)⁵, come abbiamo ipotizzato nel successivo capitolo 6;
- 3) due tipologie di strumenti - che costituiscono gli *output* del processo di *risk management* - adottati dal Titolare del trattamento, a cui fa capo l'intero sistema di *data protection*: le *policy* e le misure tecniche ed organizzative (e cioè le procedure operative).

⁵ Si veda anche la norma ISO/IEC 29134:2017, Information technology - Security techniques - Guidelines for privacy impact assessment.

Figura 23 - Ipotesi di sistema “data protection by design”



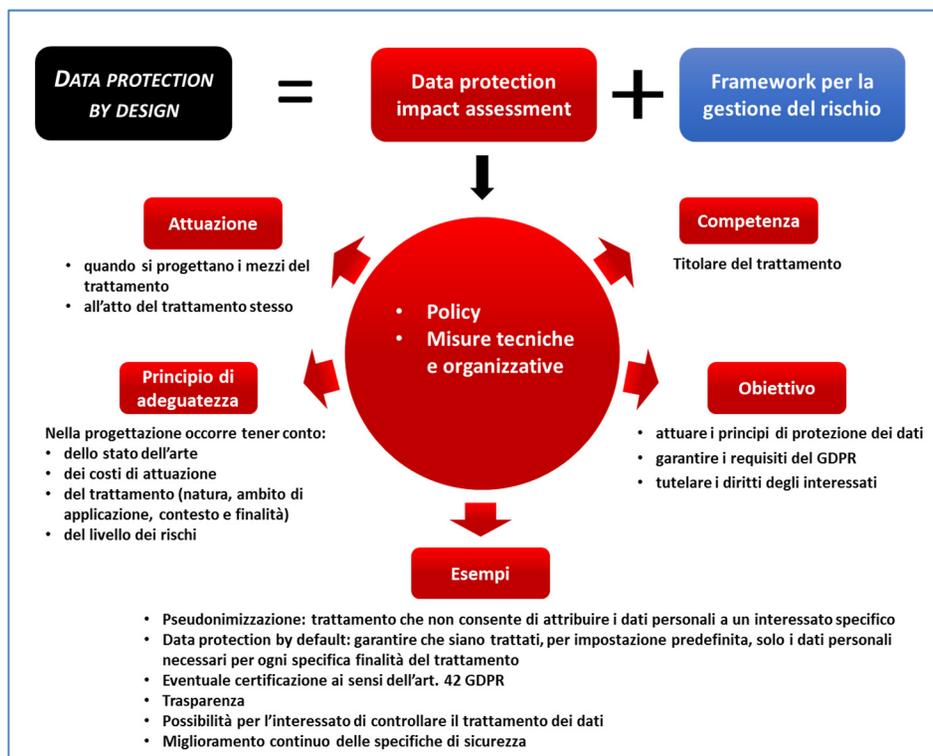
Con riferimento all'ultimo elemento, va precisato che alla progettazione deve applicarsi il principio di adeguatezza nel senso che occorre tenere conto di una serie di parametri, riportati nello schema riassuntivo contenuto nella Figura 24, che rendano *ragionevoli* le misure tecniche ed organizzative adottate.

A tal proposito appare interessante evidenziare che per l'attività relativa al *data protection by design*, anche ai fini della dimostrazione della sua adeguatezza, possono essere utilizzati⁶:

- codici di condotta;
- linee guida fornite dal Comitato;
- indicazioni fornite da un DPO, se nominato;
- il meccanismo di certificazione, di cui all'art. 42 del GDPR.

⁶ Cfr. l'art. 25, paragrafo 3, ed il considerando 77 del Regolamento UE.

Figura 24 - Il Data protection by design



In definitiva si tratta di un'attività di *risk management* che coinvolge prioritariamente il Titolare ed il Responsabile del trattamento in relazione, secondo il considerando 77:

- al rischio, e cioè alla sua individuazione e valutazione in termini di origine, natura, probabilità e gravità;
- ai presidi di controllo, e cioè alle misure dirette a mitigare i rischi.

5.3. I presupposti organizzativi

5.3.1. Corporate governance e integrazione del data protection con gli altri controlli: la necessità di un approccio sistemico

Un segnale dell'apertura delle realtà aziendali a visioni più innovative e focalizzate sulla ricerca di modelli organizzativi efficaci è rappresentato dal progressivo radicamento del concetto di *governance* e dal rilievo che esso viene sempre più assumendo tra i fattori da cui dipende la *performance* organizzativa.

In generale il concetto di *governance* è legato a standard internazionali, riconosciuti da tutti i paesi industrialmente evoluti. In particolare essa viene definita come «l'insieme dei procedimenti e delle strutture messi in atto dall'organo di go-

verno dell'organizzazione per informare, indirizzare, dirigere, gestire e controllare le attività dell'organizzazione nel raggiungimento dei suoi obiettivi»⁷.

Anche nel settore pubblico, pur non esistendo una definizione "normata", di recente comunque emerge un'elevata sensibilità rispetto al tema della *governance* e appare significativa al riguardo, oltre alla creazione di appositi organismi⁸, l'adozione, da parte di molti Stati, del *Public Internal Financial Control* (Pifc), cioè di un modello di reingegnerizzazione del sistema di controllo interno che appunto fornisce anche una panoramica esaustiva sui fondamentali principi della moderna *governance* pubblica.

Per la PA

In dottrina, la *governance* pubblica è stata definita come «*strutturazione di policy e sistema procedurale per indirizzare le attività di un'organizzazione al fine di fornire una ragionevole assicurazione che gli obiettivi siano conseguiti e che le operazioni siano eseguite in modo etico e responsabile*».

Per grandi linee, la sostanziale distinzione tra la *governance* delle strutture private e la corrispondente nozione in ambito pubblico sta nel fatto che la prima è fondamentale correlata ai diritti degli *stakeholders* mentre la seconda è principalmente rivolta ad aspetti organizzativi che coinvolgono le responsabilità, i compiti e le deleghe del *management*, definendo "chi fa cosa", assicurando, in tal modo, la credibilità dell'amministrazione pubblica ed un appropriato comportamento dei dipendenti pubblici.

In ogni caso la *governance* può definirsi come la relazione tra le funzioni amministrative e di controllo da un lato, e le scelte di governo dall'altro, attraverso strutture, processi e norme.

Essa agisce su ambiti specifici, quali ruoli, responsabilità, processi, modalità di allocazione delle risorse e, infine, sistemi di misurazione e controllo delle *performance* e del conseguente sistema premiante.

Gli elementi distintivi della *governance* sono fondamentalmente:

- le strategie e gli obiettivi: essi sono coinvolti in un processo di pianificazione (declinata a livello strategico, direzionale e operativo) che, partendo

⁷ Cfr. il glossario degli standard internazionali per la pratica professionale dell'Internal Auditing (<http://www.iiaweb.it/standard-internazionali>).

⁸ A titolo di esempio, si consideri che in seno all'Ocse opera dal 2005 il *Public Governance Committee* (Pgc), composto da delegati delle amministrazioni centrali dei Paesi membri, con lo scopo di assistere i Governi nella definizione di politiche per la modernizzazione della pubblica amministrazione nell'obiettivo di rafforzare la *governance* pubblica (si veda il sito: <http://www.oecd.org/gov/Handbook.pdf>).

dagli obiettivi da conseguire, mira ad individuare le modalità più efficaci per perseguirli, tenendo conto dell'impatto (l'*outcome*) in termini economici, sociali, territoriali, ambientali ed etici;

- l'*accountability*, e cioè il rendere conto dei risultati (cosa si è ottenuto) e dei processi implementati (come si è operato), in una concezione di "responsabilità" secondo la quale l'organizzazione deve rispondere del proprio operato;
- la *performance*, connessa a diverse prospettive (economica, finanziaria, di efficacia, di efficienza ed economicità dei processi, di apprendimento e crescita, ecc.).

Sia nel mondo aziendale che nel settore pubblico, la *governance* può essere considerata come l'insieme delle *policy*, delle procedure, delle regole formali e informali, delle strutture e dei processi, finalizzato a:

- 1) conseguire un risultato prefissato (inteso come *outcome*, cioè come impatto delle attività sul target di riferimento);
- 2) ottimizzare il rapporto risorse/attività/risultati;
- 3) fornire una ragionevole assicurazione che gli obiettivi siano conseguiti e che le operazioni siano eseguite in modo etico e responsabile;
- 4) garantire gli *stakeholder*.

In questo ambito si collocano i controlli interni che costituiscono una componente fondamentale della *governance*.

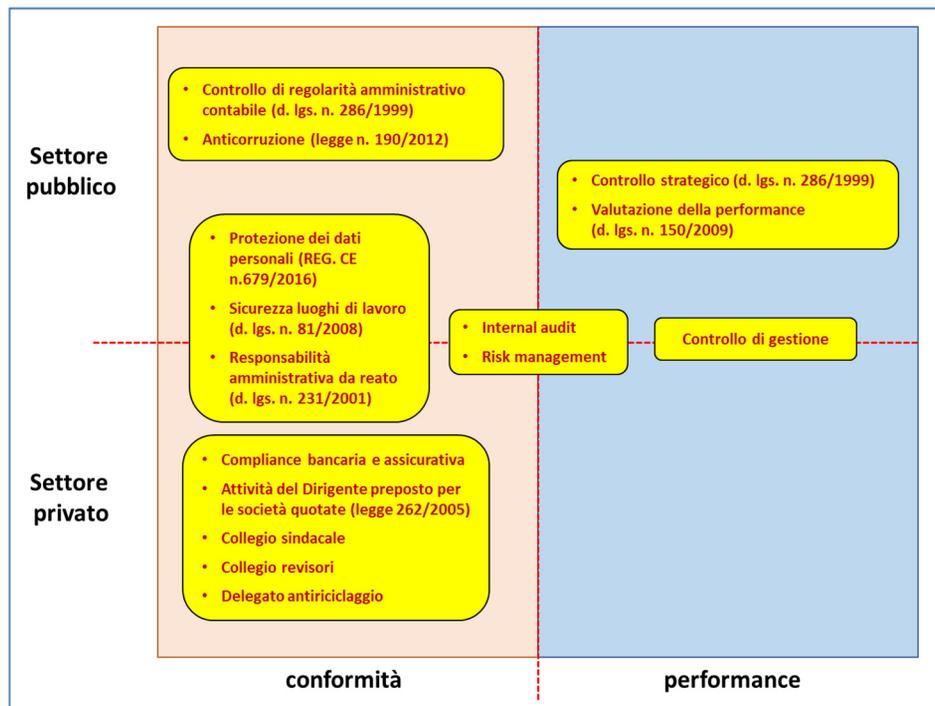
Si tratta di attività che incidono profondamente sull'organizzazione, in quanto hanno un impatto elevato su aspetti organizzativi, sulle normative interne e sulle modalità di allocazione delle risorse.

Ad esempio, la tutela del patrimonio informativo dell'organizzazione - che costituisce un asset indispensabile per il raggiungimento degli obiettivi aziendali - e quindi la gestione della sicurezza delle informazioni e la conformità alle normative, ha una stretta interdipendenza con cluster strategici, quali:

- la struttura organizzativa;
- i processi;
- le politiche di sicurezza;
- le procedure e linee guida;
- le risorse umane, finanziarie ed informatiche.

Allo scopo di conseguire adeguati livelli di efficienza organizzativa e di *compliance* normativa, il numero dei controlli e dei soggetti ad essi preposti è costantemente in aumento, come si può evincere dall'elenco esemplificativo, riportato nella Figura 25.

Figura 25 - Attività di controllo ed attori



Ciò, tuttavia, se da un lato denota un'apprezzabile tendenza a presidiare ambiti di indubbia rilevanza strategica, dall'altro determina pressanti esigenze di coordinamento per evitare sovrapposizioni, diseconomie, ambiguità su ruoli e competenze e dannose ridondanze.

La soluzione, anche in questo caso, va ricercata nella capacità di individuare un razionale modello organizzativo di controllo che, nel rispetto delle diverse competenze, consenta di armonizzare attività ed obiettivi, condividendo *know-how* specialistico, piattaforme informatiche, informazioni, cronoprogrammi.

È chiaro che non esiste un modello predefinito in generale, in quanto esso deve adattarsi alle specificità dell'organizzazione, ma il fondamentale principio a cui ispirarsi è comune: l'**integrazione**.

5.3.2. La mappatura dei processi

Sosteneva Karl E. Weick, uno dei più influenti studiosi in campo organizzativo:

«non esistono organizzazioni ma solo processi organizzativi!».

Il processo è un insieme organizzato di attività e di decisioni, finalizzato alla creazione di un *output* - e cioè di un "risultato definito e misurabile" - effettivamente richiesto dal suo destinatario, e al quale questi attribuisce un valore ben

definito: in questa ottica, il *focus* è quindi orientato verso il fruitore del servizio, a cui è destinato quell'*output*.

I processi sono quindi delle aggregazioni di attività finalizzate al raggiungimento di uno stesso obiettivo che vengono attivati da un *input* e che producono un *output*: l'*output* di un processo può poi essere l'*input* di un processo successivo così come l'*input* di un processo può essere l'*output* di quello precedente.

Attualmente non è stata ancora superata la concezione organizzativa che si fonda sulle singole funzioni e, in molte realtà, si è piuttosto lontani da una visione che focalizzi la propria attenzione sui processi, che metta in simultaneità ciò che è attualmente sequenziale, che colleghi gli *input* agli *output* per valutare l'efficienza e l'economicità.

Può quindi senz'altro affermarsi che in molte organizzazioni vi sia un approccio del tutto inadeguato, se non addirittura assente, sui processi organizzativi.

Deve comunque rilevarsi una sensibilità sempre maggiore rispetto all'esigenza di realizzare una mappatura dei processi.

Questa attività, tuttavia, presenta diverse rilevanti difficoltà, ad alcune delle quali riteniamo utile fare cenno.

Innanzitutto bisogna evitare la creazione di mappature usa e getta, realizzate per motivi contingenti e difficilmente riutilizzabili. Inoltre, poiché la mappatura rappresenta uno strumento necessario per tutti gli attori dell'azienda, è necessario che sia realizzata in sinergia tra più funzioni, senza duplicazioni per evitare ciò che accade nel mondo dell'ICT tra i cosiddetti "sistemi proprietari": impossibilità o, nel migliore dei casi, interazione difficoltosa attraverso sovrastrutture e protocolli comunque molto onerosi in termini economici e di energie profuse.

Ma è soprattutto nella vera e propria realizzazione della mappatura che emergono aspetti critici dovuti essenzialmente alla sua complessità.

Prioritariamente è necessario stabilire i contenuti, le convenzioni di rappresentazione e il livello di dettaglio, che deve essere tale da consentire sia una visione sistemica che una vista particolareggiata per quegli ambiti per i quali sia effettivamente necessario.

Al riguardo è utile la creazione di uno specifico documento, la tassonomia dei processi, che di norma è articolata in quattro ambiti di operatività.

Il primo è quello dei processi direzionali, che definiscono le strategie e le linee guida che indirizzano l'organizzazione e le sue relazioni con le entità esterne.

Il secondo riguarda i processi di relazione con il pubblico e di *customer service*, e cioè i processi che provvedono all'identificazione, generazione, erogazione dei beni e servizi.

Il terzo attiene ai processi operazionali, che sono legati alla gestione delle attività "core" dell'organizzazione.

L'ultimo ambito comprende i processi di supporto a tutte le attività operative.

Un'ulteriore criticità consiste nel fatto che ad ogni processo mappato non corrisponde una specifica figura di riferimento bensì, in genere, una serie di interlocutori che sono competenti solo di un segmento processuale.

Ciò costituisce un grave ostacolo, anche culturale, perché promuovere una cultura organizzativa orientata a operare per processi significa anche associare a ciascuno di essi un soggetto, il *process owner*, che ha appunto le responsabilità e i poteri per presidiare e garantire il buon funzionamento dell'intero processo a lui affidato.

In sostanza il problema principale è che con gli attuali modelli organizzativi (soprattutto) il *management* ha solo una visione parziale del processo e, cioè, la "quota parte" di cui è responsabile e, analogamente, ogni funzione organizzativa si concentra sul "pezzo" di propria competenza, in genere senza coordinarsi con i suoi omologhi e, nel caso in cui l'*output* sia inadeguato, si preoccupa solo di dare evidenza del fatto che "quello che gli competeva, l'aveva fatto correttamente" e che se il risultato è cattivo "la colpa non è sua".

Trasformare un'organizzazione funzionale in una per processi richiede una vera e propria rivoluzione, una redistribuzione di ruoli, competenze e responsabilità, passando da una logica verticale ad una orizzontale.

Occorre mappare tutti i processi, analizzarli, verificarne l'adeguatezza - e cioè se i processi sono in grado di produrre correttamente gli *output* previsti - e, infine, migliorarli, anche ridisegnandoli *ex novo*, se occorre.

Tutto ciò incontra, soprattutto nelle pubbliche amministrazioni, un'ulteriore specifica criticità: la confusione tra processi, procedure e procedimenti amministrativi.

Per la PA

Estrema confusione tra processi, procedure e procedimenti amministrativi.

Proviamo a fornire qualche precisazione al riguardo.

I processi, come abbiamo visto, sono una serie di attività aggregate con lo scopo unitario di realizzare un *input*.

La procedura è, invece, l'insieme delle istruzioni da seguire per lo svolgimento di una serie di attività di un processo.

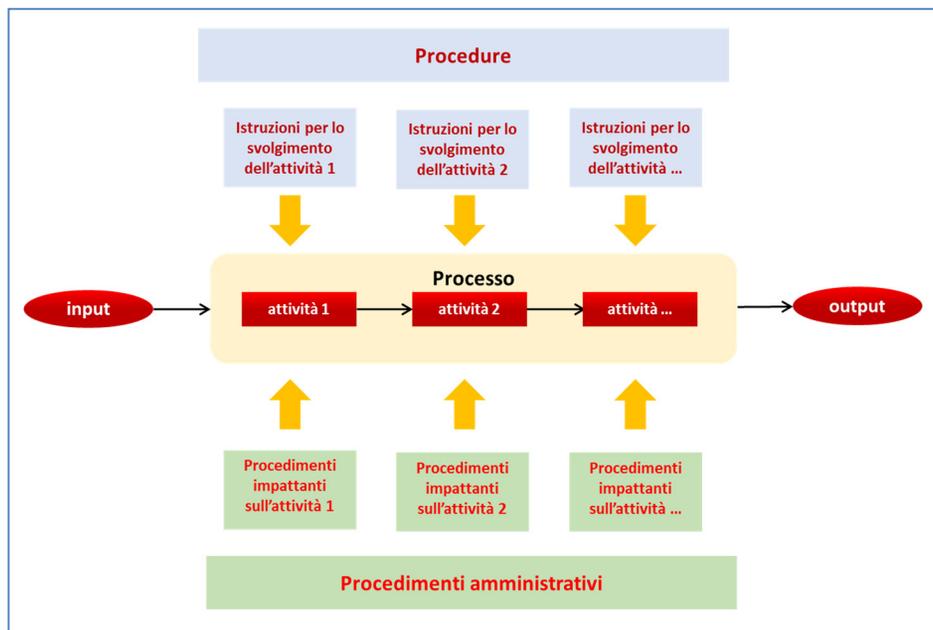
Fin qui tutto appare piuttosto chiaro. La difficoltà, invece, la troviamo quando consideriamo la nozione di procedimento amministrativo e cerchiamo di metterla "in sistema" con quelle di processo e procedura.

Il procedimento amministrativo è, in generale, una sequenza di atti ed operazioni caratterizzati dallo scopo comune e unitario di emanare un provvedimento amministrativo. Può essere considerato come una sorta di procedura eteronoma e cogente che esprime la modalità che le pubbliche amministrazioni devono seguire quando svolgono determinate attività del processo stesso, a garanzia della corretta formazione della volontà e del rispetto dei principi - sanciti dall'art. 97

della Costituzione - di legalità, imparzialità e buon andamento dell'amministrazione stessa⁹.

Lo schema riportato nella Figura 26 illustra le correlazioni descritte.

Figura 26 - Processi, procedure e procedimenti amministrativi



Una ulteriore fase critica è quella della modellizzazione dei processi.

Una volta che siano stati descritti i processi, infatti, occorre modellizzarli. La costruzione dei diagrammi di flusso è uno *step* indispensabile per ogni analisi processuale poiché permette la loro completa e chiara visualizzazione, descrivendoli in tutta la loro complessità.

La modellazione dei processi consente, inoltre, di monitorarli tramite la misurazione di un *set* di indicatori costruito con lo scopo di analizzare l'andamento del processo in termini di costi, tempi e qualità. In particolare gli indicatori devono essere in grado di far emergere, dalla grande mole di dati relativi alle attività

⁹ Si rammentano anche altri principi richiamati dalla legge 7 agosto 1990, n. 241 - la cosiddetta legge sul procedimento amministrativo - come, ad esempio, quelli di legalità, della trasparenza, di economicità, di efficienza, di efficacia, di pubblicità, di non aggravamento del procedimento. Particolare rilevanza hanno anche diversi obblighi posti a carico dell'Amministrazione quali quelli di concludere il procedimento con l'adozione di un provvedimento finale entro un termine temporale predeterminato, della chiarezza dell'*iter* formativo e delle motivazioni che hanno portato all'adozione del provvedimento, di individuare il responsabile del procedimento e di assicurare il diritto di accesso ai documenti amministrativi.

dell'organizzazione, le criticità nello svolgimento di tutte le fasi dei processi: colli di bottiglia, ridondanze e così via.

Le metodologie e le tecniche utilizzabili per la mappatura sono numerose, distinguibili per complessità, obiettivi, ecc.

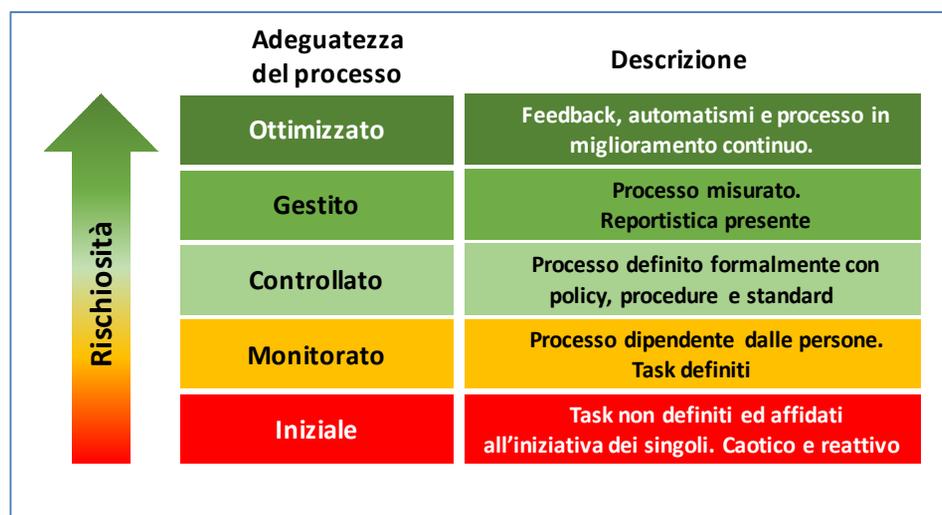
Anche per le attività di mappatura sono presenti ostacoli di tipo culturale, di cui riteniamo utile richiamarne almeno due.

Il primo è costituito dalla resistenza al cambiamento dovuta al fatto che ogni mappatura va ad incidere su equilibri consolidati in quanto determina vere e proprie riprogettazioni che coinvolgono tutte le componenti dell'organizzazione, dando origine a un insieme di interventi operativi tra loro correlati (ridefinizione dei flussi, redistribuzione delle responsabilità, realizzazione di nuovi sistemi informativi, utilizzo di nuove tecnologie, nuovi metodi di formazione, ecc.).

Il secondo ostacolo è l'effettivo coinvolgimento nell'attività di mappatura: analogamente a quanto avviene per molte altre iniziative di efficientamento delle organizzazioni, la mappatura corre il rischio di essere considerata come un mero adempimento formale.

Con riferimento specifico alla tematica del *risk management* può essere interessante cogliere le correlazioni tra il grado di adeguatezza del processo ed il suo grado di "rischiosità", così come rappresentato nella Figura 27.

Figura 27 - Grado di rischiosità rispetto all'adeguatezza del processo



Prima di concludere questo paragrafo può essere utile soffermarsi su come intervenire sui processi nel caso in cui risultino inadeguati a conseguire gli *output* prefissati.

In generale le modalità di intervento sono due: il miglioramento continuo e l'innovazione di processo.

La prima modalità è alla base del "Total Quality Management" (la nota "Qualità Totale") ed è caratterizzata dalla "continuità", per cui il miglioramento deriva da un ininterrotto ripetersi di momenti organizzati di verifica e cambiamento, che coinvolgono tutta l'organizzazione. In sostanza è rappresentata da una serie continua di miglioramenti incrementali.

La seconda modalità è anche nota come reingegnerizzazione dei processi in quanto rappresenta una discontinuità rispetto alle precedenti logiche processuali. Il "Business Process Reengineering" nasce all'inizio degli anni '90, principalmente per impulso di Michael Hammer, un professore di informatica del MIT, che partendo dagli scarsi risultati raggiunti dalle organizzazioni che hanno applicato le tecnologie dell'informazione lasciando invariati i loro processi di lavoro, afferma che occorre ripartire da capo utilizzando le opportunità dell'innovazione tecnologica per ridisegnare i processi e "ottenere *drammatici miglioramenti dei risultati*".

Questo approccio ha poi conosciuto delle forme più "morbide" che hanno assorbito anche vari elementi del "miglioramento continuo", come ad esempio quelle teorizzate da Thomas H. Davenport che si concentrano sull'utilizzo delle tecnologie come "fattore abilitante". Queste concezioni integrano l'intervento tecnologico con il cambiamento organizzativo, enfatizzano la necessità di gestire correttamente *i progetti di cambiamento allo scopo di minimizzarne i rischi*, consigliano il coinvolgimento dei "clienti" all'interno dei gruppi di lavoro per la reingegnerizzazione. In generale Davenport propone un approccio più strutturato e controllato che alterna momenti di reingegnerizzazione radicale con fasi di controllo e di miglioramento continuo. Questa nuova visione modifica completamente il ruolo delle tecnologie dell'informazione e della comunicazione.

Nel concludere, occorre evidenziare che anche nell'ambito dei controlli si sconta la frequente assenza di quel presupposto fondamentale, rispetto alla valutazione dei rischi, che è la mappatura dei processi.

È, infatti, piuttosto intuitivo rendersi conto che non è possibile verificare se i processi sono in grado di produrre correttamente gli *output* previsti - e, quindi, se sono stati attivati controlli adeguati nei confronti dei rischi che potrebbero impedire il raggiungimento dei risultati attesi - se non sono stati preventivamente mappati ... appunto i processi!

L'analisi e la gestione dei rischi - è bene ribadirlo ulteriormente - impongono, infatti, di individuare i processi, le unità organizzative e tutti i trattamenti dei dati personali (da elencare nel registro dei trattamenti) in cui i rischi si annidano rammentando, come già abbiamo precisato, che la loro gestione deve avvenire *all'interno del sistema di gestione generale dei rischi dell'organizzazione*.

L'obiettivo è quello di accrescere il livello di resilienza agli eventi critici e di coordinamento degli interventi di risposta.

5.3.3. I registri delle attività di trattamento

Il GDPR - coerentemente con il principio di responsabilizzazione in esso affermato - prevede che il Titolare (e contitolare) e il Responsabile del trattamento abbiano "un registro delle attività di trattamento svolte sotto la propria responsabilità"¹⁰.

Questo obbligo non si applica alle imprese ed organizzazioni con meno di 250 dipendenti, tranne se il trattamento:

- possa presentare un rischio per i diritti e le libertà dell'interessato;
- non sia occasionale;
- includa dati sensibili e giudiziari.

I registri, che devono essere redatti in forma scritta (anche in formato elettronico), hanno lo scopo di:

- concorrere a dimostrare l'assolvimento degli obblighi sanciti dal GDPR (è anche espressamente previsto che i registri siano messi a disposizione dell'autorità Garante nazionale);
- fornire un indispensabile strumento gestionale per la realizzazione del *Data protection by design* poiché consente di avere una visione unitaria ed organica di tutti i trattamenti dei dati personali: non si può proteggere ciò che non si conosce a fondo;
- costituire una base di conoscenza condivisa all'interno della struttura organizzativa.

Una questione di indubbio rilievo è l'armonizzazione dei due registri previsti dal GDPR, rispettivamente del Titolare e del Responsabile del trattamento, le cui tipologie di informazioni - come evidenziato nella Tavola 11 - in parte coincidono (evidenziate su sfondo grigio) ed in parte no (evidenziate in grassetto).

Tavola 11 - Informazioni contenute nei registri delle attività di trattamento

Registro del Titolare	Registro del Responsabile
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	a) 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
b) le finalità del trattamento	

¹⁰ Cfr. l'art. 30 ed il considerando 82 del Regolamento UE.

5. Il Data protection by design: progettare il trattamento dei dati

Registro del Titolare	Registro del Responsabile
	b) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento
c) una descrizione delle categorie degli 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'art. 49, la documentazione delle garanzie adeguate	c) 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'art. 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'art. 32, paragrafo 1	d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32, paragrafo 1

Come abbiamo precisato, uno degli scopi principali di questi documenti è quello di supportare l'organizzazione nelle attività di *data protection* e, in assenza di specifiche previsioni nel GDPR, ogni organizzazione deve concepire adeguate modalità per gestire le informazioni relative ai trattamenti di dati personali.

Ipotizzando uno strumento dedicato a questa esigenza, si ritiene che debbano essere previste le seguenti caratteristiche:

- *utilizzo di piattaforme informatiche* (da semplici fogli excel ad applicativi dedicati), per poter elaborare ed aggregare le informazioni attraverso specifici criteri (*query*), ottenendo anche una reportistica utile per soddisfare le varie esigenze di natura legale, operativa, ecc. (ad esempio si potrebbero estrapolare gli elenchi dei trattamenti che utilizzano dati sensibili o che prevedono specifiche misure di sicurezza);
- *integrazione delle informazioni*, nel senso che deve esistere un solo registro che comprenda ciò che è previsto sia per il Titolare che per il Responsabile del trattamento.

Di particolare interesse risultano i modelli di registro dei trattamenti suggeriti dall'autorità Garante del Regno Unito (ICO) che ha pubblicato sul proprio sito

due *template* in formato MS Excel¹¹ che contengono le informazioni indicate nella Tavola 12¹².

Come detto, sarebbe opportuno che tali modelli venissero accorpati in un unico *template*, in modo da avere un'unica vista sui trattamenti, indipendentemente dal fatto che le relative informazioni da inserire siano di competenza del Titolare o del Responsabile del trattamento.

Si noti che, molto opportunamente, alle informazioni previste dal GDPR ne sono state aggiunte altre in quanto ritenute, comunque, necessarie (indicate in corsivo e in rosso).

Tavola 12 - Esempio di modello di registro delle attività di trattamento*

Registro del Titolare del trattamento (Data controller)
<ul style="list-style-type: none">• Nome e dettagli del contatto, del DPO e del rappresentante (nome, cognome, indirizzo, e-mail, telefono)
Articolo 30 Registrazione delle attività di trattamento
<ul style="list-style-type: none">• <i>Funzione aziendale</i>• Scopo del trattamento• Nome e dati di contatto del controllore congiunto (se applicabile)• Categorie di individui• Categorie di dati personali• Categorie di destinatari• <i>Link ai contratti con il Responsabile del trattamento</i>• Paesi terzi o organizzazioni internazionali a cui i dati personali sono trasferiti (se applicabile)• Salvaguardie per trasferimenti eccezionali di dati personali verso paesi terzi o organizzazioni internazionali (se applicabile)• Programma di conservazione (se possibile)• Descrizione generale di misure di sicurezza organizzative e tecniche (se possibile)
Informativa sulla privacy
<ul style="list-style-type: none">• <i>Articolo 6 - Base giuridica per il trattamento dei dati personali</i>• <i>Articolo 9 - Base giuridica per il trattamento di dati di categorie speciali</i>• <i>Interessi legittimi per il trattamento (se applicabile)</i>• <i>Link alla registrazione di legittima valutazione degli interessi (se applicabile)</i>• <i>Diritti disponibili per gli individui</i>• <i>Esistenza di processi decisionali automatizzati, inclusa la profilazione (se applicabile)</i>• <i>La fonte dei dati personali (se applicabile)</i>

¹¹ Reperibile al link <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/>.

¹² Recentemente sono proposti modelli anche da altre autorità, come nel caso del Garante francese (CNIL), consultabili al link www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement. Più in generale sui diversi strumenti messi liberamente a disposizione (programmi open source) per gli adempimenti del GDPR, si veda il sito: www.cnil.fr/les-outils-de-la-conformite.

5. Il Data protection by design: progettare il trattamento dei dati

Consenso
<ul style="list-style-type: none">• Link alla registrazione del consenso
Richieste di accesso
<ul style="list-style-type: none">• Ubicazione dei dati personali
Valutazioni di impatto sulla protezione dei dati
<ul style="list-style-type: none">• È richiesta la valutazione dell'impatto sulla protezione dei dati?• Avanzamento della valutazione dell'impatto sulla protezione dei dati• Link alla valutazione dell'impatto sulla protezione dei dati
Violazioni dei dati personali
<ul style="list-style-type: none">• Si è verificata una violazione dei dati personali?• Link alla registrazione della violazione dei dati personali
Legge sulla protezione dei dati - Dati speciali di categoria o di condanna penale e reato
<ul style="list-style-type: none">• Condizioni per l'elaborazione• Art. 6. Base legale per l'elaborazione• Link al documento della politica di conservazione e cancellazione• I dati personali vengono conservati e cancellati in conformità alla politica di conservazione e cancellazione?• Ragioni per non aver aderito alla politica (se applicabile)

Registro del Responsabile del trattamento (Data processor)
<ul style="list-style-type: none">• Nome e dettagli del contatto, del DPO e del rappresentante (nome, cognome, indirizzo, e-mail, telefono)
Articolo 30 Registrazione delle attività di trattamento
<ul style="list-style-type: none">• Link al contratto con il Titolare• Nome e dettagli di contatto del Titolare• Nome e dettagli di contatto del rappresentante del Titolare (se applicabile)• Categorie di trattamento• Paesi terzi o organizzazioni internazionali a cui i dati personali sono trasferiti (se applicabile)• Salvaguardie per trasferimenti eccezionali di dati personali a paesi terzi o organizzazioni internazionali (se applicabile)• Descrizione generale delle misure di sicurezza tecniche e organizzative (se possibile)

* (fonte: autorità Garante del Regno Unito)

Deve infine evidenziarsi che dalla prima lettura dei registri dei trattamenti potrebbero già emergere alcuni elementi per valutare se il trattamento sia necessario e proporzionale in relazione alle finalità e alle misure di sicurezza adottate.

5.4. Il framework per la gestione del rischio

Dopo aver analizzato i più importanti presupposti di natura organizzativa - l'integrazione dei controlli, la mappatura dei processi ed il registro dei trattamenti - possiamo ora ad esaminare un componente essenziale del sistema di *risk management* dedicato alla protezione dei dati personali: il *framework*, e cioè il modello da utilizzare per la gestione del rischio.

Il GDPR, a proposito del *Data protection by design*, non cita alcun modello e pertanto, come abbiamo anticipato, faremo riferimento ad un *framework* ispirato alla norma ISO 31000:2009¹³, ossia a un modello finalizzato a progettare, attuare, monitorare, riesaminare e migliorare costantemente la gestione del rischio nell'intera organizzazione, assicurandone la piena integrazione con tutte le altre politiche e prassi strategiche ed operative.

Si tratta, in altri termini, dell'ambito in cui:

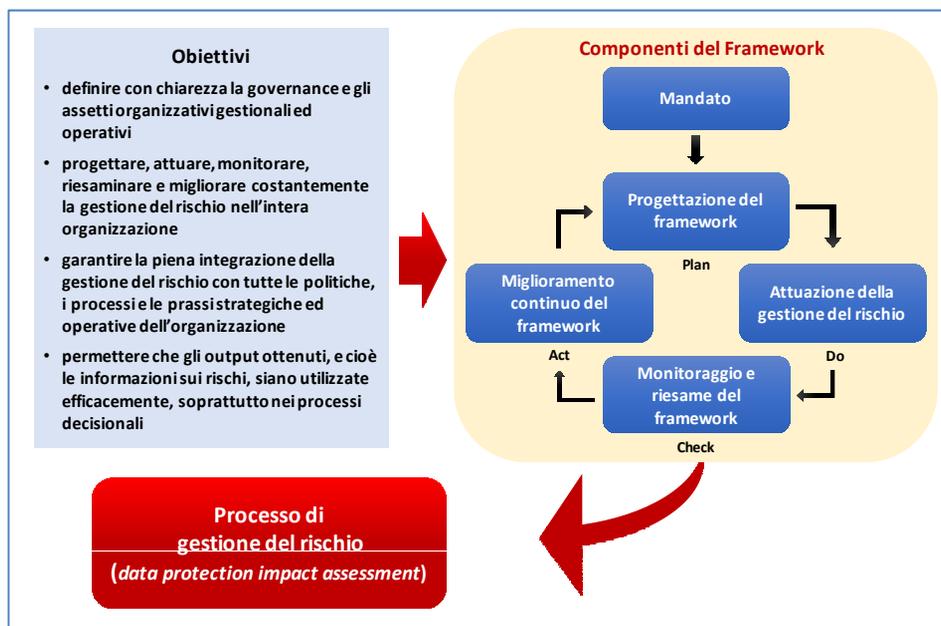
- vengono definiti con chiarezza la *governance* e gli assetti organizzativi gestionali ed operativi;
- si sviluppa il processo di gestione del rischio;
- si agisce per garantire che gli *output* ottenuti, e cioè le informazioni sui rischi, siano utilizzate efficacemente, soprattutto nei processi decisionali.

Il *framework* proposto, coerentemente con la norma ISO 31000:2009, si basa su cinque componenti.

La Figura 28 rappresenta le interrelazioni del *framework* con gli obiettivi da soddisfare e con il processo di *risk management* nonché le reciproche influenze dei cinque elementi interni che lo compongono: il mandato, la progettazione del *framework*, l'attuazione della gestione del rischio, il monitoraggio ed il riesame del *framework* e, infine, il miglioramento continuo del *framework*.

¹³ Cfr. lo standard 2.3. della norma ISO.

Figura 28 - Il Framework



5.4.1. Il mandato

Il primo componente costituisce il presupposto indispensabile per un'adeguata gestione del rischio.

È quello che viene anche chiamato, in termini aziendalistici, *commitment* e consiste nel supporto del vertice - sia sostanziale che formale - all'attività di protezione dei dati personali.

Che poi il sostegno sia dovuto a motivi ideali o alla particolare severità delle sanzioni, in questa sede poco importa: l'importante è che sia concreto e fattivo! L'obiettivo è ottenere, fin dalla fase della pianificazione strategica, l'impegno di coloro che operano, a tutti i livelli, nell'organizzazione, per cui il vertice deve definire e formalizzare la politica per la gestione del *data protection*, assicurando:

- la conformità con le norme ricercando, nel contempo, la coerenza con la cultura, le strategie e gli obiettivi dell'organizzazione;
- l'adeguatezza della struttura incaricata, attraverso l'assegnazione di congrui livelli quantitativi e qualitativi di risorse;
- che gli indicatori di prestazione della gestione del rischio da trattamento dei dati personali siano coerenti con gli indicatori della *performance* individuale ed organizzativa;
- un appropriato sistema di distribuzione delle competenze e delle responsabilità in relazione, in primo luogo, al livello gerarchico.

La necessità che il mandato del vertice sia forte è dovuta alla particolare natura dell'attività di *data protection*: si tratta, infatti, di interventi di grande impatto or-

ganizzativo che riguardano i processi, le routine operative, i rapporti tra unità organizzative, la realizzazione di una nuova mappa di poteri e di responsabilità. Sotto un certo profilo, potremmo considerare tutto questo come un cambiamento organizzativo sostanziale in grado di mettere in discussione ruoli, prassi, equilibri e, come tale, è fisiologico aspettarsi atteggiamenti di resistenza, se non di vera e propria opposizione, da parte di coloro che vedono minacciate le proprie rendite di posizione o, più semplicemente, che non hanno intenzione di rimettersi in gioco.

Per superare, appunto, questa riluttanza inerziale è indispensabile che il vertice scenda in campo per sostenere le iniziative poste in essere, attribuendo poteri, autorità e soprattutto legittimazione a chi guida ed attua questo cambiamento.

5.4.2. Progettazione del framework

La progettazione rappresenta una componente che presenta significative criticità dovute sia a motivi culturali che a *deficit* professionali.

I motivi culturali sono riconducibili alla prassi, tanto frequente quanto errata, di passare alla fase esecutiva senza una scrupolosa preventiva analisi, salvo poi dover tornare indietro per apportare correzioni e modifiche alle attività già avviate. La progettazione può essere sviluppata con riferimento alle tre aree descritte nella Tavola 13.

Tavola 13 - Le aree di progettazione del framework

	Area	Fasi	Scopo
1	Strategica	Comprensione del contesto organizzativo (interno ed esterno)	Assicurare coerenza tra l'attività di <i>risk management</i> e l'ambiente interno (cultura organizzativa, sistema di <i>governance</i> , sistema normativo, processi decisionali ed informativi, ecc.) ed esterno (utenza, contesto sociale ed istituzionale, ecc.).
		Definizione della politica per la gestione del rischio	Rendere chiari e trasparenti gli obiettivi e le modalità dell'attività di gestione del rischio, compresi i criteri di misurazione della sua efficacia ed efficienza.
2	Operativa	Definizione delle responsabilità	Definire le responsabilità, l'autorità e le competenze, ai vari livelli in relazione al <i>framework</i> e al processo di gestione del rischio; individuare gli <i>owner</i> che detengono la responsabilità e l'autorità per gestire i rischi.

	Area	Fasi	Scopo
		Definizione dei criteri di integrazione dell'attività di <i>risk management</i> nei processi organizzativi	Integrare il processo di gestione del rischio nella pianificazione strategica e commerciale e nei processi di gestione del cambiamento; evitare di creare l'ennesima sovrastruttura, separata e scoordinata con i flussi gestionali.
		Assegnazione delle risorse umane e strumentali	Soddisfare adeguati livelli qualitativi (prevedendo, anche, coerenti percorsi di carriera e di sviluppo) e quantitativi.
3	Comunicativa	Definizione dei meccanismi di comunicazione e di reporting interni ed esterni	Integrare i meccanismi di comunicazione con le politiche generali e individuare modalità e strumenti armonici con la cultura interna; concorrere al miglioramento dell'ecologia organizzativa e alla promozione della trasparenza.

Un elemento particolarmente significativo di questa componente del *framework* è il *piano di gestione del rischio* nel quale vanno programmati gli interventi da effettuare in un intervallo temporale prefissato.

Tale piano dovrebbe poi coordinarsi e integrarsi con un piano generale delle attività di controllo (comprendente il piano annuale di *audit*, il piano di *risk management*, ecc.) la cui esistenza, sebbene piuttosto rara nelle strutture aziendali e nelle amministrazioni pubbliche, dovrebbe rappresentare un rilevante obiettivo di miglioramento organizzativo.

5.4.3. Attuazione della gestione del rischio

Questa componente riguarda l'implementazione sia del *framework* che del processo di gestione del rischio.

Nel primo caso occorre innanzitutto stabilire le strategie e le politiche da adottare ed un cronoprogramma per fissare i tempi entro i quali il modello deve essere realizzato e la scansione temporale delle varie fasi.

Particolarmente importanti sono i meccanismi che devono essere previsti per assicurare che i processi decisionali dell'organizzazione tengano conto dell'esito del processo di gestione dei rischi e per evitare qualsiasi distonia tra gli obiettivi del *risk management* e gli obiettivi generali dell'amministrazione.

Un'ulteriore esigenza da soddisfare è quella di porre in essere tutte le iniziative utili a garantire la costante adeguatezza del *framework*, anche attraverso specifiche attività di formazione e di informazione.

Per quanto attiene, invece, al processo di gestione del rischio, che sarà esaminato nel prossimo capitolo, deve essere assicurato che esso si integri:

- nel piano generale di gestione dei rischi;
- in tutti i processi e le prassi,

coinvolgendo tutti i livelli e le funzioni dell'organizzazione.

5.4.4. Monitoraggio e riesame del framework

Questo componente si propone di verificare che la gestione del rischio sia efficace e continui a supportare efficacemente le prestazioni dell'organizzazione.

Allo scopo risultano necessari:

- la misurazione della performance della gestione del rischio e, quindi, l'individuazione di adeguati indicatori, da sottoporre a periodica revisione;
- la rilevazione di eventuali scostamenti dagli standard preventivamente fissati nell'apposito piano di gestione del rischio;
- la verifica periodica dell'adeguatezza del *framework* e del piano di gestione del rischio;
- la rilevazione del livello di adesione alla politica per la gestione del rischio.

5.4.5. Miglioramento continuo del framework

L'ultimo componente coincide con le decisioni relative al miglioramento del *framework*, della politica e del piano di gestione del rischio, da adottare sulla base delle informazioni acquisite soprattutto durante il monitoraggio.

5.5. Le attività critiche: la progettazione e l'informatizzazione

Al termine della descrizione delle operazioni relative alla realizzazione di un adeguato sistema di protezione dei dati, può essere utile soffermarsi su due attività particolarmente critiche, la progettazione, che abbiamo appena esaminato, e l'informatizzazione.

Si tratta di due fasi che, se non attuate adeguatamente, compromettono sicuramente la realizzazione dei risultati prefissati.

5.5.1. Come gestire i progetti: il masterplan e il diagramma di Gantt

Iniziamo con la progettazione.

Il suo rilievo è evidente, soprattutto, per la realizzazione di attività complesse - e, in particolare, per i progetti - tanto da costituire una vera e propria disciplina manageriale, il *project management*.

Dell'importanza della progettazione, purtroppo, ce ne rendiamo spesso conto soprattutto per l'effetto che produce la sua assenza o la sua inadeguatezza: il fallimento delle attività.

La progettazione richiede elevate competenze, specifiche metodologie e strumenti di supporto peculiari.

Tra questi ultimi merita un cenno particolare il *masterplan*, ossia un fondamentale elemento del *project management* che consiste nella suddivisione di un'attività complessa in singoli progetti e sottoprogetti - coordinati logicamente e temporalmente - in modo da consentirne una migliore gestibilità.

Anche nell'ambito della protezione dei dati personali il *masterplan* costituisce uno strumento indispensabile che, peraltro, richiede competenze specialistiche di natura trasversale.

Risulta, pertanto, evidente la necessità - in fase di progettazione di un sistema di *data protection* - di definire un *masterplan*, al fine di poter individuare, e poi gestire, tutti gli elementi di rilievo, in un'ottica organica e coordinata.

Le tecniche utilizzabili sono numerose ma ciò che rileva è il modello concettuale da seguire.

Le Figure 29 e 30 schematizzano un esempio di modello.

Figura 29 - Il masterplan

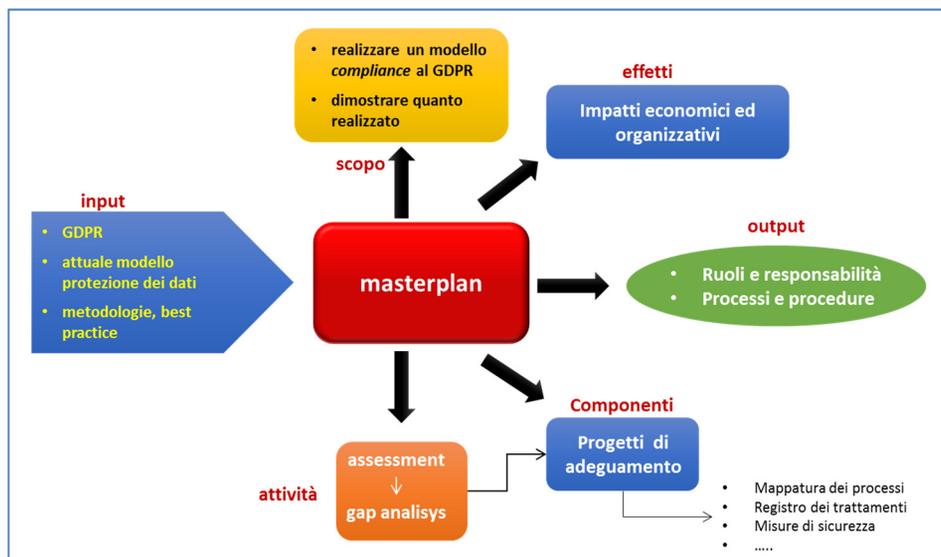
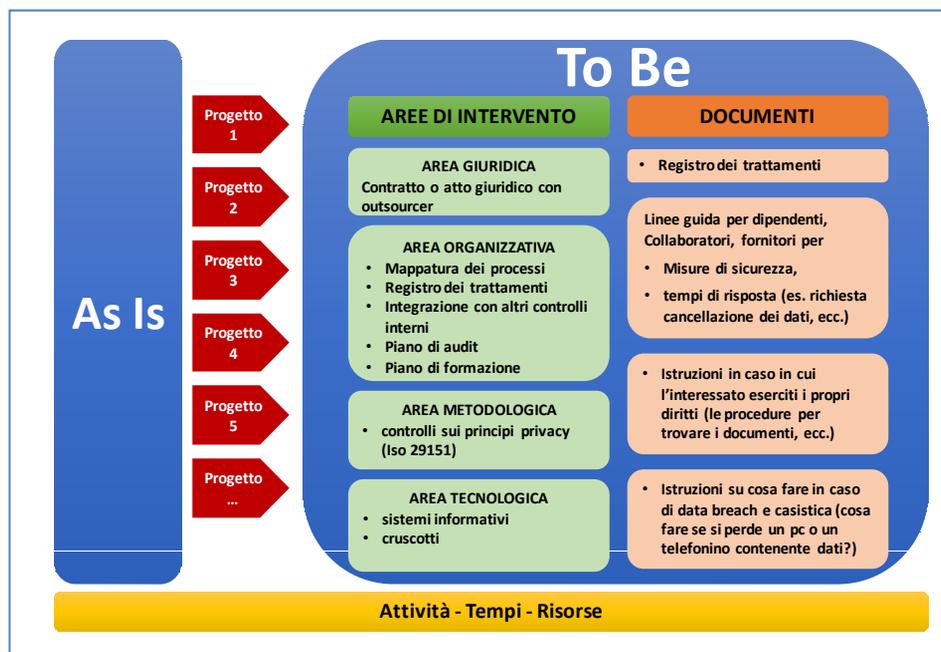


Figura 30 - Gli step del masterplan



Secondo il primo schema, innanzitutto occorre determinare quali sono i componenti dell'*input*, raggruppandoli in tre tipologie: regole da osservare (GDPR ed altre disposizioni normative), modello attuale di protezione dei dati, metodologie da utilizzare (standard, *best practices*, ecc.).

Questi elementi devono quindi essere utilizzati per svolgere le attività rivolte ad analizzare la situazione di partenza (*As Is*), confrontarla con quella prevista (*To Be*), rilevare i disallineamenti (*Gap Analysis*) e, infine, a individuare specifici progetti di adeguamento, che costituiscono l'essenza del *masterplan*.

I progetti di adeguamento:

- hanno come *output* la realizzazione di un modello di protezione dei dati conforme al GDPR attraverso la definizione di ruoli e responsabilità nonché di processi e di procedure;
- tengono conto degli impatti organizzativi ed economici;
- utilizzano tecniche di *project management* per la corretta gestione dei tempi, delle risorse e dei costi.

Deve evidenziarsi che una delle caratteristiche fondamentali del *masterplan* è quella di mettere in connessione tutti gli elementi che lo compongono, sia sotto un profilo logico - processuale che parametrando in relazione ai tempi ed alle risorse da utilizzare.

Con riferimento a questi due parametri (tempi e risorse) ed ai costi, lo strumento più utilizzato è il *diagramma di Gantt* in cui sono rappresentati:

- il tempo complessivo del progetto suddiviso in fasi incrementali (ad esempio, giorni, settimane, mesi) che possono sovrapporsi se le attività si svolgono in parallelo;
- le mansioni o attività che costituiscono il progetto.

In sintesi, possiamo definire un diagramma di Gantt come la rappresentazione grafica di un calendario utile al fine di pianificare, coordinare e tracciare le attività in un progetto dando una chiara illustrazione dello stato d'avanzamento.

Inoltre ad ogni attività possono essere in generale associati una serie di attributi: durata (o data di inizio e fine), risorse utilizzate, carichi di lavoro, costi persona/giorno.

5.5.2. Il supporto informatico

L'informatizzazione dei processi operativi e gestionali costituisce il tallone d'Achille di numerose organizzazioni.

Non è questa la sede per dilungarsi sui vantaggi del supporto tecnologico ma informatizzare, è bene sottolinearlo, non significa tanto automatizzare le attività quanto, soprattutto, ridisegnare i processi secondo una logica innovativa, utilizzando una nuova mappa mentale.

Fondamentalmente la raccolta e l'elaborazione delle informazioni, tramite un sistema informativo, consente due risultati importantissimi non altrimenti realizzabili.

Il primo è una gestione operativa altamente efficiente in termini di affidabilità e di rapidità nonostante quantità di dati in crescita esponenziale e scenari che registrano complessità sempre maggiori.

Il secondo risultato è quello di poter realizzare Sistemi di Supporto alle Decisioni (SSD) e cioè strumenti che raccolgono, organizzano, interpretano e integrano in modo automatico le informazioni necessarie per consigliare le azioni più appropriate al fine di dare una risposta alle più diverse esigenze operative e di adeguamento alle normative, siano esse strategiche a lungo termine oppure decisioni tattiche, da prendere in tempi molto brevi.

Cercando di dare un taglio più pratico a questi concetti, vediamo un'ipotesi di supporto informatico alla gestione di un sistema di *data protection*.

Le principali funzionalità di un applicativo dedicato a tale esigenza potrebbero essere quelle riportate nella Tavola 14¹⁴.

¹⁴ L'ipotesi si ispira all'intervento dell'ing. Davide Benvenga, "GDPR - Strumenti di supporto per la Governance", tenuto a Roma il 27 marzo 2018 presso ISACA (Information Systems Audit and Control Association).

Tavola 14 - Esempio di funzionalità di un applicativo dedicato al data protection

N.	Area	Funzionalità
1	Gestionale	<ul style="list-style-type: none"> • Monitoraggio dell'attività per supporto alle decisioni (SSD) e supporto operativo (sistema di alert). • Gestione del registro dei trattamenti. • Gestione dei soggetti coinvolti nelle attività. • Gestione delle richieste degli interessati. • Gestione dei consensi degli interessati. • Gestione delle violazioni.
2	Risk management	<ul style="list-style-type: none"> • Analisi del rischio e DPIA - <i>Data Protection Impact Assessment</i>.
3	Repository	<ul style="list-style-type: none"> • Archivio documentale.

La prima funzionalità, il "monitoraggio delle attività", consente di perseguire due obiettivi.

Il primo è di tipo conoscitivo che consiste nella possibilità di avere una visione complessiva sulle attività previste dal GDPR (trattamenti, DPIA, Violazioni, Richieste interessati, ecc.).

Il secondo obiettivo ha una connotazione più operativa e consiste in un sistema di *alert* che segnalano situazioni da gestire (DPIA in scadenza, scadenza del periodo previsto per evadere una richiesta dell'interessato, ecc.).

Si tratta, in sostanza, di un c.d. cruscotto che si avvale di rappresentazioni grafiche dei fenomeni di interesse, del tipo di quelle rappresentate nella Figura 31.

Figura 31 - Cruscotti SSD: esempi di monitoraggio delle attività



La "gestione del registro dei trattamenti" riguarda tutte le informazioni correlate e, innanzitutto, se il trattamento è stato oggetto di DPIA o se è stato coinvolto in violazioni (si rinvia al paragrafo 5.3.3 e, in particolare, alla Tavola 12).

La funzione - come esemplificato nella Figura 32 - dovrebbe prevedere l'aggiornamento del registro in tempo reale, la storicizzazione ed il tracciamento delle modifiche e l'estrazione in formato Excel/csv.

Figura 32 - Esempio di gestione del registro dei trattamenti

Livello rischio	Descrizione	Finalità trattamento	Soggetti interessati	Soggetti destinatari	Stato	Valutazione DPIA	Violazioni	...
Altissimo	Archivio dipendenti	Adempimenti normativi	Dipendenti	Direzione Generale	Attivato	X		
Medio	Trattamento azienda 1	Gestione reclami	Dipendenti e fornitori	Rete commerciale	Attivato	V	X	
Medio	Nuovo trattamento azienda 1 . DPIA	Gestione reclami	Dipendenti	Rete commerciale	In lavorazione	X		
Medio	Archivio dipendenti 2	Gestione risorse umane	Dipendenti	Rete commerciale	Attivato	V		

La funzionalità *"gestione dei soggetti coinvolti nelle attività"* consiste sostanzialmente nella realizzazione di una sezione anagrafica in cui sono censiti tutti i soggetti coinvolti a qualsiasi titolo nelle attività di trattamento (Titolare, Responsabile, DPO, ecc.) acquisendo i dati identificativi e di contatto e tutti i documenti pertinenti (lettere di incarico/nomina, eventuali certificazioni, ecc.) soddisfacendo, in tal modo, esigenze di natura sia normativa che organizzativa (storicizzazione dei soggetti collegati ai trattamenti, ecc.).

La *"gestione delle richieste degli interessati"*, invece, è una funzionalità che si basa su un workflow che consente, in particolare, di:

- 1) registrare i dati del richiedente e della relativa richiesta;
- 2) allegare il documento del consenso se previsto;
- 3) produrre schede dei trattamenti a cui il richiedente è associato;
- 4) produrre schede con i dati specifici del richiedente, forniti dalle strutture "owner";
- 5) produrre ed inviare la risposta finale al richiedente;
- 6) monitorare i giorni di lavorazione della pratica per attivare eventuali *alert* ed effettuare rilevazioni statistiche sui tempi del processo (tempi medi, costi giornate/persona, ecc.).

La *"gestione dei consensi degli interessati"* è una funzionalità analoga a quella precedente ed è rivolta a censire i consensi rilasciati dagli interessati per supportare le verifiche sulla conformità.

La funzione *"gestione delle violazioni"* riguarda la gestione, il tracciamento e la documentazione delle attività svolte. Prevede 4 operazioni principali:

- 1) registrazione dei dati generali della violazione (data, natura, eventuale *id* nel sistema di *Incident Management*);
- 2) generazione automatica, in base ai trattamenti coinvolti, delle informazioni relative alle categorie di dati, alle categorie dei soggetti interessati; all'utilizzo o meno di misure di sicurezza forti (informazione

- necessaria per stabilire se è necessaria anche la notifica ai soggetti interessati);
- 3) produzione automatica dei modelli da notificare al Garante e ai soggetti interessati;
 - 4) produzione dei documenti finali da inviare al Garante e agli interessati.

La funzionalità "*analisi del rischio e DPIA*" deve prevedere sicuramente le tabelle relative agli *eventi rischiosi* e alle *misure di sicurezza*, per il calcolo del rischio inerente e residuo. Per la gestione della DPIA occorre, come in casi precedenti, l'informatizzazione di un *workflow*, guidando l'utente *step-by-step* nell'esecuzione dei rispettivi compiti evitando procedure erranee (ad esempio nella DPIA possono essere coinvolti vari soggetti - *Team privacy*, DPO, IT, Sicurezza, soggetti esterni, ecc. - che, per evitare indebiti interventi, potrebbero essere vincolati al rispetto di un *workflow* di lavorazione e approvazione con profilazione delle funzionalità, e cioè in grado di inibire il compimento di qualsiasi operazione a chi non è preventivamente autorizzato in base al proprio ruolo).

Le principali tipologie di informazioni riguardano:

- i dati generali del trattamento (interessati, destinatari di comunicazioni, eventuale trasferimento dei dati all'estero, modalità di trattamento, procedure informatiche, ecc.);
- le categorie di dati (casistiche DPIA, tipologie dei dati trattati);
- gli eventi rischiosi ed i presidi di controllo;
- i pareri del DPO e di altri soggetti;
- l'eventuale consultazione del Garante;
- le determinazioni finali relative all'approvazione/revisione.

L'ultima funzionalità, l'*archivio documentale*, ha lo scopo di raccogliere e catalogare tutta la documentazione inerente le attività di *data protection*, compresa la normativa, le verifiche, i pareri, ecc.

Ma al di là dell'ipotesi di supporto informatico proposto, il concetto fondamentale è che anche gli applicativi devono essere progettati nell'ottica del *data protection by design*.

Deve infine ricordarsi che il Regolamento UE, nel prevedere le "certificazioni", può riferirsi anche ad un singolo o ad un insieme di trattamenti effettuati da un programma software¹⁵.

¹⁵ A titolo esemplificativo, si rammenta che è stato approvato da ACCREDIA lo schema proprietario ISDP©10003:2015 (conformità alle norme vigenti EU in tema di trattamenti dei dati personali) - applicabile a tutte le tipologie di organizzazioni - che consente di certificare un prodotto, processo o servizio relativamente alla gestione dei dati personali, e quindi anche un applicativo software che tratta dati personali.

5.6. Metodologie, standard internazionali e norme UNI

Come abbiamo visto, per poter applicare le disposizioni del GDPR in ambito organizzativo risulta necessario avvalersi - come in molti altri settori - di metodologie utilizzate, in genere, in ambito aziendale.

Di solito, allo scopo, si ricorre a standard, spesso internazionali, emanati da enti identificati con acronimi sul cui significato è utile soffermarci.

UNI è la sigla dell'Ente nazionale italiano di unificazione, un'associazione privata che elabora e pubblica *norme tecniche per tutti i settori industriali, commerciali e del terziario* e rappresenta l'Italia presso le organizzazioni di normazione europea (CEN) e mondiale (ISO).

CEI è l'acronimo del Comitato Elettrotecnico Italiano la cui documentazione, comunemente nota come "norme CEI", definisce la buona tecnica per i prodotti, i processi e gli impianti, costituendo il riferimento per la presunzione di conformità alla "regola d'arte".

ISO è la sigla che identifica le norme elaborate dall'Organizzazione Internazionale per la Standardizzazione, applicabili in tutto il mondo.

Dunque, se ad esempio ci imbattiamo nella norma Uni EN ISO 0000, capiamo che questa è stata emanata a livello internazionale (ISO) ed è stata recepita, sia dall'Ente nazionale italiano di unificazione (UNI) che dal Comitato europeo (EN).

IEC, invece, è l'acronimo della Commissione elettrotecnica internazionale che definisce gli standard in materia di elettricità, elettronica e tecnologie correlate, anche in collaborazione con l'ISO.

Di seguito vengono riportati i principali standard utilizzati per il *Data Protection* e negli ambiti collegati.

5.6.1. Standard specifici per il Data Protection

- 1) **ISO/IEC 29134:2017**, "Information technology - Security techniques - Guidelines for privacy impact assessment".

La norma si basa sulla ISO 31000:2009 e definisce in modo più approfondito:

- un processo articolato per lo sviluppo del Privacy Impact Assessment;
- un processo per il riesame periodico;
- un modello di rapporto per la valutazione;
- un esempio per la stima degli impatti.

Definisce inoltre un elenco di 49 minacce su cui valutare gli impatti e le probabilità (basato su scale di 4 valori).

- 2) **ISO/IEC 29151:2017**, "Information technology - Security techniques - Code of practice for personally identifiable information protection".

La norma definisce gli obiettivi di controllo, i controlli e le linee guida per l'attuazione dei controlli, per soddisfare i requisiti identificati da una valutazione di rischio e di impatto connessi alla protezione delle informazioni personali. Lo standard è basato sulle linee guida della ISO/IEC 27002 e recepisce oltre 110 controlli della ISO/IEC 27001 aggiungendone altri specifici.

- 3) **UNI 11697:2017**, "Attività professionali non regolamentate - Profili professionali relative al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza".

La norma definisce i profili professionali relativi al trattamento e alla protezione dei dati personali (DPO, Manager privacy, Specialista privacy, Valutatore privacy) coerentemente con le definizioni fornite dall'EQF e utilizzando gli strumenti messi a disposizione dalla UNI 11621-1 "Attività professionali non regolamentate - Profili professionali per l'ICT - Parte 1: Metodologia per la costruzione di profili professionali basati sul sistema e.CF".

5.6.2. Standard per la sicurezza delle informazioni

- 1) **ISO/IEC 27000:2016**, Information technology - Security techniques - Information security management system - Overview and vocabulary".

Questo standard internazionale fornisce una panoramica dei sistemi di gestione della sicurezza delle informazioni - definendo i requisiti e includendo aspetti relativi alla sicurezza logica, fisica ed organizzativa - e termini e definizioni comunemente usati nella famiglia di standard ISMS (*Information Security Management System*). Questo standard internazionale è applicabile a tutti i tipi e dimensioni di organizzazione (ad esempio imprese commerciali, agenzie governative, organizzazioni di profitto).

- 2) **ISO/IEC 27001:2013**, Information technology - Security techniques - Information security management systems -Requirements¹⁶.

La norma specifica i requisiti per stabilire, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la sicurezza delle informazioni nel contesto di un'organizzazione. Essa include anche i requisiti per la valutazione e per il trattamento dei rischi relativi alla sicurezza delle informazioni adattati alla necessità dell'organizzazione. I requisiti stabiliti sono di carattere generale e predisposti per essere applicati a tutte le organizzazioni indipendentemente dalla loro tipologia, dimensione e natura.

- 3) **UNI CEI ISO/IEC 27002:2014** - Raccolta di prassi sui controlli per la sicurezza delle informazioni

La norma - che costituisce l'adozione nazionale della norma internazionale ISO/IEC 27002 (edizione ottobre 2013) e tiene conto del *corrigendum* di settembre 2014 (Cor.1:2014) - è progettata per essere impiegata dalle organizzazioni come riferimento per la scelta dei controlli nel processo di attuazione di un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) basato sulla UNI CEI ISO/IEC 27001 oppure come documento guida per le organizzazioni che attuano i controlli comunemente riconosciuti per la sicurezza delle informazioni. La

¹⁶ È stata recepita in Italia con la UNI CEI ISO/IEC 27001:2014, "Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni. Requisiti".

norma è anche pensata per essere impiegata nello sviluppo di linee guida per interi settori o per specifiche organizzazioni in materia di sicurezza delle informazioni.

- 4) **ISO 22301:2012** - "Societal security - Business continuity management systems - Requirements"

È lo standard internazionale sviluppato per indirizzare le organizzazioni ad individuare le potenziali minacce verso i loro processi di *business*, e a costruire sistemi e processi di *backup* efficaci per salvaguardare i loro interessi e quelli degli *stakeholder*. La norma specifica i requisiti per pianificare, implementare, monitorare, revisionare e migliorare il Sistema di Gestione della continuità operativa delle organizzazioni, con l'obiettivo di ridurre l'impatto sulle attività causato dalle interruzioni.

5.6.3. Standard per il risk management

- 1) **ISO 31000:2009**, "Risk management - Principles and guidelines"¹⁷.

La norma fornisce principi e linee guida generali sulla gestione del rischio. Essa può essere utilizzata da qualsiasi impresa pubblica, privata o sociale, associazione, gruppo o individuo e, pertanto, non è specifica per alcuna industria o settore. La norma può essere applicata lungo l'intera vita di un'organizzazione e ad un'ampia gamma di attività, incluse strategie e decisioni, operazioni, processi, funzioni, progetti, prodotti, servizi e beni.

Essa può essere inoltre applicata a qualsiasi tipo di rischio, quale sia la sua natura, sia che essi abbiano conseguenze positive o negative.

- 2) **ISO Guide 73:2009**, "Risk management - Vocabulary".

Questa norma contiene un vocabolario di base per sviluppare una comune comprensione dei concetti di *risk management*, suddividendo i termini in 11 ambiti collegati al rischio¹⁸.

- 3) **ISO/IEC 31010:2009**, "Risk management - Risk assessment techniques".

Anche questo standard è di supporto alla ISO 31000:2009 nel senso che fornisce una guida per l'individuazione e l'implementazione delle tecniche da utilizzare nella valutazione del rischio. Il documento comprende anche gli annessi A e B in cui sono indicate nel dettaglio 31 tecniche, per ciascuna delle quali è indicata l'efficacia in relazione alle 3 fasi del *risk assessment* (identificazione del rischio;

¹⁷ È stata recepita in Italia con la UNI ISO 31000:2010, "Gestione del rischio - Principi e linee guida". La ISO 31000 è stata adottata come norma nazionale da oltre 50 enti nazionali di normazione, riguardando così più del 70% della popolazione globale. È stata anche adottata da un certo numero di agenzie delle Nazioni Unite e di governi nazionali come base per sviluppare i propri standard e le proprie politiche sui rischi, in particolare per quel che concerne la riduzione dei rischi in caso di catastrofe e la gestione dei rischi derivanti da catastrofi.

¹⁸ Gli 11 ambiti sono: definizione, gestione, processo, comunicazione, contesto, valutazione, identificazione, analisi, ponderazione, trattamento e monitoraggio.

analisi del rischio e cioè delle conseguenze, delle probabilità e del livello di rischio; ponderazione del rischio) nonché a 4 parametri (numero e preparazione delle risorse umane; natura e grado di incertezza; complessità del problema; possibilità di ottenere un *output* quantitativo).

- 4) **ISO/TR 31004:2013**, "Risk management - Guidance for the implementation of ISO 31000".

La norma dà una spiegazione dei concetti che stanno alla base della ISO 31000, con consigli ed esempi pratici che rispondono alle possibili esigenze specifiche dell'utilizzatore.

- 5) **CoSO Erm 2004**, "Report Internal Control - Integrated Framework sviluppato dalla Committee of Sponsoring Organizations of the Treadway Commission".

È un modello che ha lo scopo di supportare le organizzazioni nello sviluppo e nel miglioramento dei sistemi di controllo interno e nella loro integrazione con i processi, le politiche e i regolamenti esistenti.

In questo modello il concetto di controllo è centrale: esso è considerato strettamente collegato a quello di rischio che, a sua volta, è percepito come parte integrante di ogni attività in quanto coinvolge tutti i processi e gli attori. Si compone di due volumi: il primo è suddiviso in due parti, l'Executive Summary ed il *Framework*, mentre il secondo, l'Application Techniques, è dedicato alle tecniche da utilizzare nell'applicazione del *framework* che, con un'efficace rappresentazione grafica, ormai diffusissima, è rappresentato dalla Figura 33.

Figura 33 - Il CoSO ERM



5.6.4. Standard per l'internal auditing

- 1) **UNI EN ISO 19011:2012** - Linee guida per *audit* di sistemi di gestione.

Fornisce linee guida sugli *audit* di sistemi di gestione, compresi i principi dell'attività di *audit*, la gestione dei programmi di *audit* e la conduzione degli *audit* di sistemi di gestione. Costituisce una guida per la valutazione delle persone coinvolte nel processo di *audit*, incluse la persona che gestisce il programma di *audit*, gli *auditor* e i gruppi di *audit*. Applicabile a qualsiasi organizzazione che abbia l'esigenza di condurre *audit* di sistemi di gestione o di gestire un programma di *audit*. È possibile l'applicazione della norma ad altri tipi di *audit*, posto che sia prestata particolare attenzione alla specifica competenza richiesta.

- 2) **Standard internazionali per la pratica professionale dell'internal auditing dell'IIA** (Institute of Internal auditors):2016.

Contengono le indicazioni su come deve essere svolta l'attività di *internal audit* e, in particolare, forniscono un quadro di riferimento per lo sviluppo e l'effettuazione delle attività, definiscono i parametri per la valutazione delle prestazioni e promuovono il miglioramento dei processi organizzativi e operativi.

Gli standard, inoltre, sono dotati di un glossario che fornisce il significato di termini e concetti contenuti nelle definizioni in cui, tra l'altro, si usa il termine "deve" per specificare un requisito assolutamente vincolante e la parola "dovrebbe" per indicare un requisito che può essere invece derogato ove se ne giustifichi il motivo. Negli standard internazionali si distinguono gli standard di connotazione (serie 1000), che riguardano le caratteristiche delle organizzazioni e degli individui che svolgono l'attività di *audit* interno, e gli standard di prestazione (serie 2000), che riguardano la natura e le modalità di svolgimento di tale attività.

Gli standard internazionali vengono periodicamente sottoposti ad un processo di revisione da parte dell'International Auditing Standards Board (iasb).

5.6.5. Standard per la prevenzione della corruzione

- 1) **ISO 37001:2016**, "Anti-bribery management system - Requirements with guidance for use"¹⁹.

Specifica requisiti e fornisce una guida per stabilire, mettere in atto, mantenere, aggiornare e migliorare un sistema di gestione per la prevenzione della corruzione. Il sistema può essere a sé stante o integrato in un sistema di gestione complessivo.

¹⁹ È stata recepita in Italia con la UNI ISO 37001:2016, "Sistemi di gestione per la prevenzione della corruzione - Requisiti e guida all'utilizzo".



6. Il Data protection impact assessment (DPIA)

6.1. Il DPIA come modello giuridico

Secondo il GDPR, quando un tipo di trattamento è caratterizzato da un **rischio elevato per i diritti e le libertà delle persone fisiche**, il Titolare del trattamento in fase di analisi (e quindi prima di procedere al trattamento) – supportato dal Responsabile del trattamento¹ e consultandosi con il DPO, se designato - deve svolgere una specifica attività di *risk management*, la *valutazione d'impatto sulla protezione dei dati*, ormai nota con l'acronimo DPIA (*Data protection impact assessment*)^{2 3}.

Il *rischio elevato* può derivare:

- dall'uso di nuove tecnologie;
- dalla natura, dall'oggetto, dal contesto e dalle finalità del trattamento;
- dai trattamenti di nuovo tipo;
- dai trattamenti iniziati da lungo tempo.

Si tratta, a ben vedere, di fattispecie che comprendono un numero elevato di ipotesi di trattamenti tra le quali il GDPR ne richiama espressamente tre e, cioè, quando sono previsti:

- 1) un monitoraggio sistematico automatizzato – basato sulla profilazione - su aspetti personali sul quale si fondano decisioni che incidono significativamente sugli interessati;
- 2) un trattamento di dati sensibili e giudiziari che interessino un numero elevato di soggetti⁴;
- 3) una sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Alla genericità di queste prescrizioni vengono in soccorso le linee guida del Gruppo "articolo 29"⁵ che fissa 9 criteri – sintetizzati nella Tavola 15 - per individuare i trattamenti di dati personali che possano presentare un rischio elevato

¹ Il considerando 95 prevede che il Responsabile del trattamento - sia d'iniziativa, se ritenuto necessario, sia su richiesta, deve assistere il Titolare del trattamento.

² Cfr. l'art. 35 ed i considerando 84, 89 – 93 e 95 del Regolamento UE.

³ Per un insieme di trattamenti simili, che presentano rischi elevati analoghi, può procedersi con un unico DPIA.

⁴ Non è considerato trattamento su larga scala quello che riguarda dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato per cui, in tali casi, non è obbligatorio procedere al DPIA.

⁵ Cfr. le linee guida WP 248 rev. 01 (versione aggiornata del 4 ottobre 2017) del Gruppo "articolo 29".

per i diritti e le libertà delle persone fisiche e che, pertanto, richiedono obbligatoriamente l'effettuazione del DPIA.

Tavola 15 – Criteri per individuare trattamenti di dati ad alto rischio

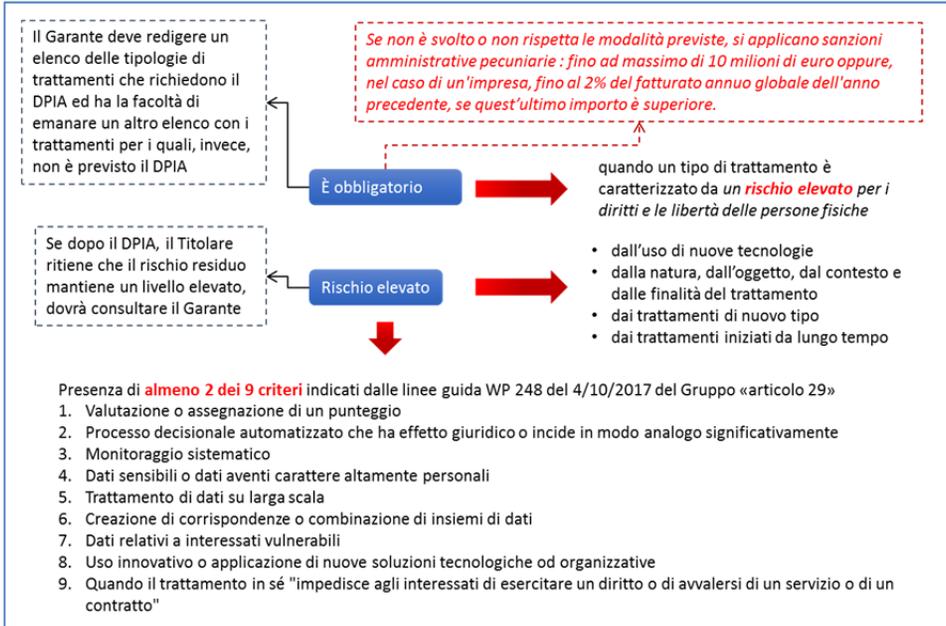
N.	Criterio	Descrizione
1	Valutazione o assegnazione di un punteggio	Il trattamento deve riguardare aspetti quali il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato.
2	Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente	Il criterio non si applica se il trattamento non ha effetto o ha soltanto un effetto limitato sulle persone.
3	Monitoraggio sistematico	È un trattamento utilizzato per osservare, monitorare o controllare gli interessati (es. negli spazi pubblici può essere impossibile per le persone evitare di essere soggette a tale trattamento).
4	Dati sensibili o dati aventi carattere altamente personali	Il trattamento comprende i dati di cui agli artt. 9 e 10 del GDPR e può includere anche documenti personali, messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone.
5	Trattamento di dati su larga scala	Il trattamento è su larga scala in base ai seguenti criteri: <ul style="list-style-type: none"> ● numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; ● il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; ● la durata, ovvero la persistenza, dell'attività di trattamento; ● la portata geografica dell'attività di trattamento.
6	Creazione di corrispondenze o combinazione di insiemi di dati	Trattamento, ad esempio, con dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da Titolari del trattamento diversi.

N.	Criterio	Descrizione
7	Dati relativi a interessati vulnerabili	Gli interessati vulnerabili possono includere i minori, i dipendenti, infermi di mente, richiedenti asilo o anziani, pazienti, ecc. e quando sia possibile individuare uno squilibrio tra la posizione dell'interessato e quella del Titolare del trattamento.
8	Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative	Le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute (es. alcune applicazioni di "Internet delle cose"; combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici).
9	Quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto"	Un esempio di ciò è rappresentato dal caso in cui una banca esamina i suoi clienti rispetto a una banca dati di riferimento per il credito al fine di decidere se offrire loro un prestito o meno.

Per la precisione le linee guida affermano che, in generale, in presenza di due criteri il trattamento dei dati deve essere sottoposto a DPIA ma - viene aggiunto - nei casi dubbi è raccomandato di effettuare comunque la DPIA. A titolo esplicativo, linee guida riportano infine alcuni esempi.

Qualora il DPIA – nei casi in cui sia obbligatorio - non venga svolto o non rispetti le modalità previste, si applicano sanzioni amministrative pecuniarie piuttosto rilevanti: fino ad un massimo di 10 milioni di euro oppure, nel caso di un'impresa, fino al 2% del fatturato annuo globale dell'anno precedente, se quest'ultimo importo è superiore.

Figura 34 – Il modello giuridico del DPIA



Ma cos'è, in particolare, il DPIA?

Il GDPR non ne dà una definizione formale che quindi dobbiamo estrapolare dai riferimenti normativi e dalle linee guida del Gruppo "articolo 29"⁶. In sintesi possiamo considerarlo come un processo che contribuisce a gestire i rischi - per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali - attraverso:

- la descrizione del trattamento, valutandone la necessità e la proporzionalità rispetto alle finalità perseguite dal Titolare (e cioè alle esigenze che intende soddisfare);
- la valutazione dei rischi;
- la individuazione dei presidi di controllo per un'adeguata gestione dei rischi;
- modalità trasparenti che consentano di soddisfare le esigenze di *accountability*: non basta la "compliance" ma occorre anche poterla dimostrare!

⁶ La norma ISO/IEC 29134:2017, Information technology – Security techniques – Guidelines for privacy impact assessment, punto 3.7, definisce il privacy impact assessment come un "processo generale di identificazione, analisi, valutazione, consultazione, comunicazione e pianificazione del trattamento di potenziali impatti sulla privacy in relazione al trattamento di informazioni di identificazione personale, inquadrate all'interno di un più ampio quadro di gestione dei rischi di un'organizzazione".

Nel valutare come Titolari o Responsabili hanno effettuato il DPIA – e cioè la qualità del processo – deve tenersi conto anche se sono stati rispettati i codici di condotta approvati, di cui all'articolo 40 del GDPR.

È infine previsto che il DPIA venga nuovamente eseguito ogni qualvolta vi siano variazioni del tipo e del livello di rischio (ad esempio, a causa di modifiche delle attività di trattamento).

In ogni caso, il DPIA non si applica per i trattamenti connessi ad obblighi legali ed ai pubblici poteri che siano già disciplinati dalla normativa comunitaria o nazionale, salvo diversa volontà del singolo Stato⁷.

Per la PA

In generale, la valutazione d'impatto sulla protezione dei dati non si applica ai trattamenti connessi ad obblighi legali ed ai pubblici poteri che siano già disciplinati dalla normativa comunitaria o nazionale.

Deve infine sottolinearsi come il DPIA costituisca anche uno degli ambiti in cui il ruolo dell'autorità Garante nazionale è particolarmente significativo. Egli infatti deve redigere e rendere pubblico un elenco delle tipologie di trattamenti che richiedono il DPIA ed ha la facoltà di emanare un altro elenco con i trattamenti per i quali, invece, non è previsto il DPIA⁸.

6.2. Il DPIA come processo “ordinario” di risk management

Nell'ambito della progettazione del trattamento dei dati, come abbiamo anticipato nel precedente capitolo 5, paragrafo 5.2, risulta indispensabile definire un processo per valutare e gestire il rischio.

Abbiamo anche visto come il GDPR preveda uno specifico processo, il DPIA che, però, risulta obbligatorio solo quando un tipo di trattamento “*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*”.

Ma come posso stabilire se un rischio sia o meno elevato se non lo valuto (e cioè se non attivo un processo di *risk assessment*)?

⁷ Cfr. anche le già citate linee guida WP 248 che enumerano cinque casi in cui il DPIA non è richiesto: trattamento che non presenta un rischio elevato; trattamento simile ad un altro per il quale è stato svolto il DPIA; trattamenti ante GDPR già verificati da autorità Garante nazionale; trattamenti connessi ad obblighi legali ed ai pubblici poteri; trattamento incluso nell'elenco facoltativo dell'autorità Garante nazionale.

⁸ Se i trattamenti sono finalizzati all'offerta di beni o servizi a interessati stabiliti in più Stati membri oppure se le attività possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'UE, l'autorità Garante attiva il Comitato per ottenere un parere preventivo.

In realtà, quindi, ogni trattamento richiede una valutazione del rischio inerente al trattamento, da intendersi come il rischio di impatti negativi sulle libertà e sui diritti degli interessati.

In particolare occorre analizzare tutti gli impatti negativi, che possono derivare dai rischi da trattamento, attraverso un apposito processo di valutazione che tenga conto delle minacce, delle vulnerabilità e delle misure tecniche e organizzative che devono essere adottate per mitigare tali rischi.

All'esito di questa valutazione di impatto il Titolare del trattamento – a cui fa capo l'intera attività - deciderà se iniziare o meno il trattamento oppure, se ritiene che il rischio residuo mantiene un livello elevato, dovrà consultare l'autorità Garante nazionale che fornirà indicazioni su come gestire il rischio oppure potrà esercitare i poteri di indagine, correttivi, autorizzativi e consultivi previsti dall'art. 50 del GDPR.

In definitiva appare, pertanto, indispensabile che per ogni trattamento (o gruppi di trattamenti simili con rischi analoghi) debba sempre essere eseguito un processo di *risk management*.

Tale processo è condotto, come già precisato, dal Titolare del trattamento che:

- è responsabile dell'esecuzione del DPIA, indipendentemente dal fatto che venga in concreto effettuato da un altro soggetto;
- se il DPO è stato nominato, deve consultarsi con lui (il suo parere va acquisito nella documentazione del DPIA), il quale deve anche sorvegliare lo svolgimento del DPIA;
- può far eseguire il DPIA, anche in parte, dal Responsabile del trattamento.

Per ragioni di coerenza logica e metodologica si ritiene, in conclusione, che il processo di *risk management* dovrebbe essere sempre condotto, per tutti i tipi di trattamento, ed identificarsi con il DPIA.

In sostanza, per la gestione del rischio da trattamento dovrebbe essere adottato il modello del DPIA⁹ applicandolo in via generalizzata a tutti i trattamenti, fermo restando che le conseguenze giuridiche direttamente connesse alla sua mancata adozione rimarranno circoscritte ai soli casi in cui la sua obbligatorietà è espressamente sancita dal GDPR.

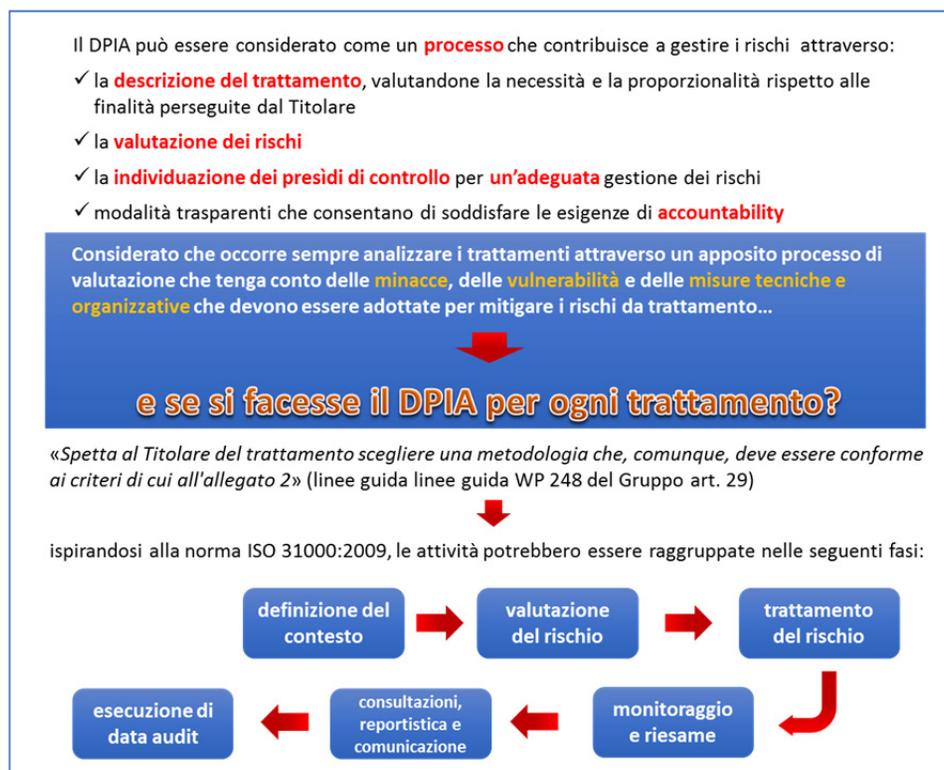
In quest'ottica il DPIA può quindi considerarsi come un processo che si sviluppa attraverso una sequenza strutturata di attività che, prendendo spunto dagli standard internazionali - ed in particolare dalla norma ISO 31000:2009 - potremmo raggruppare nelle seguenti fasi:

- 1) definizione del contesto;

⁹ L'autorità Garante francese (CNIL) mette a disposizione un software *open source*, in francese, in inglese e in spagnolo (altre traduzioni sono in corso di sviluppo), basato sul metodo EBIOS di gestione dei rischi pubblicato dall'ANSSI, in conformità con le linee guide del G29 e compatibile con la norma ISO 31000: <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment>.

- 2) valutazione del rischio;
- 3) trattamento del rischio;
- 4) consultazioni, reportistica e comunicazione;
- 5) monitoraggio e riesame;
- 6) esecuzione di *data audit*.

Figura 35 – Una concezione “operativa” del DPIA



Deve peraltro evidenziarsi – come evidenziato nella Figura 35 - che, secondo le linee guida linee guida WP 248, “spetta al Titolare del trattamento scegliere una metodologia che, comunque, deve essere conforme ai criteri di cui all'allegato 2, riportato nella Figura 36.

Figura 36 – Criteri per la validità di un DPIA

Allegato 2 - Criteri per una valutazione d'impatto sulla protezione dei dati accettabile

Il WP29 propone i seguenti criteri che i titolari del trattamento possono utilizzare per stabilire se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno oppure se una metodologia per lo svolgimento di una tale valutazione sia sufficientemente completa per garantire il rispetto del regolamento generale sulla protezione dei dati:

- una descrizione sistematica del trattamento è fornita (articolo 35, paragrafo 7, lettera a)):
 - la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90);
 - vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;
 - viene fornita una descrizione funzionale del trattamento;
 - sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);
 - si tiene conto del rispetto dei codici di condotta approvati (articolo 35, paragrafo 8);
- la necessità e la proporzionalità sono valutate (articolo 35, paragrafo 7, lettera b)):
 - sono state determinate le misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90):
 - misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:
 - finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b));
 - liceità del trattamento (articolo 6);
 - dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c));
 - limitazione della conservazione (articolo 5, paragrafo 1, lettera e));
 - misure che contribuiscono ai diritti degli interessati:
 - informazioni fornite all'interessato (articoli 12, 13 e 14);
 - diritto di accesso e portabilità dei dati (articoli 15 e 20);
 - diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);
 - diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);
 - rapporti con i responsabili del trattamento (articolo 28);
 - garanzie riguardanti trattamenti internazionali (capo V);
 - consultazione preventiva (articolo 36).
- i rischi per i diritti e le libertà degli interessati sono gestiti (articolo 35, paragrafo 7 lettera c)):
 - l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:
 - si considerano le fonti di rischio (considerando 90);
 - sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
 - sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;
 - sono stimate la probabilità e la gravità (considerando 90);
 - sono determinate le misure previste per gestire tali rischi (articolo 35, paragrafo 7, lettera d) e considerando 90);
- le parti interessate sono coinvolte:
 - si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2);
 - si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (articolo 35, paragrafo 9).

6.3. Definizione del contesto

6.3.1. Il contesto esterno ed interno

La definizione del contesto risulta fondamentale per individuare i parametri da tenere in considerazione per la valutazione e la gestione del rischio.

Per il rischio da trattamento, l'organizzazione è condizionata dal contesto esterno soprattutto, ad esempio, in relazione agli aspetti normativi nazionali e comunitari nonché alle tecnologie che impattano sulle infrastrutture informatiche.

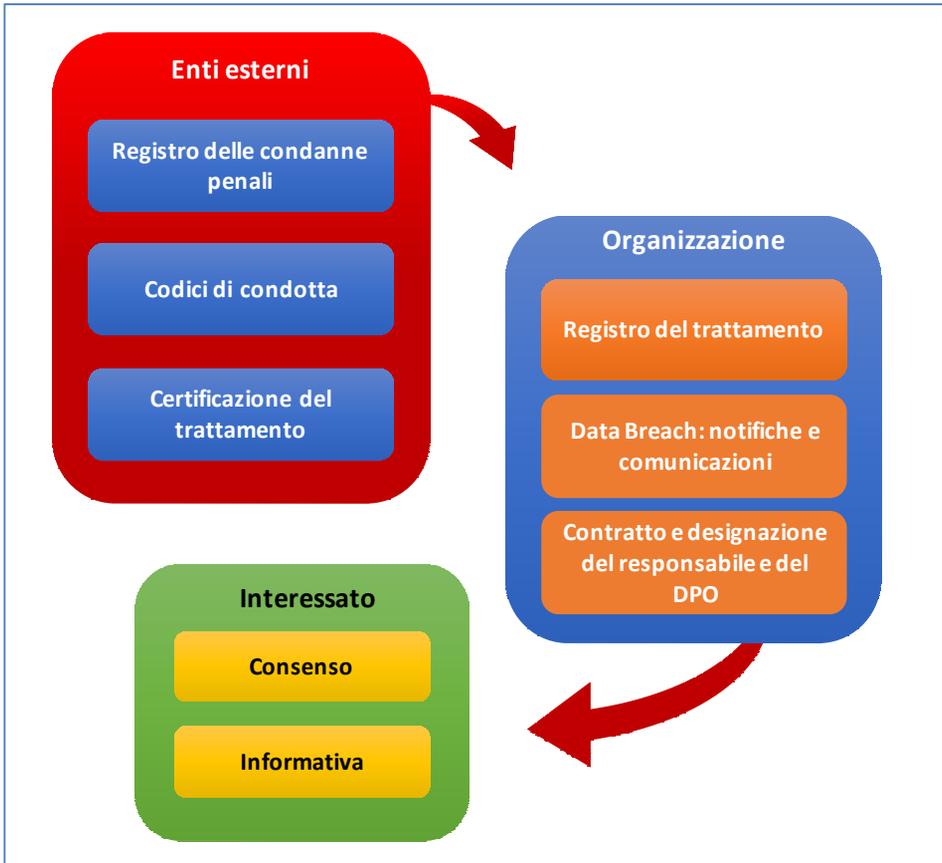
Il contesto interno, invece, riguarda innanzitutto la struttura organizzativa, la mappatura dei processi, la redazione e la tenuta dei vari documenti previsti (tra i quali assume particolare rilevanza il registro dei trattamenti, che abbiamo analizzato nel capitolo precedente).

Al termine della fase della "definizione del contesto" dovranno risultare definiti i *risk criteria* ed il programma esecutivo per la fase successiva di *risk assessment*.

6.3.2. I documenti

Il GDPR prevede una serie di documenti – richiamati dalla Figura 37 - di estremo rilievo per ogni organizzazione, sia quali componenti indispensabili per la costruzione e la gestione di un efficace modello di *data protection* che per le responsabilità che alcuni di essi possono determinare.

Figura 37 – Gli output documentali del GDPR



Si tratta in sostanza della documentazione derivante dalle diverse disposizioni contenute nel Regolamento UE, descritte ed esaminate nei vari capitoli del libro,

che comunque concorrono a determinare il contesto interno di ogni organizzazione.

6.3.3. I risk criteria

Abbiamo visto che tra gli *output* della fase di definizione del contesto assumono fondamentale importanza i *risk criteria*, e cioè i criteri che l'organizzazione deve definire per valutare la significatività dei rischi.

Essi devono essere fissati all'inizio di qualsiasi processo di gestione del rischio e sottoposti ad un continuo riesame.

In generale possono distinguersi in *criteri obbligatori*, e cioè derivanti da normative giuridiche, e in *criteri autonomi*, fissati dall'organizzazione sulla base della propria politica di gestione del rischio definita in base al contesto, ai propri valori, agli obiettivi ed alle risorse disponibili.

I *criteri autonomi* di maggior rilievo sono le modalità da utilizzare per misurare il livello di rischio, ossia la combinazione tra la probabilità di un evento e le relative conseguenze.

I *risk criteria* comprendono anche il *risk appetite*, e cioè il livello di rischio che l'organizzazione è disposta ad accettare o tollerare.

Nella protezione dei dati personali – rispetto ad altri ambiti – risultano particolarmente significativi i *risk criteria* di tipo obbligatorio in quanto l'intera materia è soggetta a misure eteronome cogenti a cui ogni organizzazione è tenuta ad uniformarsi.

6.3.4. segue: i criteri per la misurazione del livello del rischio

I *risk criteria* di natura autonoma comprendono anche le modalità di misurazione dei rischi che verranno poi valutati e, eventualmente, trattati.

I metodi che possono essere utilizzati per questo tipo di operazione sono suddivisi in tre categorie: quantitativi, qualitativi e semi-quantitativi.

Quello più diffuso, per economicità e semplicità di implementazione, è di tipo qualitativo e consiste nella matrice probabilità/impatto – rappresentata nella Figura 38 – che fornisce una stima del livello di rischio in relazione alla combinazione di due elementi: la probabilità di accadimento dell'evento rischioso e la gravità delle conseguenze sugli obiettivi.

Il livello del rischio, e quindi la probabilità e la gravità del rischio, deve essere determinato¹⁰ con riguardo:

- alla natura;
- all'ambito di applicazione;
- al contesto;
- alle finalità del trattamento.

¹⁰ Cfr. il considerando 76 del Regolamento UE.

Figura 38 – Matrice probabilità/impatto

		Probabilità				
		Raro	Poco Probabile	Probabile	Molto probabile	Quasi certo
Impatto	Catastrofico	5	10	15	25	25
	Grave	4	8	12	16	20
	Medio	3	6	9	12	15
	Moderato	2	4	6	8	10
	Trascurabile	1	2	3	4	5

Tabella impatto	
Valore	Livello
5	Catastrofico
4	Grave
3	Medio
2	Moderato
1	Trascurabile

Tabella probabilità	
Valore	Livello
5	Quasi certo
4	Molto probabile
3	Probabile
2	Poco probabile
1	Raro

Livello rischio	
Rischio alto	$R > 10$
Rischio medio	$5 \leq R \leq 10$
Rischio basso	$R < 5$

6.4. La valutazione del rischio

La valutazione del rischio comprende le attività rivolte a identificare, analizzare e stabilire quali siano i rischi "accettabili" in relazione ai presidi di controllo già in atto o previsti e ai *risk criteria* definiti nella precedente fase di analisi del contesto e quali, invece, siano da trattare¹¹.

Questa fase si suddivide in tre momenti: l'identificazione del rischio, l'analisi del rischio e la ponderazione del rischio.

L'*identificazione del rischio*, in sostanza, comporta la redazione di una vera e propria tassonomia dei rischi riferita a tutti i trattamenti di dati personali indicati nei registri di cui all'art. 30 del GDPR, "mappandoli" anche nell'ambito dei processi organizzativi e delle unità organizzative.

¹¹ Secondo il considerando 90 del Regolamento UE "è opportuno che il Titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio. La valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio assicurando la protezione dei dati personali e dimostrando la conformità al presente regolamento".

Figura 39 – Rischi più comuni



L'*analisi del rischio*, invece, consiste nel rilevare gli attributi del rischio (fonti di rischio, minacce, vulnerabilità), i presidi di controllo e nel misurare il livello del rischio inerente e residuo (e cioè il rischio misurato prima e dopo l'attuazione dei presidi di controllo)¹².

In particolare, tale attività richiede che per ciascun trattamento (o categoria di trattamento) vengano in particolare verificate le condizioni che assicurano la liceità del trattamento e, quindi, la sua necessità e proporzionalità attraverso l'esame dei seguenti elementi:

- l'indicazione di finalità determinate, esplicite e legittime;
- l'impiego di dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità e alle modalità con cui il Titolare assicura l'accuratezza dei dati;
- la limitazione della conservazione ad un arco di tempo non superiore al conseguimento delle finalità;
- il presupposto di legittimità del trattamento (es: consenso, obbligo legale, legittimo interesse del Titolare e così via).

I trattamenti identificati vengono quindi presi in esame, analizzandone il ciclo di vita e prendendo in considerazione le tecnologie impiegate e i soggetti autorizzati a trattarli.

¹² Il considerando 84 precisa che il Titolare deve "determinare, in particolare, l'origine, la natura, la particolarità e la gravità" del rischio per determinare "le misure da adottare per dimostrare che il trattamento dei dati personali rispetta" il Regolamento UE.

Successivamente, in primo luogo devono essere ricercate le possibili fonti di rischio, riferite innanzitutto al mancato rispetto del GDPR (violazione dei diritti degli interessati, ecc.) ed alla violazione dei dati personali (accessi non autorizzati, alterazione, perdita o distruzione dei dati, sottrazione delle credenziali, *virus* informatici, sottrazione di strumenti contenenti dati, eventi distruttivi naturali o artificiali, ecc.).

In secondo luogo sono valutate le probabilità con cui tali rischi potrebbero realizzarsi e l'impatto qualora si dovessero realizzare, assegnando per ciascun rischio individuato un livello di probabilità di realizzazione e un grado di potenziale impatto. Si tratta della valutazione della magnitudo o del livello del rischio inerente.

Infine si valutano i presidi di controlli, ossia le misure di mitigazione e, conseguentemente, si misura la magnitudo del rischio residuo.

Tale analisi può determinare l'esigenza di aggiornare il sistema dei presidi di controllo in relazione ad alcune situazioni di rischio emerse (ad esempio l'introduzione di una nuova disposizione giuridica imporrà l'adeguamento normativo per rimuovere il rischio).

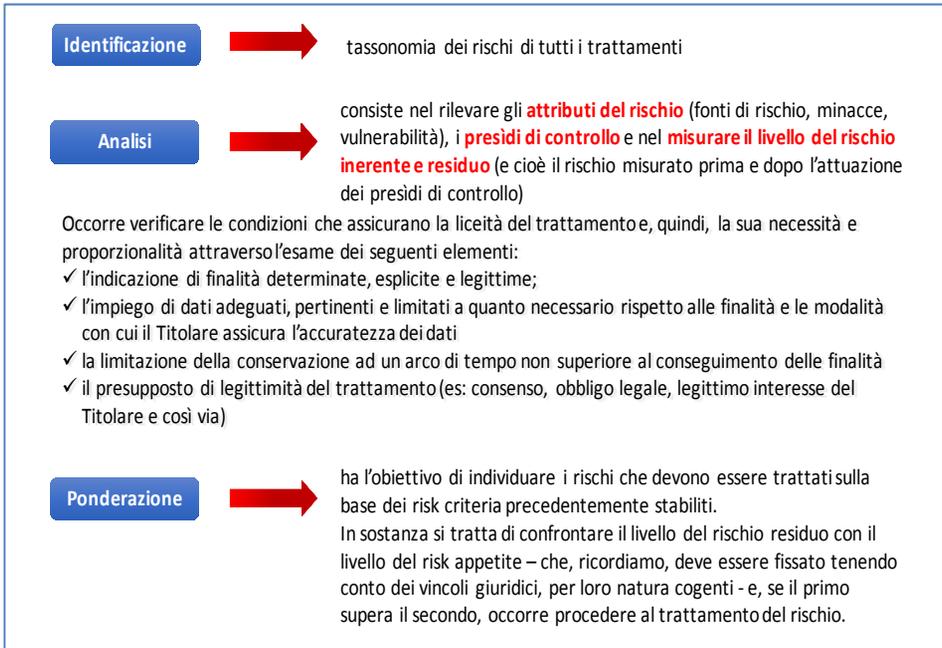
Indipendentemente dalla effettiva rilevanza del rischio, emersa dalla sua analisi, deve evidenziarsi che esistono dei trattamenti di dati personali che si presumono comunque legati a rischi di livello elevato.

Ci si riferisce ai trattamenti per i quali la DPIA è obbligatoria, come precisato nel paragrafo 6.1 e nella Tavola 15, dedicata ai criteri guida.

La terza tipologia di attività, la *ponderazione del rischio*, ha l'obiettivo di individuare i rischi che devono essere trattati sulla base dei *risk criteria* precedentemente stabiliti. In sostanza si tratta di confrontare il livello del rischio residuo con il livello del *risk appetite* – che, ricordiamo, deve essere fissato tenendo conto dei vincoli giuridici, per loro natura cogenti - e, se il primo supera il secondo, occorre procedere al trattamento del rischio.

La Figura 40 riassume l'intera fase della valutazione del rischio.

Figura 40 – La fase della valutazione del rischio



6.5. Il trattamento del rischio: l'opzione della "mitigazione del rischio"

6.5.1. Le opzioni del risk treatment

La fase di trattamento del rischio ha come *output* il "come" gestire i rischi che, attraverso la fase precedente, è stato stabilito di dover trattare. In generale, le opzioni sono le seguenti¹³:

- 1) mitigare il rischio (modificare la probabilità e/o le conseguenze);
- 2) accettare, anche in parte, il rischio;
- 3) evitare il rischio, decidendo di non avviare o non continuare l'attività che comporta l'insorgere del rischio;
- 4) condividere o trasferire il rischio (ad es. con un contratto di assicurazione)¹⁴.

¹³ Cfr. la norma ISO/IEC 27000:2016, punto 3.5.4.

¹⁴ Secondo linee guida WP 248 rev. 01 (versione aggiornata del 4 ottobre 2017) del Gruppo "articolo 29", "I Titolari del trattamento non possono sottrarsi alla loro responsabilità coprendo i rischi stipulando polizze assicurative" (pag. 6, nota 10).

Il trattamento del rischio si svolge attraverso un processo circolare articolato nelle seguenti fasi:

- attuazione dell'opzione di trattamento del rischio;
- valutazione del trattamento del rischio;
- decisione circa la tollerabilità del livello di rischio residuo;
- e, se il livello di rischio non è ritenuto tollerabile:
- nuovo trattamento del rischio;
- valutazione dell'efficacia di tale trattamento.

Nell'affrontare l'argomento, si limiterà l'approfondimento alla sola opzione della "mitigazione del rischio", ritenendo che le ulteriori opzioni non diano luogo a particolari problemi interpretativi ed applicativi.

6.5.2. La mitigazione del rischio

La mitigazione del rischio rappresenta l'opzione attraverso la quale il Titolare del trattamento interviene con specifici presidi di controllo in grado di ridurre la magnitudo, e cioè il livello del rischio.

Il presupposto è costituito dalla fase di *valutazione del rischio*, e specificamente dalla *ponderazione del rischio*, facendo riferimento ai *risk criteria*, già esaminati nel paragrafo 6.3 - che sono i criteri che l'organizzazione ha preventivamente definito per valutare la significatività dei rischi - e, in particolare, al *risk appetite*, o propensione al rischio, e cioè al livello di rischio, e quindi all'impatto negativo, che l'organizzazione ha preventivamente stabilito di essere disposta a tollerare.

Una volta stabilito che il rischio non è accettabile e che, pertanto, va mitigato, si procede alla scelta dei presidi di controllo (detti anche semplicemente "controlli") da attuare per rendere accettabile il livello di rischio.

Ma se al termine della fase di mitigazione del rischio, il livello rimane superiore alla soglia del *risk appetite* (e dei *risk criteria* in generale) cosa succede?

In generale, secondo le prassi utilizzate nel *risk management*, in questo caso il rischio viene nuovamente trattato con ulteriori controlli a meno che il vertice dell'organizzazione stabilisca di accettare comunque il livello del rischio residuo: questa disponibilità ad accettare il rischio è definita *risk tolerance*.

La determinazione del *risk tolerance* dipende soprattutto dal bilanciamento tra costi/sforzi di attuazione e benefici, nonché da altri fattori, quali, il mix conseguenze/probabilità (ad esempio i rischi con elevate conseguenze negative ma con bassa probabilità vengono maggiormente accettati rispetto a quelli con basse conseguenze ed alte probabilità).

Tuttavia, il *risk tolerance* risulta molto modesto, se non inesistente, quando si confronta con esigenze di *compliance* normativa - come nel caso, appunto, della protezione dei dati personali) e di impegno sociale (responsabilità sociale, protezione dell'ambiente, ecc.).

Nel *data protection*, in particolare, è previsto uno specifico meccanismo nel caso in cui il rischio non sia riportato ad un livello inferiore rispetto al *risk appetite*.

Si tratta della *consultazione preventiva*, da parte del Titolare del trattamento, dell'autorità Garante nazionale che gli fornisce un parere scritto e può avvalersi dei poteri di cui all'articolo 58 del GDPR, come vedremo in dettaglio nel paragrafo 6.5.4.

Ne consegue che, tranne il caso in cui l'autorità Garante eserciti poteri inibitori o conformativi, il Titolare del trattamento continuerà ad avere l'esclusiva competenza sulle misure da adottare per il trattamento del rischio e, pertanto, a lui faranno anche capo le relative eventuali responsabilità giuridiche per le quali si terrà conto dell'adeguamento o meno al parere ricevuto.

6.5.3. I presidi di controllo. Misure "organizzative" vs misure "tecnologiche"

I presidi di controllo (o semplicemente *controlli*) sono tutte le misure utili a mitigare il rischio, e cioè a "trattarlo".

Esse costituiscono, sostanzialmente, l'*output* principale del sistema *Data protection by default* e cioè di tutta quell'attività di *risk management* descritta in questo capitolo ed in quello precedente.

Al riguardo, infatti, viene costantemente ribadito che tali misure vanno progettate per poter poi essere *calate* nella realtà organizzativa e, pertanto, in primo luogo devono essere "personalizzate".

In ogni caso, nello scegliere e poi applicare queste misure dovranno prendersi in considerazione sia i rischi "patologici" incombenti sui dati personali oggetto di trattamento – cioè, in sostanza, i gradi di severità e di probabilità che si verifichino le "violazioni dei dati" definite all'art. 4 GDPR ("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") – che i rischi per i diritti e le libertà delle persone fisiche.

Queste misure si sviluppano attraverso due dimensioni.

La prima è quella strategica che comprende le *politiche* del Titolare sul *data protection*¹⁵ che consistono in indicazioni di alto livello utili per orientare le decisioni e le iniziative di dettaglio.

La seconda dimensione è quella gestionale in cui agiscono le *procedure operative* e, cioè, le misure organizzative e tecnologiche vere e proprie, ispirate, appunto, alle politiche.

A titolo esemplificativo si riportano alcune di queste misure¹⁶:

- misure di sicurezze fisiche (misure di protezione di aree ed apparecchiature, ecc.);
- misure di sicurezza logiche (*backup*, piano di *disaster recovery*, ecc.);

¹⁵ Cfr. l'art. 24 e Considerando 78.

¹⁶ Cfr. anche gli artt. 25 e 32 ed il considerando 78 e 83 del Regolamento UE.

- la tempestiva pseudonimizzazione dei dati personali (e cioè impedire l'associazione dei dati ad un determinato interessato);
- la cifratura dei dati;
- la riduzione al minimo dei dati personali da trattare;
- la trasparenza per quanto riguarda le funzioni e il trattamento di dati personali;
- la possibilità per l'interessato di controllare il trattamento dei dati fornendo anche indicazioni sulle procedure;
- l'indicazione dei soggetti a cui rivolgersi per ottenere informazioni o per esercitare i propri diritti;
- tenere conto delle migliori pratiche in materia di trattamento dei dati fin dalle fasi di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati appunto su tale trattamento o che trattano dati personali per svolgere le loro funzioni;
- chiara ripartizione delle competenze tra il Titolare ed il Responsabile del trattamento;
- previsione di procedure volte a testare, verificare e valutare l'efficacia delle misure adottate.

Tra queste misure assume particolare rilievo anche il *data protection by default*, e cioè quei provvedimenti che limitano il trattamento, *per impostazione predefinita*, ai soli dati personali necessari, limitazione che si riferisce espressamente alla quantità dei dati personali raccolti, alla portata del trattamento, al periodo di conservazione e all'accessibilità.

Ma c'è una differenza reale tra l'efficacia delle misure organizzative e quelle tecnologiche?

Sì, senza ombra di dubbio, ed è anche abissale!

La Figura 41 pone a confronto queste misure, indicandone le caratteristiche principali.

Ma allora, perché non sono adeguatamente utilizzati i controlli tecnologici se sono così efficaci? La risposta rinvia al contesto organizzativo. La preconditione, infatti, è che esso sia evoluto, e cioè che esistano la mappatura e la formalizzazione di processi e procedure, approcci ingegneristici, competenze informatiche, tutti elementi che sono in grado di assicurare adeguati controlli sistematici su gran parte delle attività.

Figura 41 – Misure organizzative e misure tecnologiche

Misure organizzative	Misure tecnologiche
<p>Le misure organizzative sono attività manuali di tipo tradizionale che si basano, in genere, su disposizioni contenute in circolari, direttive, linee guida, ecc.</p> <p>Sono misure talvolta superate ed evidenziano criticità rilevabili anche nella dirigenza: non si conoscono le banche dati della propria organizzazione, non si sanno analizzare i processi, non si propongono adeguate azioni migliorative che, nella quasi totalità dei casi, presuppongono invece <i>routine</i> informatizzate.</p> <p>A volte, purtroppo, si traducono nel «suggerire» al <i>process owner</i> controlli che si basano su esperienze datate, quali doppie e triple firme su documenti predisposti per i controlli delle attività “a rischio” anziché su controlli automatizzati in grado in tempo reale, di bloccare le procedure, o di attivare specifiche segnalazioni, in presenza di situazioni anomale preventivamente individuate e di tracciare, storicizzandole, le operazioni compiute imputandole a chi le ha effettuate.</p>	<p>Richiedono un’organizzazione evoluta, e cioè che disponga della mappatura e formalizzazione di processi e procedure, di approcci ingegneristici, di competenze informatiche, ecc.</p> <p>Esempi di controlli automatizzati, cioè <i>system based</i>:</p> <ul style="list-style-type: none"> • sistemi di identificazione e di autorizzazione, attraverso i cosiddetti privilegi, per l’uso delle risorse informatiche • attività di logging (per il tracciamento delle operazioni e per la rilevazione di anomalie, delle statistiche di esercizio eccetera) • data entry “guidati” • inibizioni automatiche alle procedure in caso di eventi predeterminati • indicatori di rischio • indicatori di anomalia (<i>alert</i>)

6.5.4. Consultazione preventiva

Come abbiamo visto, nell’ambito della fase del trattamento del rischio – rispetto a quanto previsto nella norma ISO 31000:2009 – l’art. 36 del GDPR prevede uno specifico meccanismo che consiste nella consultazione preventiva dell’autorità Garante nazionale, da parte del Titolare del trattamento, qualora a seguito del DPIA – nei casi in cui sia obbligatorio – risulti che il trattamento continuerebbe a presentare un rischio elevato e cioè “*non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e costi di attuazione*”¹⁷.

In sostanza “ogniquale volta il Titolare del trattamento non è in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile (ossia i rischi residui restano comunque elevati) è necessario consultare l’autorità di controllo”¹⁸.

Tuttavia, per i trattamenti riferiti all’esecuzione di un compito di interesse pubblico, tra cui quelli connessi alla protezione sociale e alla sanità pubblica, la normativa nazionale può prescrivere che i Titolari del trattamento consultino comunque l’autorità Garante nazionale e ne ottengano l’autorizzazione preliminare.

¹⁷ Cfr. l’art. 36 ed i considerando 94-96 del Regolamento UE.

¹⁸ Cfr. pag. 23 delle Linee guida del Gruppo “Articolo 29” WP 248 rev.01, aggiornate al 4 ottobre 2017, in materia di valutazione d’impatto sulla protezione dei dati.

Per la PA

Lo Stato membro può prescrivere al Titolare – in presenza di rischi elevati - l'obbligo dell'autorizzazione preliminare dell'autorità Garante nazionale per i trattamenti necessari per l'esecuzione di un compito di interesse pubblico

- le responsabilità del Titolare, dei contitolari e dei Responsabili del trattamento;
- le finalità e i mezzi del trattamento previsto;
- le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati;
- i dati di contatto del Titolare della protezione dei dati;
- la valutazione d'impatto sulla protezione dei dati.

Dopo aver ricevuto la richiesta di consultazione, l'autorità Garante nazionale provvede a:

- fornire al Titolare (ed eventualmente anche al Responsabile del trattamento) un parere scritto entro otto settimane, prorogabili di ulteriori sei settimane in relazione alla complessità del trattamento;
- avvalersi, se lo ritiene, dei poteri di cui all'articolo 58, e cioè di poteri d'indagine, correttivi, autorizzativi e consuntivi.

In termini generali, il meccanismo della consultazione preventiva lascia al Titolare del trattamento la competenza di individuare ed attuare i presidi di controllo, ferma restando l'incidenza del suo mancato adeguamento al parere dell'autorità Garante sulla valutazione di sue eventuali responsabilità in relazione a possibili violazioni del GDPR e danni causati dal trattamento.

Al riguardo, tuttavia, si registrano due eccezioni e, cioè, quando l'autorità Garante ritiene di vietare il trattamento o di imporre determinate modalità nonché quando, a seguito della consultazione, debba rilasciare anche l'autorizzazione preliminare, e cioè nei casi in cui il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

Occorre infine rammentare l'obbligo di conservare la documentazione della valutazione d'impatto sulla protezione dei dati e di ogni aggiornamento.

6.6. Consultazioni, reportistica e comunicazione

Nel corso del processo di valutazione d'impatto possono essere raccolte le opinioni degli interessati o dei loro rappresentanti (es. dipendenti o sindacati)¹⁹.

Queste *consultazioni* risultano opportune affinché possa essere garantita una visione complessiva del processo conferendo altresì trasparenza alle modalità di svolgimento di tale attività.

Le consultazioni dovrebbero avvenire non solo all'interno dell'organizzazione del Titolare ma – auspicabilmente – anche all'esterno coinvolgendo le altre organizzazioni o terze parti con cui il Titolare condivide i dati.

Le modalità di consultazione sono lasciate alla discrezionalità del Titolare del trattamento che potrà decidere, ad esempio, se avvalersi di specifici questionari ovvero organizzare incontri, sessioni e gruppi di lavoro.

Speculare a questa esigenza è quella di fornire un feedback all'esterno, soddisfacendo così due esigenze:

- realizzare l'*accountability*, e cioè il dar conto del cosa è stato fatto e come;
- acquisire consapevolezza sulla situazione analizzata.

Lo strumento da utilizzare è quello della *reportistica* che costituisce, tra l'altro, la premessa indispensabile per porre in essere, se necessario, adeguati interventi correttivi. Nella prassi, troppo spesso, questo strumento è però assente o mal costruito con aggregazioni poco significative di dati e, quindi, con *output* con scarso valore informativo.

Tra i vari *report*, quello che assume importanza primaria è il *report finale* che rappresenta il momento di rendicontazione delle attività svolte, in cui le informazioni precedentemente raccolte e analizzate vengono presentate in maniera sistematica e funzionale unitamente alle misure e ai rimedi elaborati e da implementare per contrastare i rischi emersi.

Oltre alle informazioni raccolte nelle precedenti fasi, il *report* dovrà in ogni caso indicare:

- i componenti del *team* che ha svolto la valutazione d'impatto, unitamente ai dati di contatto di un referente;
- i soggetti consultati e l'esito delle consultazioni;
- le misure e i rimedi volti a mitigare i rischi individuati.

Pur non esistendo un obbligo di pubblicare il DPIA, si ritiene opportuno farlo per dare concretezza – come abbiamo più volte precisato - ai principi di trasparenza e di *accountability* affermati nel GDPR.

Ciò, peraltro, è suggerito dalle linee guida WP 248, in particolare per le organizzazioni il cui trattamento di dati riguarda la generalità dei consociati (ad esempio, le autorità pubbliche), ma rappresenta ad ogni modo una buona prassi per tutte le organizzazioni.

¹⁹ Cfr. l'art. 35, paragrafo 9, del Regolamento UE.

Per la PA

È consigliata la pubblicazione del report della DPIA (o di un suo estratto) per valorizzare in ambito pubblico i principi di trasparenza ed *accountability*.

Passiamo ora alla comunicazione ed alla sua rilevanza strategica.

Deve innanzitutto considerarsi che anche la DPIA, come tutte le attività di verifica, in quanto invasiva e suscettibile di determinare conseguenze premiali o sanzionatorie, può essere vista, soprattutto nella sua fase iniziale, con una certa prevenzione.

Per favorire un clima di fiducia e reciproca collaborazione, la comunicazione è fondamentale!

La DPIA, sotto certi aspetti, può essere rappresentata come un insieme di flussi comunicativi che si sviluppano tra il sistema di *data protection* e gli altri soggetti dell'organizzazione.

Tali flussi si caratterizzano anche per i canali di comunicazione utilizzati che possiamo distinguere, fundamentalmente, in relazione al fatto che si basino o meno su un'interazione personale.

Il primo caso è sicuramente più complesso perché entrano in gioco, oltre ai contenuti, anche le relazioni umane con i conseguenti impatti.

In queste dinamiche, diversamente da quanto in genere si ritiene, la posizione più delicata è quella dell'ascolto in quanto è concreto il rischio di concentrarci soprattutto su ciò che dobbiamo dire precludendoci, pertanto, la possibilità di conoscere cosa gli altri hanno da dirci e i loro punti di vista.

Quando ciò accade, si verificano problemi e malintesi e, quindi, occorre evitare atti che condizionino i flussi di comunicazione come, ad esempio, finire le frasi altrui, interrompere spesso, monopolizzare la conversazione, "ascoltare" quello che si sta pensando anziché quello che dice l'interlocutore.

Un altro aspetto attiene alla necessità di saper utilizzare la comunicazione verbale, non verbale e gli stili linguistici.

Si tratta di dimensioni molto distanti tra di loro, in quanto ognuna di esse ha caratteristiche proprie.

In genere la modalità più difficile da gestire è la comunicazione non verbale che utilizziamo in maniera non sempre consapevole. Essa è costituita da una serie di elementi, quali:

- la prossemica (la disciplina che studia lo spazio e le distanze all'interno di una comunicazione, sia verbale che non verbale);
- la cinesica che riguarda i movimenti ed i gesti (es. un arricciamento del naso, sollevarsi sui talloni, alzare il pollice per dire "va bene!", annuire ve-

locemente e ripetutamente lasciando intendere: "muoviti che voglio prendere la parola!");

- la paralinguistica e, cioè, l'insieme dei suoni emessi nella comunicazione verbale, indipendentemente dal significato delle parole (il tono, la frequenza, il ritmo, il silenzio);
- gli artefatti (uso di oggetti, abbigliamento, codici relazionali, ecc.).

Prima di concludere questi cenni sulla comunicazione, riteniamo utile analizzare, nei loro tratti essenziali, due fondamentali strumenti di comunicazione: la riunione e l'intervista.

Con questi due strumenti sono veicolati contenuti empatici ed informativi e la loro principale criticità è riferita al fatto che viene ignorata la prima tipologia di contenuti - quella empatica - dimenticando che ogni attività comunicativa poggia non solo su una dimensione informativa ma anche, seppur in maniera meno palese, su una relazionale.

È facile poter rilevare, ad esempio, come numerose riunioni diventino interminabili, nonostante una soluzione accettata da tutti sia stata raggiunta in poco tempo, a causa di interventi ripetitivi e pretestuosi finalizzati, da parte di chi li effettua, a cercare di acquisire la paternità della decisione finale, a dimostrazione che per costoro il problema più impellente sia quello dell'autoaffermazione.

In molti altri casi, è altrettanto agevole constatare come non sia possibile giungere ad un accordo a causa di motivi personali (antipatia, risentimenti pregressi, mancato rispetto dello *status* degli interlocutori) più che per disaccordi su aspetti sostanziali.

Un approccio strutturato che miri a risolvere i problemi legati alla dimensione relazionale, ma non solo ad essa, potrebbe essere quello che prevede il presidio di quattro aree strategiche - relative al risultato, al lavoro, alle relazioni e alla qualità - attraverso la definizione di specifici ruoli, come si evince dalla Figura 42²⁰.

²⁰ Si rinvia al volume, ormai un vero e proprio "classico", G.P. Quaglino, S. Casagrande, A. Castellano, *Gruppo di lavoro, lavoro di gruppo*, Cortina Raffaello, 1992, pagg. 108 e ss.

Figura 42 – Le riunioni: fasi e ruoli

Le fasi	I ruoli
<p>Prima:</p> <ul style="list-style-type: none">• inviare l'agenda ai partecipanti con almeno 3 giorni di anticipo <p>Durante:</p> <ul style="list-style-type: none">• arrivare puntuali• attenersi all'agenda (argomenti e tempistica)• evitare conversazioni "private"• ascoltare• partecipare• essere aperti e incoraggiare le idee• cercare di raggiungere il consenso• criticare le idee, non le persone• ricordare che durante la riunione tutti sono allo stesso livello• riassumere in non più di cinque minuti• finire puntualmente <p>Dopo:</p> <ul style="list-style-type: none">• distribuire il meeting report, di massima entro 2 giorni	<p>1. Area del risultato</p> <ul style="list-style-type: none">• conservatore (memoria storica. Impedisce di riprendere ogni volta il problema dall'inizio)• realizzatore (visione pragmatica. Impedisce di ricercare solo soluzioni perfette) <p>2. Area del lavoro</p> <ul style="list-style-type: none">• metodologo (fa seguire correttamente il metodo di lavoro)• negoziatore (individua soluzioni condivise) <p>3. Area delle relazioni</p> <ul style="list-style-type: none">• comunicatore (cura lo sviluppo, l'efficacia e l'efficienza dei flussi comunicativi)• facilitatore (interviene negli snodi critici, es. clima scarsamente collaborativo) <p>4. Area della qualità</p> <ul style="list-style-type: none">• innovatore (si occupa di nuove metodologie)• creativo (si occupa di nuovi "punti di vista")

I primi due ruoli, che appartengono all'area del risultato, sono quelli del *conservatore* e quello del *realizzatore*. Il primo rappresenta la memoria storica e quindi impedisce la pericolosa tendenza a riprendere il problema dal momento iniziale. Il secondo aiuta a mantenere una visione concreta e pragmatica allontanando il rischio di non giungere "*in tempi ragionevoli a soluzioni ragionevoli*", a causa del desiderio di voler perseguire solo soluzioni perfette.

La seconda area, quella del lavoro, vede due figure chiave: il *metodologo* e il *negoziatore*. Il primo si preoccupa di far seguire correttamente il metodo di lavoro mentre il secondo si interessa di favorire l'individuazione di soluzioni condivise tra i partecipanti.

Nella terza area, quella della relazioni, risultano fondamentali i ruoli del *comunicatore*, che agevola lo sviluppo, l'efficacia e l'efficienza dei flussi comunicativi, e del *facilitatore* che interverrà negli snodi critici, quali la ritrosia a farsi coinvolgere di qualche partecipante o il clima poco collaborativo che talvolta prende piede.

Nell'ultima area da presidiare, quella della qualità, i ruoli di spicco sono l'*innovatore* e il *creativo*. Il primo si occupa delle nuove metodologie mentre il secondo favorisce nuovi "punti di vista".

Dopo aver definito i ruoli occorre affrontare una seconda criticità costituita dalla frequente superficialità e scarsa professionalità mostrata nella preparazione e nell'esecuzione della riunione.

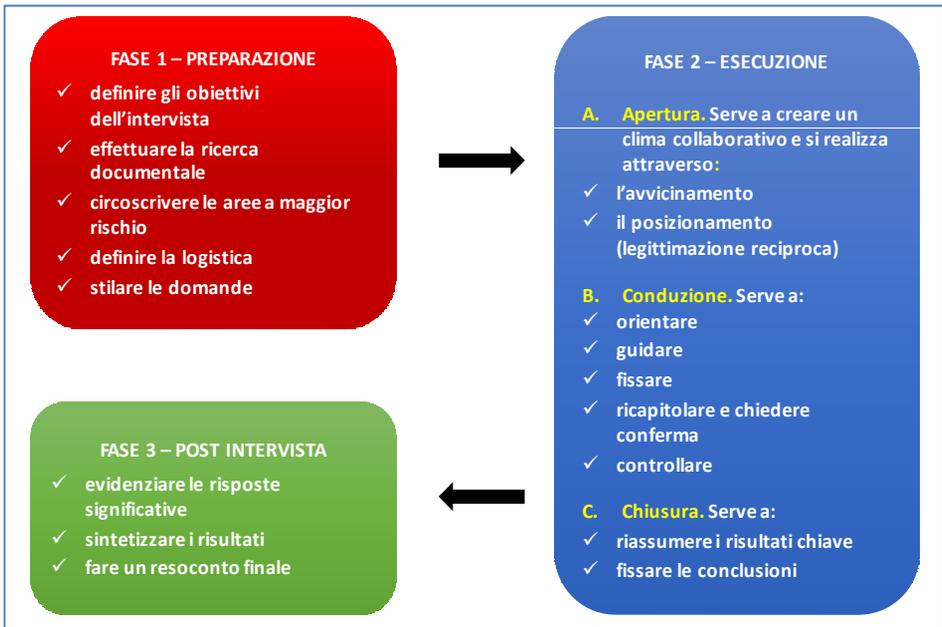
È utile ricordare, con riguardo alla fase esecutiva, che la riunione, sotto un ordine logico-sequenziale, si sviluppa attraverso i seguenti obiettivi:

- illustrare l'esigenza da soddisfare (scopo della riunione);
- individuare e analizzare i sottostanti problemi da risolvere;
- elaborare le soluzioni potenziali;
- adottare una soluzione.

Vediamo ora l'intervista. Essa consiste in un colloquio condotto da un intervistatore e finalizzato ad acquisire determinate tipologie di informazioni (fatti ed opinioni) attraverso domande specifiche e l'analisi di ciò che l'interlocutore riferisce spontaneamente.

L'intervista si può articolare nelle fasi riportate nella Figura 43.

Figura 43 – Fasi dell'intervista



Un accorgimento molto utile è quello di prendere appunti per non dimenticare un'informazione o un'evidenza verificata, chiarendo tale motivazione all'intervistato che, altrimenti, potrebbe mettersi sulla difensiva.

Inoltre, nel caso in cui si stia prendendo nota di una irregolarità, è necessario spiegarla all'intervistato, dandogli la più ampia possibilità di fornire chiarimenti, evitando che ne prenda coscienza a distanza di tempo con la lettura della relazione finale, con ciò rischiando di compromettere la possibilità di creare un serio rapporto di fiducia.

In sintesi devono essere adottati tutti gli accorgimenti necessari per accreditarsi non solo sotto il profilo della professionalità e delle serietà, ma anche della disponibilità.

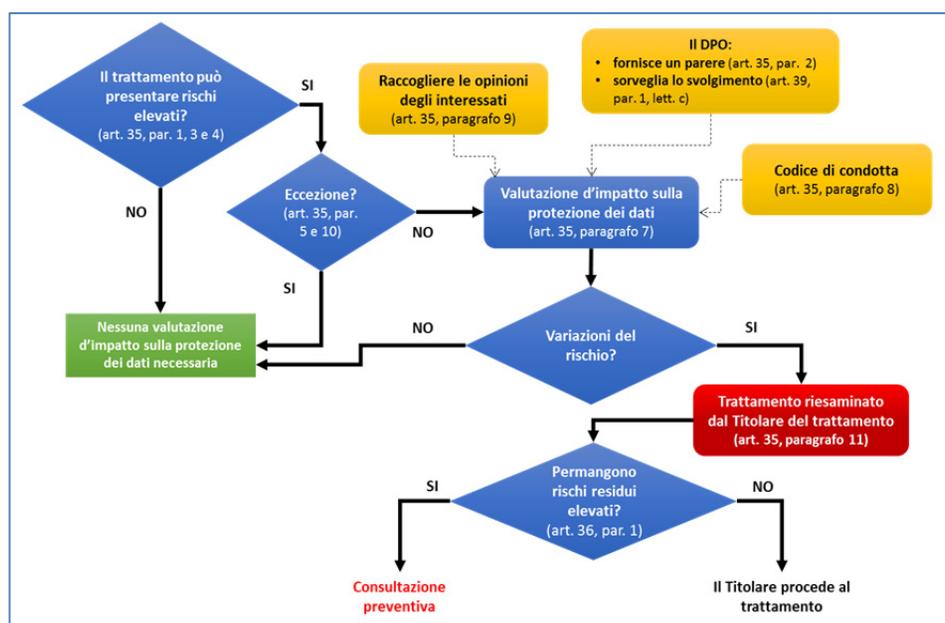
6.7. Il monitoraggio e il riesame

La valutazione d'impatto rappresenta un "processo continuo" da riesaminare periodicamente ovvero ogniqualvolta vi sia un mutamento significativo circa la natura, la finalità o le modalità del trattamento, ivi compresa l'introduzione di nuove norme o di nuove tecnologie.

Le attività di monitoraggio, riesame e aggiornamento sono dunque momenti rilevanti nel processo di valutazione d'impatto, poiché sono volti ad evitare che eventuali mutamenti incidano sull'osservanza della disciplina, garantendo così la costante conformità al Regolamento UE.

Al fine di verificare la sussistenza delle condizioni connesse alla DPIA, appare molto utile lo schema riportato nelle specifiche linee guida del "Gruppo articolo 29"²¹, rielaborato nella Figura 44.

Figura 44 – Condizioni per lo sviluppo ed il riesame della DPIA



6.8. I data audit

Il sistema GDPR, una volta progettato, viene infine "messo in produzione" e, indipendentemente dalla specifica metodologia scelta per la sua attuazione, deve infine essere *auditato* per verificare se:

- è effettivamente conforme alla normativa (verifica di conformità);

²¹ Cfr. pag. 7 del documento WP 248 rev.01, «Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679», revisionate il 4 ottobre 2017, pag. 7.

- risponde ai criteri di efficacia e di efficienza, a cui deve tendere qualsiasi attività organizzata, precedentemente definiti (verifica di performance).

Questa esigenza viene soddisfatta attraverso l'esecuzione di verifiche - le attività di **internal audit**, normalmente definite *data audit* - per le quali occorre fare chiarezza su tre aspetti: a chi fanno capo, come si svolgono e quali sono i metodi applicabili.

6.8.1. A chi compete la responsabilità dei data audit

Per questo primo aspetto non si registra identità di vedute tra gli operatori. Le soluzioni, grossomodo, sono riconducibili a due distinti orientamenti.

Il primo è quello che attribuisce la responsabilità di questa attività ad un soggetto esterno che, su richiesta del Titolare, valuta il sistema realizzato ed esprime una valutazione sulla sua adeguatezza.

A supporto di questa concezione, viene richiamata la norma UNI 11697:2017 che specifica i "Profili professionali relativi al trattamento e alla protezione dei dati personali" e, nel contempo, individua quattro figure, analizzate in dettaglio nel paragrafo 4.6.

In particolare, oltre al DPO, previsto dal GDPR, vengono introdotti ex novo altri tre soggetti, e cioè il manager privacy, lo specialista privacy e, appunto, il valutatore privacy.

Quest'ultimo, secondo la norma UNI, "è un profilo pertinente a soggetti indipendenti con conoscenze e competenze nel settore informatico/tecnologico e di natura giuridica/organizzativa che conducono attività del trattamento e della protezione dei dati personali che possono comunque avvalersi di specialisti in entrambi gli ambiti per effettuare attività di audit".

Ulteriori attributi sono riportati nella Tavola 16.

Tavola 16 – Specifiche del valutatore privacy

Definizione sintetica
Controlla la conformità del trattamento di dati personali a leggi e regolamenti applicabili.
Missione
Esamina periodicamente il trattamento di dati personali, valutando il rispetto di leggi e regolamenti applicabili e approva le misure necessarie per eliminare eventuali non-conformità rilevate, mantenendo una posizione indipendente da chi svolge attività manageriali e operative.
Risultati attesi (Deliverables)
<ul style="list-style-type: none"> • Responsabile (Accountable): Report di audit. • Referente (Responsible): Programma di audit per la protezione e il trattamento dei dati personali.

Compiti principali

- Programmare, pianificare e svolgere le attività di audit.
- Riesaminare la documentazione relativa al trattamento e alla protezione dei dati personali ed effettuare interviste al personale ad ogni livello dell'organizzazione.
- Descrivere gli scostamenti rilevati rispetto a leggi e regolamenti applicabili.

Il secondo orientamento, invece, attribuisce la responsabilità dei *data audit* al DPO, circoscrivendo la valenza della UNI 11697:2017 alla descrizione del bagaglio tecnico-professionale di chi deve materialmente svolgere i *data audit* (che la norma indica con il termine "valutatore privacy").

In altri termini, secondo questa opinione, la norma UNI non può intervenire a livello ordinativo ed organizzativo, introducendo ulteriori specifiche figure oltre a quelle previste dal GDPR.

In effetti questa interpretazione appare più convincente in considerazione soprattutto delle caratteristiche che connotano la figura del DPO, sostanzialmente analoghe a quelle previste per il Responsabile dell'*internal audit*, come può rilevarsi dalla Tavola 17 in cui sono raffrontati il GDPR e gli Standard internazionali per la pratica professionale dell'*internal auditing* – 2017²².

Tavola 17 – Raffronto tra DPO e Responsabile Internal audit

DPO	Responsabile Internal audit
Competenza	
È richiesta una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati (art. 37, par. 5) e, comunque, il Titolare e il Responsabile del trattamento gli forniscono le risorse necessarie per assolvere i compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica (art. 38, par. 2).	Il Responsabile I.A. deve rifiutare l'incarico di consulenza, oppure dotarsi di valido supporto e assistenza, nel caso in cui gli <i>internal auditor</i> non posseggano le conoscenze, le capacità o le altre competenze necessarie per lo svolgimento di tutto o di parte dell'incarico (standard 1210.A1 e 1210.C1).
Autonomia e indipendenza	
Il Titolare e il Responsabile del trattamento si assicurano che il DPO non riceva alcuna istruzione per quanto riguarda l'esecuzione dei suoi compiti. Il DPO riferisce direttamente al vertice gerarchico del Titolare del trattamento o del Responsabile del trattamento (art. 38, par. 3).	L'attività di I.A. deve essere indipendente e gli <i>internal auditor</i> devono essere obiettivi nella esecuzione del loro lavoro (standard 1100); in particolare il Responsabile I.A. deve riportare a un livello gerarchico che consenta all'attività di I.A. il pieno adempimento delle proprie responsabilità. Il Responsabile I.A. deve confermare al board, almeno una volta l'anno, lo

²² Si vedano anche i principi dell'attività di audit, riportati al paragrafo 4 della norma UNI EN ISO 19011:2012 "Linee guida per audit di sistemi di gestione".

	stato di indipendenza organizzativa dell'attività di internal audit (standard 1110).
Conflitto di interessi	
Il Titolare e il Responsabile del trattamento si assicurano che i compiti e le funzioni del DPO non diano adito a un conflitto di interessi (art. 38, par. 6).	Gli internal auditor devono avere un atteggiamento imparziale e senza pregiudizi ed evitare qualsiasi conflitto di interessi (standard 1120).
Gestione del rischio	
Sorveglia l'osservanza della normativa sulla protezione dei dati nonché delle politiche del Titolare o del Responsabile (art. 39, par. 1, b).	L'attività di internal audit deve valutare l'efficacia e contribuire al miglioramento dei processi di gestione del rischio (standard 2120).

Dal raffronto appare evidente che il DPO, come il Responsabile dell'*internal audit*, svolge le attività di *assurance*²³ e di consulenza nei confronti del vertice (Titolare, Responsabile, ecc.), ha una funzione indipendente, deve evitare situazioni anche potenziali di conflitto di interesse (e quindi non può ricoprire nell'organizzazione incarichi di gestione) e deve valutare e contribuire a migliorare i processi di gestione del rischio.

Da ciò può affermarsi la sussistenza delle condizioni organizzative e normative per incardinare sul DPO la responsabilità dei *data audit* anziché prevedere un ulteriore soggetto.

Anticipando una possibile obiezione - e cioè perché non attribuire i *data audit* alla responsabilità dell'eventuale struttura già esistente di *internal audit* - deve evidenziarsi che nonostante le analogie **fattuali** rilevate, a livello di sistema i *data audit* non possono essere considerati come gli *audit* interni ordinari perché:

- i *data audit* hanno una specificità fissata dalla legge (appunto il GDPR) che li fa rientrare nei controlli specialistici di 2°;
- gli *audit* interni ordinari, che fanno capo alla struttura di *internal audit*, rientrano invece nei controlli di 3° livello che, come abbiamo visto, esercitano la tipica funzione di controllo nei confronti dell'intero sistema di controllo dell'organizzazione, compreso quello riferito al *Data Protection*.

Di conseguenza, al di là delle caratteristiche comuni che per certi versi assimilano le due tipologie di *audit*, la diversità degli ambiti su cui agiscono determi-

²³ Secondo gli standard dell'AIIA "I servizi di *assurance* comportano un'obiettiva valutazione delle evidenze da parte degli internal auditor finalizzata alla formulazione di giudizi o conclusioni riferiti a un'organizzazione, attività, funzione, processo, sistema o altro. L'internal auditor definisce la natura e l'ampiezza dell'incarico di *assurance*. Tre sono le parti generalmente coinvolte nei servizi di *assurance*: (1) il process owner, cioè la persona o il gruppo direttamente coinvolti nell'organizzazione, attività, funzione, processo, sistema o altro, (2) l'internal auditor, cioè la persona o il gruppo che effettua la valutazione e (3) l'utente, cioè la persona o il gruppo che utilizzerà tale valutazione".

rebbe un conflitto di interessi tra le funzioni del DPO e del Responsabile I.A. nel caso in cui venisse attribuita a quest'ultima figura la responsabilità dei *data audit*.

A conclusione della questione, deve sottolinearsi che, in ogni caso, l'*auditor*, oltre ai requisiti specifici previsti dall'UNI 11697:2017, in base alla ISO 19011:2011²⁴, deve possedere una serie di conoscenze e abilità:

- di carattere generale, riferite a: principi, procedure e metodi di *audit*; perimetro dell'attività di *audit*; contesto organizzativo; requisiti legali e contrattuali che si applicano all'organizzazione oggetto dell'*audit*;
- di carattere specifico riferite al settore d'intervento.

6.8.2. Come si svolgono i data audit

Lo svolgimento dei *data audit* deve seguire una modalità standardizzata e, cioè, una procedura formalizzata in modo che vengano soddisfatti due requisiti: uno metodologico, riguardante la regolarità, l'efficacia e l'efficienza delle attività, e l'altro relativo all'*accountability*, e cioè alla necessità di dar conto e rendere trasparente il modo con cui si conduce un *audit*, aspetto che costituisce anche un elemento di garanzia per chi lo "riceve".

Tra le metodologie utilizzate, la più diffusa è quella definita dalla già citata norma ISO 19011:2011 "Linee guida per *audit* di sistemi di gestione", che costituisce un aggiornamento dell'originaria versione del 2002.

La norma – applicabile a qualsiasi tipo di organizzazione - non fornisce una guida specifica sul processo di gestione del rischio (*risk management*) dell'organizzazione, ma si focalizza, ad esempio, sui principi su cui si basa l'attività di *audit*, sul programma di *audit* e su come pianificare e condurre un *audit*.

I principi, indicati nel capitolo 4, sono così definiti:

- 1) *integrità*: è il fondamento della professionalità;
- 2) *presentazione imparziale*: obbligo di elaborare rapporti veritieri e accurati;
- 3) *dovuta professionalità*: applicazione di diligenza e di giudizio nel corso dell'attività di *audit*;
- 4) *riservatezza*: sicurezza delle informazioni;
- 5) *indipendenza*: è la base per l'imparzialità dell'*audit* e l'obiettività delle conclusioni dell'*audit*;
- 6) *approccio basato sull'evidenza*: è il metodo razionale per raggiungere conclusioni dell'*audit* affidabili e riproducibili in un processo di *audit* sistematico.

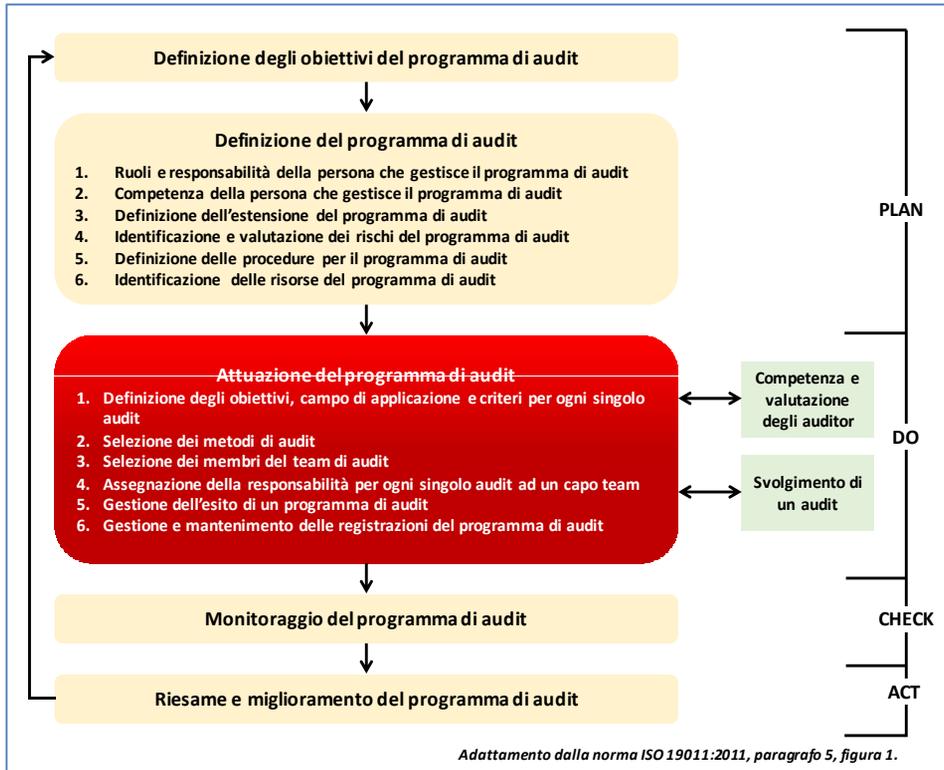
Passiamo al programma di *audit*. Esso deve comprendere le informazioni e le risorse necessarie per organizzare e condurre gli *audit* in modo efficace ed efficiente in un arco temporale specificato (in genere l'anno) e la sua attuazione

²⁴ Si vedano, in particolare, il capitolo 7 e l'appendice A.

deve essere monitorata e misurata per assicurare che i relativi obiettivi siano stati raggiunti.

In particolare il ciclo del programma di *audit* è articolato in 5 fasi, rappresentate nella Figura 45.

Figura 45 – Processo per la gestione di un programma di audit



Appare evidente che il programma di *audit* non dovrebbe essere costituito da un semplice cronoprogramma ma contenere delle descrizioni su alcuni aspetti di rilievo, quali gli obiettivi (verifica sulla conformità ad una norma oppure sul raggiungimento di determinati obiettivi di miglioramento), i metodi (*audit* con visite sul posto o da remoto), le risorse informatiche da impiegare (banche dati, applicativi di supporto alla DPIA, Sistemi di *Business Intelligence*, ecc.).

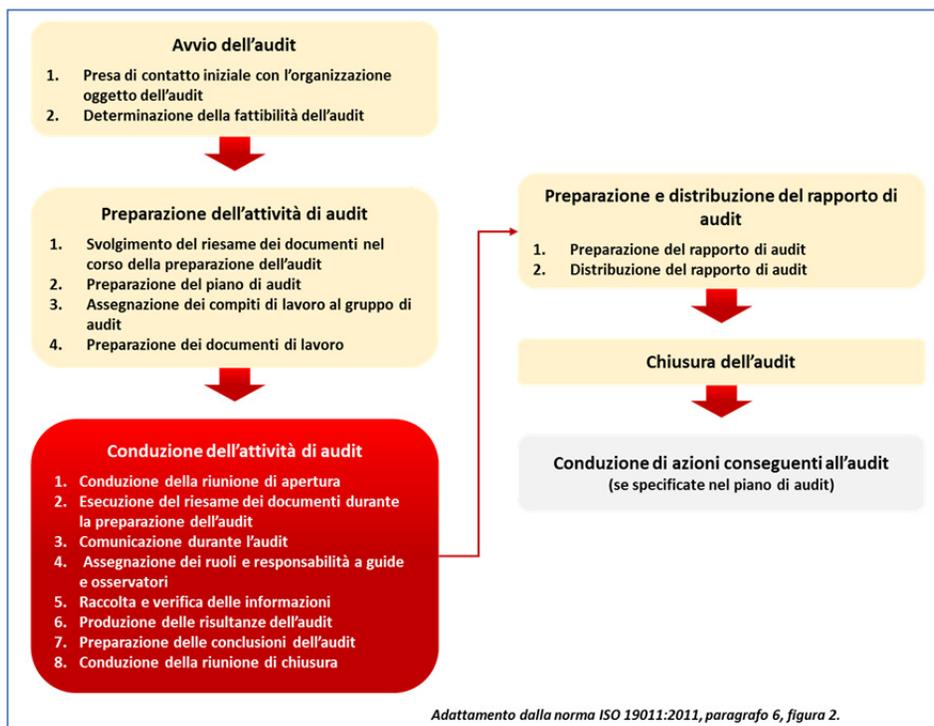
Le criticità più significative di un programma di *audit* sono:

- incaricare *auditor* non sufficientemente competenti o in numero inferiore alle necessità;
- non programmare accuratamente i vari aspetti e, in particolare, gli obiettivi, il campo di applicazione, i criteri e le tempistiche dei singoli *audit*;
- trascurare la corretta gestione degli aspetti logistici e di comunicazione che devono riguardare sia gli *auditor* che i soggetti *auditati*;

- la gestione dei risultati degli *audit* e delle relative registrazioni (piani e rapporti di *audit*, rapporti di non conformità, azioni correttive, ecc.);
- il monitoraggio, riesame e miglioramento del programma di *audit* (es. il *feedback* da parte delle persone *auditate* e il rispetto dei tempi e degli obiettivi prefissati).

Veniamo ora alla parte fondamentale della norma ISO 19011, e cioè alle attività tipiche relative allo svolgimento di un *audit*, rappresentate nella Figura 46, che vanno i) dall'avvio dell'*audit* con la presa di contatto del responsabile del team con i responsabili delle attività *auditate*, ii) alla preparazione dell'*audit* con la pianificazione dell'*audit* e la predisposizione dei documenti di lavoro (ad es. *check-list*), iii) fino alla conduzione vera e propria dell'*audit* e iv) alle attività conclusive (emissione e distribuzione del rapporto, chiusura dell'*audit* ed attività di *follow-up*).

Figura 46 – Processo di audit



L'inizio del processo di *audit* – e cioè le **fasi dell'avvio e della preparazione dell'attività di audit** – ha come *output* principale il piano di *audit*. Esso assume un rilievo particolare perché dalla sua adeguatezza dipenderà se ci saranno o meno le condizioni per il successo dell'*audit*.

Nella realtà, però, in questa fase si registra spesso superficialità e fretta di passare all'azione senza aver prima analizzato i dati di fatto, aver distribuito i compiti

tra gli *auditor* e organizzato le carte di lavoro, con ciò compromettendo l'esito finale delle attività.

La **fase di conduzione dell'attività di audit** è quella più complessa.

Essa inizia con la *riunione di apertura* che ha lo scopo di presentare il team di *audit* e condividere con il soggetto *auditato* il piano di *audit* (obiettivi, modalità operative, tempistica, canali di comunicazione informazioni sulla riunione di chiusura, ecc.).

Successivamente si esegue il **riesame della documentazione** per stabilire se e quali altre informazioni devono essere raccolte e se, a livello documentale, l'oggetto di *audit* sia o meno conforme ai criteri prestabiliti (norme, procedure, risultati, ecc.).

Il terzo *step* riguarda la **comunicazione**, ossia le modalità con cui il team di *audit* si relaziona al proprio interno e con la struttura soggetta a verifica, soprattutto per valutare periodicamente l'avanzamento dell'*audit* e, in caso di necessità, riprogrammare attività anche riassegnando singoli compiti.

L'elemento successivo ha natura prettamente logistica e di "facilitazione" in quanto riguarda l'**assegnazione di ruoli e responsabilità** a guide ed osservatori e cioè a coloro che assistono il *team* di *audit*.

Il quinto *step* è quello della **raccolta e verifica delle informazioni**.

Tali informazioni, se supportate da oggettività, costituiscono delle evidenze (prove) che possono essere valutate in base ai criteri dell'*audit* e porteranno alle risultanze dell'*audit* che, opportunamente riesaminate, determineranno le conclusioni dell'*audit* (ad esempio, conformità o non conformità del processo esaminato).

I metodi di raccolta delle informazioni comprendono interviste, osservazioni, riesame dei documenti, campionamenti (attività particolarmente complessa per i profili statistici e di rappresentatività) e, soprattutto, l'uso di banche dati.

L'ulteriore attività, la **produzione delle risultanze dell'audit**, dovrebbe comprendere le conformità/non conformità, le buone prassi riscontrate, le opportunità di miglioramento ed eventuali raccomandazioni per l'organizzazione.

Le *non conformità* - che vanno classificate in gradi di severità differenti - devono essere riesaminate con l'organizzazione oggetto dell'*audit* per accertarsi che siano comprese nonché al fine di ottenere il riconoscimento che le evidenze dell'*audit* siano ben circostanziate; gli eventuali aspetti non condivisi devono essere documentati e registrati.

Il settimo *step*, la **preparazione delle conclusioni dell'audit** - che dovrebbe essere preceduta da una riunione del team di *audit* per riesaminare tutte le risultanze e condividere le conclusioni dell'*audit* - deve tendere ad evidenziare, soprattutto, le cause delle non conformità e le conseguenti azioni richieste.

La fase della conduzione dell'attività di *audit*, infine, termina con la *riunione di chiusura dell'audit* che ha l'obiettivo di presentare i risultati dell'*audit* alla direzione dell'organizzazione (Titolare del trattamento) ed ai responsabili delle fun-

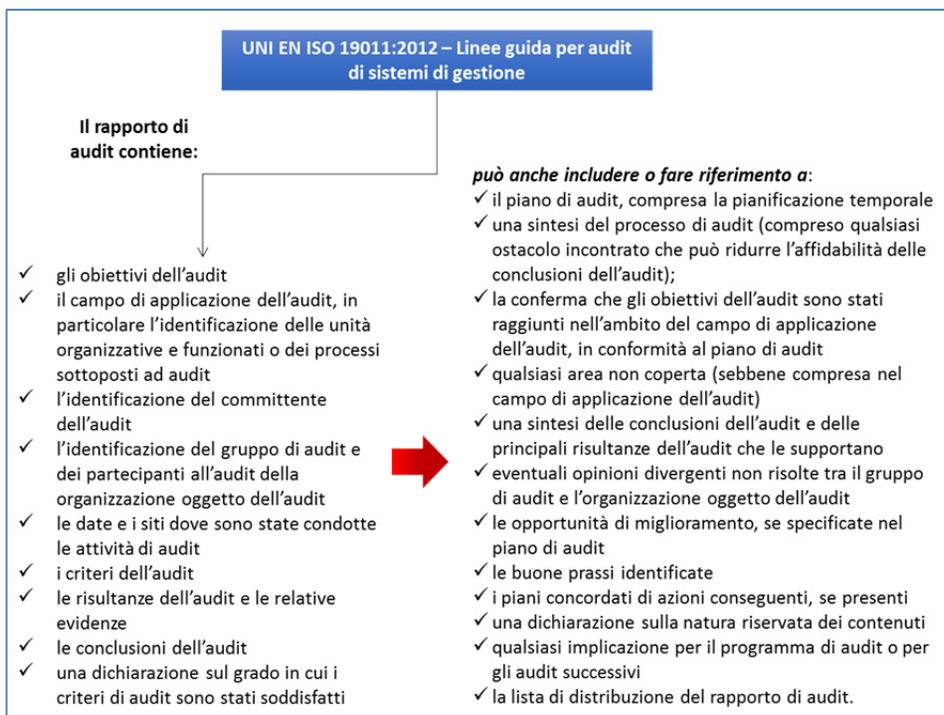
zioni/processi verificati. Ciò implica anche una discussione – anche sui rilievi e sulle eventuali divergenze – che deve essere documentata.

Nella fase di **preparazione e distribuzione del rapporto di audit** il responsabile del *team* di *audit* riporta i risultati in un documento idoneo a fornire una registrazione completa, accurata, concisa e chiara dell'*audit* facendo riferimento a vari elementi, tra cui:

- le risultanze dell'*audit* e le relative evidenze;
- le conclusioni dell'*audit*;
- le eventuali opinioni divergenti tra il *team* di *audit* e la struttura a cui fa capo l'oggetto di *audit*;
- le opportunità di miglioramento;
- le buone prassi identificate;
- i piani concordati di azioni conseguenti, se presenti.
- la lista di distribuzione del rapporto di *audit*.

Il rapporto di *audit*, poi, dovrebbe essere emesso entro un periodo di tempo concordato.

Figura 47 – Il rapporto di audit



L'ultima fase è la chiusura dell'audit. In sostanza consiste nella conservazione dei documenti – normalmente gestiti nel rispetto di severi criteri di riservatezza

– che peraltro costituiranno gli strumenti da utilizzare nel processo di miglioramento continuo riferito all'oggetto di *audit*.

A questa fase può seguire la **conduzione di azioni conseguenti all'audit**, e cioè l'attuazione di azioni correttive e di miglioramento, eventualmente concordate in sede di *audit*, la cui efficacia potrà essere valutata in un *audit* successivo (*follow up*).

6.8.3. I metodi applicabili ai data audit

La scelta dei metodi dipende da una serie di fattori (obiettivi, campo di applicazione, criteri di *audit*, durata, tipo di organizzazione, competenza dell'*auditor*, ecc.).

La Tavola 18 indica i più comuni metodi di *audit* – utilizzabili in tutte le fasi del processo di *audit* e descritte in dettaglio nell'appendice B della ISO 19011:2011 - evidenziando la correlazione tra l'interazione dell'*auditor* con i soggetti della struttura *auditata* e il luogo dove l'attività di *audit* è svolta (sul posto o "da remoto").

Tavola 18 – Metodi di audit

METODO	Audit sul posto		Audit a distanza	
	Interazione umana	Nessuna interazione umana	Interazione umana	Nessuna interazione umana
Condurre interviste.	X		X*	
Compilazione di liste di controllo e questionari con la partecipazione dell'organizzazione oggetto dell'audit.	X		X*	
Condurre il riesame dei documenti con la partecipazione della organizzazione oggetto dell'audit.	X	X	X*	X
Campionamento.	X		X	
Osservazione del lavoro svolto.		X		X**
Condurre la visita in campo.		X		
Compilazione di liste di controllo.		X		
Campionamento (per esempio prodotti).		X		
Analisi dei dati.				X

* Con mezzi di comunicazione interattiva.
 ** Tramite mezzi di sorveglianza, tenendo conto dei requisiti sociali e legali.
 Le attività di audit sul posto sono svolte nel sito dell'organizzazione oggetto dell'audit. Le attività di audit a

METODO	Audit sul posto		Audit a distanza	
	Interazione umana	Nessuna interazione umana	Interazione umana	Nessuna interazione umana
<p>distanza sono svolte in qualsiasi luogo ad eccezione del sito dell'organizzazione oggetto dell'<i>audit</i>, indipendentemente dalla distanza.</p> <p>Le attività di audit interattivo implicano l'interazione tra il personale dell'organizzazione oggetto dell'audit e il team di audit. Le attività di audit non interattive non implicano interazione umana con le persone che rappresentano l'organizzazione oggetto dell'audit, ma comportano l'interazione con apparecchiature, mezzi e documentazione.</p> <p>Adattamento dalla norma ISO 19011:2011, Appendice B, Prospetto B1.</p>				

In relazione ai metodi indicati appaiono utili alcune precisazioni, limitandosi al campionamento e alle interviste, e cioè alle attività più "strategiche".

Iniziando con il "*campionamento*", deve evidenziarsi che esso ha luogo quando non è pratico o non è economicamente vantaggioso esaminare tutte le informazioni disponibili (per esempio quando le registrazioni sono troppo numerose o troppo disperse geograficamente). Si tratta di un'attività particolarmente delicata perché se i campioni non sono "costruiti" in modo da risultare rappresentativi di un universo, le evidenze possono risultare addirittura fuorvianti.

Attualmente l'esigenza di fare ricorso al campionamento è sempre più limitata, potendosi fare ricorso alle informazioni contenute nei *database*, sempre più complete, e che consentono di elaborare enormi quantità di dati – in genere l'intero "universo" – anche con semplici formule excel!

Passando alle interviste²⁵ possiamo definirle come uno dei mezzi più importanti di raccolta delle informazioni e sono effettuate tenendo conto di una serie di fattori come, ad esempio, della situazione, del soggetto intervistato, se viene svolta con modalità *face to face* o attraverso mezzi di comunicazione interattiva (es. videoconferenza).

In ogni caso, l'*auditor* deve rammentare che le interviste dovrebbero essere:

- tenute con persone di livello gerarchico e di funzione appropriati;
- eseguite, ove possibile, durante il normale orario di lavoro e nel consueto posto di lavoro della persona intervistata.

Inoltre, per il buon esito dell'intervista, occorre tener sempre presente l'esigenza di:

- mettere l'intervistato a proprio agio prima e durante l'intervista;
- spiegare la ragione dell'intervista e di qualsiasi annotazione presa;
- iniziare chiedendo alle persone di descrivere il loro lavoro;
- scegliere accuratamente il tipo di domanda (per esempio domanda aperta, domanda chiusa, domanda che orienta la risposta);

²⁵ Per un approfondimento sulle fasi dell'intervista si rimanda alla Figura 43 contenuta nel paragrafo 6.6.

- riassumere e riesaminare i risultati dell'intervista con la persona intervistata;
- ringraziare le persone intervistate per la loro partecipazione e cooperazione e, comunque, curare la c.d. "fase di rilascio" dell'intervistato, per favorire il consolidamento della cultura del controllo.

In conclusione, per la corretta implementazione di *data audit*, risulta indispensabile la definizione di un chiaro quadro di riferimento che comprenda gli attori, le competenze, le metodologie, i processi e le tecniche affinché si possa definire un modello per la gestione degli *audit* idoneo a verificare non solo la conformità del sistema GDPR ma anche a ottimizzarne l'impatto sui processi e sulle funzioni dell'intera organizzazione.



Glossario, acronimi e abbreviazioni

- **Accountability:** concetto legato a quello di responsabilità, consiste nel dare conto di cosa è stato fatto e delle modalità utilizzate.
- **Alert:** segnale o messaggio di avviso, allarme, avvertimento.
- **Anonimizzazione:** trattamento che ha lo scopo di impedire l'identificazione dell'interessato; i dati anonimizzati non sono ritenuti dati personali.
- **Asset:** ogni entità materiale o immateriale suscettibile di valutazione economica.
- **Assurance:** valutazione indipendente dei processi di governance, di gestione del rischio e di controllo dell'organizzazione.
- **Autorità Garante nazionale:** Autorità di controllo prevista dall'art. 51 del GDPR.
- **Best practice:** prassi che hanno permesso di ottenere i migliori risultati negli ambiti di specifica applicazione.
- **Business intelligence (processi):** sistemi, processi aziendali e strumenti utilizzati per raccogliere dati ed analizzare informazioni strategiche.
- **CEDU:** Corte Europea dei diritti dell'Uomo.
- **Check list:** è un qualsiasi elenco esaustivo di cose da fare o da verificare per eseguire una determinata attività, solitamente utilizzato in un processo.
- **CGUE:** Corte di Giustizia dell'Unione Europea.
- **Cifratura dei dati:** è il processo di codifica delle informazioni tale da impedire a parti non autorizzate di leggerle; si basa, di solito, su un algoritmo di cifratura e su una passphrase (una password, ma più lunga e complessa) che "apre" e "chiude" la modalità di comprensione dei dati.
- **Cluster:** in generale, raggruppamento di elementi omogenei.
- **Comitato:** Comitato europeo per la protezione dei dati previsto dall'art. 68 del GDPR.
- **Compliance:** conformità a determinate norme, regole o standard.
- **Considerando:** elemento del preambolo che si inserisce tra i «visto» e l'articolato dei testi normativi dell'UE. I «considerando» sono numerati e devono motivare in modo conciso le norme (fonte: Guida pratica comune del Parlamento europeo, del Consiglio e della Commissione per la redazione dei testi legislativi dell'Unione europea, 2013).
- **CSV (Comma-Separated Values):** è un formato di file utilizzato per l'importazione ed esportazione di una tabella di dati in fogli elettronici o database. Si tratta di un semplice file di testo.

- **Data analytics (DA):** è il processo di esame dei set di dati al fine di trarre conclusioni sulle informazioni che contengono, sempre con l'ausilio di sistemi e software specializzati.
- **Data controller:** Titolare del trattamento.
- **Data processor:** Responsabile del trattamento.
- **Diagramma di Gantt:** è uno strumento di supporto al project management, in quanto permette di modellizzare la pianificazione dei compiti necessari alla realizzazione di un progetto.
- **Disaster recovery:** nell'ambito della sicurezza informatica, si intende l'insieme delle misure tecnologiche e logistico/organizzative per ripristinare sistemi, dati e infrastrutture, a fronte di gravi emergenze che ne intacchino la regolare attività.
- **DPO:** Data Protection Officer, ossia il Responsabile della protezione dei dati.
- **DPIA:** Data Protection Impact Assessment (oppure Privacy Impact Assessment - PIA), ossia Valutazione d'impatto sulla protezione dei dati.
- **Face to face:** modalità di comunicazione che prevede la contestuale presenza fisica dei soggetti.
- **Feedback:** informazione di ritorno.
- **Framework:** quadro concettuale di riferimento o, in informatica, un'infrastruttura.
- **GDPR:** General Data Protection Regulation; è il Regolamento CE 27 aprile 2016, n. 2016/679/UE, "Regolamento generale sulla protezione dei dati", pubblicato nella G.U.U.E. 4 maggio 2016, n. L 119.
- **GEPD:** Garante europeo della protezione dei dati.
- **I.A.:** Internal audit.
- **KPI (key performance indicator):** è una metrica che indica il livello di raggiungimento di un dato obiettivo da parte di un individuo, di un reparto o di un'azienda.
- **Masterplan:** piano che si riferisce ad un programma o ad un'iniziativa complessa che può essere articolata in progetti e sottoprogetti: la logica è quella di suddividere il programma in parti più piccole e, quindi, più facilmente gestibili.
- **Paragrafo:** Parte dell'articolo delle norme UE che corrisponde al comma delle norme nazionali.
- **Performance:** risultato e modalità di raggiungimento del risultato.
- **PLA (Privacy Level Agreement):** Livello di protezione dei dati personali garantito da un fornitore nell'erogazione di servizi a propri clienti, concettualmente simile ad uno SLA.
- **Problem solving (processo):** processo rivolto a individuare, definire, analizzare e risolvere un problema.
- **Process owner:** responsabile del processo.

- **Processi di customer service:** processi che provvedono all'identificazione, generazione ed erogazione di beni e servizi.
- **Project management:** è un sistema gestionale volto a raggiungere determinati risultati attraverso uno sforzo organizzato e l'impiego efficace delle risorse necessarie, e cioè rispettando i vincoli legati a tempi, costi, risorse allocate, obiettivi e qualità del prodotto finito.
- **Pseudonimizzazione dei dati:** è una misura di sicurezza che consiste nel conservare i dati in una forma che impedisce l'identificazione del soggetto senza l'utilizzo di informazioni aggiuntive.
- **Query:** operazione che estrapola dati da un database per compiere determinate operazioni sui dati (selezione, inserimento, cancellazione dati, aggiornamento, ecc.).
- **RPCT:** Responsabile per la prevenzione della corruzione e trasparenza.
- **Sistema di gestione (management system):** insieme di procedure, di sistemi informativi e di sistemi informatici dedicati al governo di un processo tipicamente operativo, produttivo o amministrativo.
- **Skill:** abilità.
- **SLA (Service Level Agreement):** Documento che definisce gli obiettivi di supporto tecnico o di prestazioni di business ivi incluse le misurazioni di prestazione e le conseguenze del loro non raggiungimento. È condiviso tra il fornitore di servizi ed il cliente.
- **SSD (Decision Support System):** sistemi di supporto alle decisioni (si veda business intelligence).
- **Stakeholders:** soggetti portatori di un interesse rilevante in un certo contesto (in un'azienda, ad esempio, clienti, azionisti, dipendenti).
- **Template:** modulo; in informatica indica un documento o programma nel quale su una struttura standard esistono spazi da riempire successivamente.
- **Total Quality Management:** corrisponde al concetto espresso in italiano con "Qualità totale". Si tratta di un modello organizzativo che adotta la "Gestione totale della qualità" attraverso il coinvolgimento e la mobilitazione dei dipendenti e la riduzione degli sprechi in un'ottica di ottimizzazione degli sforzi.