Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

DOCUMENTO DI RICERCA

LA CONSULENZA IN AMBITO PRIVACY: UNA GUIDA PER I COMMERCIALISTI

AREA DI DELEGA	CONSIGLIERI DELEGATI
COMPLIANCE E MODELLI ORGANIZZATIVI DELLE IMPRESE	FABRIZIO ESCHERI ELIANA QUINTILI

-- NOVEMBRE 2022

Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

A CURA DI:

FLORIANA CARLINO

ASCENSIONATO RAFFAELLO CARNÀ

ANDREA DI GIALLUCA

MARIA LUCIANA FRAGALÀ

MARCO MANGANIELLO

CRISTINA RENNA

ARMANDO URBANO

PAOLA ZAMBON

CON LA COLLABORAZIONE DI:

ANNALISA DE VIVO - *Ufficio Legislativo CNDCEC*

ABSTRACT

La consulenza offerta dai professionisti alle imprese, agli enti del terzo settore e alla Pubblica Amministrazione negli ultimi anni è sempre più rivolta alla compliance rispetto alle normative che prevedono l'adozione di presidi e procedure per la mitigazione di rischi di vario tipo, previa valutazione degli stessi.

La privacy, come ridisegnata dal Regolamento europeo 2016/679, rientra a pieno titolo tra le norme di compliance, posto che il suo rispetto costituisce il presupposto indispensabile per il corretto svolgimento di qualsiasi attività che comporti il trattamento di dati personali.

Poter disporre di un data base di dati personali acquisiti lecitamente ai sensi del GDPR costituisce un asset di elevato valore: a tal fine l'impresa deve valutare tutti i rischi connessi al trattamento dei dati personali necessari per lo svolgimento dell'attività e, conseguentemente, adottare le misure di sicurezza richieste.

Si tratta di un percorso complesso, in cui alla conoscenza della normativa e della prassi in materia – costantemente alimentata dai pareri del Garante Privacy e dei comitati tecnici europei – deve abbinarsi quella delle dinamiche giuridico-economiche d'impresa.

È intuitivo che, trattandosi di un ambito professionale nel quale sono richieste competenze giuridiche, economiche, informatiche e organizzative, la professionalità del Commercialista può costituire un elemento di forza con riferimento ai diversi ruoli richiesti, principalmente quelli del consulente e/o del DPO.

Nell'ambito della sua attività professionale, infatti, il Commercialista tratta quotidianamente dati personali, sovente particolari, in una complessa opera di analisi sotto il profilo giuridico, economico, organizzativo e informatico. Con riferimento a quest'ultimo aspetto, il processo di digitalizzazione delle imprese richiede il rafforzamento delle competenze per l'organizzazione dei dati nel rispetto delle normative di riferimento e, in particolare, del GDPR.

Rispetto a tali ruoli l'osservazione del mercato evidenzia una domanda crescente, anche alla luce dell'accelerazione alla digitalizzazione, impressa dalla pandemia, di tutte le attività economiche e non: si pensi, solo per fare qualche esempio, allo smartworking, al fascicolo sanitario, agli algoritmi dell'Agenzia delle entrate, alle criptovalute e alla blockchain, ma anche alle start up che sviluppano attività a contenuto esclusivamente digitale.

In tali contesti il diritto alla riservatezza deve essere bilanciato con quello alla libera circolazione dei dati, il che richiede una complessa attività di interpretazione ad opera dei soggetti di volta in volta investiti dei diversi ruoli privacy (titolare del trattamento, DPO, consulente).

Aumenta, di conseguenza, il bisogno di una maggiore cultura della privacy a tutti i livelli, dal cittadino all'imprenditore fino al professionista.

Ed è proprio a quest'ultimo che è destinato il presente documento: una sintesi ragionata, che non ha pretesa di essere esaustiva, della complessa disciplina del trattamento dei dati personali, unitamente ad un primo set di indicazioni per tutti i Commercialisti che vogliono sviluppare le proprie competenze professionali al fine di offrire una consulenza qualificata anche in questo ambito.

SOMMARIO

PRIMA PARTE – IL RUOLO DEL COMMERCIALISTA NELL'AMBITO DELLA CONSULENZA PRIVACY

1. Cenni sul Regolamento Europeo per la protezione dei dati personali (GDPR)

Al fine di armonizzare e completare il quadro normativo comunitario in tema di protezione dei dati personali, dopo un ampio iter, nel 2016 è stato approvato il "pacchetto protezione dati" per contenere due strumenti importanti per tutti gli Stati membri dell'Unione:

1. il "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione Dati)";
2. la "Direttiva (UE) 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".

La direttiva, entrata in vigore il 5 maggio 2016, per propria natura, ha avuto la necessità di essere recepita nei rispettivi ordinamenti nazionali (in Italia dal D.Lgs. 18 maggio 2018, n. 51). Essendo riferita al trattamento dei dati personali nel settore della polizia, della giustizia e della sicurezza, essa non è oggetto in questa sede di ulteriore approfondimento; nondimeno, è doveroso citarla anche per la rilevanza delle indicazioni fornite con riferimento alla tutela del dato relativo alle persone offese, ai testimoni e agli indagati.

Il regolamento europeo (*General Data Protection Regulation*, d'ora in avanti anche "GDPR" o "Regolamento"), è invece entrato in vigore il 24 maggio 2016 in tutti gli Stati membri dell'Unione (essendo per propria natura direttamente applicabile senza necessità di recepimento negli ordinamenti nazionali), ma ha trovato piena applicazione solo a partire dal 25 maggio 2018, con l'abrogazione definitiva della precedente direttiva 95/46/CE. L'impianto normativo di quest'ultima era ormai superato, considerato il differente contesto geografico – mancavano molti dei Paesi Ue che si sono nel tempo adeguati – e tecnologico in cui tale direttiva era stata concepita. Peraltro, nonostante gli encomiabili tentativi di esegesi da parte del WP29[1], al fine di renderla maggiormente aderente alla moderna realtà, la direttiva in questione era stata diversamente interpretata da uno Stato membro all'altro in sede di recepimento (in Italia prima vi era la famosa L. 675/96 e, grazie alla direttiva 95/46, è stato emanato il D.Lgs. 196/2003). Ad ogni modo, secondo il considerando 171 del GDPR, gli effetti prodotti dalla direttiva permangono per quanto inerenti alle interpretazioni comunitarie fornite in passato, a meno di non venire sostituiti nel tempo da specifici atti di modifica, abrogazione o

[1] Il Gruppo di lavoro articolo 29 (*Working Party article 29* o WP29, appunto perché previsto dall'art. 29 della direttiva europea 95/46), è il gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dei dati. Con l'avvento del GDPR il WP29 è stato sostituito dal Comitato europeo per la protezione dei dati (*European Data Protection Board* - EDPB).

sostituzione. Di conseguenza, è sempre utile consultare – ai fini dell'eventuale applicazione per analogia al caso specifico – la documentazione prodotta dalla Commissione europea o dalle Autorità di controllo su taluni argomenti.

Il GDPR nasce, pertanto, dalla necessità di intervenire in una Europa ormai sempre più attenta all'ICT (Information Communication Technology) per armonizzare la tutela dei diritti e delle libertà fondamentali rispetto alle attività di trattamento dei dati personali e affinché la libertà personale del singolo e i relativi diritti possano essere tutelati e, al contempo, sia garantita anche la libera circolazione dei dati per le imprese.

Rispetto alla direttiva 95/46/CE, perciò, il GDPR consente di aumentare più concretamente il controllo esercitato dalle persone fisiche sui dati che esse stesse generano.

Proprio come il noto "*right to privacy*" del 1890[2], che veniva richiamato in risposta a quella che era considerata una necessaria riflessione sull'evoluzione tecnologica e che nasceva dall'interesse al diritto negativo di non essere violati nella propria riservatezza, il legislatore comunitario è intervenuto per tentare di fornire una risposta al problema che lo sviluppo della rete aveva sollevato, con la raccolta e il trattamento di dati personali effettuati tramite diversi dispositivi spesso connessi tra loro e/o nel cloud, l'esponenziale utilizzo dei social, delle app e dell'IOT (internet delle cose). Quanto appena detto anche alla luce di un quadro normativo che, in assenza del GDPR, veniva percepito come fonte di meri adempimenti cartacei (le sottoscrizioni dei "famosi" consensi), privi di effettiva tutela, trasparenza e chiarezza verso gli interessati al trattamento.

Nel tempo si è così rafforzata la necessità di individuare, da un lato, uno specifico diritto alla protezione dei dati personali affinché il loro trattamento possa avvenire previo esplicito consenso o per espressa indicazione normativa o interesse pubblico, a meno che non vi siano altre basi di liceità, e, dall'altro, un diritto positivo di mantenere il controllo delle proprie informazioni.

Il dato collegato o collegabile ad una persona, perciò, deve essere protetto nel rispetto del diritto alla riservatezza, ma sempre bilanciando i diritti e le libertà altrui. L'informazione deve essere intesa nelle storiche accezioni di contenuto, finalità e risultato. Il diritto alla protezione dei dati personali, su espressa indicazione del GDPR, non dovrà mai essere ritenuto assoluto ma relativo. Pertanto, vi possono sempre essere casi in cui il diritto ad essere informati sul trattamento dei propri dati personali debba essere compresso o limitato per garantire altri diritti altrui o il rispetto di alcune norme che sono considerate giuridicamente prioritarie rispetto ad esso.

Nel suo incipit, il GDPR evidenzia che il diritto alla protezione dei dati delle persone fisiche è un diritto fondamentale (*ex* art. 8, co.1 della Carta dei diritti fondamentali dell'Unione Europea e art. 16, par. 1 del Trattato sul funzionamento dell'Unione Europea), che mira alla tutela delle libertà fondamentali delle persone fisiche rispetto al trattamento di dati personali effettuato: ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano, nel rispetto di tutti i diritti fondamentali

[2] *The right to privacy* è il saggio che due giuristi americani, Samuela Warren e Louis Brandeis, scrissero nel 1890.

e in modo che i dati stessi possano liberamente circolare nella stessa Unione in totale conformità al regolamento in parola.

Nel contesto italiano il GDPR non ha abrogato il Codice Privacy (D.Lgs. 196/2003), mentre è stato ritenuto necessario un aggiornamento dello stesso per adeguarne i contenuti tramite il D.Lgs. 10 agosto 2018, n. 101 con avviso di rettifica (in G.U. 27/09/2018, n.225). Nel tempo, il Codice Privacy domestico è stato ulteriormente aggiornato anche per inserire regole deontologiche, recentemente con il DL 8 ottobre 2021, n. 139, noto come "Decreto capienza". Tale ultima modifica ha una notevole rilevanza in termini di trattamento di dati personali per finalità di interesse pubblico, poiché di fatto conferisce un nuovo potere, anche regolamentare, alla P.A., che può decidere di indicare una finalità di trattamento diversa rispetto a quella prevista per legge, se la considera necessaria per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri a essa attribuiti. Inoltre, questa norma ha abrogato l'obbligo per la PA, titolare del trattamento svolto per l'esecuzione di un compito di interesse pubblico, di effettuare la consultazione preventiva dell'Autorità di controllo, nei casi in cui la relativa valutazione d'impatto sulla protezione dei dati rilevi un rischio elevato, anche in assenza di misure adottate dal titolare per attenuare il rischio. La medesima normativa ha ridotto inoltre il termine per l'acquisizione dei pareri del Garante privacy anche sulle riforme del PNRR a 30 giorni, decorsi infruttuosamente i quali il Governo può procedere indipendentemente dall'acquisizione del parere.

Infine, la conservazione dei tabulati telefonici, per le finalità di accertamento e repressione dei reati, è stata privata delle misure prescritte dal Garante a garanzia dell'interessato. Modifiche che generano, peraltro, non poche perplessità in ordine alle riduzioni di garanzie nei confronti degli interessati al trattamento e che in alcuni frangenti sembrano anche essere lontane dai principi fondamentali del GDPR.

Senza pretesa di esaustività, infatti, va osservato che il GDPR ha apportato alcune importanti novità nel panorama europeo della privacy e in particolare:

1. ha meglio definito la nozione di "**dato personale"**: "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale". Infatti, "le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle.";
2. ha introdotto la definizione di "**categorie particolari di dati**" che precedentemente rientravano in parte nella nozione di "dati sensibili" ovvero "che rivelino l'origine razziale o etnica, le opinioni

politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale" nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica e i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

3. introdotto anche la definizione di "**pseudonimizzazione"**: "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

Inoltre, il GDPR ha allargato l'ambito di applicazione territoriale della normativa all'attività di uno stabilimento nell'Unione, anche se il trattamento non è effettuato nell'Unione e anche se lo stesso avvenga per il tramite di strumenti ubicati in territori extra-comunitari, o sia effettuato da titolari (o responsabili) non stabiliti nell'Unione, o ancora se il trattamento effettuato riguardi l'offerta di beni o prestazione di servizi (siano essi gratuiti che a pagamento) o implichi un monitoraggio del comportamento dell'interessato all'interno dell'Unione. La norma in esame garantisce così l'uniformità del livello di protezione dei dati personali per tutti i cittadini europei.
Infine, tra i vari aggiornamenti apportati dal GDPR, occorre non dimenticare alcuni principi molto importanti e alcune novità dallo stesso introdotte, come:

- la c.d. *accountability* (responsabilizzazione): il titolare del trattamento deve essere in grado di dimostrare la propria competenza e aderenza alla normativa in merito alla protezione dei dati personali ed essere in grado di comprovarlo (si veda il successivo approfondimento);
- l'adeguatezza delle misure tecniche e organizzative per garantire un livello di sicurezza commisurato al rischio (es. pseudonimizzazione, resilienza, ecc.) nel proteggere i dati personali (soprattutto se massivi ed effettuati con strumenti informatici). A tale adeguatezza corrisponde la speculare responsabilità del titolare (e altresì quella del contitolare e dei responsabili del trattamento). Tra le misure da adottare, soprattutto quando il trattamento pone un particolare alto rischio per i diritti e per le libertà delle persone fisiche, vi è la valutazione di impatto che, oltre che in relazione alle fattispecie espressamente indicate nell'art. 35 GPDR, deve essere effettuata per tutte le tipologie di trattamenti elencate da ciascuna Autorità di controllo dell'UE;
- l'allargamento del già noto concetto di *privacy by design* (protezione dei dati fin dalla progettazione), completato da quello di *privacy by default* (per impostazione predefinita), in modo che dal momento in cui si inizia a progettare un trattamento di dati personali si effettuino le corrette valutazioni per adottare le misure adeguate e gli strumenti idonei ed efficaci al fine di garantire il rispetto della normativa, trattando unicamente i dati necessari rispetto alle finalità del trattamento;
- il maggior rilievo attribuito ai doveri di trasparenza e di chiara informazione agli interessati sul trattamento di dati personali posto in essere. Con linguaggio semplice e chiaro l'informativa erogata deve riportare i vari diritti che l'interessato al trattamento dei dati personali possiede

proprio in virtù del GDPR, con riconoscimenti espressi del diritto all'oblio e del diritto alla portabilità del dato;

- l'introduzione della figura del *Data Protection Officer* (DPO) o Responsabile della Protezione Dati (RPD), che per competenza (in quanto detentore della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati), autonomia ed assenza di conflitto di interessi, integrità ed indipendenza professionale, nonché per la capacità di assolvere i compiti che il GDPR gli affida, possa fungere anche da referente con il Garante nel caso di violazioni (c.d. *data breach*). In alcuni casi il GDPR ha previsto che la designazione del DPO sia obbligatoria e non facoltativa;
- il particolare risalto dato a tutti i principi fondamentali in materia di trattamento di dati personali (es.: liceità del trattamento, finalità, qualità dei dati, correttezza, responsabilità) che vengono espressi in diversi articoli e commentati nel ricco Considerando iniziale.

Il GDPR è una norma che ha nel cuore la protezione del dato della persona e che pone in capo al titolare del trattamento il dovere di attuarla rendicontandone le modalità. Anche per tale motivo non è una norma statica, ma necessita, per chi deve prestare assistenza nell'adempimento, di aggiornamento continuo e di un approccio dinamico basato sul rischio, anche per allinearsi con l'evoluzione tecnologica alla quale è intimamente collegata. Pochi Stati nel mondo sono ormai totalmente privi di normative in tema di privacy e possiedono, come minimo, disegni normativi per porle in atto: nell'Unione europea il GDPR è certamente un solido pilastro per chi intende trattare dati personali, fornendo (anche con la direttiva e-Privacy relativa alla tutela della vita privata nel settore delle comunicazioni elettroniche) un quadro giuridico solido e affidabile per la protezione dei dati personali.

La quantità di dati generati da enti pubblici, imprese e cittadini è in costante ed esponenziale crescita e aumenterà sempre di più la loro condivisione tra diversi titolari con l'evoluzione tecnologica sempre in costante cambiamento.

Il Commercialista, da sempre vicino alle imprese, alla PA e agli ETS, in qualità di consulente privacy o di DPO, può indubbiamente apportare il proprio contributo professionale per consigliare al meglio i titolari o i responsabili che intendano porre in essere trattamenti di dati personali in conformità normativa.

2. I soggetti obbligati: casistica

I soggetti obbligati al rispetto, e di conseguenza all'adeguamento al GDPR, sono tutti quelli che effettuano un trattamento automatizzato o non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

Il regolamento riporta i casi di esclusione dall'adeguamento, collegandolo ai trattamenti che sono effettuati:

a) per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;

b) dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, del Trattato sull'Unione Europea (TUE);

c) da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;

d) dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

Di seguito sono sintetizzati i profili delle figure soggettive coinvolte in ambito privacy.

2.1. Il titolare del trattamento dei dati

La definizione di titolare del trattamento dei dati personali è contenuta al punto 7 dell'art. 4 del GDPR, nel quale si specifica che per titolare del trattamento si intende *"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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri".*

Ne deriva che il titolare del trattamento è sempre rappresentato dal vertice dell'organizzazione aziendale o dell'Ente.

Nelle ditte individuali, compresi gli studi professionali, il titolare dell'attività è anche titolare del trattamento dei dati; nelle società, invece, il titolare del trattamento è la società stessa e le funzioni vengono assunte dal legale rappresentante.

Per quanto riguarda la persona giuridica, il titolare del trattamento è la struttura nel suo complesso ovvero la persona fisica alla quale competono le scelte di fondo sulla raccolta e sull'utilizzazione dei dati. Sul punto, l'Autorità Garante per la protezione dei dati personali ha chiarito che se i "titolari" sono le imprese, nelle società entreranno in gioco i rispettivi amministratori secondo le regole che disciplinano ciascuna struttura, pertanto:

- l'amministratore unico;
- l'amministratore delegato;
- il consiglio di amministrazione.

Negli studi associati e nelle società tra professionisti il titolare del trattamento è rappresentato dal sodalizio stesso in persona del suo legale rappresentante. Una considerazione va fatta con riferimento al mandato professionale svolto da uno o più professionisti (soci dello studio o della società), che assumeranno la qualifica di contitolari del trattamento *ex* art. 26 del Regolamento UE 2016/679.

Nel settore pubblico**,** come specificato dal Garante Privacy, il titolare del trattamento è l'ente nel suo complesso, ad esempio la società, il ministero, l'ente pubblico, l'associazione[3].

Il titolare del trattamento è responsabile del rispetto dei principi applicabili al trattamento di dati personali, ai sensi dell'art. 5 del GDPR, e pertanto deve assicurarsi che tali dati siano trattati con liceità, correttezza e trasparenza, raccolti per finalità determinate, esplicite e legittime, adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità, conservati in modo che siano identificabili gli interessati e in maniera da garantire la sicurezza dei dati. Inoltre, il titolare ha la responsabilità generale per qualsiasi trattamento di dati personali effettuato direttamente o indirettamente per il tramite di terzi che operano per suo conto (responsabile esterno o incaricato interno).

Il titolare del trattamento, così come previsto dall'art. 24 del Regolamento, è tenuto ad adottare tutte le misure tecniche e organizzative adeguate per garantire la conformità del trattamento al GDPR e l'efficacia delle misure attuate; tali misure devono tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche e devono essere aggiornate e riesaminate ogni qualvolta lo si reputi necessario.

È importante ricordare che i dati personali vengono raccolti, trattati e conservati; durante questi trattamenti è fondamentale che gli stessi non vengano manipolati in modo illecito, distrutti, cancellati o modificati sin dalla fase della progettazione.
Il titolare del trattamento ha l'obbligo di:

- determinare, singolarmente o assieme ad altri, le finalità e i mezzi di trattamento dei dati personali;
- tutelare tutti i diritti dell'interessato previsti dagli artt. da 15 a 22 del Regolamento (*infra*);
- adottare le misure tecniche e organizzative adeguate per garantire la sicurezza del trattamento dei dati;
- rilasciare all'interessato l'informativa di cui agli artt. 13 e 14 del Regolamento, tranne nei casi disciplinati dal paragrafo 4 dell'art. 13 e dal paragrafo 5 dell'art. 14 del Regolamento[4];
- non usare, comunicare o divulgare i dati al di fuori del trattamento che viene effettuato (obbligo di riservatezza);
- formalizzare un accordo ai sensi dell'art. 26 GDPR con eventuali contitolari del trattamento;

[3] Autorità garante per la protezione dei dati personali, Circolare n. 291/S del 13 novembre 1997 recante direttive in materia di protezione dei dati personali.
[4] La norma citata fa riferimento ai seguenti casi:
a) l'interessato dispone già delle informazioni;
b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato;
c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure
d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

- nominare gli addetti interni al trattamento (dipendenti che hanno accesso ai dati) e fornire loro la lettera di incarico relativa agli obblighi e alle istruzioni da rispettare;
- designare il/i responsabile/i del trattamento;
- designare il responsabile della protezione dei dati (Data Protection Officer) nelle casistiche previste dal Regolamento e quando lo ritenga opportuno;
- designare il rappresentante in Italia, nei casi espressamente previsti, se il titolare del trattamento non è stabilito nell'UE;
- tenere, redigere e aggiornare il registro di trattamenti nei casi previsti dal Regolamento e ogniqualvolta lo ritenga opportuno;
- formare il personale dipendente con frequenza almeno annuale;
- effettuare le comunicazioni al Garante in tutti i casi previsti dal Regolamento:
  a) consultazione preventiva *ex* art. 36 GDPR, quando il rischio inerente all'attività del trattamento risulta alto in assenza di misure per attenuare il rischio;
  b) violazione dei dati personali (*data breach*);
  c) dati di contatto del DPO nominato;
- cooperare con l'Autorità Garante.

Il titolare del trattamento risponde per i danni materiali o immateriali causati all'interessato, per violazione delle norme del Regolamento UE 2016/679, o di altre disposizioni in materia di protezione dei dati personali previste dalle norme attuative. Egli è tenuto al risarcimento di tale danno, salvo che dimostri che sono state adottate tutte le misure ritenute idonee al fine di evitare il danno o che l'evento dannoso non è a lui imputabile.

2.2. Il contitolare del trattamento dei dati

Il contitolare del trattamento dei dati è una nuova figura della privacy prevista dall'art. 26 del GDPR ed emerge nella fattispecie in cui due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento stesso.

Tra i contitolari del trattamento deve essere redatto un accordo interno (tramite un atto giuridicamente valido ai sensi del diritto nazionale) nel quale si determinano le rispettive responsabilità, in modo trasparente, in merito all'osservanza degli obblighi del Regolamento e di tutta la normativa in materia di privacy, il rispettivo ambito di responsabilità, i rispettivi compiti, con particolare riguardo all'esercizio dei diritti degli interessati.

L'interessato potrà esercitare i propri diritti, previsti dal Regolamento, indifferentemente nei confronti di e contro ciascun titolare del trattamento.

Il contitolare del trattamento ha gli stessi compiti, obblighi e responsabilità del titolare del trattamento.

Una fattispecie tipica di contitolarità nel trattamento dei dati si determina nel caso di studio associato, ove il titolare del trattamento è lo studio e il contitolare il professionista che dovrà occuparsi della prestazione di servizi richiesta dall'interessato.

2.3. Il responsabile del trattamento dei dati

Il responsabile del trattamento è la persona fisica o giuridica designata dal titolare per trattare, per suo conto, i dati personali degli interessati.

La nomina del responsabile del trattamento deve avvenire mediante un contratto o un altro atto giuridico, che vincoli il responsabile al titolare del trattamento e che contenga la materia disciplinata, la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Questo ruolo deve essere attribuito a una persona qualificata, che conosce la materia, in grado di mettere in atto misure tecniche e organizzative adeguate per far sì che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

La nomina scritta deve prevedere che il responsabile del trattamento:

- tratti i dati personali soltanto su istruzione documentata del titolare del trattamento;
- garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adotti tutte le misure richieste dalla sicurezza del trattamento;
- assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- assista il titolare del trattamento nel garantire il rispetto degli obblighi di sicurezza del trattamento, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti.

Il responsabile del trattamento può ricorrere ad un altro responsabile (sub-responsabile del trattamento) solo previa autorizzazione scritta, specifica o generale, del titolare del trattamento.

Infatti, il Regolamento consente la nomina di sub-responsabili del trattamento da parte di un responsabile, per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo risponde al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile".

Rispetto al previgente testo del D.Lgs. 196/2003 non vi è più traccia della figura del responsabile interno del trattamento; pertanto, secondo quanto previsto dal Regolamento UE 2016/679, il responsabile del trattamento può essere solo qualificato come figura esterna all'organizzazione del titolare del trattamento, tale da poterlo definire "responsabile esterno".

Un esempio di responsabile esterno del trattamento è rappresentato dal consulente del lavoro quando elabora le paghe dei dipendenti di un'azienda o di uno studio professionale; sono altresì responsabili esterni i professionisti, nel caso in cui la loro prestazione sia resa in relazione ad attività che il cliente può svolgere autonomamente (si pensi al commercialista che elabora scritture contabili per conto di un'azienda o all'avvocato domiciliatario), le società informatiche che prestano assistenza alle aziende, le società che conservano gli archivi informatici delle aziende in cloud, ecc.

Il Regolamento prevede i seguenti obblighi specifici in capo ai responsabili del trattamento:

- adottare le misure tecniche e organizzative adeguate a garantire la sicurezza del trattamento dei dati;
- non usare, comunicare o divulgare i dati al di fuori del trattamento che viene effettuato (obbligo di riservatezza);
- designare il responsabile della protezione dei dati (Data Protection Officer) nelle casistiche previste dal Regolamento e quando lo ritenga opportuno;
- designare il rappresentante in Italia, nei casi espressamente previsti, se il responsabile del trattamento non è stabilito nell'UE;
- tenere, redigere e aggiornare il registro di trattamenti nei casi previsti dal Regolamento e ogniqualvolta lo ritenga opportuno.

Nel caso di trattamento in violazione delle norme del regolamento europeo, il responsabile risponde, congiuntamente al titolare, per il danno cagionato all'interessato.

Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha rispettato gli obblighi del regolamento specificatamente diretti ai responsabili del trattamento, ovvero se ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

Se più titolari (titolare e contitolare) o responsabili del trattamento, oppure entrambi (titolare e responsabile del trattamento), sono coinvolti nello stesso trattamento e sono responsabili del danno causato dal trattamento, ogni titolare, contitolare e responsabile ne risponde in solido per l'intero ammontare del danno, al fine di garantire l'intero risarcimento effettivo all'interessato.

Da ciò deriva che l'interessato potrà rivolgersi ad ognuno di essi per ottenere il risarcimento del danno oppure chiedere i danni a tutti i coobbligati in solido. Il titolare o il responsabile del trattamento che abbia pagato l'intero risarcimento del danno ha il diritto di regresso e potrà rivalersi verso gli altri titolari del trattamento o responsabili del trattamento, coinvolti nello stesso trattamento, per la parte del risarcimento corrispondente al danno ad essi imputabile.

2.4. Il rappresentante

Il rappresentante di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione è una figura prevista dall'art. 27 del Regolamento. Allorquando il titolare del trattamento non sia stabilito all'interno dell'Unione Europea, ma tratta però dati personali di interessati che sono stabiliti nell'Unione, il rappresentante deve essere obbligatoriamente designato per iscritto dal titolare o dal responsabile del trattamento.

L'obbligo di designazione non si applica:

- se il trattamento dei dati è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati, di cui all'art. 9, paragrafo 1, del Regolamento[5] o di dati personali relativi a condanne penali e a reati di cui all'art. 10 del Regolamento, ed è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento;
- alle autorità pubbliche o agli organismi pubblici.

Pertanto, in sintesi, il rappresentante deve essere nominato quando:

- il titolare o il responsabile del trattamento dei dati non è stabilito nell'Unione Europea;
- gli interessati si trovano nell'Unione europea;
- il trattamento svolto non è occasionale;
- il mandante non è un soggetto pubblico;
- il trattamento riguarda, su larga scala, dati sensibili o giudiziari;
- presenta un probabile rischio per gli interessati, tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento.

Il rappresentante deve essere stabilito in uno degli Stati membri in cui si trovano gli interessati e agisce per conto del titolare e del responsabile del trattamento con riguardo agli obblighi che a questi derivano dal Regolamento; inoltre, funge da interlocutore con le autorità di controllo e con gli interessati, in aggiunta o in sostituzione del titolare del trattamento o del responsabile del trattamento, per tutte le questioni riguardanti il trattamento.

Il rappresentante deve svolgere i suoi compiti nel rispetto del mandato conferitogli.

La designazione di un rappresentante non incide sulla responsabilità generale del titolare del trattamento o del responsabile del trattamento e pertanto fa salve le azioni legali che potrebbero essere promosse dagli interessati contro lo stesso titolare del trattamento o responsabile del trattamento.

[5] Ci si riferisce ai dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, ai dati genetici e biometrici intesi a identificare in modo univoco una persona fisica, nonché ai dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

3. La figura del consulente privacy per l'assistenza ai soggetti obbligati

L'avvento del GDPR ha imposto all'attenzione degli operatori economico-giuridici una nuova figura professionale, quella del consulente privacy ("data protection specialist", o anche "privacy officer").

L'importanza strategica di tale figura è evidente alla luce della necessità delle aziende di adeguarsi correttamente alla normativa in commento, garantendo la tutela dei diritti e della dignità nel trattamento dei dati personali dei soggetti interessati e, al contempo, la libera circolazione dei dati per legittimo interesse di business.

In effetti il consulente privacy sembra essere una figura necessaria all'interno di qualsiasi azienda, dal momento che l'adeguamento al GDPR implica, da un lato, una conoscenza approfondita della particolare branca del diritto rivolta alla protezione dei dati personali e, dall'altro, l'adozione di procedure di *risk assessment* finalizzate alla individuazione delle misure di sicurezza più appropriate da adottare.

Rispetto al DPO, il consulente privacy si pone quale interlocutore qualificato per conto dell'azienda, fermo restando che gli adempimenti privacy devono essere espletati esclusivamente dai soggetti individuati dal GDPR (titolare, eventuale contitolare e responsabile del trattamento).

È opportuno rammentare che il titolare e, ove presente, il contitolare del trattamento ha la responsabilità generale per qualsiasi trattamento di dati personali effettuato, direttamente o indirettamente per il tramite di terzi che operino per suo conto (responsabile esterno o incaricato interno).

Il responsabile del trattamento risponde, congiuntamente al titolare del trattamento, per il danno cagionato all'interessato nel caso di trattamento in violazione delle norme del Regolamento.

Il titolare e il responsabile del trattamento saranno **esonerati da responsabilità** se riescono a dimostrare, alternativamente, che sono state adottate tutte le misure ritenute idonee al fine di evitare il danno o che l'evento dannoso non è imputabile alla loro condotta, ma è dipeso da una causa esterna alla loro sfera di controllo.

Nelle aziende in cui la nomina del DPO è obbligatoria, o che comunque hanno nominato un DPO, il consulente privacy può agire sinergicamente con quest'ultimo, al fine di ottimizzare i risultati in termini di *compliance* e di supervisione. Di contro, nelle aziende in cui la figura del DPO non è presente, il ruolo del consulente privacy è ancor più incisivo in quanto il titolare e il responsabile (o i responsabili) del trattamento non necessariamente sono dotati delle competenze tecniche richieste per l'implementazione di un modello privacy adeguato.

Tale ultima attività impatta in modo significativo sulla struttura organizzativa, dovendo il modello privacy raccordarsi con le altre misure organizzative di tipo preventivo eventualmente già adottate dall'azienda, dalla sicurezza sul lavoro al sistema di gestione della qualità, fino al modello di organizzazione, gestione e controllo *ex* D.Lgs. 231/2001. In tal senso il consulente privacy deve abbinare alla conoscenza specialistica della normativa e della prassi in materia di protezione dei dati

personali anche quella dei principali sistemi di controllo, del risk management e dell'analisi dei processi.

Un tale know how può senz'altro agevolare alcune delle attività che di tutta evidenza possono essere demandate al consulente privacy, *in primis* la valutazione dello stato di *compliance* dell'azienda alla normativa vigente e l'identificazione delle attività necessarie all'adeguamento, ma anche l'affiancamento nell'assolvimento degli obblighi imposti dal GDPR, anche al fine di evitare le pesanti conseguenze sanzionatorie connesse all'inadempimento.

Le competenze specifiche del consulente privacy risultano indispensabili anche con riferimento agli obblighi di formazione dei dipendenti, ai quali occorre fornire le nozioni necessarie e illustrare i principi comportamentali da rispettare al fine di garantire la protezione dei dati e prevenire le eventuali violazioni della sicurezza dei medesimi.

Quanto alla individuazione del consulente privacy, è chiaro che l'eventuale assenza nell'organigramma aziendale di una figura con le caratteristiche sinteticamente descritte, ipotesi molto probabile nel caso di aziende di dimensioni ridotte, rende necessario reperire all'esterno il relativo servizio.

Al riguardo, giova evidenziare che allo stato attuale la qualifica di consulente privacy non è formalmente riconosciuta: ciò vale non già a ridimensionare la valenza della certificazione di "consulente privacy" rilasciata all'esito degli ormai numerosi corsi di formazione all'uopo organizzati, bensì a ribadire che i professionisti in possesso di comprovate competenze giuridico-economiche ben possono svolgere attività in questo ambito.

Sotto questo aspetto, la conoscenza approfondita delle problematiche aziendali rappresenta un *plus* per tutti quei professionisti, soprattutto commercialisti ed esperti contabili che intendano ampliare la propria sfera di operatività – perché profondi conoscitori dei processi di acquisizione, elaborazione, trasferimento e condivisione dei dati e dei soggetti coinvolti – affiancando i clienti anche nel percorso di adeguamento alla privacy, ovviamente nella consapevolezza che tale attività comporta un ulteriore e costante sforzo di aggiornamento. La conoscenza della normativa e dei provvedimenti tempo per tempo diffusi dal Garante Privacy non solo in ambito italiano, ma anche europeo, costituiscono, infatti, lo strumentario che il professionista deve possedere per poter fornire una assistenza qualificata ai propri clienti, anche nella qualità di consulente privacy.

4. L'incarico di DPO (Data Protection Officer)

L'art. 37 e il Considerando 97 del GDPR disciplinano la figura del Responsabile della protezione dei dati (DPO).

Si tratta di un soggetto incaricato dal titolare o dal responsabile del trattamento di assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR.

Questa figura rappresenta un elemento fondante ai fini della responsabilizzazione, e la sua nomina può facilitare l'osservanza della normativa anche attraverso strumenti di *accountability*[6].

L'obbligo di nomina del DPO è previsto per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche ovvero trattino su larga scala categorie particolari di dati personali. Sono esempi di amministrazioni ed enti pubblici: le amministrazioni dello Stato, gli enti pubblici non economici nazionali, regionali e locali, le Regioni e gli enti locali, le università, le Camere di commercio, industria, artigianato e agricoltura, le aziende del Servizio sanitario nazionale, le autorità indipendenti.

L'art. 37 del Regolamento prevede che le autorità giudiziarie non hanno l'obbligo di nominare il DPO, salvo disporre all'art. 2 *sexiesdecies* del D.Lgs. 196/2003 (Codice Privacy), così come introdotto dal D.Lgs. 101/2018, che il responsabile della protezione dei dati è designato anche in relazione ai trattamenti di dati personali effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni.

Il Gruppo di lavoro Art. 29 raccomanda, in termini di buone prassi, che gli organismi privati, incaricati di funzioni pubbliche o che esercitano pubblici poteri (ad esempio concessionari di servizi pubblici), designino comunque un DPO pur non sussistendone l'obbligatorietà[7]. Nelle medesime linee guida, in merito al responsabile della protezione dei dati, per gli altri soggetti non pubblici, vengono elencati una serie di fattori da tenere presenti onde stabilire se un trattamento sia da ritenersi effettuato su larga scala:

1. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
2. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
3. la durata, ovvero la persistenza, dell'attività di trattamento;
4. la portata geografica dell'attività di trattamento.

Si riportano di seguito alcuni esempi di trattamento su larga scala:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Di contro, non costituiscono trattamenti su larga scala:

[6] Di cui si dirà al successivo paragrafo 5.
[7] Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016, disponibili sul sito www.garanteprivacy.it.

- il trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- il trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Sul sito ufficiale del Garante sono pubblicate le Faq relative al DPO[8], che si aggiungono alle risposte già fornite dal Gruppo di lavoro Art. 29, in allegato alle Linee Guida sul DPO. Tra le varie precisazioni, il Garante ha rimarcato quali sono i soggetti privati (titolare e responsabile del trattamento) obbligati alla designazione del DPO.

Si tratta di soggetti le cui principali attività (c.d. di "core business") consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala di categorie particolari di dati personali o di dati relative a condanne penali e a reati. Il diritto dell'Unione o degli Stati membri può prevedere ulteriori casi di designazione obbligatoria del responsabile della protezione dei dati (art. 37, par. 4, GDPR).

Pertanto, i soggetti privati, la cui attività principale consiste in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala dei dati sensibili relativi alla salute o alla vita sessuale, finanziari, genetici, giudiziari e biometrici delle persone fisiche, possono essere rappresentati, a titolo esemplificativo e non esaustivo, da: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; Caf e patronati; società operanti nel settore delle *utilities* (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento, ecc.

Nei casi diversi da quelli previsti dall'art. 37, par. 1, lett. b) e c), GDPR, la designazione del responsabile del trattamento non è obbligatoria (ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti[9]).

Per gli studi associati e le società tra professionisti, poiché il Garante per la protezione dei dati personali ha precisato che non ritiene obbligatoria la nomina del DPO "in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale", si ritiene che detta nomina sia quantomeno consigliata.

La nomina di un DPO, come già precisato, può essere effettuata o dal titolare del trattamento o dai responsabili del trattamento, oppure da entrambe le figure e in quest'ultimo caso i soggetti saranno poi tenuti alla reciproca collaborazione. Qualora il titolare del trattamento sia tenuto alla nomina di un

[8] Più precisamente, in data 15 dicembre 2017 sono state pubblicate le Faq relative al Responsabile della protezione dei dati in ambito pubblico e il 26 marzo 2018 (ult. agg. maggio 2021) quelle che interessano il DPO che opera in ambito privato.
[9] Si veda anche il considerando 97 del Regolamento, in relazione alla definizione di attività "accessoria".

DPO e il suo eventuale responsabile del trattamento al contrario non sia obbligato a tale designazione, la nomina del DPO, anche da parte del responsabile del trattamento, può costituire una buona prassi.

A tal proposito il Gruppo di lavoro Art. 29 ha proposto alcuni esempi per chiarire le fattispecie che di seguito si riportano:

1. Una piccola azienda a conduzione familiare operante nel settore della distribuzione di elettrodomestici in una città si serve di un responsabile del trattamento la cui attività principale consiste nel fornire servizi di tracciamento degli utenti del sito web, oltre all'assistenza per attività di pubblicità e marketing mirati. Le attività svolte dall'azienda e dai clienti non generano trattamenti di dati "su larga scala", in considerazione del ridotto numero di clienti e della gamma relativamente limitata di attività.
   Tuttavia, il responsabile del trattamento, che conta numerosi clienti come questa piccola azienda familiare, svolge, nel suo complesso, trattamenti su larga scala. Ne deriva che il responsabile del trattamento deve nominare un DPO ai sensi dell'articolo 37, paragrafo 1, lettera b); al contempo, l'azienda a conduzione familiare in quanto tale non è soggetta all'obbligo di nomina del DPO.
2. Un'azienda di medie dimensioni che produce rivestimenti in ceramica incarica un responsabile esterno della gestione dei servizi di salute occupazionale; tale responsabile ha un numero elevato di clienti e svolge, nel suo complesso, trattamenti su larga scala. Il responsabile del trattamento è tenuto a nominare un DPO ai sensi dell'articolo 37, paragrafo 1, lettera b), poiché svolge trattamenti su larga scala. Tuttavia, l'azienda non è tenuta necessariamente allo stesso adempimento.

4.1. Competenze, compiti e ruoli del DPO

L'articolo 37, paragrafo 5, specifica che il DPO "*è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39*".

Nel considerando 97 si prevede che il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento.

La normativa non prevede specifiche qualità professionali da prendere in considerazione nella nomina di un DPO, ma è fondamentale che egli abbia un'ottima e approfondita conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati e del GDPR. Il livello di conoscenza specialistica deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento. Sotto questo aspetto, pur non essendo richieste attestazioni formali o l'iscrizione ad appositi albi professionali, il possesso di attestati di partecipazione a master e corsi può essere un valido strumento di valutazione per il possesso dei giusti requisiti. È preferibile, inoltre, che il DPO sia a conoscenza dello specifico settore di attività e della struttura organizzativa del titolare del trattamento. Nel caso di nomina da parte di un'autorità pubblica o di un organismo pubblico, il DPO

dovrebbe possedere anche una conoscenza approfondita delle norme e procedure amministrative applicabili.

Al fine di poter svolgere i suoi compiti in totale assenza di conflitti di interessi, al DPO è richiesto l'imprescindibile requisito dell'indipendenza. Di conseguenza un DPO non può rivestire, all'interno dell'organizzazione del titolare del trattamento o del responsabile del trattamento, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali. Ad esempio, possono sussistere situazioni di conflitto d'interesse all'interno dell'organizzazione del titolare del trattamento o del responsabile del trattamento riguardo a ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT), ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento.

I principali compiti che il DPO si troverà a svolgere nell'ambito del suo incarico sono innanzitutto il controllo, il rispetto e l'osservanza del regolamento, con annessa la valutazione dei rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità.

Egli, inoltre, contribuisce a dare attuazione a elementi essenziali del regolamento, quali i principi fondamentali del trattamento, i diritti degli interessati, la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita, oltre a collaborare con il titolare/responsabile del trattamento dei dati, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA).

Infatti, il titolare del trattamento o il responsabile del trattamento devono essere assistiti dal DPO nell'attività di controllo del rispetto a livello interno del Regolamento, con riferimento alla quale il DPO:

- raccoglie le informazioni per individuare i trattamenti svolti;
- analizza e verifica i trattamenti in termini di loro conformità;
- svolge attività di informazione, consulenza e indirizzo nei confronti del titolare e/o del responsabile.

Per quanto riguarda la valutazione d'impatto, il titolare del trattamento deve consultarsi con il DPO, fra l'altro, sulle seguenti tematiche:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al GDPR.

Inoltre, il DPO deve informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati; supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento, alla sicurezza dei trattamenti e alla notifica e comunicazione delle violazioni di dati personali.

Il responsabile della protezione dei dati coopera con l'Autorità e costituisce il punto di contatto per le questioni connesse al trattamento dei dati personali (artt. 38 e 39 del Regolamento) svolgendo la sua attività come organo indipendente.

Il ruolo di DPO può essere ricoperto sia da un dipendente del titolare o del responsabile, a patto che sia a conoscenza della realtà operativa in cui avvengono i trattamenti, sia da un soggetto esterno che garantisca l'effettivo assolvimento dei compiti che il GDPR assegna a tale figura.

Qualora il DPO venga nominato all'interno della realtà aziendale, tale nomina deve avvenire mediante uno specifico atto "di designazione", e dovrà trattarsi necessariamente di persona fisica. Il DPO scelto all'esterno, che potrà essere anche una persona giuridica, dovrà invece operare in base a un contratto di servizi. Entrambe le nomine devono essere redatte in forma scritta e dovranno indicare espressamente i compiti attribuiti, le risorse assegnate per il loro svolgimento, nonché ogni altra utile informazione in rapporto al contesto di riferimento.

Il settimo comma dell'art. 37 del Regolamento prevede che il nominativo del DPO e i relativi dati di contatto siano pubblicati (sul sito internet dell'azienda o dello studio professionale) e comunicati in via telematica all'Autorità di controllo[10]. L'eventuale rigetto della comunicazione, e la relativa motivazione, saranno comunicati esclusivamente al soggetto che effettua la stessa, mediante l'invio di un'e-mail all'indirizzo indicato nel modulo.

Nel caso in cui la comunicazione venga accolta:

- il soggetto che effettua la stessa riceverà, mediante comunicazione inviata all'indirizzo e-mail individuato nel modulo, l'indicazione del numero di protocollo utilizzato per la registrazione dei dati comunicati;
- il soggetto titolare/responsabile riceverà, mediante comunicazione inviata all'indirizzo PEC individuato nel modulo (o all'altro riferimento e-mail, qualora trattasi di soggetto privo di PEC), un documento informatico contenente le informazioni inserite all'atto della compilazione del modulo e l'indicazione del numero di protocollo utilizzato per la registrazione dei dati comunicati;

[10] La comunicazione deve essere effettuata utilizzando esclusivamente la procedura on-line fruibile al seguente link: https://servizi.gpdp.it/comunicazione-rpd/compilaModulo. Al termine della fase di inserimento on-line di tutte le informazioni richieste, il soggetto che effettua la comunicazione riceverà un'e-mail contenente le istruzioni per completare la procedura. In particolare, bisognerà scaricare un file che dovrà essere sottoscritto con firma digitale (o firma elettronica qualificata) in formato CAdES (file con estensione p7m) e successivamente caricato in una specifica sezione della piattaforma applicativa. La procedura di caricamento deve essere completata entro 48 ore dalla ricezione della mail contenente le istruzioni.

- il soggetto designato quale DPO riceverà, mediante comunicazione inviata all'indirizzo PEC individuato nel modulo, un documento informatico contenente le informazioni inserite all'atto della compilazione del modulo e l'indicazione del numero di protocollo utilizzato per la registrazione dei dati comunicati.

Per tutte le eventuali successive comunicazioni con l'Autorità bisognerà far riferimento al numero di protocollo e non all'identificativo provvisorio della comunicazione. Qualora il titolare/responsabile proceda alla designazione di un nuovo DPO, indipendentemente dalla motivazione, non dovrà effettuare la revoca della comunicazione dei dati di contatto del precedente DPO, ma dovrà effettuare una nuova comunicazione che sostituirà automaticamente quella effettuata in precedenza[11]. Queste disposizioni mirano a garantire che sia gli interessati che le autorità di controllo possano contattare il DPO in modo facile e diretto senza doversi rivolgere ad altri soggetti (titolare e responsabile del trattamento).

Il Responsabile della protezione dei dati deve poter disporre di un'adeguata autonomia con le necessarie risorse per svolgere in modo efficace i propri compiti; pertanto, il titolare o il responsabile del trattamento dovranno mettere a disposizione del DPO le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

Il DPO, in estrema sintesi, dovrà rispettare determinati requisiti fondamentali:

1. operare alle dipendenze del titolare o del responsabile del trattamento oppure sulla base di un contratto di servizio come professionista esterno.
2. adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse. Egli, ad esempio, non può essere un soggetto che abbia potere decisorio sulle finalità o sugli strumenti del trattamento di dati personali;
3. possedere ottima padronanza della normativa e delle prassi di gestione dei dati personali, anche per quel che concerne le misure tecniche e organizzative o le misure atte a garantire la sicurezza dei dati.

I gruppi di imprese o soggetti pubblici, ai sensi dell'articolo 37, paragrafo 2, possono nominare un unico DPO, a condizione che sia "facilmente raggiungibile da ciascuno stabilimento", sia in grado di comunicare in modo efficace con gli interessati e di collaborare con le autorità di controllo. Il concetto di raggiungibilità si riferisce ai compiti del DPO in quanto punto di contatto per gli interessati, l'autorità di controllo e i soggetti interni all'organismo o all'ente, visto che uno dei compiti consiste nell' "*informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento*". La necessità che il DPO sia raggiungibile, vuoi fisicamente all'interno dello stabile ove operano i dipendenti, vuoi

[11] Sul sito del Garante, nella sezione regolamento UE area rpd, è presente anche il modulo per la revoca della comunicazione dei dati del DPO, in formato .pdf; tale modello deve essere utilizzato esclusivamente per le seguenti casistiche:
1) errata indicazione del titolare/responsabile del trattamento;
2) non sussistono le condizioni che obbligano il titolare/responsabile del trattamento alla designazione di un DPO;
3) altro (specificare).

attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione, è fondamentale al fine di garantire all'interessato il contatto con lo stesso. Le comunicazioni, quindi, devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa.

Nelle citate Linee Guida, il Gruppo di lavoro Art. 29 incoraggia la nomina su base volontaria del DPO anche ove il regolamento non imponga in modo specifico la sua designazione. In tal caso verranno applicati gli stessi requisiti che valgono per le designazioni obbligatorie.

Gioverà, infine, evidenziare che il titolare o il responsabile del trattamento che abbiano designato un responsabile per la protezione dei dati personali restano comunque pienamente responsabili dell'osservanza della normativa in materia di protezione dei dati e devono essere in grado di dimostrarla[12], in quanto il DPO non risponde personalmente in caso di inosservanza del GDPR.

[12] Vd. art. 5, par. 2, del Regolamento; vd. anche i punti 3.2 e 3.3. delle Linee guida del WP29 sul DPO.

SECONDA PARTE – GLI ADEMPIMENTI PRIVACY

5. Il principio di responsabilizzazione (accountability) e gli altri principi della normativa sulla privacy

Sebbene sia quello maggiormente noto nell'ambito della riformata normativa sulla privacy, il principio di *accountability* costituisce solo un pilastro di un ben più articolato e interconnesso sistema di principi di matrice unionale.

Come accennato in premessa, i principi fondamentali che regolano il GDPR sono:

- liceità, correttezza e trasparenza;
- limitazione della finalità e della conservazione;
- minimizzazione dei dati;
- esattezza, integrità e riservatezza;
- *accountability*;
- *privacy by design* e *privacy by default*.

I menzionati principi, oltre ad una (pur rilevante) valenza teorica, hanno un impatto operativo immediato e diretto per tutti i titolari e i responsabili del trattamento dei dati: per queste ragioni, appare opportuno riassumerne brevemente gli impatti.

Il principio di liceità comporta che il trattamento deve essere fondato su una base giuridica idonea tra quelle indicate nel Regolamento[13] e che, una volta verificata l'esistenza di tale presupposto, il trattamento deve essere conforme al diritto UE (es. Carta dei diritti Fondamentali dell'UE) e degli Stati membri (es. Costituzione).

Il principio in oggetto impone dunque, prima ancora che il trattamento dei dati abbia inizio, l'identificazione della base giuridica del medesimo, motivo per cui il suo impatto operativo è rilevantissimo, tanto più che la base giuridica è elemento da individuare anche ai fini di altri adempimenti, come l'informativa sulla privacy piuttosto che il registro dei trattamenti. Si ricorda, d'altronde, che il GDPR, salvo regole particolari, prevede che il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

[13] Art. 6 GDPR.

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Il principio di correttezza comporta, per il titolare del trattamento, un divieto di trattare i dati personali in un modo che, seppur non formalmente in violazione di norme di legge, abusi della buona fede dei soggetti interessati. Il principio di trasparenza comporta, altresì, che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice, chiaro e coinciso.

Il principio di limitazione delle finalità[14] impone che i dati siano raccolti e poi successivamente trattati per finalità determinate, esplicite e legittime. Esso è strettamente correlato al principio di limitazione della conservazione[15] in base al quale i dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento: da qui l'obbligo di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario e, dunque, non superiore al conseguimento delle finalità per le quali sono trattati. Per effetto di quanto precede, ciascun titolare del trattamento dovrà individuare procedure idonee a perimetrare il periodo di conservazione adeguato dei dati personali trattati, il quale dovrà essere compatibile con quanto previsto sia dal Regolamento che da altre normative che potrebbero imporre processi di conservazione diversi, come, ad esempio, la normativa civilistica, fiscale e antiriciclaggio[16].

Il principio di esattezza[17] impone che i dati personali siano esatti e, se necessario, aggiornati. Ciò comporta che il titolare del trattamento dovrà ragionevolmente riscontrare l'esattezza del dato fornito sin dalla fase di raccolta dei dati e poi monitorare il suo aggiornamento nel tempo, procedendo, ove necessario, anche su impulso dell'interessato, alle opportune rettifiche[18]. I dati, infine, dovranno anche rispettare il principio

[14] Art. 5, par. 1, lett. b), GDPR.

[15] Considerando 39 GDPR e art. 5, par. 1, lett. e), GDPR. Si ricorda, peraltro, che la conservazione dei dati configura una modalità di trattamento tra quelle espressamente delineate dall'art. 4 GDPR.

[16] Si rinvia sul punto al Documento CNDCEC – FNC "*Il regolamento Ue/2016/679 General Data Protection Regulation (GDPR): nuove regole comunitarie e precisazioni in materia di protezione dei dati personali*", aprile 2018, ove è stato ritenuto condivisibile il criterio civilistico che individua in dieci anni il periodo di conservazione dei documenti rilevanti ai fini contabili, tributari e antiriciclaggio, in conformità con quanto previsto dalle norme di riferimento anche in relazione alla decorrenza dell'obbligo.
È opportuno peraltro precisare che la normativa sulla privacy è espressamente richiamata a proposito delle modalità di conservazione dei dati e delle informazioni ai fini della normativa antiriciclaggio (art. 32, D.Lgs. 231/2007). Si prevede, in particolare, che i soggetti obbligati devono adottare sistemi di conservazione dei documenti, dei dati e delle informazioni idonei a garantire il rispetto delle norme dettate dal codice in materia di protezione dei dati personali, nonché il trattamento dei medesimi esclusivamente per le finalità di cui al suddetto decreto.

[17] Art. 5, par. 1, lett. d), GDPR.

[18] Ai sensi dell'art. 16 GDPR il titolare dovrà, in ogni momento, riscontrare la richiesta dell'interessato di ottenere dal titolare del trattamento la rettifica o l'integrazione dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo. Inoltre,

di integrità e riservatezza[19]: in base al Regolamento, infatti, i dati personali devono essere trattati in maniera da garantirne un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. Sicché, il titolare del trattamento è tenuto ad adottare misure (tecniche ed organizzative) adeguate a tutelare l'accuratezza e l'integrità dei dati personali trattati, al fine di evitare alterazioni effettuate con dolo o con colpa da parte di agenti interni o esterni rispetto all'organizzazione.

A questo punto, è possibile effettuare qualche approfondimento sul principio di *accountability*.

Tale principio, anche noto come "principio di responsabilizzazione", non è contenuto in un'unica disposizione, ma permea l'intero Regolamento[20].

Esso, in sintesi, prevede che il titolare del trattamento (o il responsabile del trattamento) è competente per il rispetto di tutti i principi applicativi del GPDR e deve essere in grado di comprovarlo.

Detto principio rappresenta un'evoluzione rispetto a quanto previsto dal previgente Codice della Privacy, il quale imponeva delle misure minime di sicurezza per ciascun titolare del trattamento. Rispetto al passato, l'approccio normativo è stravolto: non esistono più prescrizioni dettagliate, ma è invece imposta una maggiore responsabilizzazione del titolare del trattamento che è tenuto, in base ad un comportamento proattivo, a modulare e ad attuare caso per caso i principi del Regolamento. Naturalmente, dovrà essere considerato anche il rischio inerente al trattamento: in altri termini le misure tecniche ed organizzative attuate dal titolare del trattamento dovranno essere adeguate alle singole realtà operative, tenuto conto non solo della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, ma anche dei rischi per i diritti e le libertà degli interessati.

Sotto il profilo operativo, pertanto, il titolare del trattamento dovrà non solo mettere in atto misure adeguate ed efficaci con riguardo ai trattamenti effettuati, ma anche effettuare un monitoraggio continuo al fine di verificarne la tenuta e la solidità nel tempo.

Infine, il titolare dovrà essere in grado di dimostrare la conformità delle attività di trattamento con il Regolamento, comprovando – o, ancor meglio, rendicontando – tutte le attività poste in essere al fine di rispettare le prescrizioni del GDPR.

Per questa ragione, il principio di *accountability* può essere pienamente compreso ed attuato solo in funzione degli altri principi precedentemente ricordati: nessun trattamento potrà essere rispondente al principio in oggetto se, ad esempio, sia posto in essere in maniera illecita (i.e. privo di una base giuridica adeguata), non trasparente o eccedente le finalità per le quali era stato avviato.

Il principio in oggetto comporterà, dunque, sotto il profilo operativo:

---

ai sensi dell'art. 18 GDPR, allorché l'interessato contesti l'esattezza dei dati personali trattati, il titolare del trattamento dovrà "limitare il trattamento" ovverosia "sospenderlo" per il periodo necessario per verificare l'esattezza di tali dati personali.

[19] Art. 5, par. 1, lett. f), GDPR.

[20] Si vedano tra gli altri gli artt. 5, par. 2, 24 e 32 e il Considerando 74, 77, 78 e 85 del Regolamento.

- la valutazione delle misure tecnico-organizzative meglio aderenti alle specifiche realtà operative e organizzative, anche in funzione del rischio inerente al trattamento;
- l'identificazione della base giuridica del trattamento dei dati personali;
- l'individuazione effettiva dei ruoli, dei compiti e delle responsabilità di ciascun soggetto coinvolto nel trattamento dei dati;
- il concreto e integrale rispetto di tutti i diritti dell'interessato (es. predisposizione di una apposita procedura per l'esercizio dei diritti);
- l'effettuazione di tutti gli adempimenti richiesti dalla normativa sulla privacy, (quali, a titolo esemplificativo, e non esaustivo: la somministrazione dell'informativa, l'adozione del registro dei trattamenti, l'effettuazione della valutazione d'impatto, la nomina del DPO);
- l'adesione volontaria a meccanismi premiali (codici di condotta e/o certificazioni);
- l'istituzione di procedure relative al c.d. *data breach* (di cui si dirà nel prosieguo).

Non è inoltre trascurabile che, in forza del principio di *accountability*, il titolare possa essere chiamato ad adottare misure di carattere volontario, eccedenti quelle previste ai fini del rispetto formale degli adempimenti richiesti dal regolamento, ma che alla luce di una valutazione complessiva di rispetto dei principi del GDPR si pongano come doverose in relazione allo specifico trattamento effettuato. Rispetto a questa particolare sfumatura che il principio di *accountability* assume, i codici di condotta riferiti al settore di attività in cui opera il titolare rappresentano un'importante occasione di facilitazione, sia nell'individuazione delle misure di sicurezza da adottare, sia nella dimostrazione della loro efficienza.

Strettamente correlati al principio di *accountability* sono infine i principi di *privacy by design* (o "protezione dei dati fin dalla progettazione") e di *privacy by default* (o "protezione per impostazione predefinita")[21].

Il principio del *privacy by design* impone al titolare di garantire la protezione dei dati fin dalla fase di ideazione e di progettazione di un trattamento di dati personali. Pertanto, ogni attività posta in essere dal titolare che preveda un trattamento di dati personali dovrà essere progettata e sviluppata in modo da assicurare il rispetto dei principi posti (e sopra ricordati) a tutela della privacy dell'interessato[22]. Il principio del *privacy by default* si pone in linea di continuità con il precedente e costituisce una specificazione dei principi di "minimizzazione dei dati", "limitazione della finalità" e di "limitazione della conservazione". Il principio di *privacy by default* potrà dirsi rispettato se l'architrave organizzativa predisposta dal titolare sia rispettosa dei principi del GDPR, garantendo in particolare che vengano raccolti soltanto i dati necessari al perseguimento delle finalità del trattamento, che queste ultime siano quanto più possibile limitate e che le attività di trattamento e la conservazione dei dati raccolti

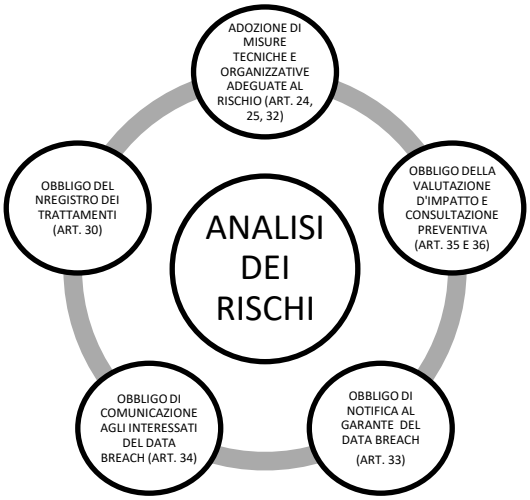
[21] Art. 25 GDPR.
[22] Il Regolamento stabilisce infatti che "sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del (...) regolamento e tutelare i diritti degli interessati".

siano il più possibile ridotte nel tempo[23]. La limitazione deve attenere anche al numero dei soggetti autorizzati dal titolare al trattamento dei dati.

6. L'analisi dei rischi

6.1. Premessa

L'analisi dei rischi è una fase centrale del processo di valutazione del trattamento dei dati personali, da cui scaturiscono obblighi e decisioni, come rappresentato nel seguente schema.



6.2. Definizione di rischio GDPR

È bene precisare che il rischio da valutare è quello in capo agli interessati e non quello aziendale, che talune volte può anche essere superiore rispetto al primo.

Ad esempio, nell'ambito di una impresa di trasporti di materiale edile, la perdita di un file che riporta il nominativo del cliente, la data e il luogo della consegna, presenta un rischio GDPR basso o nullo (se i clienti sono tutti soggetti giuridici), a fronte di un rischio, in termini di perdite economiche, alto per l'impresa.

Il considerando 75 del Regolamento individua come rischi quelli che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali.

[23] È richiesto infatti che il titolare adotti misure tecniche e organizzative adeguate a garantire che siano trattati per impostazione predefinita solo i dati personali necessari per ogni specifica finalità del trattamento. Il rispetto del principio di minimizzazione vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.
Nei considerando dedicati ai suddetti principi si chiarisce che il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, (...) consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati (...), i produttori (...) dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni.

Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

Quindi la prima domanda da porsi quando si effettua l'analisi dei rischi è la seguente: quali sono i rischi in capo all'interessato in caso di violazione dei dati personali?

6.3. Un tool per effettuare l'analisi dei rischi

Per effettuare l'analisi dei rischi sul trattamento dei dati personali, l'Agenzia UE per la sicurezza informatica (ENISA) ha lanciato una piattaforma online che fornisce indicazioni per individuare il proprio profilo di rischio.

ENISA propone la valutazione dei rischi partendo dalla tipologia delle violazioni previste dal GDPR (R.I.D. – Riservatezza, Integrità, Disponibilità), che sono classificate come segue:

1. "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
2. "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
3. "violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Lo schema logico del *tool* Enisa è il seguente:

a) definizione del processo di trattamento e del contesto (non si può valutare qualcosa che non si conosce);

b) valutazione dell'impatto sull'interessato in caso di violazione della riservatezza, dell'integrità e della disponibilità. Ciascuno dei tre passaggi deve essere valutato con una scala a 4 livelli (basso, medio, medio-alto, alto), secondo quanto illustrato nella seguente tabella:

LIVELLO DI IMPATTO	DESCRIZIONE
Basso	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.)
Medio	Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.)
Medio alto	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.)
Alto	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte)

Schematizzando:

Valutazione impatto sull'interessato)

RISERVATEZZA	INTEGRITÀ	DISPONIBILITÀ
Basso	Basso	Basso
Medio	Medio	Medio
Medio alto	Medio alto	Medio alto
Alto	Alto	Alto

Il più alto di questi livelli è considerato come il risultato finale della valutazione dell'impatto.

Esempio: Riservatezza = basso
Integrità = medio
Disponibilità = alto

Il risultato finale sarà Impatto = alto

c) valutazione della probabilità che si verifichi la minaccia, da effettuare prendendo in considerazione singolarmente:

- le risorse tecniche;
- i processi di trattamento;
- i soggetti coinvolti nel processo di trattamento;
- il settore commerciale e le dimensioni del trattamento.

La probabilità delle minacce deve essere valutata con una scala a 3 livelli attribuendo un punteggio da 1 a 3, secondo quanto illustrato nella seguente tabella:

LIVELLO DI PROBABILITÀ	DESCRIZIONE	PUNTEGGIO
Basso	È improbabile che la minaccia si materializzi	1
Medio	C'è una ragionevole possibilità che la minaccia si materializzi	2
Alto	La minaccia potrebbe materializzarsi	3

Valutazione delle minacce (PROBABILITÀ) su:

Risorse tecniche (HD, rete, ecc.)	Processi di trattamento	Soggetti coinvolti nel processo di trattamento	Settore attività e dimensione del trattamento
Basso	Basso	basso	Basso
Medio	Medio	medio	Medio
Alto	Alto	alto	Alto

La probabilità totale scaturisce dalla sommatoria dei punteggi in base alla seguente scala:

SOMMA GLOBALE DELLA PROBABILITÀ DI OCCORRENZA DI UNA MINACCIA	LIVELLO DI PROBABILITÀ DELLE MINACCE
4-5	**Basso**
6-8	**Medio**
9-12	**Alto**

d) valutazione del rischio complessivo del trattamento

Dopo aver valutato l'impatto dell'operazione di trattamento sui dati personali e la probabilità che si verifichino le relative minacce, la valutazione del rischio è definita in base al seguente schema:

		IMPATTO		
		BASSO	MEDIO	ALTO/MOLTO ALTO
PROBABILITÀ DELLE MINACCE	BASSO			
	MEDIO			
	ALTO			

Dopo aver individuato il rischio occorre definire le misure di sicurezza, come descritto nel paragrafo 8 del presente documento.

7. La valutazione di impatto (Data Protection Impact Assessment)

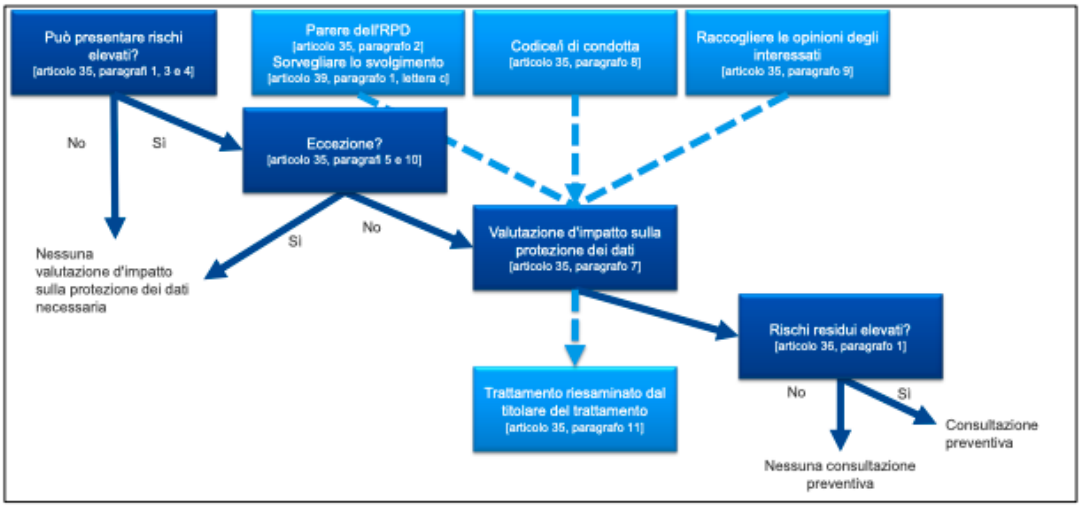
7.1. Premessa normativa

La valutazione d'impatto trova il suo presupposto giuridico nell'art. 35 del GDPR, che al paragrafo 1 prevede: "Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi".

La materia della valutazione d'impatto è stata oggetto di specifiche linee guida, denominate WP248[24].

Il seguente schema, presente nelle linee guida WP248, sintetizza il processo di valutazione d'impatto dettato dagli artt. 35 e 36 del GDPR.

[24] Gruppo di lavoro articolo 29 per la protezione dei dati, 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, adottate il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017, https://ec.europa.eu/newsroom/article29/items/611236.



Punto di partenza della valutazione d'impatto è l'analisi dei rischi che dovrà consentire di individuare i trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati per cui è necessario effettuare la valutazione d'impatto.

La valutazione d'impatto fa parte dell'*accountability*, in grado di dimostrare la compliance alla normativa del titolare del trattamento.

7.2. Criteri per definire l'obbligatorietà della valutazione d'impatto

Premesso che è sempre consigliata una DPIA (Data Protection Impact Assessment) per i trattamenti che si effettuano, segnaliamo che l'obbligatorietà della stessa può evincersi attraverso la compilazione di un questionario strutturato sulla base di nove criteri (definiti dalle linee guida WP248).

I nove criteri presi in esame sono:

NUMERO	CRITERI	RISPOSTA (SI/NO)
1	Trattamento di dati sensibili (dati particolari art. 9 GDPR)	
2	Trattamento su "larga scala" (considerando 91): - numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; - volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; - durata, o persistenza, dell'attività di trattamento; - ambito geografico dell'attività di trattamento.	
3	Dati relativi a interessati "vulnerabili", come ad esempio minori e anziani (considerando 75)	
4	Trattamento che di per sé impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (art. 22 e considerando 91), come ad esempio screening dei dati di clienti di una banca con banche dati centrale rischi che possono determinare l'ammissione a finanziamenti	

5	Trattamento automatizzato, valutativo o scoring, compresa la profilazione a partire da "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (considerando 71 e 91)	
6	Combinazione o raffronto di insieme di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti	
7	Applicazione nuove tecnologie, come l'associazione fra tecniche dattiloscopiche e riconoscimento del volto per migliorare il controllo degli accessi fisici …(art. 35, paragrafo 1, e considerando 89 e 91)	
8	Monitoraggio sistematico, trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o "la sorveglianza sistematica di un'area accessibile al pubblico" (art. 35, paragrafo 3, lettera c)	
9	Decisioni automatizzate che producono significativi effetti giuridici o di altra natura, come i trattamenti finalizzati ad assumere decisioni su interessati che possano per esempio, comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione (art. 35, paragrafo 3, lettera a)	

I Garanti europei prevedono la "regola del due", per cui solo i trattamenti che soddisfano almeno due criteri richiedono una valutazione d'impatto.

Tale regola non può essere considerata assoluta in quanto:

a) il titolare è tenuto ad effettuare la valutazione d'impatto anche in caso di un solo criterio, quando si è in presenza di un rischio elevato;

b) il titolare può non effettuare la valutazione d'impatto in presenza di due criteri, motivandola documentalmente.

Si segnala che il Garante Privacy ha fornito il seguente elenco delle tipologie di trattamenti da sottoporre a valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, co. 4, del GDPR[25].

	ELENCO DELLE TIPOLOGIE DI TRATTAMENTI, SOGGETTI AL MECCANISMO DI COERENZA, DA SOTTOPORRE A VALUTAZIONE D'IMPATTO
1	Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato".
2	Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).

[25] Autorità garante per la protezione dei dati personali, Provvedimento n. 467 dell'11 ottobre 2018, Allegato 1 (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018).

3	Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza, ecc.
4	Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
5	Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
6	Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
7	Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01.
8	Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
9	Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).
10	Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11	Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12	Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

7.3. Risultato del processo di valutazione d'impatto

La valutazione d'impatto può condurre al seguente risultato:

- DPIA non accettabile

La non accettabilità della DPIA comporta un riesame dei rischi relativi al trattamento, con contestuale individuazione di nuove misure più idonee a garantire la sicurezza dei dati personali (rifacimento della DPIA fino alla sua accettabilità).

L'art. 36 del GDPR al paragrafo 1 prevede che "Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio" (c.d. consultazione preventiva).

- DPIA accettabile ma migliorabile

La valutazione "migliorabile" significa che le informazioni fornite durante la fase di edizione sono sufficienti, ma alcune azioni correttive devono essere adottate per migliorare la conformità o la sicurezza del trattamento. Scegliendo questa valutazione, è obbligatorio descrivere le azioni correttive che saranno aggiunte al piano d'azione.

- DPIA accettabile

La valutazione "accettabile" significa che le informazioni fornite durante la fase di edizione sono sufficienti e che il trattamento è conforme e protegge in modo ottimale i dati personali.

L'Autorità francese di protezione dei dati personali (CNIL) ha reso disponibile, anche in versione italiana, un software open source per la redazione della DPIA, disponibile sul sito del Garante italiano[26].

Si rinvia all'Allegato 1 "Redazione di una DPIA relativa all'installazione di un sistema di videosorveglianza (mediante utilizzo del software messo a disposizione dal CNIL)".

8. Le misure di sicurezza

In precedenza, si è già accennato ad una valutazione dei rischi collegata al livello di gravità, aspetto base per mettere in pratica il concetto di *accountability* richiesto dalla normativa privacy (art. 24 e 25 GDPR).

Analizzare la tipologia dei rischi in materia di Data Privacy comporta una gestione ordinata e strutturata del trattamento dei dati.

All'art. 32 del GDPR vengono indicati gli obblighi per il titolare e per il responsabile del trattamento, nonché i requisiti necessari per trattare dati personali: "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio che comprendono, tra le altre, se del caso:

1. la pseudonimizzazione e la cifratura dei dati personali;

[26] Il software è reperibile al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/8581268.

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

Ma come fare a valutare i rischi?

Il Legislatore, volutamente, non fornisce indicazioni precise sulle misure di sicurezza da implementare; prima dell'entrata in vigore del GDPR, infatti, vi era il riferimento chiaro alle misure minime di sicurezza indicate nell'Allegato B del D.Lgs. 196/2003, con i provvedimenti dell'Autorità Garante. La loro applicazione è ancora oggi da considerare, di massima, il livello minimo accettabile per il trattamento dei dati personali, ma chiaramente non può bastare: con la nuova normativa, il Garante passa il testimone al titolare dei dati che, conoscendo e analizzando i trattamenti in atto, o in procinto di attuare, è colui che meglio di chiunque altro può porre in essere quelle misure di sicurezza necessarie per tutelare i dati e rendere sicuri i trattamenti stessi.

Sul punto, senza pretesa di esaustività, di seguito si riporta una modalità operativa utile per individuare le aree critiche o potenzialmente critiche.

In primo luogo, è opportuno soffermarsi sui trattamenti che vengono effettuati in azienda (che dovrebbero essere già tutti elencati nel Registro del trattamento, ai sensi dell'art. 30 del Regolamento) e valutare il rischio potenziale, non considerando quindi eventuali controlli e misure di sicurezza adeguate e magari già implementate, ma individuando tipologia e quantità dei dati trattati, per poi individuare i potenziali rischi che si potrebbero causare agli interessati.

In questo modo verranno indicati nel Registro del trattamento (che ricordiamo essere un documento "vivo" necessario per una corretta gestione della Data Privacy) i punti di attenzione imprescindibili per l'analisi e gli interventi di sicurezza.

Allo stesso modo si dovrà calcolare il rischio effettivo netto, valutando le contromisure di sicurezza applicate: l'efficacia di queste ultime dovrebbe essere dimostrata dalla riduzione del rischio dal potenziale al netto (in base alle misure di sicurezza applicate e ai controlli eseguiti, si andrà a ridurre la probabilità del rischio analizzato, oltre all'eventuale impatto).

Si ricorda che la valutazione del rischio si effettua partendo dalla valutazione dell'impatto e procedendo poi con la valutazione della probabilità delle minacce. Il rischio complessivo risulta dall'intersezione dei due valori e dal risultato del rischio complessivo discenderanno poi le misure di sicurezza da implementare all'interno dell'organizzazione per il mantenimento del rischio a valori accettabili.

A seconda della valutazione emersa sarà quindi possibile implementare soluzioni tecniche e organizzative così da ridurre eventuali rischi, con l'attenzione di definire e dare evidenza dei tempi necessari e dei costi relativi.

ENISA fornisce uno strumento per la valutazione del rischio di sicurezza secondo lo standard ISO/IEC 27001:2013[27].

A titolo non esaustivo si riportano alcuni esempi:

- politica di controllo degli accessi
- gestione delle risorse
- business continuity
- addestramento del personale

Tale analisi andrà verificata a cadenza regolare e riaggiornata di conseguenza, sempre con attenzione alle misure di sicurezza implementate, che magari necessitano di un aggiornamento alle procedure e ai documenti, oltre che al rapporto con eventuali terze parti.

Nonostante le attività implementate e le misure di sicurezza previste, in alcuni trattamenti possono persistere rischi elevati, per cui sarà necessario effettuare una valutazione d'impatto sulla protezione dei dati (DPIA, art. 35 del Regolamento), sulla base di quanto previsto e indicato dal Garante stesso.

Bisogna sempre prestare attenzione alla conservazione da parte del titolare del trattamento delle evidenze delle attività eseguite, dei documenti utilizzati e dei piani di adeguamento in corso, che rappresentano la documentazione minima di riscontro proprio per dimostrare il principio di *accountability* su cui si basa la normativa di riferimento in tema di trattamento dei dati.

Tale attività, nel suo complesso, richiede in molti casi conoscenze ed esperienze tecniche specifiche, come conoscenza degli standard di gestione e controllo, modalità di valutazione e gestione dei rischi, tecniche informatiche per la protezione dei dati, raccolta di evidenze in modo sicuro.

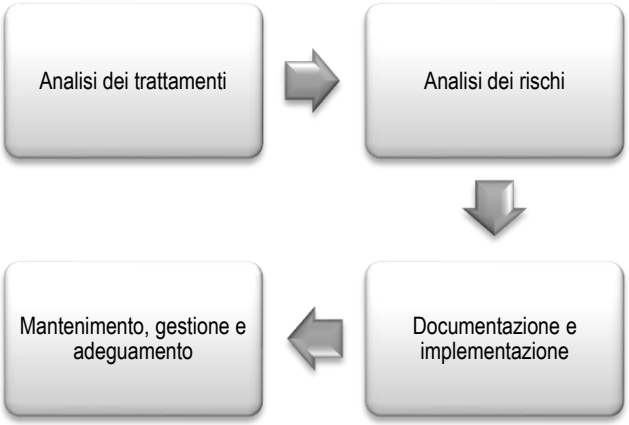
Per questo motivo il coinvolgimento di un DPO, esperto in argomento, rende l'analisi più corretta e completa, e tranquillizza il titolare sui risultati delle valutazioni ottenute, oltre a consentire spesso di ottimizzare i costi di gestione, anche negli aspetti legati alla sicurezza.

La nomina del DPO non deve essere considerata solo come un obbligo, cercando quindi di ridurne il costo al minimo, anche a scapito della qualità del servizio; la scelta di un professionista qualificato come il DPO può infatti permettere di gestire i dati in maniera più funzionale, creando nuove

[27] Il 16.03.2022 ENISA ha pubblicato un documento: "RISK MANAGEMENT STANDARDS, Analysis of standardisation requirements in support of cybersecurity policy", in cui descrive metodologie e strumenti che possono essere utilizzati per conformarsi o implementare tali standard. Tra i sistemi di certificazione per la sicurezza delle informazioni c'è la UNI CEI EN ISO/IEC 27001:2017, Tecnologie Informatiche – Tecniche di sicurezza – Sistemi di gestione della sicurezza dell'informazioni *https://www.enisa.europa.eu/publications/risk-management-standards.*

opportunità o nuovi trattamenti sui dati stessi (come attività di marketing e/o di profilazioni più strutturate) e diventare dunque fondamentale per l'azienda.

In conclusione, l'intero processo di gestione della privacy in azienda si può riassumere nel diagramma di seguito rappresentato.



Da tale schema si evince come l'attività privacy in azienda, svolto l'iter iniziale di analisi e valutazione, implementato l'aspetto documentale, organizzativo e procedurale, va comunque sempre mantenuta "viva", così da poter recepire non solo le novità normative, ma anche la crescita e lo sviluppo dell'azienda stessa che si pone come titolare nel trattamento dei dati. In questo modo la normativa privacy non si configura soltanto come l'ennesimo adempimento da rispettare, ma come una possibilità per poter gestire al meglio e in maniera più funzionale i dati trattati, oltre che poter svolgere ulteriori attività sugli stessi, avendo un patrimonio a disposizione di dati corretti, aggiornati, lecitamente acquisiti e trattati e, dunque, aderenti a quanto richiesto dalla normativa.

Nell'Allegato 2 al presente documento si fornisce un esempio di check list utile per poter valutare e, se del caso, implementare misure di sicurezza sia tecniche che organizzative.

9. La violazione dei dati personali (data breach)

Con la locuzione "violazione di dati personali", ai sensi degli artt. 33 e 34 del GDPR, ci si riferisce ad una 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.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

Il Garante per la Protezione dei Dati Personali, sul proprio sito internet[28], ha fornito alcuni esempi di violazione dei dati personali, che vengono di seguito riportati:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Le violazioni possono essere classificate come segue:

- "violazione della riservatezza", in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- "violazione della disponibilità", in caso di perdita accidentale o non autorizzata di accesso o distruzione di dati personali;
- "violazione dell'integrità", in caso di alterazione non autorizzata o accidentale dei dati personali.

Inoltre, le cause più comuni si possono categorizzare in:

- "violazione involontaria o accidentale", quale ad esempio lo smarrimento di un supporto cartaceo, come un documento, un device o un supporto elettronico come un'unità flash USB;
- "furto" perpetrato con chiare intenzioni illecite, come ad esempio il furto dei detti supporti cartacei e/o elettronici;
- "volontarietà illecita da parte di dipendenti", quando la violazione viene causata da un soggetto interno all'organizzazione, accedendo in maniera autorizzata alle informazioni, ma trattandole poi illegittimamente;
- "accesso non autorizzato/alterazione dei dati", quando viene condotto un attacco avente come fine l'accesso senza autorizzazioni ai sistemi informatici, l'acquisizione dei dati personali e/o l'alterazione/divulgazione degli stessi[29].

In considerazione del fatto che la tutela dei diritti e delle libertà delle persone fisiche costituisce uno dei principali obiettivi del GDPR, le violazioni di dati personali che assumono rilievo sono quelle che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali.

A tali effetti avversi significativi possono essere ricondotti, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita

[28] https://www.garanteprivacy.it/regolamentoue/databreach.
[29] Si vedano, sul punto, gli artt. 5 e 32 del GDPR e il Considerando 49 dello stesso.

finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale, ecc.

Nel corso del 2020 e del 2021, anni in cui le aziende si sono trovate a dovere gestire in maniera improvvisa le nuove necessità connesse alla pandemia causata dal COVID-19, le violazioni di dati si sono moltiplicate sotto forma di "attacchi esterni" ai sistemi aziendali. Tali attacchi sono stati facilitati dai seguenti fattori:

- massivo ricorso allo smart working secondo modalità non definite da misure di sicurezza fisiche e logiche adeguate da parte delle organizzazioni;
- cambio delle abitudini degli utenti, che si sono trovati a lavorare nell'ambito del contesto familiare, creando un abbassamento del livello di attenzione e un uso dei dispositivi aziendali "allargato" rispetto al contesto professionale tradizionale;
- accesso alla rete aziendale con dispositivi personali non configurati preventivamente per svolgere l'attività lavorativa da casa;
- aumento degli accessi esterni alla rete aziendale.

Nel caso in cui si verifichi una delle summenzionate violazioni, il titolare del trattamento, dopo averne avuto notizia, è chiamato ad inviare apposita notifica al Garante per la Protezione dei Dati Personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la citata notifica non sia effettuata entro 72 ore, la stessa deve essere corredata dai motivi del ritardo.

Da quanto precedentemente riportato emerge come la violazione di dati personali rappresenti un momento di crisi all'interno dell'organizzazione aziendale, che deve essere gestito in maniera tempestiva da personale qualificato e preparato alla gestione degli incidenti, con il supporto di consulenti specializzati e di eventuali responsabili del trattamento, nonché tramite l'utilizzo di una metodologia adeguata.

Di seguito verrà illustrato, senza alcuna pretesa di completezza, come può essere gestita una violazione di dati personali, con l'obiettivo di limitare i danni che dalla stessa potrebbero derivare sia all'organizzazione aziendale che ai diretti interessati, proprietari dei dati coinvolti.

È importante precisare, innanzitutto, che una corretta gestione del fenomeno del *data breach* non può limitarsi alla "notificazione" della stessa al Garante per la Protezione dei Dati Personali, ma deve consistere anche nell'implementazione di misure tecniche e organizzative, preventivamente studiate e testate, quali:

- l'implementazione di misure preventive (tecniche e organizzative) volte a ridurre il rischio di una violazione di dati personali;
- l'adozione di una procedura specifica che assegni chiaramente ruoli e responsabilità;

- l'organizzazione ed erogazione di corsi di formazione. Con riferimento a tale aspetto, si specifica che la formazione del personale è fondamentale e dovrebbe essere accompagnata da almeno una simulazione di incidente per testare la risposta tempestiva dei soggetti preposti alle diverse operazioni.

Da un punto di vista pratico, si può rilevare che le fasi di gestione di una violazione di dati personali possono essere individuate nelle seguenti:

a) segnalazione e identificazione;
b) valutazione del rischio;
c) notifica al Garante;
d) comunicazione agli interessati;
e) registrazione dell'incidente;
f) risoluzione e piano di rimedio.

a) Segnalazione e identificazione

Si è detto che una gestione efficace delle violazioni di dati personali conforme al GDPR deve essere consapevole e di veloce attuazione.

Tale assunto presuppone che l'organizzazione sia in grado di riconoscere immediatamente una presunta violazione, sappia a chi comunicare questa situazione e conosca gli obblighi gravanti sul datore di lavoro in tali circostanze al fine di segnalare tempestivamente l'accaduto.

È fondamentale quindi – lo si ribadisce – che l'ente abbia formato e sensibilizzato il proprio personale in merito ad una corretta gestione del *data breach*.

Per questo motivo il Titolare del Trattamento, anche datore di lavoro, ha il compito di:

- conferire delle specifiche deleghe interne volte a designare i soggetti individuati e coinvolti nella gestione e risoluzione dell'incidente;
- fornire istruzioni precise all'insieme dei dipendenti;
- definire la gestione del processo aziendale relativo alle violazioni di dati personali con una procedura dettagliata;
- porre in essere azioni periodiche di sensibilizzazione e formazione del personale al fine di alzare la soglia di attenzione e la conoscenza delle azioni da svolgere in caso si verifichi l'incidente;
- organizzare simulazioni di incidenti.

A seguito del ricevimento della notifica – che può essere effettuata sia da un dipendente che da un soggetto esterno all'organizzazione aziendale – dell'incidente di sicurezza, il titolare del trattamento è chiamato a procedere immediatamente alla verifica della natura dello stesso e a ricostruire i fatti, al fine di valutare se ci si trovi effettivamente in presenza di un *data breach*.

Nel caso in cui l'incidente non coinvolga dati personali, il titolare del trattamento ha il compito di verificare l'origine dello stesso e valutare l'opportunità di svolgere ulteriori approfondimenti, indipendentemente dagli obblighi derivanti dal GDPR. È opportuno che nello svolgimento dell'indagine il titolare del trattamento si faccia supportare dalla funzione aziendale di information technology, al fine di risolvere le criticità esistenti e mettere al sicuro i sistemi e la rete.

Nell'ipotesi in cui, invece, il *data breach* coinvolga dati personali, il titolare del trattamento è chiamato a mettere in atto tutti i mezzi e a svolgere tutte le azioni necessarie per ottenere il maggior numero possibile di informazioni relative alla violazione e capire in che modo la stessa si è verificata (ad esempio, se sia stata originata da attacchi esterni o interni al perimetro aziendale; la categoria di dati personali coinvolti; il numero di dati violati; le possibili conseguenze di tale violazione).

In caso di violazione dei dati ancora in essere, da cui potrebbe derivare una fuoriuscita di dati personali dall'azienda, il titolare del trattamento ha il compito di coinvolgere i dipartimenti interni e le terze parti che si occupano della gestione dei sistemi e della rete aziendale, al fine di bloccare immediatamente la fuga di dati e limitare al massimo gli impatti negativi sui soggetti coinvolti.

Nelle fattispecie di dati trattati da responsabili del trattamento, è necessario informare immediatamente le terze parti dell'accaduto e ottenere il necessario supporto nella gestione dell'incidente.

Grazie all'ottenimento del maggior numero possibile di informazioni relative all'incidente, il titolare del trattamento può procedere alla valutazione dei rischi per i diritti e le libertà dei soggetti coinvolti, ovvero di coloro ai quali i dati oggetto della violazione si riferiscono.

b) Valutazione del rischio

Al fine di fornire un valido supporto al titolare del trattamento nel complesso compito della valutazione dei rischi, il Garante per la Protezione dei Dati Personali ha reso disponibile, sul proprio sito web istituzionale, un utile strumento esplicativo della gestione delle violazioni di dati personali (*data breach*)[30] e uno strumento di auto-valutazione dell'incidente[31], ribadendo che, come già accennato in precedenza, la valutazione finale rientra nella esclusiva competenza e responsabilità del titolare del trattamento stesso.

Nella pratica, anche se il titolare del trattamento non dispone immediatamente di tutte le informazioni necessarie, lo stesso deve comunque iniziare, con tempestività, a stimare l'impatto della violazione e ad avviare una valutazione del rischio sulla base delle informazioni in suo possesso in modo da poter rispettare, se del caso, i termini richiesti dal GDPR.

La valutazione del rischio ha i seguenti scopi:

[30] https://www.garanteprivacy.it/regolamentoue/databreach.
[31] https://servizi.gpdp.it/databreach/s/self-assessment.

- individuare i tipi di conseguenze possibili sulla base delle categorie di dati oggetto della violazione e del contesto della violazione;
- individuare chi può essere venuto a conoscenza delle informazioni;
- comprendere se le informazioni sono definitivamente perse oppure recuperabili;
- valutare le possibili conseguenze;
- definire il livello di rischio;
- decidere se la violazione va notificata al Garante per la Protezione dei Dati Personali;
- definire le azioni di comunicazione da mettere in opera per ridurre al massimo l'impatto negativo per gli interessati.

Per essere attendibile, la valutazione della violazione deve essere svolta da un gruppo definito di persone, interno o esterno all'organizzazione, scelte per le loro competenze e la loro esperienza in modo da tenere sotto controllo il processo e definire chiaramente le responsabilità.

I valutatori avranno necessità di entrare in contatto con il soggetto che ha segnalato l'incidente, i diversi dipartimenti aziendali coinvolti e le eventuali terze parti, al fine di ottenere maggiori elementi che consentano un approfondimento informativo.

La valutazione del rischio deve svolgersi in modo oggettivo e deve consentire di verificare la possibilità che si verifichi uno degli eventi avversi di seguito elencati, nonché di stimarne la relativa gravità:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

All'esito della valutazione, il livello di gravità del *data breach* potrà essere:

LIVELLO DI RISCHIO	DESCRIZIONE
BASSO	È improbabile che si verifichi una violazione dei diritti e delle libertà per gli individui interessati, che potrebbero solamente subire degli inconvenienti minori facilmente risolvibili (necessità di inserire nuovamente i propri dati personali, disagi minori, irritazione, ecc.)
MEDIO	È probabile che si verifichi una violazione dei diritti e delle libertà per gli individui interessati, i quali potrebbero incontrare taluni disagi, che saranno in grado di superare nonostante alcune difficoltà (costi

	aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, discriminazione lieve, stress, ecc.).
ALTO	È probabile che si verifichi una violazione dei diritti e delle libertà per gli individui interessati, i quali potrebbero incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in black-list, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento delle condizioni di salute, ecc.).
MOLTO ALTO	È probabile che si verifichi una violazione dei diritti e delle libertà per gli individui interessati, i quali potrebbero incontrare conseguenze significative, o addirittura irreversibili, che difficilmente riusciranno a superare (difficoltà finanziarie, incapacità lavorativa, disturbi psicologici o fisici a lungo termine, gravi lesioni o morte, ecc.).

Nel caso in cui l'incidente venga classificato come alto o molto alto, il delegato del titolare del trattamento[32] informerà i vertici aziendali di riferimento (in particolare, il legale rappresentante della società titolare del trattamento) e il DPO qualora non fossero stati già informati in precedenza.

In base al livello di rischio per gli interessati identificato, il titolare del trattamento dovrà porre in essere gli adempimenti riportati nella seguente tabella:

LIVELLO DI RISCHIO	NOTIFICA AL GARANTE ENTRO LE 72 ORE	COMUNICAZIONE ALL'INTERESSATO SENZA INGIUSTIFICATO RITARDO
Alto / Molto alto	SI	SI
Medio	SI	NO / da valutare
Basso	NO	NO

c) Notifica al Garante

L'art. 33 del GDPR impone al titolare del trattamento di notificare all'autorità di controllo competente la violazione di dati personali entro 72 ore dal momento in cui ne venga a conoscenza, nel caso in cui esista un rischio per la tutela dei diritti e delle libertà degli interessati.

Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo. Di conseguenza, non tutte le violazioni di dati personali vanno comunicate all'Autorità Garante.

È quindi di fondamentale importanza, come visto anche in precedenza, che il titolare del trattamento effettui una valutazione dei rischi relativamente all'incidente e che tenga traccia di tale attività, dal

[32] Con il termine delegato del titolare del trattamento deve intendersi il soggetto designato dal titolare del trattamento per la supervisione delle attività sulla protezione dei dati personali nell'organizzazione.

momento che è proprio dall'esito di tale valutazione che scatta o meno l'obbligo di notifica all'Autorità garante.

È importante ricordare che, nel caso in cui la violazione di dati si produca presso il responsabile del trattamento, l'obbligo di comunicazione al Garante grava, comunque, sul titolare del trattamento.

Si rappresenta che, ai sensi dell'art. 28 del GDPR, «i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento».

A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/.

Nel caso in cui il titolare non possa compilare tutte le sezioni della notifica, lo stesso è chiamato a ad eseguire una notifica "preliminare" e ad assicurarsi di compilare successivamente una notifica integrativa a completamento della precedente.

L'eventuale ritardo nella notifica deve essere giustificato; il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione, ovvero:

- l'esercizio dei poteri previsti dall'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati);
- l'imposizione di sanzioni amministrative individuate dall'art. 83 GDPR, che prevede una sanzione pecuniaria fino a euro 10.000.000 o, per le imprese, fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore.

d) Comunicazione agli interessati

Anche la comunicazione agli interessati deve avvenire sulla base dell'esito della valutazione dei rischi effettuata relativamente all'incidente.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche il titolare del trattamento deve comunicare, senza ingiustificato ritardo, la violazione agli interessati, ovvero alle persone fisiche i cui dati sono stati oggetto di violazione.

La comunicazione ha come obiettivo quello di consentire agli interessati di prendere le precauzioni necessarie per proteggersi da eventuali conseguenze derivanti dalla violazione.

Il GDPR raccomanda di effettuare tale comunicazione non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti dalla stessa.

Risulta evidente che la comunicazione agli interessati può comportare un danno reputazionale, anche rilevante, per il titolare del trattamento; i contenuti della stessa, quindi, vanno ponderati con attenzione dal titolare del trattamento dopo avere informato il DPO.

Secondo l'art. 34 del GDPR, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. La comunicazione deve fornire almeno le seguenti informazioni:

- una descrizione della natura della violazione;
- il nome e i dettagli di contatto del DPO o di altri punti di contatto presso cui ottenere più informazioni;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o che il titolare propone di adottare per porre rimedio alla violazione, comprese, se del caso, misure per mitigarne gli eventuali effetti negativi.

La notifica, inoltre, deve essere presentata in un linguaggio chiaro e di facile comprensione per il soggetto interessato.

Sono presenti delle eccezioni relativamente all'obbligo di notifica di una violazione di dati agli Interessati.

L'art. 34, paragrafo 3 GDPR, stabilisce infatti le tre condizioni seguenti che, se soddisfatte, non richiedono la comunicazione agli interessati in caso di violazione:

- il titolare del trattamento ha applicato misure tecniche e organizzative adeguate a proteggere i dati personali prima della violazione, in particolare quelle misure che rendono i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi (es. cifratura);
- immediatamente dopo la violazione, il titolare del trattamento ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati. Le Linee Guida wp250[33] riportano l'esempio del titolare del trattamento che potrebbe avere immediatamente identificato e intrapreso un'azione contro la persona che ha avuto accesso illegittimo ai dati personali prima che questi avesse potuto fare qualcosa con tali dati. Le Linee Guida sottolineano tuttavia che, in ogni caso, è necessario tenere in debito conto le possibili conseguenze di eventuali violazioni della riservatezza, a seconda della natura dei dati in questione;
- quando la comunicazione agli interessati comporterebbe uno sforzo sproporzionato, come nell'ipotesi in cui i loro dettagli di contatto siano stati persi a causa della violazione o non siano noti in primo luogo. In questi casi, Il titolare del trattamento deve fare una comunicazione pubblica o prendere una misura simile, in modo che le persone ne siano informate.

Conformemente a quanto richiesto dal principio di responsabilizzazione (*accountability*), il titolare del trattamento deve essere in grado di dimostrare all'autorità di supervisione di soddisfare una o più di queste condizioni.

[33] Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 - WP 250.

Nel caso in cui il titolare del trattamento decida di non procedere alla comunicazione agli interessati, l'autorità Garante, esaminando gli elementi della notificazione, potrebbe esprimere parere diverso e richiedere comunque la comunicazione.

Inoltre, il titolare del trattamento deve prevedere l'opportuna gestione del riscontro ad eventuali richieste provenienti da parte degli interessati che riceveranno la comunicazione.

e) Registrazione dell'incidente

Come precedentemente riportato, il titolare del trattamento – nel rispetto del principio di *accountability* e in conformità a quanto richiesto dalla normativa vigente – deve adottare tutte le misure tecniche ed organizzative ritenute appropriate al fine di limitare i rischi connessi al trattamento dei dati personali e garantire un livello di sicurezza adeguato.

È inoltre necessario che il titolare del trattamento sia sempre in grado di dimostrare di avere svolto i predetti adempimenti e di avere fatto tutto quanto in suo potere per tutelare al meglio i dati personali trattati; lo stesso, pertanto, deve essere in possesso di evidenze attendibili di tale conformità.

In termini di *accountability*, il titolare del trattamento, a prescindere della notifica all'Autorità Garante, ha il compito di svolgere correttamente tutti gli adempimenti riportati ai punti precedenti, nonché di tenerne traccia.

Le violazioni di dati personali vanno annotate in uno specifico registro, in cui deve essere tenuta traccia di tutte le informazioni relative alla violazione, alla gestione svolta e alle azioni intraprese, comprese le motivazioni che hanno condotto alla decisione di inviare o meno la notifica al Garante e l'eventuale comunicazione diretta agli interessati.

Il registro può essere tenuto sia in formato cartaceo che elettronico; la scelta sulla modalità di conservazione deve essere effettuata dal titolare del trattamento.

Il registro va conservato dal titolare del trattamento o da un suo delegato ed esibito all'Autorità Garante su richiesta della stessa.

Il registro, inoltre, deve consentire di verificare, in caso di ispezione o di richiesta specifica, il rispetto degli adempimenti in capo al titolare del trattamento nella gestione delle violazioni dei dati personali.

Al fine di conferire al registro efficacia probatoria, è consigliabile l'archivio annuo del registro in formato PDF con marca temporale.

f) Risoluzione e piano di rimedio

Secondo quanto previsto dall'art. 33, paragrafo 3, lettera d) del GDPR, il titolare ha il compito di descrivere le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

In questo contesto, il titolare del trattamento deve:

- mettere in atto adeguate misure tecnico-organizzative valutate in funzione del livello di rischio;
- definire – al fine di prevenire nuovi episodi di *data breach* – un piano di azione correttivo, proponendo nuove azioni da implementare per migliorare la sicurezza e diminuire i possibili effetti negativi.

Pertanto, nel periodo compreso tra l'individuazione della violazione di dati e la risoluzione della stessa, il titolare del trattamento deve poter prendere misure adeguate ed efficaci che possano contenere gli effetti dannosi dell'incidente, oppure interrompere la situazione di rischio creatasi.
La fase in esame, definita "risoluzione", ha i seguenti obiettivi:

- minimizzare l'impatto degli eventi malevoli;
- individuare ed attuare in maniera tempestiva idonee misure di contrasto/contenimento;
- individuare ed attuare tutte le attività di ripristino e di ritorno alla normalità a seguito di un incidente;
- esporre denuncia alla Polizia Postale;
- mettere in atto le azioni correttive che possono risolvere le criticità legate all'incidente;
- predisporre un report di chiusura dell'incidente contenente la documentazione degli interventi posti in atto e dei risultati ottenuti, specificando, particolarmente per gli incidenti sistemici, i sistemi/servizi coinvolti e la documentazione degli interventi attuati, delle attività di ripristino effettuate con la data/ora di chiusura dell'incidente.

Le azioni di mitigazione vanno documentate e integrate nella documentazione relativa all'incidente di violazione di dati personali, anche con log di sistema, al fine di dimostrare la tempestività degli interventi posti in essere dal titolare del trattamento.

A seguito dell'incidente, sulla base dell'esperienza acquisita e con il contributo di esperti specializzati in protezione dei dati, cyber security e risk management dei dipartimenti aziendali implicati nei processi di sicurezza, nonché dei dipartimenti che sono stati coinvolti nell'incidente, l'azienda interessata dovrà svolgere un'analisi accurata:

- delle cause dell'incidente, ossia le minacce che hanno reso possibile l'incidente;
- delle conseguenze dell'incidente;
- dei sistemi coinvolti;
- delle modalità di sviluppo dell'incidente, nonché delle circostanze e/o delle vulnerabilità che lo hanno reso possibile;
- della gestione interna dell'incidente;
- dell'adeguatezza delle misure di sicure tecnico-organizzative in essere prima dell'incidente;
- dell'efficacia e l'efficienza delle azioni intraprese durante la gestione dell'evento;
- del rispetto della normativa dei dati personali;
- dei tempi di risoluzione e di ripristino della situazione;

- del ruolo svolto da eventuali responsabili del trattamento.

Le analisi svolte dovranno essere seguite:

- dalla definizione di un piano di rimedio sulla base delle criticità rilevate con riferimento alle procedure, all'organizzazione, alla tecnologia, formazione;
- dallo svolgimento di analisi periodiche di dati per produrre statistiche in grado di alimentare il processo di analisi proattiva, finalizzato al rilevamento di eventi sospetti o di comportamenti sospetti ripetuti nel tempo. In tale fase, un rilevante contributo può essere fornito dai feedback ricevuti dai soggetti coinvolti, che consentono di aumentare il grado di sensibilità verso le tematiche di sicurezza informatica e il livello di sicurezza delle infrastrutture tecnologiche gestite.

Le azioni individuate nel piano di rimedio dovranno, quindi, essere sottoposte a verifica e validazione da parte di un auditor interno o di un consulente esterno specificamente incaricato e successivamente implementate e testate con cadenza periodica.

Nella prassi, si riscontra come in aziende organizzate e attente alla sicurezza viene generalmente implementata una procedura di gestione degli incidenti di sicurezza.

Al fine di rivelarsi efficace, tale procedura deve prevedere azioni di sicurezza predittiva e preventiva, con un piano di vigilanza e di rilevamento periodici idonei a rilevare eventuali minacce esistenti (es. Penetration test).

Il titolare del trattamento ha il dovere di valutare le misure di sicurezza in essere e portare miglioramenti ai processi coinvolti, al fine di cercare di minimizzare il più possibile il rischio di commissione di successivi *data breach*.

10. I registri dell'accountability

10.1. Il registro dei trattamenti

L'art. 30 del Regolamento prevede che ogni titolare del trattamento e il suo eventuale rappresentante, nonché il responsabile del trattamento e il suo eventuale rappresentante, redigano un registro delle attività di trattamento svolte sotto la propria responsabilità. Il registro è, quindi, uno strumento atto a fornire una situazione aggiornata dei trattamenti in essere all'interno di una realtà aziendale o pubblica, ed è anche indispensabile per la valutazione e l'analisi del rischio connesso al trattamento.

Il Garante della Privacy ha pubblicato, sul proprio sito[34], le Faq sul Registro delle attività di trattamento per chiarire alcuni dubbi in merito all'obbligatorietà, all'uso, alla compilazione e conservazione del registro stesso; inoltre, il Garante ha messo a disposizione due fac-simile di modelli di registro e nello specifico il modello semplificato delle attività di trattamento del titolare per PMI e il modello semplificato delle attività di trattamento del responsabile per PMI.

[34] Le Faq sono reperibili all'indirizzo https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento.

Il Garante per la protezione dei dati personali, nella Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali[35], dispone che: "*il registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali*", e invita tutti i titolari del trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a dotarsi di tale registro.

Il Garante si rivolge, quindi, a tutti i soggetti, prescindendo dalle dimensioni dell'organizzazione, anche se l'art. 30 chiarisce che l'obbligo della tenuta di questi registri non è obbligatorio per le imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa categorie di dati come quelli di cui all'art. 9 del GDPR (particolari) o all'art. 10 del GDPR (dati relativi a condanne penali, reati o connessi a misure di sicurezza). La consequenziale deduzione è che il registro dei trattamenti va sempre redatto a prescindere dal numero di dipendenti.

Nella categoria delle "organizzazioni" rientrano anche le associazioni, le fondazioni e i comitati.

Il Garante per la protezione dei dati personali ha chiarito che devono redigere il registro, ad esempio:

- esercizi commerciali, esercizi pubblici o artigiani con almeno un dipendente (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);
- liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);
- associazioni, fondazioni e comitati ove trattino "categorie particolari di dati" e/o dati relativi a condanne penali o reati (i.e. organizzazioni di tendenza; associazioni a tutela di soggetti c.d. "vulnerabili" quali ad esempio malati, persone con disabilità, ex detenuti ecc.; associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull'orientamento sessuale, politico o religioso ecc.; associazioni sportive con riferimento ai dati sanitari trattati; partiti e movimenti politici; sindacati; associazioni e movimenti a carattere religioso);
- il condominio ove tratti "categorie particolari di dati" (es. delibere per interventi volti al superamento e all'abbattimento delle barriere architettoniche ai sensi della L. n. 13/1989; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all'interno dei locali condominiali).

Inoltre, il Garante ha precisato che le imprese e le organizzazioni con meno di 250 dipendenti obbligate alla tenuta del registro potranno comunque beneficiare di alcune misure di semplificazione, potendo circoscrivere l'obbligo di redazione del registro alle sole specifiche attività di trattamento sopra individuate (es. ove il trattamento delle categorie particolari di dati si riferisca a quelli inerenti a un

[35] La Guida è disponibile all'indirizzo http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali.

solo lavoratore dipendente, il registro potrà essere predisposto e mantenuto esclusivamente con riferimento a tale limitata tipologia di trattamento).

È opportuno ricordare che poiché i responsabili della protezione dei dati (DPO), tra i loro compiti, annoverano quello di monitorare tutti i trattamenti della realtà organizzativa di riferimento, è prassi consolidata che essi coadiuvino il titolare nella redazione del registro dei trattamenti, compilato sulla base delle informazioni fornitegli dai vari uffici o settori che trattano i dati personali.

Ecco perché è consigliato a tutti di predisporre in ogni caso un registro delle attività di trattamento a prescindere dagli obblighi normativi; in tal modo si realizza un importante elemento di valutazione ai fini:

- del rispetto del principio di *accountability;*
- del rispetto del principio di responsabilizzazione del titolare (art. 24);

e nello stesso tempo si facilitano le eventuali attività ispettive dell'Autorità.

Il registro deve essere tenuto in forma scritta, o anche in formato elettronico, a condizione che sia consultabile su richiesta al Garante e che fornisca una lista di contenuti obbligatori. In realtà, l'aspetto formale non è standardizzato in quanto è possibile adottare una struttura che meglio si adatti alla realtà in cui si colloca, motivo per cui può essere redatto sotto forma di schema oppure descrittivo, per mezzo di un foglio di calcolo o ancora in formato tabellare: ciò che conta è che vi siano tutti gli elementi richiesti dall'art. 30 del Regolamento. Ogni responsabile del trattamento e il suo eventuale rappresentante devono istituire ed aggiornare il registro delle attività di trattamento che deve avere i seguenti dati obbligatori:

1. il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
2. le finalità del trattamento: le Faq hanno chiarito che in questo campo, oltre alla precipua indicazione delle stesse, distinta per tipologie di trattamento (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini), sarebbe opportuno indicarne anche la base giuridica. Inoltre, sarebbe parimenti opportuno, in caso di trattamenti di "categorie particolari di dati", indicare una delle condizioni di cui all'art. 9, par. 2 del GDPR, mentre in caso di trattamenti di dati relativi a condanne penali e reati, riportare la specifica normativa (nazionale o dell'Unione europea) che ne autorizza il trattamento ai sensi dell'art. 10 del GDPR. Infine, con particolare riferimento al "legittimo interesse", il registro potrebbe riportare la descrizione dell'obiettivo concretamente perseguito, le "garanzie adeguate" eventualmente approntate, nonché, ove effettuata, la preventiva valutazione d'impatto posta in essere dal titolare;
3. una descrizione delle categorie di interessati e delle categorie di dati personali: in questo campo andranno specificate sia le tipologie di interessati (es. clienti, fornitori, dipendenti) sia quelle di

dati personali oggetto di trattamento (es. dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, ecc.);

4. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali: in tale campo andranno riportati, anche semplicemente per categoria di appartenenza, gli altri titolari cui siano comunicati i dati (ad esempio, enti previdenziali cui debbano essere trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi). Inoltre, il Garante ritiene opportuno che siano indicati anche gli eventuali altri soggetti ai quali, in qualità di responsabili e sub-responsabili del trattamento, siano trasmessi i dati da parte del titolare (ad esempio, soggetto esterno cui sia affidato dal titolare il servizio di elaborazione delle buste paga dei dipendenti o altri soggetti esterni cui siano affidate in tutto o in parte le attività di trattamento); ciò al fine di consentire al titolare medesimo di avere effettiva contezza del novero e della tipologia dei soggetti esterni cui sono affidate le operazioni di trattamento dei dati personali;
5. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49, la documentazione delle garanzie adeguate: in questo campo andrà riportata l'informazione relativa ai suddetti trasferimenti unitamente all'indicazione relativa al Paese/i terzo/i cui i dati sono trasferiti e alle "garanzie" adottate ai sensi del capo V del GDPR (ad esempio, decisioni di adeguatezza, norme vincolanti d'impresa, clausole contrattuali tipo, ecc.);
6. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati: dovranno essere individuati ed indicati i tempi di cancellazione per tipologia e finalità di trattamento (ad esempio, "in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall'ultima registrazione – v. art. 2220 del c.c."). Ad ogni modo, ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a criteri (come norme di legge o prassi settoriali, a titolo non esaustivo) indicativi degli stessi (a titolo d'esempio, "in caso di contenzioso, i dati saranno cancellati al termine dello stesso");
7. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative: il Garante nelle Faq specifica che andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell'art. 32 del GDPR (la pseudonimizzazione e la cifratura dei dati personali; la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento), tenendo presente che tale elenco costituisce una lista aperta e non esaustiva, essendo rimessa al titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere. Tale lista ha di per sé un carattere dinamico, dovendosi continuamente

confrontare con gli sviluppi della tecnologia e l'insorgere di nuovi rischi. Le misure di sicurezza possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo delle stesse in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (come le procedure organizzative interne, la security policy, ecc.).

Ogni responsabile del trattamento e il suo eventuale rappresentante tengono un registro di tutte le categorie di attività di trattamento dei dati personali svolte per conto di un titolare del trattamento, contenente:

1. nome e 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 dell'eventuale responsabile della protezione dei dati;
2. le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento; in questo campo è possibile far riferimento a quanto contenuto nel contratto di designazione a responsabile che, ai sensi dell'art. 28 del RGPD, deve individuare, in particolare, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati oggetto del trattamento, nonché la durata di quest'ultimo. Invece, in caso di sub-responsabile, il registro delle attività di trattamento svolte da quest'ultimo potrà specificatamente far riferimento ai contenuti del contratto stipulato tra lo stesso e il responsabile;
3. ove applicabile, i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49, la documentazione delle garanzie adeguate, con indicazione dell'autorizzazione del titolare;
4. ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative.

Per quanto concerne i punti 3 e 4, ai fini della compilazione si dovrà fare riferimento, rispettivamente, ai punti 5 e 7 relativi alla compilazione del Registro dei trattamenti del titolare.

Inoltre, nelle proprie Faq il Garante ha precisato che nel caso in cui uno stesso soggetto agisca in qualità di responsabile del trattamento per conto di più clienti quali autonomi e distinti titolari (es. società di software house), le informazioni dovranno essere riportate nel registro con riferimento a ciascuno dei suddetti titolari. In questi casi il responsabile dovrà suddividere il registro in tante sezioni quanti sono i titolari per conto dei quali agisce. Allorquando, a causa dell'ingente numero di titolari per cui si operi, l'attività di puntuale indicazione e di continuo aggiornamento dei nominativi degli stessi, nonché di correlazione delle categorie di trattamenti svolti per ognuno di essi, risulti eccessivamente difficoltosa, il registro del responsabile potrebbe riportare il rinvio, ad esempio, a schede o banche dati anagrafiche dei clienti (titolari del trattamento), contenenti la descrizione dei servizi forniti agli stessi, ferma restando la necessità che comunque tali schede riportino tutte le indicazioni richieste dall'art. 30, paragrafo 2, del GDPR.

Questi sono i requisiti minimi che vengono richiesti all'interno del registro, ma è possibile integrarne i contenuti con tutte le informazioni ritenute utili dal titolare del trattamento al fine di dimostrare di aver correttamente adempiuto agli obblighi imposti dalla normativa privacy.

Su richiesta, il titolare del trattamento o il responsabile del trattamento e l'eventuale rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

È importante ricordare, però, che il registro dei trattamenti non è un documento che viene redatto una volta sola e resta immutato nel tempo, atteso che va inteso piuttosto come uno strumento di lavoro passibile di modifiche, ma soprattutto di aggiornamenti che lo rendano sempre attuale.

Infatti, esso deve essere aggiornato almeno una volta all'anno, nonché ogniqualvolta vi siano delle modifiche che impattano sulla normativa privacy e che richiedono la trascrizione.

Il novellato D.Lgs. 196/2003 (ad opera del D.Lgs. 101/2018) prescrive che il Registro deve recare, in maniera verificabile, la data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento), unitamente a quella dell'ultimo aggiornamento. In quest'ultimo caso il Registro dovrà recare una annotazione del tipo:

- "scheda creata in data: **XX/XX/XXXX**";
- "ultimo aggiornamento avvenuto in data: **XX/XX/XXXX**".

Per far sì che un registro sia mantenuto costante e corretto nel tempo è necessario individuare, all'interno dell'organizzazione, coloro che conoscono meglio le dinamiche operative e che possono quindi occuparsi di gestire tale attività in modo che sia garantito l'accesso solo alle persone coinvolte nel suo mantenimento e costante aggiornamento.

Come sottolineato dal Garante Privacy, il registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali.

10.2. Registro delle violazioni

Qualsiasi violazione di dati deve essere tempestivamente annotata nel costituito registro delle violazioni, come indicato dal WP29, nelle Linee guida "WP250" sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679. Il titolare del trattamento è incentivato alla tenuta di un registro interno delle violazioni, indipendentemente dal fatto che sia obbligato ad effettuare la notifica o meno. Spetta al titolare del trattamento determinare quale metodo e struttura utilizzare per documentare una violazione; nondimeno, dovrebbero essere sempre incluse determinate informazioni chiave, quali i dettagli relativi alla violazione, comprese le cause, i fatti e i dati personali interessati, gli effetti e le conseguenze della violazione e i provvedimenti adottati per porvi rimedio.

Il Regolamento UE non individua un periodo di conservazione della documentazione e quindi la relativa determinazione compete al titolare del trattamento nella misura in cui può essere chiamato a

fornire prove all'autorità di controllo in merito al rispetto di tale obbligo e, più in generale, del principio di responsabilizzazione.

Ricade sul titolare e sul DPO, se presente, la responsabilità di valutare tempestivamente la violazione, e, nel caso in cui la stessa comporti un rischio elevato per i diritti e le libertà delle persone, notificarla - entro 72 ore dalla scoperta - al Garante, dandone comunicazione anche a tutti gli interessati attraverso i canali più idonei e prendendo misure tali da ridurne l'impatto[36].

10.3. Registro dell'esercizio dei diritti degli interessati

Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. In caso di esercizio dei diritti (artt. 15-22) da parte degli interessati, benché sia il solo titolare a dover dare riscontro, il responsabile è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati (art. 28, paragrafo 3, lettera e)).

A tal fine è consigliabile che il titolare istituisca un registro in cui annotare tutte le istanze pervenute dagli interessati e tutte le attività poste in essere per adempiervi.

Per tutti i diritti (compreso il diritto di accesso) il termine per la risposta all'interessato è pari a un mese, estendibile fino a tre mesi in casi di particolare complessità. Il titolare deve comunque dare un riscontro all'interessato entro un mese dalla richiesta, anche in caso di diniego.

Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate, eccessive o anche ripetitive (art. 12.5), a differenza di quanto prevedono gli artt. 9, co. 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3). In quest'ultimo caso, il titolare deve tenere conto dei costi amministrativi sostenuti. Il riscontro all'interessato, di regola, deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità e può essere fornito oralmente solo se così richiede l'interessato stesso (art. 12, paragrafo 1; si veda anche l'art. 15, paragrafo 3).

La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

I diritti degli interessati sono sanciti dagli artt. 12 a 18.

Artt. 12 - 13 - 14	Trasparenza e modalità (le informative)
Art. 15	Diritto di accesso
Art. 16	Diritto di rettifica
Art. 17	Diritto alla cancellazione
Art. 18	Diritto alla limitazione del trattamento

[36] L'argomento è stato analizzato nel paragrafo 7 del presente documento.

11. I codici di condotta e i sistemi di certificazione privacy

I codici di condotta e i meccanismi di certificazione, pur non essendo una novità assoluta della normativa sulla privacy, assumono indubbia rilevanza nell'ambito del Regolamento.

L'adesione ai codici di condotta o ad un meccanismo di certificazione può essere infatti di ausilio al fine di rispettare il principio di accountability, nonché i principi di privacy by design e di privacy by default. Pertanto, l'adesione ad un codice di condotta o a un meccanismo di certificazione, pur essendo facoltativa, costituisce uno dei parametri di valutazione del rispetto della normativa sulla privacy da parte di un titolare del trattamento o di un responsabile del trattamento.

Questo sarà in particolare un elemento di cui l'autorità dovrà tenere conto, per esempio, nell'applicare eventuali sanzioni o nell'analizzare la correttezza di una valutazione di impatto effettuata dal titolare: in questo senso, i codici di condotta rappresentano anche uno strumento per documentare il rispetto degli obblighi imposti con riguardo alle misure volte a garantire la sicurezza del trattamento.

Nel dettaglio, i codici di condotta hanno l'obbiettivo di supportare l'applicazione efficace, coerente ed omogenea del Regolamento da parte dei titolari e dei responsabili del trattamento appartenenti ad un medesimo settore.

È compito delle associazioni e degli altri organismi che rappresentano le categorie di titolari o responsabili del trattamento elaborare i codici di condotta, modificarli o prorogarli. Non si tratta tuttavia di un processo "unilaterale": da un lato, infatti, nell'elaborare un codice di condotta, le associazioni e gli organismi devono coinvolgere anche le parti interessate, quando ciò è possibile, e tenere conto delle osservazioni ricevute e delle opinioni espresse in sede di consultazione; dall'altro, in ogni caso, i codici devono essere sottoposti al vaglio dell'Autorità garante. Una volta approvato, come detto, ciascun titolare o responsabile del trattamento potrà aderire facoltativamente al codice di condotta.

I codici di condotta assumono rilevanza con riferimento a numerosi aspetti disciplinati dal GDPR.

Nello stabilire l'ambito della responsabilità del titolare rispetto all'assolvimento degli obblighi di accountability, l'adesione ad un codice di condotta è un elemento utile a dimostrare il rispetto di tali obblighi da parte del titolare e del responsabile del trattamento.

Quanto alla nomina dei responsabili del trattamento, i titolari del trattamento e a loro volta i responsabili del trattamento possono delegare le attività di trattamento rispettivamente soltanto a responsabili e sub-responsabili che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato; a tal fine l'adesione ad un codice di condotta può essere utilizzato come elemento utile per dimostrare il rispetto delle garanzie richieste dal GDPR.

Ancora, l'adesione ad un codice di condotta può essere utilizzata come elemento utile per il titolare del trattamento o per i responsabili del trattamento per dimostrare l'approntamento delle misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio. Ai fini della valutazione

di impatto sulla protezione dei dati personali effettuato dai titolari o responsabili del trattamento, è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta.

Il trasferimento dei dati verso un Paese terzo o un'organizzazione internazionale da parte del titolare o del responsabile, in mancanza di una decisione di adeguatezza, è consentito solo se il destinatario ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. A tal fine, costituisce garanzia adeguata, tra le altre, l'adozione di un codice di condotta unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel Paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.

Infine, l'autorità di controllo è obbligata a considerare, nella valutazione dell'*an* e del *quantum* della sanzione da irrogare, tra gli altri elementi, l'adesione del titolare e del responsabile ad un codice di condotta.

Dal punto di vista dell'ambito oggettivo, i codici di condotta (che possono peraltro essere dal punto di vista dell'efficacia territoriale, nazionali, riferiti al trattamento effettuato in più Paesi membri oppure aventi validità generale in uno stato membro) devono necessariamente regolamentare almeno i seguenti aspetti:

- il trattamento corretto e trasparente dei dati;
- i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;
- la raccolta dei dati personali;
- la pseudonimizzazione dei dati personali;
- l'informazione fornita al pubblico e agli interessati;
- l'esercizio dei diritti degli interessati;
- l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;
- le misure e le procedure per la responsabilizzazione e la protezione dei dati fin dalla progettazione e per impostazione predefinita (artt. 24 e 25 del GDPR), nonché le misure volte a garantire la sicurezza del trattamento (art. 32 del GDPR);
- la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato;
- il trasferimento di dati personali verso Paesi terzi od organizzazioni internazionali;
- le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento.

Come anticipato, si tratta di un elenco di materie esemplificativo. Nell'elaborazione del codice, valorizzando la natura di auto-regolamentazione dello stesso, si potranno altresì introdurre e

disciplinare ulteriori aspetti di interesse per quel "settore di trattamento", pur in conformità e ad integrazione (e mai in deroga) di quanto previsto dal GDPR.

Il Regolamento prevede, infine, che il controllo della conformità ad un codice di condotta sia effettuato da un organismo in possesso del livello adeguato di competenze riguardo al contenuto del codice ed accreditato dell'autorità di controllo competente.

L'organismo accreditato deve adottare le opportune misure in caso di violazione del codice di condotta da parte di un titolare del trattamento o di un responsabile del trattamento, tra cui la sospensione o l'esclusione dal codice del titolare del trattamento o del responsabile del trattamento. Esso deve inoltre informare l'autorità di controllo competente di tali misure e dei motivi della loro adozione.

Il Regolamento, oltre che i codici di condotta, promuove anche la certificazione accreditata della protezione dei dati personali, di sigilli e marchi, al fine di attestare la conformità dei trattamenti effettuati dai titolari e dai responsabili del trattamento.

In particolare, dunque, anche i meccanismi di certificazione hanno l'obiettivo di dimostrare la conformità al GDPR dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento i quali, in tal modo, possono contare su un valido elemento a riprova del rispetto del principio di accountability. Ad esempio, essi possono dimostrare l'attuazione di misure tecniche e organizzative adeguate nel trattamento dei dati. Naturalmente, come ben chiarito dal Regolamento, la certificazione non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al GDPR e lascia altresì impregiudicati i compiti e i poteri delle Autorità di controllo competenti.

Sotto il profilo soggettivo, la certificazione può essere richiesta da qualsiasi ente o azienda che operi in qualità di titolare o responsabile del trattamento di dati personali. In Italia i soggetti legittimati a rilasciare la certificazione (c.d. organismi di certificazione) sono gli organismi di certificazione accreditati da Accredia. Detti organismi svolgono non solo la funzione di rilasciare la certificazione, ma anche quella di intervenire (anche su indicazione del Garante della privacy) nell'ipotesi del venir meno della conformità del trattamento alla certificazione: ad esempio, l'organismo potrà disporre la revoca o la sospensione della certificazione anche prima della sua naturale scadenza (prevista per un massimo di 3 anni).

L'oggetto della certificazione è un trattamento di dati personali: esso potrà avere dunque ad oggetto una sola operazione di trattamento o più operazioni di trattamento svolte dal titolare o dal responsabile del trattamento, finanche un "servizio" o un "prodotto" nel suo complesso. L'oggetto specifico della certificazione richiesta dal singolo titolare o responsabile è poi espressamente indicato nel certificato rilasciato dall'organismo di certificazione.