i seminari della rete nazionale dei servizi

IL NUOVO REGOLAMENTO EUROPEO 679/2016 SULLA PROTEZIONE DEI DATI

LUCA PETRONE – Ufficio Legale Federcoop Romagna

legacoop

RETE NAZIONALE SERVIZI

La **privacy** non deve essere intesa solamente quale diritto a proteggere i propri dati personali e volto ad **evitare ingerenze nella propria sfera privata**.

La disciplina sulla privacy è rivolta anche a controllare l'utilizzo che viene fatto dei propri dati personali e la relativa circolazione ed ha **origine anglosassone**.

In tal senso appare più corretto parlare di **diritto alla protezione dei dati**.

Le informazioni personali, infatti, rappresentano un bene rilevante all'interno della cosiddetta società dell'informazione.

Infatti, l'informazione ha una duplice natura:

- bene economico, in quanto l'informazione (e quindi il dato personale) rappresenta un bene giuridico, essendo economicamente valutabile;
- diritto fondamentale collegato alla tutela della **dignità umana** (art. 8, Carta dei diritti fondamentali dell'UE).

L'inizio della storia del diritto alla privacy è nell'articolo «**Right to privacy**», apparso il 15 dicembre 1890 sulla **Harvard Law Review,** ad opera di due giovani avvocati bostoniani, Samuel D. Warren e Louis D. Brandeis, i quali analizzarono in maniera molto precisa e articolata il rapporto tra il diritto di informare ed essere informati e la riservatezza.

Warren aveva una moglie di abitudini mondane, che frequentava balli notturni e che rincasava spesso tardi, anche accompagnata da gentiluomini che non erano il marito. La cronaca di Boston si interessava di continuo alle abitudini della signora, rendendone noti i fatti privati tramite un giornale locale venduto ogni giorno in circa 80000 copie. Per tale ragione, Warren e Brandeis decisero di scrivere un articolo scientifico in materia giuridica nel quale esaminarono diffusamente tutti gli aspetti del rapporto tra diritto ad informare, diritto dell'opinione pubblica ad essere informata e rispetto della riservatezza.

L'articolo seppe distinguere tra il diritto ad informare e ad essere informati, con l'assenza di particolari limiti, se l'oggetto dell'informazione è una persona che riveste una carica pubblica (essendo tale informazione giustificata nella presenza di responsabilità pubbliche in capo al soggetto coinvolto dalla notizia), e il diritto alla riservatezza se la persona è un privato cittadino, perché in tal caso manca l'interesse pubblico finalizzato a conoscerne i comportamenti.

Il nuovo Regolamento sulla privacy entrerà in vigore dal prossimo **25 maggio 2018** e sostituirà integralmente l'attuale Codice in materia di trattamento di dati personali dettato dal Decreto Legislativo n. 196/2003.

Tale Regolamento rappresenta un'ulteriore tappa ad un percorso iniziato con la **Direttiva 95/46/CE**. Tale provvedimento aveva recepito un dibattito dottrinale e culturale sviluppatosi nei decenni precedenti ed era volto a fornire una tutela che, causa evoluzione tecnologica, oggi non risulta più essere adeguata.

Il contenuto della Direttiva era stato recepito in Italia dal **D.lgs. n. 196/2003**, attraverso il quale, per la prima volta, ha trovato nel nostro ordinamento riconoscimento positivo il diritto alla riservatezza.

Privacy: il nuovo Regolamento UE 679/16

Attraverso il nuovo Regolamento si intende **allineare su tutto il territorio dell'Unione la disciplina relativa al trattamento dei dati personali**.

Il testo del Regolamento è stato pubblicato sulla Gazzetta Ufficiale dell'U.E. il 4 maggio 2016, dando ai vari Stati membri tempo due anni per il recepimento della relativa disciplina.

In tal senso, il 6 novembre 2017 è stata pubblicata in Italia la Legge n. 163/2017, contenente la delega per l'adeguamento della normativa nazionale alle disposizioni del nuovo Regolamento comunitario. La **delega dovrà essere esercitata entro il 21 maggio 2018** ed il Governo dovrà adottare uno o più decreti legislativi entro tale data al fine di:

- Abrogare la disciplina contenuta del D. Lgs. 196/2003 incompatibile con il nuovo Regolamento;
- Coordinare le disposizioni vigenti in materia di trattamento dei dati personali con quelle del Regolamento.

Fino a quando non saranno adottate le norme relative all'adeguamento, la disciplina che regola il trattamento dei dati è **incompleto**.

Privacy: il nuovo Regolamento UE 679/16

Gli stati "*dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione del presente regolamento*" né si esclude che "*il diritto degli stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito*" (Considerando 10).

Dove **non vi è compatibilità** tra quanto disposto dal Codice della della Privacy e quanto previsto dal Regolamento 679/2016 ,il Codice della Privacy lascia il passo alle nuove disposizioni europee: la legge statale deve essere disapplicata in favore del *Gdpr*.

- Laddove **vi sia compatibilità** tra le due norme, il D. Lgs. n. 196/2003 rimane applicabile continuando a dettare legge, anche in maniera più specifica rispetto al *Gdpr*.
- Laddove il Codice della Privacy **disciplini in maniera più dettagliata** aspetti e ambiti che il Regolamento non approfondisce, occorre chiedersi se l'esistente normativa interna è in linea con gli scopi del nuovo Regolamento.

Privacy: il nuovo Regolamento UE 679/16

Il Regolamento 679/2016 trova applicazione con riguardo al trattamento dei dati personali delle **persone fisiche**, mentre **NON** disciplina il trattamento dei dati delle persone giuridiche, né intende riferirsi al trattamento effettuato dalla persona fisica per l'esercizio di attività esclusivamente a carattere personale o domestico (art. 2, par. 2, lett. c).

L'intento del legislatore comunitario è quello di rafforzare i diritti delle persone fisiche, fornendogli gli strumenti adeguati al fine di tutelare il trattamento dei dati personali che le riguardano.

Obiettivo del Regolamento è quello di:

- **armonizzare** la normativa europea in tema di privacy;
- **adeguarla allo sviluppo tecnologico**, con particolare attenzione anche al trattamento dei dati cosiddetto automatizzato.

Il Regolamento richiede una riorganizzazione interna ed investimenti per adeguare strutture e personale.

Ai sensi dell'art. 3, il nuovo Regolamento di applica:

- Al trattamento effettuato da Titolari/Responsabili **stabiliti** nell'Unione Europea;
- Al trattamento dei dati personali di individui stabiliti nel territorio dell'Unione da parte di Titolari/Responsabili **non stabiliti** nel territorio dell'UE.

Purché le attività di trattamento riguardino:

- L'offerta di beni o la prestazione di servizi, anche gratuiti, ai cittadini UE;
- Il monitoraggio del comportamento dei cittadini dell'UE.

L'art. 4 del Regolamento 679/2016 concerne le **definizioni** che il legislatore comunitario ha inteso fornire degli elementi e termini più ricorrenti all'interno del testo.

In particolare, al punto 1) si fa riferimento al **dato personale**, inteso come «*qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*».

Es. di dato personale: nome e cognome, numero di telefono/cellulare, indirizzo mail, codice fiscale, immagina fotografica di una persona, registrazione vocale, targa automobilistica, indirizzo IP, ecc…

Privacy: il nuovo Regolamento UE 679/16

I dati personali sono *(cfr. Considerando 39)*:

a) Trattati in modo **lecito**, **corretto** e **trasparente** nei confronti dell'interessato (liceità, correttezza e trasparenza);

b) Raccolti per **finalità determinate**, **esplicite** e **legittime**, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89 par. 1, considerato incompatibile con le finalità iniziali (limitazione delle finalità);

c) **Adeguati**, **pertinenti** e **limitati a quanto necessario** rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);

d) **Esatti** e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (esattezza);

e) **Conservati** in una forma che consenta l'identificazione degli interessati **per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati**; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89,par. 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato (limitazione della conservazione);

f) Trattati in maniera da garantire **un'adeguata sicurezza** dei dati personali, compresa la protezione, mediante **misure tecniche e organizzative adeguate,** da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale (integrità e riservatezza).

«… I principi di protezione dei dati non dovrebbero pertanto applicarsi a ***informazioni anonime****, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca.*» (v. *Considerando 26*).

Ad ogni modo, in caso di dubbi sull'interpretazione o identificazione di un'informazione come Dato Personale, si suggerisce di trattare quell'informazione come se lo fosse, nella sua più ampia accezione.

Il punto 2) prende in considerazione il «***trattamento***», ossia «*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*»;

Inoltre:

- «***profilazione***»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica; in linea generale, la profilazione è vietata. Tuttavia è ammessa in circostanze specifiche e previo consenso esplicito dell'interessato. (v. *Considerando 30*)

- «***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; in tal senso le informazioni aggiuntive devono essere conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata i identificabile;
- «***dati biometrici***»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; **ad es.**: le informazioni matematiche elaborate a partire dal volto di una persona, dalle impronte digitali, dalle caratteristiche dell'iride, elementi misurabili dal modo di camminare, ecc…
- «***dati relativi alla salute***»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; (v. *Considerando n. 35*)

Il *Considerando 28* riconosce che «*L'applicazione della* ***pseudonimizzazione*** *ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati. L'introduzione esplicita della «pseudonimizzazione» nel presente regolamento non è quindi intesa a precludere* ***altre misure di protezione dei dati***».

Tale strumento rappresenta una misura aggiuntiva che i Titolari del trattamento potrebbero assumere al fine meglio rispondere agli obblighi di protezione dei dati.

Il *Considerando 29*, sull'argomento, aggiunge che «*Al fine di creare incentivi per l'applicazione della pseudonimizzazione nel trattamento dei dati personali, dovrebbero essere possibili misure di pseudonimizzazione con possibilità di analisi generale all'interno dello stesso titolare del trattamento, qualora il titolare del trattamento abbia adottato le misure tecniche e organizzative necessarie ad assicurare, per il trattamento interessato, l'attuazione del presente regolamento, e che le informazioni aggiuntive per l'attribuzione dei dati personali a un interessato specifico siano conservate separatamente. Il titolare del trattamento che effettua il trattamento dei dati personali dovrebbe indicare le persone autorizzate all'interno dello stesso titolare del trattamento.*»

Il *Gdpr* obbliga i Titolari ad individuare ed esporre nell'**informativa** *privacy* le ragioni che giustificano il trattamento dei dati personali e le relative finalità.

Le **condizioni di legittimità** che il *Gdpr* conferma rispetto all'impianto precedente sono:

- il consenso dell'interessato;
- l'esecuzione di un contratto;
- l'adempimento di un obbligo legale;
- l'esecuzione di un compito di interesse pubblico.

Si consiglia di **verificare sempre la base giuridica** del trattamento ed eventualmente riesaminare il consenso degli eventuali trattamenti.

I **soggetti** coinvolti dalla disciplina sulla privacy sono:

a) l'**interessato**;

b) il **Titolare del trattamento**;

c) il **Responsabile del trattamento** e ***sub*responsabili**;

d) soggetti che agiscono sotto l'autorità del Titolare o del Responsabile (**Incaricati**).

L'interessato è la persona fisica, identificata o identificabile, alla quale si riferiscono i dati.

I controlli sono svolti dal **Nucleo Ispettivo della Guardia di Finanza** su **segnalazione** (senza avviso da parte del Garante) o **a campione** (con avviso preliminare comunicato almeno 7-10 giorni prima).

Durante le attività ispettive i funzionari possono svolgere anche **interviste** ai dipendenti.

Privacy: il nuovo Regolamento UE 679/2016

Per **Titolare del trattamento** (art. 4, punto 7) si intende la persona fisica/giuridica che determina le finalità e i mezzi di trattamento.

Nelle persone giuridiche è l'**entità nel suo complesso** (NON il legale rappresentante o l'amministratore delegato).

Il titolare è colui che ha in concreto il **potere di prendere in autonomia le decisioni operative** su:

- finalità;
- modalità del trattamento;
- strumenti impiegati per il trattamento.

Consigli pratici:

1) i Titolari devono assicurarsi che i trattamenti da loro effettuati siano **conformi ai principi** privacy;
2) i Titolari devono rivedere ed **aggiornare** gli esistenti programmi di *compliance* privacy;
3) i Titolari devono **sviluppare o, laddove già esistenti, aggiornare** le *policy* interne e i piani di risposta alle violazioni (*Data Breach*);
4) dedicare adeguata **formazione al personale** interno.

Il Titolare ha la **generale responsabilità** di assicurarsi che il trattamento sia svolto in conformità con le disposizioni del *Gdpr*. Detta responsabilità copre sia i trattamenti effettuati direttamente dal titolare, sia quelli effettuati per suo conto.

All'interno di strutture complesse (art. 4, punto 7) può essere presente un'area con poteri decisori in merito al trattamento dei dati e, in tal caso, può essere individuata come Titolare (…*i servizi*…).

Quando in riferimento ad un trattamento, due o più entità (solitamente persone giuridiche) decidono e determinano congiuntamente le finalità ed i mezzi del trattamento, questi sono «**contitolari**» del trattamento stesso (art. 26).

Il *Gdpr* obbliga i contitolari a sottoscrivere un **accordo interno** con il quale vengono ripartite le responsabilità e stabiliti i ruoli dei singoli soggetti contitolari.

Il contenuto dell'**accordo** dovrà essere sintetizzato e **messo a disposizione degli interessati**.

Ogni Titolare, indipendentemente dall'altro, potrà essere adito dinnanzi al Garante e/o la autorità giudiziaria dall'interessato.

Il *Gdpr* rende i Responsabili pienamente responsabili nei confronti dell'interessato.

Unico modo per sollevarsi da responsabilità è **fornire prova di non aver partecipato all'attività lesiva**.

Si ritiene **sconsigliabile la contitolarità nell'ambito della esternalizzazione dei servizi** (esempio servizio paghe) a causa delle responsabilità che ricadono in capo al Titolare in caso di violazioni.

Nelle Holding, ciascun titolare risponde del proprio trattamento.

Il **Responsabile del trattamento** è il soggetto persona fisica/giuridica che tratta i dati per conto del titolare e che deve fornire **adeguate garanzie** sul trattamento dei dati.

Anche il Responsabile ha un potere decisorio, ma esercitabile entro i limiti indicati dal Titolare.

Il Regolamento ha rafforzato la figura del Responsabile, il cui rapporto col Titolare deve essere regolamentato da apposito **contratto in forma scritta**.

La figura del Responsabile può essere sia **interna**, che **esterna**, anche se nella disciplina comunitaria si fa riferimento al solo soggetto esterno.

Il Garante sul trattamento dei dati personali non ha fornito indicazioni in tal senso e sembra confermandosi l'impostazione adottata dall'attuale Codice.

Per distinguere tra la figura di Titolare e Responsabile è necessario individuare **chi dispone di poteri decisori in merito al trattamento dei dati**.

A **titolo esemplificativo**, generalmente studi legali e di commercialisti dei quali si avvalgono le imprese sono Titolari dei dati e non Responsabili, mentre chi ha in gestione le buste paga è tendenzialmente un Responsabile.

Occorre **valutare sempre in concreto** i poteri decisori e la relativa ampiezza.

La figura del ***sub*responsabile** (che segue lo schema del subappalto nel settore privato), deve essere nominato dal Responsabile (**previa autorizzazione** del Titolare per iscritto).

Dei **danni** cagionati dal *sub*responsabile nel trattamento dei dati risponde anche il Responsabile.

La figura dell'**incaricato al trattamento** non è più letteralmente citato dal testo del Regolamento (art. 29) e, conseguentemente, sembrerebbero essere venuti meno i relativi adempimenti formali di nomina.

Tuttavia Titolare e Responsabile faranno bene a continuare a formalizzare l'incarico per due ordini di ragioni:

- a fini probatori;
- al fine di delimitare gli ambiti di trattamento e gli accessi ai dati.

Devono essere **obbligatoriamente formati**.

Per affrontare la nuova disciplina sulla tutela dei dati personali occorre predisporre un «**modello organizzativo privacy**».

I titolari del trattamento entro il 25 maggio devono adottare **comportamenti proattivi** e le azioni opportune per dimostrare la concreta adozione del Regolamento.

Una delle principali novità introdotte dal Regolamento è data dal **principio dell'accountability**, attraverso il quale viene attribuito ai titolari il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali.

Tra i **principali nuovi adempimenti** il Regolamento 679/2016 prevede:

- Implementazione dei contenuti dell'**informativa**;
- la designazione del ***Data Protection Officer*** (DPO);
- l'istituzione del **Registro delle attività di trattamento**.

L'**informativa** (artt. 13 – 14) diventa sempre più centrale per rispondere agli obblighi di trasparenza e per permettere agli interessati l'esercizio dei propri diritti.

Rispetto all'attuale informativa, quella definita dal nuovo Regolamento prevede l'**implementazione del relativo contenuto**, in particolare richiedendo che siano inserite le seguenti ulteriori informazioni:

- I dati di contatto del DPO;
- ove applicabile, l'intenzione del titolare di trasferire i dati in un Paese terzo;
- il **periodo di conservazione** dei dati personali;
- l'esistenza del **diritto dell'interessato** di chiedere al titolare del trattamento l'**accesso** ai dati personali, la loro **rettifica** e **cancellazione**;
- il **diritto di proporre reclamo** all'Autorità di controllo;
- il consenso dell'interessato dovrà essere ottenuto con riguardo a ciascuna specifica attività di trattamento.

I titolari sono tenuti a **redigere l'informativa**:

- ✓ pianificando un **linguaggio semplice e chiaro** e predisponendo dei documenti dal **contenuto conciso, intelligibile, e facilmente accessibile**. Informative eccessivamente lunghe e troppo complesse non saranno ritenuti conformi al *Gdpr*.

Inoltre viene suggerito di mettere a disposizione degli interessati un ***link* dove potranno trovare la *privacy policy*** contenente un maggiore dettaglio su come vengono usati i dati personali.

N.B.: il **richiamo al sito per l'informativa** estesa non è mai stata osteggiata da parte del Garante, pur non essendo perfettamente adeguata alla normativa.

Quindi si ritiene possibile fornire agli interessati un'informativa semplificata e poi rimandare per quella completa al proprio sito aziendale.

L'informativa deve essere **sempre resa all'interessato**, **anche se non è necessario il consenso** al trattamento, dovendo sempre essere indicata la base giuridica che lo giustifica.

Se il dato è **raccolto presso terzi**, il Titolare deve comunque informare l'interessato entro i 30 giorni successivi, salvo l'ipotesi in cui la comunicazione dell'informativa possa comportare uno sforzo sproporzionato.

Le **condizioni per il consenso** (art. 7) sono le seguenti:

- manifestazione di volontà **libera**, **specifica**, **informata** e **inequivocabile** dell'interessato;
- deve essere **espresso**: non è ammissibile il consenso tacito o presunto;
- deve essere **documentato**;
- è **revocabile**: la revoca non pregiudica la liceità dei precedenti trattamenti.

Non si ritiene valido il consenso ottenuto se l'interessato non ha possibilità di rifiutare il trattamento dei propri dati o se non può revocarlo quando vuole senza subire un danno.

È **esclusa l'ipotesi del silenzio – assenso** e delle caselle preselezionate su internet.

Il consenso è valido se espresso da soggetto che ha compiuto **almeno 16 anni** (quindi il consenso è valido anche se espresso da minori).

Non è necessario documentare il consenso per iscritto, anche se è consigliabile, soprattutto a fini probatori.

Il trattamento **può essere lecito anche in assenza del consenso**, purché si verifichi una delle ipotesi di cui all'**art. 6** del Regolamento:

- il trattamento è **necessario all'esecuzione di un contratto** di cui l'interessato è parte;
- il trattamento è **obbligatorio per adempiere ad un obbligo legale**;
- il trattamento è valido per la **salvaguardia di interessi vitali** dell'interessato o di altra persona fisica;
- il trattamento è **necessario per l'esecuzione di un compito di interesse pubblico**;
- 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 o le libertà fondamentali dell'interessato** che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore (lett. f).

La lett. f) richiede un bilanciamento degli interessi, la cui valutazione è rimessa al Titolare.

La nomina del ***Data Protection Officer*** (DPO) o Responsabile della Protezione dei Dati (RPD) sarà obbligatoria:

- Pubbliche amministrazioni;
- Tutti i **soggetti la cui attività principale (*core business*)** consista in **trattamenti che richiedono un controllo regolare e sistematico** degli interessi;
- Tutti i **soggetti la cui attività principale (*core business)*** consiste nel trattamento **su larga scala di dati sensibili**.

La disciplina nazionale può prevedere ulteriori casi.

Il significato di «**larga scala**» e di «**monitoraggio regolare e sistematico**» è stato oggetto delle valutazioni operate dal WP29 all'interno delle relative linee guida.

In particolare, al fine di stabilire se un trattamento è su **larga scala** si raccomanda di tenere conto:

- del numero di soggetti interessati dal trattamento (…);
- il volume dei dati e/o le diverse tipologie di dati trattati;
- la durata dell'attività di trattamento;
- la portata geografica dell'attività.

L'aggettivo «**regolare**» ha uno dei seguenti significati:

- che avviene in modo continuo o ad intervalli definiti;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o ad intervalli periodici.

L'aggettivo **sistematico**, invece, ha almeno uno dei seguenti significati:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta dati;
- svolto nell'ambito di una strategia.

Tra le esemplificazioni: utilizzo di telecamere a circuito chiuso, sistema di geolocalizzazione (nell'ambito delle imprese di trasporto) o monitoraggio con videosorveglianza delle catene di montaggio (previo accordo sindacale).

Il **DPO** può **far parte del personale** del titolare o del responsabile, ovvero assolvere ai suoi compiti in base ad un **contratto di servizi**. Se dipendente, per garantire autonomia ed indipendenza, deve ricoprire ruoli apicali.

Se nominato da parte del Titolare e/o Responsabile, i relativi **dati di contatto devono essere comunicati al Garante e pubblicati sul proprio sito internet**.

Il DPO **non è responsabile personalmente** in caso di inosservanza del Regolamento, ma unicamente in caso di **inadempimento contrattuale**. La responsabilità sul trattamento ricade sempre e comunque sul Titolare che dovrà essere in grado di dimostrare che il trattamento dei dati è avvenuto conformemente alla disciplina comunitaria (art. 24).

Il DPO, dunque, **non assumerebbe diretta responsabilità** per sanzioni o risarcimenti nei confronti degli interessati.

Tuttavia, qualora gli inadempimenti alla normativa siano dipesi da **colpa** o da **dolo** del DPO, essi potranno costituire oggetto di pretese risarcitorie «interne» da parte del titolare o del responsabile.

La responsabilità del DPO è una responsabilità professionale. In caso di svolgimento di detta attività è consigliabile avere polizze assicurative adeguate.

I **requisiti** richiesti per ricoprire la figura del **DPO**:

- adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, quindi deve avere competenze giuridiche ed informatiche (misure di sicurezza);
- adempiere alle sue funzioni in piena indipendenza ed in assenza di conflitti di interesse;
- operare alle dipendenze del titolare o del responsabile o sulla base di un contratto di servizi.

Le competenze del DPO **non devono essere necessariamente attestate da certificati** o altre attestazioni formali, né è richiesta un'iscrizione ad un Albo professionale.

Il DPO deve necessariamente **essere coinvolto** nell'applicazione dei modelli di privacy by design, progettazione dei trattamenti, tenuta del registro dei trattamenti, nella Valutazione Impatto Privacy (*Data Protection Impact Assessment*).

Il DPO dovrà:

a) **informare e consigliare** il titolare o il responsabile, nonché i dipendenti in merito agli obblighi derivanti dal Regolamento europeo;

b) **verificare l'attuazione e l'applicazione del Regolamento**, la sensibilizzazione e **formazione** del personale e gli **audit** relativi;

c) **fornire**, se richiesto, **pareri** in merito alla valutazione d'impatto sulla protezione dei dati e **sorvegliare** i relativi adempimenti.

d) fungere da punto di **contatto con gli interessati**;

e) fungere da punto di **contatto per il Garante** oppure consultare il Garante di propria iniziativa.

Sono tenuti alla nomina, a titolo esemplificativo e non esaustivo:

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.

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**: v. anche considerando 97 del Regolamento, in relazione alla definizione di attività «accessoria»).

In ogni caso, resta comunque raccomandata, anche alla luce del principio di «**accountability**» che permea il Regolamento, la designazione di tale figura, i cui criteri di nomina, in tale evenienza, rimangono gli stessi sopra indicati.

Appare preferibile evitare di assegnare il ruolo di responsabile della protezione dei dati personali a soggetti con incarichi di alta direzione (amministratore delegato; membro del consiglio di amministrazione; direttore generale; ecc.), ovvero nell'ambito di strutture aventi potere decisionale in ordine alle finalità e alle modalità del trattamento (direzione risorse umane, direzione marketing, direzione finanziaria, responsabile IT ecc.).

Da valutare, in assenza di conflitti di interesse e in base al contesto di riferimento, l'eventuale assegnazione di tale incarico ai responsabili delle funzioni di staff (ad esempio, il responsabile della funzione legale).

Per quanto concerne i **Registri delle attività di trattamento** (del Titolare ed, eventualmente del Responsabile esterno), questi devono essere tenuti in **forma scritta o in formato elettronico**.

Il Registro, in caso di richiesta, deve essere **messo a disposizione dell'Autorità di controllo**.

Il Registro è **obbligatorio** per le imprese con almeno 250 dipendenti o per quelle che **effettuano un trattamento tale da rappresentare un rischio per i diritti e le libertà dell'interessato o il trattamento non sia occasionale o includa categorie particolari di dati sensibili e giudiziari**. Tale previsione di fatto impone l'estensione dell'obbligo di adottare il registro a tutti.

In ogni caso, l'adozione del Registro è **caldamente consigliata** anche per le imprese esentate dall'obbligo.

Il Registro deve documentare tutte le attività di trattamento e le eventuali violazioni (perdita chiavetta, rottura di dischi rigidi, ecc… vanno documentati).

Il Registro delle attività di trattamento deve **contenere**:

a) nome e **coordinate contatto** del titolare e di ogni corresponsabile, del rappresentante e del DPO;
b) le **finalità** del trattamento;
c) le categorie degli **interessati** e quelle dei dati;
d) i **destinatari** a cui saranno, eventualmente, comunicati i dati;
e) i **trasferimenti** dei dati ai Paesi Terzi o organizzazione internazionale;
f) i **termini** ultimi per la cancellazione dei dati (che possono essere decisi a discrezione del titolare);
g) una descrizione generale delle **misure di sicurezza** tecniche ed organizzative.

Anche ogni Responsabile del trattamento deve tenere un Registro di tutte le categorie di trattamento svolte per conto di un titolare del trattamento.

I Registri è bene siano contenuti per **iscritto**.

Tra i nuovi principi introdotti dal Regolamento UE 679/2016 possono essere citati:

a) il **principio dell'accountability** (art. 24);
b) il **principio della privacy impact assessment** (art. 35);
c) il **principio della privacy by design e by default** (art. 25).

Per quanto concerne il **principio della accountability** (o di responsabilizzazione del titolare), il titolare deve assicurare e comprovare, per ciascuna operazione, la conformità alle disposizioni del Regolamento. La responsabilizzazione si attua:

- osservando i principi;
- dimostrando che i principi vengono concretamente rispettati.

Il **principio di responsabilizzazione** significa che si chiede al Titolare del trattamento di mettere in atto **misure** tecniche ed organizzative **adeguate a garantire**, ed essere in grado di **dimostrare**, che il trattamento è effettuato conformemente al Regolamento.

Non esistono più misure minime di sicurezza.

In tal senso il **Titolare documenta** qualsiasi violazione dei dati, incluse le circostanze in cui si sono verificate, le relative conseguenze ed i provvedimenti adottati per porvi rimedio.

Tutto ciò che viene svolto in ambito del trattamento occorre renderlo **tracciabile e motivare qualsivoglia scelta** (anche quando si decide di non adottare determinate misure).

Ovviamente la sicurezza, in questo settore in particolare, è un concetto dinamico che impone al Titolare di compiere un'attività di **continuo monitoraggio**.

Al fine di dimostrare la conformità al Regolamento ci si potrà avvalere:

- di **certificazion**i;
- adesione a **codici di condotta** (da parte di associazioni di categoria e altri soggetti**)**.

I Titolari ed i Responsabili possono dimostrare la conformità del proprio operato al *Gdpr* tramite l'adozione di **codici di condotta** o tramite l'ottenimento di **certificazioni**.

I **codici di condotta** possono essere elaborati (art. 40) dalle **associazioni e dagli altri organismi di rappresentanza** della categoria alla quale appartiene il Titolare.

Nell'elaborazione di tali codici, le associazioni e gli altri organismi sono invitati a **coinvolgere le parti interessate** e a tenere in debito conto le **caratteristiche specifiche dei trattamenti** e le **esigenze delle micro imprese e delle piccole e medio imprese**.

I codici di condotta devono poi essere formalmente approvati dal Garante.

Le **certificazioni** (art. 42) hanno lo scopo principale di dimostrare la conformità dei trattamenti al *Gdpr*.

Il Regolamento 679/2016 prevede un sistema di certificazioni e accreditamento su **base volontaria**.

Attenzione: l'ottenimento della certificazione non riduce la responsabilità.

La certificazione è rilasciata per un periodo massimo di **3 anni**, potendo essere **rinnovata** alle stesse condizioni.

Gli organismi di certificazione (ancora da individuare) potranno comunque **revocare la certificazione** rilasciata qualora ritengano che i requisiti ai fini del rilascio della stessa non siano più soddisfatti.

Da un punto di vista **operativo** il **principio dell'accountability** potrà esplicarsi secondo le seguenti modalità:

Fase 1) mappatura degli archivi; verifica circa la liceità del trattamento; individuazione soggetti interessati al trattamento; individuazione delle figure responsabili all'interno dell'azienda.

Fase 2) stesura documenti; stesura Registro; verifica applicazione delle misure minime di sicurezza (all. B, D. lgs. n. 196/2003).

Altro principio è quello del «**privacy impact assessment**» (valutazione d'impatto sulla privacy).

Tale principio trova applicazione nel caso in cui il trattamento preveda l'utilizzo di nuove tecnologie, dalle quali possa derivare un **rischio elevato per i diritti e le libertà delle persone** fisiche.

In tali situazioni il titolare del trattamento effettua, **prima** di procedere al trattamento stesso, una **valutazione dell'impatto dei trattamenti** previsti sulla protezione dei dati personali.

La **DPIA** (*Data Protection Impact Assessment*) non è sempre necessaria. Quindi occorre una valutazione da parte del Titolare.

La c.d. ***valutazione di impatto*** è richiesta, ad esempio, se i dati sono trattati per effettuare profilazioni, in caso di utilizzo di dati biometrici, sorveglianza di zone accessibili al pubblico, trattamento di categorie particolari di dati personali o di dati relativi a condanne penali e reati.

La DPIA va fatta nei seguenti casi:

a) viene svolta da parte del titolare una **valutazione sistematica e globale** di aspetti personali relativi a persone fisiche, basata sul trattamento automatizzato dei dati, compresa la profilazione;

b) viene eseguito un trattamento su **larga scala** di dati sensibili e/o giudiziari;

c) viene svolta una **sorveglianza sistematica** di una zona accessibile al pubblico su larga scala.

*il criterio di larga scala ha natura quantitativa e geografica;

*la **profilazione deve essere intesa in senso ampio**; in tal senso, ad esempio capire tra i clienti chi paga e chi è insolvente al fine di interrompere le forniture.

Se il Titolare non esegue la DPIA deve **fornire adeguata motivazione** e darne riscontro nel Registro.

Attraverso il Regolamento 679/2016 il legislatore comunitario ha **spostato il focus**, responsabilizzando il Titolare.

È il Titolare a dover valutare ed adottare le misure di sicurezza necessarie a garantire il trattamento dei dati.

Le **misure indicate nell'allegato B** del Codice della privacy **non esistono più** e rappresentano strumenti, ormai, anacronistici.

Il fatto che il nuovo Regolamento non preveda specifiche misure tecniche è dovuto alla consapevolezza della **celerità con la quale hanno luogo i cambiamenti a livello digitale**.

Non esistono obblighi calati dall'alto: Titolare e Responsabile devono scegliere le opzioni tecniche più adeguate alla propria realtà.

La **DPIA** può svolgersi secondo **tre diverse modalità**:

a) Attraverso un'**analisi generica** demandata al Titolare del trattamento (**art. 24**) che dovrà adottare le misure tecniche adeguate alla propria struttura (privacy by design). Nelle realtà meno strutturate l'attività di analisi del rischio può anche fermarsi a questa fase.

b) Quando il trattamento comporta un **rischio elevato per i diritti e le libertà delle persone fisiche** (**art. 35**), prima di procedere al trattamento, il Titolare deve effettuare adeguata valutazione d'impatto e confrontarsi con il DPO, se nominato. Tale attività deve essere **necessariamente documentata**.

c) Attraverso una richiesta di **valutazione preventiva da parte dell'Autorità di controllo** (Garante), nel caso la valutazione *ex* art. 35 ha evidenziato un rischio elevato e l'assenza di misure adottate per eliminare tali rischi (**art. 36**). È il Titolare a decidere se coinvolgere il Garante.

Il controllo si sposta sempre in una fase *ex post*; mai *ex ante*.

Infine per «**privacy by design**» si deve intendere la protezione dei dati **fin dalla progettazione**, selezione ed utilizzo di applicazioni o sistemi di gestione aventi ad oggetto il trattamento di dati personali.

Il titolare dovrà **ridurre al minimo il trattamento** dei dati personali, mediante l'utilizzo di misure (tecniche ed organizzative) quali **ad esempio la pseudonimizzazione** dei dati personali.

Invece, per «**privacy by default**», deve essere inteso che la tutela della protezione del dato deve diventare l'impostazione predefinita.

Il Titolare deve adottare misure tecniche ed organizzative adeguate a garantire che i dati siano trattati, **per impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità di trattamento.

Altra novità rilevante introdotta dal Regolamento è data dalla disciplina predisposta per rispondere ad eventuali **violazioni dei dati personali trattati** da parte del Titolare (**data breach** – artt. 33 e 34).

Nel caso si verificassero violazioni, il Titolare del trattamento dovrà comunicarle **entro 72 ore** all'Autorità nazionale di protezione dei dati (Garante del Trattamento dei dati personali).

Sempre entro le 72 ore i Titolari devono essere in grado di identificare le violazioni, revisionare l'eventuale documentazione, adottare procedure/atti in grado di mitigare il danno arrecato.

Le **procedure interne** relative ai *data Breach*, devono essere sviluppate, testate ed aggiornate costantemente. Per poter procedere in tal senso è necessario che sia **coinvolto il dipartimento IT** del titolare o un responsabile IT esterno che possa adottare le misure tecniche ed organizzative più appropriate.

Se la violazione, per altro, dovesse rappresentare una **minaccia per i diritti e le libertà delle persone**, il titolare dovrà **informare** in modo chiaro, semplice ed immediato anche **tutti gli interessati** ed offrire indicazioni su come intende limitare le possibili conseguenze negative (onere rischioso per il titolare, esponendolo ad eventuali pretese risarcitorie).

È bene che il Titolare riveda le **polizze assicurative** al fine di prevedere tra i rischi da assicurare anche i fenomeni di *data breach*.

Inoltre, se il numero delle **persone coinvolte è elevato o gli interessati non sono identificabili,** è comunque richiesta una comunicazione pubblica o adatta a raggiungere quanti più interessati possibili (esempio tramite inserzione su quotidiani o comunicazione sul sito web del Titolare).

In ogni caso, il Garante può imporre al Titolare di informare gli interessati sulla base di proprie autonome valutazioni in merito alla violazione dei dati.

La **comunicazione non è richiesta** se:

- Il Titolare ha **adottato le misure di sicurezza adeguate** alla protezione dei dati;
- Le protezioni adottate sono volte a **scongiurare rischi elevati** per gli interessati;
- La comunicazione comporterebbe **sforzi sproporzionati** (in questo caso è richiesta la comunicazione pubblica).

Quando **appare necessaria la notifica al Garante**?

La segnalazione appare dovuta quando al Titolare sono **sottratti fisicamente i dati** (ad esempio perdita o sottrazione del PC portatile di alcuni dipendenti, fatto salva l'ipotesi nella quale i dati contenuti all'interno del dispositivo siano criptati).

A seguito della segnalazione è molto **probabile un'ispezione** da parte del nucleo ispettivo della Guardia di Finanza.

Le **misure tecniche ed organizzative** devono arginare e prevenire i rischi inerenti il trattamento, quali:

- ✓ distruzione accidentale o illegale;
- ✓ la perdita;
- ✓ la modifica;
- ✓ la rivelazione o l'accesso non autorizzato a dati personali, trasmessi, conservati o comunque elaborati che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

Qualche **esempio di misure tecniche**: pseudonimizzazione; cifratura; minimizzazione dei dati e trattamenti; definizione del periodo di conservazione ed accessibilità dei dati.

Qualche **esempio di misure organizzative**: designazione e suddivisione delle responsabilità; predisposizione di policy; disciplinari, linee guida interne; formazione di incaricati; adesioni a codici di condotta o conseguimento di certificazioni.

Le misure di sicurezza per essere adeguate devono tenere conto del **progresso tecnologico**, dei relativi **costi di attivazione** e dell'**attività in concreto svolta** da parte del Titolare/Responsabile.

L'elenco di cui all'art. 32 non è esaustivo («*…tra le altre…*»), né rappresenta un insieme di misure sempre realizzabili («*…se del caso…*»).

Il nuovo Regolamento UE 679/2016 amplia la tutela riconosciuta agli interessati attraverso l'introduzione di **nuovi diritti e l'estensione di diritti già esistenti**, quali:

- il diritto alla **portabilità dei dati** (art. 20)
- il **diritto all'oblio** (art. 17);
- il **diritto di opposizione** (art. 21);
- il **diritto alla limitazione del trattamento** (art. 18);
- Il **diritto di rettifica** (art. 16);
- il **diritto di accesso** (art. 15).

Il Titolare e il Responsabile devono garantire il **R.I.D.**, ossia la Riservatezza, l'Integrità, la disponibilità del dato.

Il **diritto alla portabilità dei dati** ha la finalità di garantire agli interessati un controllo rafforzato nel caso in cui i relativi dati personali siano trattati per il tramite di **mezzi automatizzati** e consiste nella facoltà di **trasferire** i propri dati da un titolare all'altro (es. si potrà cambiare il provider di posta elettronica senza perdere i contatti e/o messaggi). Tale diritto non è esercitabile nei confronti della P.A.

L'interessato ha diritto ad ottenere dal titolare originario una **copia dei propri dati** ed il **salvataggio** dei propri dati personali **su un *device* personale**.

Il **diritto all'oblio** (art. 17) può essere definito come il **diritto di un individuo ad essere dimenticato** o, meglio, a non essere ricordato per i fatti che lo riguardano e che in passato possono essere stati oggetto di cronaca (sentenza Corte di Giustizia Europea, C – 131/12, nota come «*Google Spain*»).

Il presupposto è che le informazioni dell'interessato riguardino un **fatto passato** e, quindi, le informazioni sono diventate inadeguate.

In questi casi l'interessato ha diritto di chiedere al Titolare la cancellazione dei dati personali che lo riguardano **senza ingiustificato ritardo** in presenza di alcuni motivi (es. quando i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti e trattati; a seguito di revoca del consenso, ecc.).

L'interessato può sempre opporsi al trattamento dei suoi dati personali attraverso l'esercizio del **diritto di opposizione** (art. 21).

I tipi di trattamento ai quali può opporsi sono:

- *marketing* diretto e profilazione (unica ipotesi di diritto assoluto, non essendo necessario che l'interessato fornisca adeguata motivazione);
- quelli effettuati per fini statistici, storici o di ricerca.

Suggerimenti: **opportuno aggiornare le informative** e le privacy policy per assicurare all'interessato una piena consapevolezza della possibilità di esercitare i propri diritti.

Il *Gdpr*, inoltre, consente all'interessato di chiedere la **limitazione del trattamento** avente ad oggetto i propri dati personali **se**:

- è messa in **discussione l'accuratezza** dei dati trattati;
- i **dati personali** dell'interessato **non sono più necessari** ai fini del perseguimento delle finalità originariamente supposte dal titolare;
- è pendente, nell'ambito di una richiesta di cancellazione dati personali, la verifica dell'esistenza di un motivo legittimo prevalente.

Il titolare deve appurare di aver predisposto **procedure interne** al fine di **permettere l'agevole esercizio** del diritto da parte dell'interessato.

L'interessato può chiedere al titolare la **rettifica** (art. 16) di qualsivoglia dato personale che ritenga caratterizzato da errori.

In tal senso non si registrano variazioni significative rispetto alla Direttiva 95/46/CE.

Viceversa, il **diritto di accesso** (art. 15) ai propri dati personali da parte dell'interessato è stato ampliato in modo significativo, determinando per il titolare una serie di oneri amministrativi ed economici.

A seguito di richiesta di accesso il Titolare **fornisce all'interessato**, senza ingiustificato ritardo e, comunque, al più tardi **entro 30 giorni** dal ricevimento della richiesta (termine prorogabile di due mesi se necessario tenuto conto della complessità aziendale e/o numero richieste).

Le informazioni sono rese **gratuitamente**.

Se le richieste di accesso ai dati sono manifestamente infondate o eccessive, il Titolare può: a) addebitare un contributo spese ragionevole; b) rifiutarsi di soddisfare la richiesta.

La **formazione** diventerà obbligatoria per gli incaricati, così come richiamato dall'**art. 32**, **c. 4**, attraverso il quale viene disposto quanto segue:

«*Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento (…)*»

La formazione dovrà essere **costante e continua** nel corso del tempo.

Al fine di dimostrare la formazione degli incaricati non sarà sufficiente una mera prova documentale (es. raccolta firme) ma, in caso di ispezione, il funzionario potrà verificare oralmente (**audit**) ciò che è stato trasmesso agli incaricati.

Per quanto riguarda l'**impianto sanzionatorio** occorre prima di tutto considerare che, chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il **risarcimento del danno** dal Titolare o dal Responsabile del trattamento.

Il diritto al risarcimento potrà essere invocato dagli interessati o da terzi danneggiati dal trattamento dei dati illecito.

Il **Titolare** risponde per **qualunque danno**, mentre il **Responsabile solo se** non ha adempiuto ai propri obblighi (senza solidarietà col titolare) o se ha agito in maniera difforme rispetto alle indicazioni fornite dal Titolare.

Il Titolare potrà esonerarsi da responsabilità dimostrando che l'evento dannoso non gli è in alcun modo imputabile.

La **responsabilità ha natura extracontrattuale** (art. 2050 c.c.).

Gli interessati possono chiedere al Titolare del trattamento che ponga rimedio alle violazioni che, gli stessi, hanno ravvisato.

Laddove non ricevessero risposta, gli interessati possono adire il Garante, mediante **reclamo** (modulo di denuncia presente sul sito dell'Autorità).

Se l'interessato non è soddisfatto dal provvedimento del Garante (avente natura vincolante), questi può rivolgersi **all'Autorità Giudiziaria**.

Per quanto concerne le **sanzioni amministrative** si terrà conto della natura, della gravità e della durata della violazione, del carattere doloso o colposo e del grado di cooperazione con l'Autorità di controllo.

L'autorità competente ad applicare le sanzioni contenute nel Regolamento è il *Garante per la protezione dei dati personali*.

Le **sanzione amministrativa** possono arrivare fino a **10.000.000€** o, **per le imprese**, **fino a 2% del fatturato mondiale** totale annuo dell'esercizio precedente, per le **violazioni lievi** (ad esempio mancata consultazione preventiva dell'Autorità; mancata designazione del DPO);

per le **violazioni gravi** la sanzione può arrivare fino a **20.000.000€** o, **per le imprese**, **fino al 4% del fatturato mondiale** totale annuo dell'esercizio precedente (ad esempio: illiceità del trattamento, mancanza del consenso; violazione diritti interessato, ecc..).

Le sanzioni sono impugnabili davanti al Garante e, successivamente, davanti al Giudice ordinario.

Le sanzioni, che hanno carattere amministrativo, sono diventate pesanti rispetto alla precedente normativa.

Tuttavia, la sanzione pecuniaria non rappresenta la strada principale che il *Garante* generalmente percorre. Infatti, prima di arrivare a questo tipo di sanzioni, vengono esercitati i **poteri correttivi** (art. 58) attraverso la comunicazione di avvertimenti, moniti o ingiunzioni; possono essere imposte determinate limitazioni; ordinate rettifiche o sospensioni nell'utilizzo dei dati.

Le sanzioni devono essere irrogate dal *Garante* secondo i seguenti principi:

- **effettività**;
- **proporzionalità**;
- **dissuasività**.

Inoltre deve essere valutato il carattere doloso o colposo delle eventuali inadempienze, le eventuali misure prese dal Titolare per attenuare il danno subito dagli interessati, nonché la natura, gravità e durata della violazione.

Per la ***compliance* aziendale** al Regolamento è necessario:

- ✓ definire l'organigramma interno sulla *privacy*;
- ✓ elaborare il Registro dei trattamenti ed il Registro dei consensi;
- ✓ predisporre procedure per la gestione dei *data breach*;
- ✓ mappare gli *asset* aziendali (per *asset* possono intendersi anche persone fisiche) ed analizzare i rischi;
- ✓ rendere immediatamente consultabili i documenti di nomina, le informative, ecc…;
- ✓ realizzare audit periodici coinvolgendo i dipendenti che trattano dati nello svolgimento delle proprie mansioni;
- ✓ disporre di *sofware* conformi al nuovo *Gdpr* (*privacy by design* e *by default*).

Tra i **dati tutelabili** devono essere compresi numeri di telefono e indirizzo di posta elettronica.

Occorre sempre **verificare quali tipologie di dati tratto** e come ho **ottenuto i dati** che tratto ed, eventualmente, **con chi li condivido**.

Necessario **ampliare il contenuto dell'informativa** e predisporre procedure per garantire un **accesso tempestivo** agli interessati ai propri dati personali.

Occorre **riprendere i consensi** laddove non siano stati ottenuti i modo inequivocabile (a prescindere da quello che può essere il numero).

Verificare il flusso documentale (ad esempio rimuovendo i dati su carta in luoghi di accesso comune).

Si può provare a **mitigare il rischio** relativo alla gestione dei dati su dispositivi tramite blocco schermo, la criptazione delle *mail*, rendendo l'accesso alle reti *wifi* sicuro, utilizzando *client* di messaggistica sicuri, criptando l'*hard disk* del *PC*.