TUTELA DEL TRATTAMENTO DEI DATI PERSONALI:
REGOLAMENTO EUROPEO 2016/679 (GDPR) E CODICE PRIVACY D.LGS196/03 MODIFICATO DAL D.LGS 101/18

Storia e quadro normativo

EUROPA

Artt. 7 (Rispetto della vita privata e della vita familiare) e 8 (Protezione dei dati di carattere personale) Carta Diritti Fondamentali Unione Europea;

- **Direttiva 95/49/CE:** relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- **Direttiva 97/66/CE:** sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni
- **Direttiva 2002/58/CE:** relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche
- **Regolamento 2016/679:** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (che abroga la direttiva 95/46/CE)

Storia e quadro normativo

ITALIA

- **Legge 675/96:** Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;
- **DPR 318/99:** Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali;
- **D.lgs. 196/2003**: Codice in materia di protezione dei dati personali;
- **D.lgs. 101/2018**: Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

Che cos'è il GENERAL DATA PROTECTION REGULATION?

Il nuovo Regolamento Generale Europeo sulla Protezione dei Dati Personali n. 2016/679 (GDPR), con i suoi 99 articoli ha **riscritto la disciplina della Privacy a livello europeo.**

La necessità di emanare un Regolamento Europeo in materia di privacy nasce dalla **continua evoluzione** degli stessi concetti di privacy e protezione dei dati personali e quindi della relativa tutela dovuta principalmente **alla diffusione del progresso tecnologico.**

Quando si parla di privacy parliamo di dati relativi alle Persone Fisiche

Come prevede l'art. 99 il Regolamento si applica a decorrere dal **25 maggio 2018 obbligatoriamente per tutti gli sati membri**

OBIETTIVI ED IMPLICAZIONI DEL GDPR PER LE ORGANIZZAZIONI

Obiettivi

- Definire una BASELINE per la protezione dei dati
- Proteggere e tutelare meglio la protezione dei dati di tutti I cittadini in Europa
- Armonizzare la normativa in Europa in materia Privacy eliminando le differenze di approccio tra Stati membri

Implicazioni

- Sanzioni fino a €20,000,000 o al 4% del fatturato (tra i due valori verrà scelto quello più gravoso)
- Rischio Reputazionale
- Incrementare il potere degli individui qualora si verificasse una violazione dei dati personali

OGGETTO, FINALITA' E AMBITO DI APPLICAZIONE

Oggetto e finalità: il regolamento ha ad oggetto la **protezione di tutte le persone fisiche relativamente al trattamento dei dati personali** e della **loro libera circolazione nell'Unione Europea,** che non può essere limitata o vietata.

Ambito di applicazione materiale: Il regolamento si applica a qualsiasi **trattamento** interamente o parzialmente **automatizzato o non automatizzato** di dati personali **contenuti in un archivio** o destinato a figurarvi, intendendosi per archivio qualsiasi insieme strutturato di dati personali indipendentemente dal fatto che sia cartaceo o digitale.

OGGETTO, FINALITA' E AMBITO DI APPLICAZIONE

Ambito di applicazione territoriale: Dal punto di vista "geografico", la nuova disposizione europea rovescia il tradizionale principio di stabilimento, sancendo **l'applicabilità della disciplina** dettata "***indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione***" e stabilendo l'applicazione delle sue regole anche nei confronti dei Titolari e Responsabili non stabiliti nell'UE, quando le attività di trattamento riguardano:

a) l'offerta di beni o la prestazione di servizi ai suddetti **interessati nell'Unione**, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure

b) il **monitoraggio del loro comportamento** nella misura in cui tale comportamento **ha luogo all'interno dell'Unione.**

OGGETTO, FINALITA' E AMBITO DI APPLICAZIONE

Esclusioni:

- il regolamento invece NON si applica al trattamento di dati effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico
- oppure nel trattamento dei dati effettuati dalle autorità competenti a fini di prevenzione, indagine o accertamento di reati, o per la salvaguardia contro minacce alla sicurezza pubblica

COSA SI INTENDE PER DATO PERSONALE

Ai fini del regolamento per "**dato personale**" si intende 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.

Definizioni

«**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

Definizioni

Dati particolari: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Definizioni

dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

dati biometrici: 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;

Definizioni

- Una particolare attenzione, meritano i dati relativi a condanne penali, consentiti solo sotto il controllo dell'autorità pubblica;
- i dati dei minori per i quali il regolamento prevede che se il minore abbia almeno 16 anni, il consenso prestato dallo stesso è valido e conseguentemente il trattamento è lecito, se il minore ha meno di 16 anni il consenso deve essere sempre prestato da chi esercita la responsabilità genitoriale sul minore.

Definizioni

- Infine, i dati personali riguardanti persone decedute;

il regolamento non prevede tutele specifiche, tuttavia, consente ai singoli stati membri di prevedere norme riguardanti il trattamento dei dati di persone decedute. A tal proposito va ricordato che il nostro codice della privacy riconosce ai dati della persona defunta le stesse garanzie in termini di protezione previste per le persone in vita che possono essere esercitate dai familiari del defunto, salva eventuale espressa opposizione formulata in vita dall'interessato (art. 2 terdecies testo unico e smi)

Definizioni

Cos'è il **trattamento** di un dato?

Qualsiasi attività di gestione del dato come:

- la raccolta,
- la conservazione,
- la modifica,
- la consultazione,
- la comunicazione,
- la cancellazione

su qualsiasi supporto

- informatico,
- cartaceo o analogico,

sia attraverso operatori sia con processi automatizzati

Definizioni

196/2003

"**trattamento**", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

GDPR

«**trattamento**»: 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;

Definizioni

196/2003

"**misure di sicurezza**", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali, di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31

GDPR

Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

Principio di Accountability

Definizioni

196/2003

Art. 33. **Misure minime** 1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

GDPR

Protezione dei dati fin dalla progettazione (by design) e protezione per impostazione predefinita (by default)

…il titolare del trattamento mette in atto misure tecniche e organizzative adeguate…

…per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento…

Principio di minimizzazione

Definizioni

196/2003

GDPR

«**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;

Definizioni

«**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

I 7 PRINCIPI DEL GDPR

- LICEITA',CORRETTEZZA E TRASPARENZA
- LIMITAZIONE DELLE FINALITA' DEI TRATTAMENTI
- MINIMIZZAZIONE
- ESATTEZZA
- LIMITAZIONE DELLA CONSERVAZIONE
- INTEGRITA' E RISERVATEZZA
- RESPONSABILIZZAZIONE

PRINCIPIO DI LICEITA'

- **Consenso:** l'interessato ha dato il consenso al trattamento dei propri dati personali per uno o più scopi specifici;
- **Esecuzione contrattuale:** l'elaborazione è necessaria per l'esecuzione di un contratto di cui l'interessato è parte o per prendere provvedimenti su richiesta dell'interessato prima di stipulare un contratto;
- **Obbligo legale:** l'elaborazione è necessaria per adempiere a un obbligo legale a cui è soggetto il responsabile del trattamento;

PRINCIPIO DI LICEITA'

- **Interesse vitale delle persone:** il trattamento è necessario per proteggere gli interessi vitali dell'interessato o di un'altra persona fisica;
- **Interesse pubblico:** il trattamento è necessario per l'esecuzione di un compito svolto nell' interesse pubblico o nell'esercizio di pubblici poteri conferiti al responsabile del trattamento;
- **Interesse legittimo:** il trattamento è necessario ai fini degli interessi legittimi perseguiti dal responsabile del trattamento o da una terza parte;

Sempre nel rispetto della dignità e delle libertà fondamentali dell'individuo.

PRINCIPIO DI CORRETTEZZA

- **La correttezza del trattamento** è essenzialmente legata all'idea che gli interessati devono essere **consapevoli** del fatto che i loro dati personali saranno trattati, compreso il modo in cui i dati saranno raccolti, conservati e utilizzati, per consentire loro di **prendere una decisione informata**

PRINCIPIO DI TRASPARENZA

- Il **principio della trasparenza** impone 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 e chiaro.
- Il principio di Trasparenza non è direttamente spiegato nel GDPR, se ne fa maggiore chiarezza nell'Art. 12

PRINCIPIO DI TRASPARENZA

Art. 12

Il Titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni e le comunicazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

PRINCIPIO DI TRASPARENZA

"**conciso e trasparente**" i Titolari dovrebbero presentare le informazioni/comunicazioni in modo efficiente e succintamente al fine di evitare l'affaticamento delle informazioni. Queste informazioni dovrebbero essere chiaramente differenziate da altre informazioni non relative alla privacy, come le disposizioni contrattuali. In un contesto online, l'uso di una dichiarazione / informativa sulla privacy a più livelli consentirà a un soggetto dei dati di navigare verso la particolare sezione della dichiarazione/informativa sulla privacy a cui desiderano accedere immediatamente, piuttosto che dover scorrere grandi quantità di testo alla ricerca di particolari problemi.

PRINCIPIO DI TRASPARENZA

"intelligibile" significa che dovrebbe essere compreso da un membro medio del pubblico previsto. Ciò significa che il Titolare deve prima identificare il pubblico previsto e accertare il livello medio di comprensione del membro. Poiché il pubblico previsto può, tuttavia, differire dal pubblico effettivo, il Titolare dovrebbe anche controllare regolarmente se le informazioni/comunicazioni sono ancora adattate al pubblico reale (in particolare dove comprende minori), e apportare modifiche se necessario. I Titolari possono dimostrare la loro conformità con il principio di trasparenza testando l'intelligibilità delle informazioni e l'efficacia delle interfacce/comunicazioni/politiche utente ecc., attraverso i pannelli utente.

PRINCIPIO DI TRASPARENZA

Consequence: Una considerazione centrale del principio di trasparenza delinea che **l'interessato dovrebbe essere in grado di determinare in anticipo quale sia l'ambito e le conseguenze del trattamento.** Il WP29 ritiene che i Titolari non dovrebbero solo fornire le informazioni prescritte ai sensi degli articoli 13 e 14, ma anche pronunciare separatamente in un linguaggio non ambiguo quali sono le conseguenze più importanti del l'elaborazione non basandosi su esempi di elaborazione dei dati "innocenti" e prevedibili, ma fornendo una panoramica dei tipi di trattamento che potrebbero avere il maggiore impatto sui diritti e le libertà fondamentali dei dati soggetti in relazione alla protezione dei propri dati personali.

PRINCIPIO DI TRASPARENZA

"**facilmente accessibile**" significa che l'interessato non deve cercare le informazioni e che dovrebbero essere immediatamente evidente a loro dove è possibile accedere a queste informazioni, ad esempio fornendole direttamente a loro, collegandole ad esse, segnalandole chiaramente o come risposta a una domanda di lingua naturale (ad esempio in una privacy online a più livelli), dichiarazione / avviso, FAQ, tramite popup contestuali che si attivano quando un soggetto di dati compila un modulo online o in un contesto digitale interattivo attraverso un'interfaccia chatbot, ecc.).

PRINCIPIO DI TRASPARENZA

"**Linguaggio chiaro e semplice**" devono essere seguite le migliori pratiche per una scrittura chiara. Il richiamo al linguaggio chiaro è presente anche nel Considerando 42. Le informazioni dovrebbero essere fornite nel modo più semplice possibile, evitando complesse perifrasi. L'informazione dovrebbe essere concreta e definitiva; non dovrebbe essere formulato in termini astratti o ambivalenti o lasciare spazio a interpretazioni diverse.

PRINCIPIO DI TRASPARENZA

“**in particolare nel caso di informazioni destinate specificamente ai minori**”. Se un Titolare si rivolge ai minori o se è consapevole del fatto che la sua offerta è utilizzata dai minori (facendo affidamento sul consenso del minore- over 16), dovrebbe utilizzare un vocabolario, un tono e uno stile appropriato per un sedicenne. Un utile esempio di linguaggio centrato sul bambino usato come alternativa alla lingua legale può essere trovato nella "Convenzione delle Nazioni Unite sui diritti dell’infanzia”.

PRINCIPIO DI LIMITAZIONE DELLE FINALITA'

- I Titolari devono innanzitutto identificare le particolari finalità per le quali i dati personali saranno trattati (by design)
- Tali scopi diverranno i limiti entro i quali i dati personali devono essere raccolti e utilizzati dai responsabili del trattamento dei dati.
- Il trattamento secondario può essere effettuato legalmente solo quando tale trattamento è considerato compatibile con lo scopo originale per il quale i dati personali sono stati raccolti

PRINCIPIO DI LIMITAZIONE DELLE FINALITA'

- Al fine di poter dimostrare la conformità con il presente regolamento il titolare adotta politiche interne e attua misure che soddisfano in particolare i principi della protezione dei dati fin dalla progettazione e della **protezione dei dati di default.**
- Questo implica la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

PRINCIPIO DI LIMITAZIONE DELLE FINALITA'

Esempio1

I Titolari raccolgono ed elaborano i dati personali per offrire servizi legati a **un'applicazione mobile di fitness.** Lo scopo del trattamento dei dati è analizzare i dati per raccomandare all'utente una routine di allenamento personalizzata.

Un ulteriore elaborazione dei dati per identificare errori tecnici dell'applicazione sarà considerata compatibile, poiché migliorare l'efficienza dell'app è in linea con lo scopo originale.

Esempio2

Per assistere i **pazienti diabetici nell'erogazione di farmaci,** viene sviluppata un'app che offre il monitoraggio dei livelli di concentrazione di zucchero nel sangue.

L'app condivide le informazioni personali con un'azienda che vende farmaci per il diabete. La promozione e la commercializzazione dei farmaci per il diabete non sono compatibili con lo scopo originale.

Esempio3

Un **professionista della salute raccoglie dati personali** per essere in grado di valutare e trattare le condizioni mediche dei suoi pazienti.

La condivisione dell'elenco dei pazienti con una compagnia assicurativa per consentire alla compagnia assicurativa di offrire i propri servizi (ad es. Assicurazione sulla vita o sanitaria) non sono compatibili con lo scopo originale per il quale i dati personali sono stati raccolti.

PRINCIPIO DI MINIMIZZAZIONE DEI DATI

Il principio della "minimizzazione dei dati" indica che un Titolare del trattamento dei dati dovrebbe limitare la raccolta di informazioni personali a ciò che è **direttamente rilevante e necessario per aggiungere uno scopo specifico.**

PRINCIPIO DI ESATTEZZA

- I dati raccolti dovranno essere esatti e, se necessario, aggiornati.
- Di conseguenza le Aziende dovranno adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente eventuali dati inesatti rispetto alle finalità per le quali sono trattati.

PRINCIPIO DI ESATTEZZA

Esempi

Se un individuo si è trasferito da Roma a Milano, un record che mostra che attualmente vive a Roma è ovviamente impreciso. Se l'archivio rappresenta lo storico abitativo invece è esatto. Deve sempre essere chiaro cosa è destinato a mostrare l'archivio.

Un giornalista include informazioni derivate da Internet sull'arresto per guida pericolosa. Se il giornalista riporta "la fonte non è stata verificata" il dato è esatto. Se non lo fa, lasciando intendere al pubblico che l'informazione è verificata, il dato è inesatto.

Il Postcode Address File contiene gli indirizzi postali delle abitazioni nel Regno Unito. Riflette la consegna la posta della Royal Mail. Capita che un indirizzo postale sia collegato a una città in una contea (ad es. Stoke-on-Trent nello Staffordshire) anche se l'ubicazione reale è in un'altra contea (ad es. Cheshire). Il file PAF è esatto per la sua funzione (consegna posta).

"è accettabile tenere registri di eventi accaduti per errore, a condizione che tali registri non siano fuorvianti riguardo ai fatti". Ad esempio: "Una diagnosi errata di una condizione medica viene mantenuta come informazione all'interno della cartella clinica di un paziente, anche dopo che la diagnosi è stata rettificata, perché è rilevante ai fini della spiegazione del trattamento dato al paziente o di ulteriori problemi di salute".

PRINCIPIO DI LIMITAZIONE DELLA CONSERVAZIONE

Il GDPR non stabilisce alcun periodo minimo o massimo per la conservazione dei dati personali ma solo che non devono essere conservati per un periodo superiore a quello necessario per lo scopo o per la finalità per cui vengono trattati.

Il Titolare del trattamento deve conservare i dati **solo per il tempo necessario** a raggiungere lo scopo.

Eccezioni: il trattamento è consentito per periodi più lunghi se:

- archiviazione di pubblico interesse
- ricerca scientifica o storica
- fini statistici

sempre nel rispetto delle regole dettate dal Regolamento.

PRINCIPIO DI INTEGRITA' E RISERVATEZZA

I dati dovranno essere sempre trattati in maniera da garantire una sicurezza adeguata, il che prevede l'adozione di misure di sicurezza tecniche ed organizzative adeguate per proteggere i dati stessi da trattamenti non autorizzati o illeciti, dalla loro perdita o distruzione o dal danno accidentale.

PRINCIPIO DI ACCOUNTABILITY

- Il principio di responsabilizzazione o accountability prevede che il titolare sia in grado di dimostrare di aver adottato ogni misura necessaria per garantire il rispetto dei principi applicabili al trattamento dei dati personali.
- Non basterà dunque mettere in campo delle formule standard, perché il titolare dovrà dimostrare di aver elaborato un progetto complessivo specifico per il trattamento dei dati personali che provi il rispetto dei principi sanciti dal regolamento: dalla corretta informativa e autorizzazione al trattamento dei dati, all'effettuazione di valutazioni d'impatto sul rischio, alla tenuta del registro delle attività di trattamento.

Informativa

- L'informativa costituisce lo strumento cardine per poter **informare correttamente l'interessato** del trattamento dei propri dati. Il Regolamento dedica specifiche disposizioni al contenuto dell'informativa, distinguendo a seconda che il dato sia raccolto direttamente presso l'interessato o presso terzi.

Informativa

Ai sensi dell'articolo 12 del Regolamento, l'informativa deve essere resa:

- in forma concisa, facilmente accessibile, con un linguaggio chiaro
- per iscritto o con altri mezzi, esempio elettronici
- oralmente solo se richiesto dall'interessato e purché sia comprovata con altri mezzi l'identità dell'interessato
- anche in combinazione con l'utilizzo di icone standardizzate

Informativa

Inoltre ai sensi dell'articolo 13 del Regolamento l'informativa deve contenere, obbligatoriamente, i seguenti dati:

- l'identità e i dati di contatto del Titolare del trattamento
- i dati di contatto del DPO,
- le finalità del trattamento e gli eventuali destinatari dei dati
- l'eventuale intenzione del Titolare di trasferire i dati a un paese terzo o a una organizzazione internazionale

Informativa

Infine, per garantire il più corretto trattamento il Titolare deve fornire all'interessato le seguenti ulteriori informazioni:

- il periodo di conservazione dei dati, oppure, se non è possibile, i criteri utilizzati per determinare tale periodo
- l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento l'accesso ai propri dati personali, la loro rettifica, la loro cancellazione, la loro limitazione o portabilità
- l'esistenza dei diritto di revocare, in qualsiasi momento, il consenso al trattamento dei propri dati
- il diritto di proporre reclamo a un'autorità di controllo

Consenso

- E' definito "qualsiasi **manifestazione di volontà** libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, che i dati personali che lo riguardano siano oggetto di trattamento"
- Il consenso per essere valido deve essere espresso mediante un atto positivo libero, specifico, informato ed inequivocabile.

Consenso

- Dunque il consenso espresso da un interessato che non è in grado di operare una scelta autenticamente libera non sarà valido.
- E tantomeno sarà valido un consenso generale, relativo a finalità non ben identificate o specificate.
- Infine, il consenso può essere revocato in qualsiasi momento senza che pregiudichi la liceità del trattamento basato sul consenso prima della revoca.

Diritti dell'interessato

- Diritto di informazione ed accesso, articolo 15
- Diritto di rettifica, articolo 16
- Diritto di cancellazione o Oblio, articolo 17
- Diritto di limitazione di trattamento, articolo 18
- Diritto di Portabilità, articolo 20
- Diritto di Opposizione, articolo 21
- Diritto di revoca, articolo 7

Diritto di informazione ed accesso art. 15

L'articolo 15 garantisce all'interessato il diritto di Accesso, ovvero di ottenere dal Titolare del trattamento la **conferma che sia o meno in corso un trattamento di dati che lo riguardano** e di ottenere l'accesso alle seguenti informazioni:

- la finalità del trattamento
- le categorie dei dati trattati
- i destinatari e le categorie di destinatari
- il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

Diritto di informazione ed accesso art. 15

- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- il diritto di proporre reclamo a un'autorità di controllo;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

Diritto di rettifica, articolo 16

L'articolo 16 del Regolamento stabilisce invece che "l'interessato ha il diritto di ottenere dal Titolare **la rettifica dei dati personali inesatti che lo riguardano,** nonché l'integrazione dei dati personali incompleti.

Consiste nel dare la possibilità all'interessato di modificare i propri dati nel caso siano inesatti, è fondamentale quindi prevedere metodi che facilitino l'esercizio di questo diritto ed è compito del titolare informare l'interessato dell'avvenuta integrazione facendo in modo che tali modifiche non valgano solo per quelli in suo possesso, ma anche per quei dati che nel frattempo sono stati comunicati a terzi.

Diritto di cancellazione o Oblio art. 17

All'articolo 17 il regolamento introduce una novità nell'ambito del diritto alla protezione dati: il cosiddetto Diritto all'oblio. In particolare l'articolo dispone che l'interessato "ha il diritto di ottenere dal Titolare **la cancellazione dei suoi dati personali**"

Il diritto all'oblio può essere esercitato se:

- i dati non sono più necessario per le finalità per le quali sono stati raccolti
- l'interessato revoca il consenso su cui si basa il trattamento

Diritto di cancellazione o Oblio art. 17

- l'interessato si oppone al trattamento e non sussiste alcun legittimo prevalente motivo per procedere al trattamento
- i dati sono stati trattati illecitamente.

Lo stesso articolo riconosce espressamente il "diritto all'oblio" anche nel caso di **revoca del consenso** o quando l'interessato si sia **opposto al trattamento** dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali **non sia altrimenti conforme al Regolamento**.

Diritto di cancellazione o Oblio art. 17

Nel caso in cui il Titolare abbia reso pubblici i dati e sia obbligato a cancellarli, deve adottare tutte le misure ragionevoli per informare i Titolari che stanno trattando quei dati di cancellare qualsiasi link, copia o riproduzione di quei dati.

In ambito nazionale il Garante della Privacy ha chiarito tramite una propria pronuncia come lo stesso **diritto all'oblio debba essere bilanciato con il diritto di cronaca**; difatti, gli utenti non possono ottenere da Google la cancellazione dai risultati di ricerca di una notizia che li riguarda se si tratta di un fatto recente e di rilevante interesse pubblico.

Diritto di limitazione di trattamento, articolo 18

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

- **l'interessato contesta l'esattezza dei dati personali;**
- **il trattamento è illecito** e l'interessato **si oppone alla cancellazione** dei dati personali, chiedendone solo la limitazione;
- i dati sono **necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria,** mentre al titolare del trattamento non servono più a fini del trattamento;

Diritto di limitazione di trattamento, articolo 18

- **l'interessato si è opposto al trattamento** e si è in attesa delle verifiche necessarie per determinare se i motivi legittimi del titolare del trattamento prevalgano su quelli dell'interessato.

In questo caso i dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

Diritto Portabilità, articolo 20

Si intende il riconoscimento sia del diritto dell'interessato a **trasferire i propri dati** (es. quelli relativi al proprio "profilo utente") da un sistema di trattamento elettronico (es. Social Network) ad un altro senza che il Titolare possa impedirlo, sia del diritto **di ottenere gli stessi in un formato elettronico strutturato e di uso comune** che consenta di farne ulteriore uso.

Diritto di Opposizione, articolo 21

- La possibilità di opporsi al trattamento, va garantito quando la base giuridica è il legittimo interesse o l'esecuzione di un compito di interesse pubblico.
- Anche questo diritto ha i suoi limiti in quanto ci potranno essere casi in cui prevale l'interesse legittimo del titolare rispetto a quello dell'interessato, fondamentale sarà effettuare il giusto bilanciamento indicandolo nell'informativa, oppure il trattamento è necessario per un compito di interesse pubblico o l'accertamento, la difesa o l'esercizio di un diritto di fronte ad un giudice. (cons. 69)

Diritto di revoca, articolo 7

- Riguarda i trattamenti basati sul consenso, una base giuridica da utilizzare solamente quando non possono essere utilizzate le altre.
- L'interessato dovrà poter conoscere come revocarlo e, nel caso, andranno cancellati i dati legati al trattamento oggetto di revoca.
- La revoca del consenso dovrà poter essere effettuata con la stessa facilità con cui è stato prestato ed è onere del titolare agevolare l'esercizio della revoca.

Le figure: il Titolare del trattamento

- Il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee, è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza. A tali fini mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali sia effettuato in modo conforme.

Il Contitolare

- Chi decide in modo congiunto di trattare dei dati per una finalità comune.

Esempio: una banca dati riguardante dei clienti insolventi, gestita congiuntamente da diversi istituti di credito.

Il Responsabile del trattamento

- Uno o più Dirigenti/Quadri/Responsabili di U.O. delle strutture di massima dimensione in cui si articola l'organizzazione dell'azienda, è nominato Responsabile del trattamento di tutte le banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza.
- Il Responsabile deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative di cui all'art. 5 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.

Il Responsabile del trattamento

- E' consentita la nomina di sub-responsabili del trattamento (gli incaricati del trattamento nel Codice Privacy) da parte di ciascun responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario;

Nota Bene

- Il Responsabile risponde, anche dinanzi al Titolare dell'inadempimento, dell'operato del subresponsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sul suo operato.

Il Responsabile esterno

Il titolare del trattamento può scegliere se avvalersi o meno dell'esternalizzazione del servizio di trattamento dei dati, ma una volta optato per tale soluzione non può fare a meno di designare il soggetto in questione quale responsabile del trattamento.

In realtà il GDPR (art. 28) non parla di nomina, bensì stabilisce che i trattamenti del responsabile debbano essere disciplinati da un contratto o altro atto giuridico 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.

Il Responsabile esterno

Il contratto deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28 al fine di dimostrare che il responsabile fornisca garanzie sufficienti, quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento.

Data Protection Officer (artt. 37 e ss.)

- Tra i nuovi adempimenti è prevista l'adozione di una nuova figura professionale obbligatoria: **il Responsabile per la protezione dei dati personali** (*Data Protection Officer* o *"DPO"*).
- Il *DPO* è un supervisore indipendente che sarà designato da soggetti apicali sia dalle pubbliche amministrazioni che in ambito privato.

Data Protection Officer (artt. 37 e ss.)

Sarà obbligatorio all'interno di tutte:

a) le **aziende pubbliche** nonché in tutte quelle ove i trattamenti presentino specifici rischi;

b) le aziende nelle quali sia richiesto un **monitoraggio regolare e sistematico degli "interessati"** su larga scala,

c) le aziende che trattano i c.d. "**dati sensibili**".

Data Protection Officer (artt. 37 e ss.)

Il Responsabile per la protezione dei dati personali è tenuto a:

- **informare e consigliare** il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento;
- **verificare** l'attuazione e l'applicazione della normativa, oltre alla sensibilizzazione e formazione del personale e dei relativi auditors;
- **fornire,** se richiesto, **pareri** in merito alla valutazione d'impatto sulla protezione dei dati e a sorvegliare i relativi adempimenti;

Data Protection Officer (artt. 37 e ss.)

- fungere da **punto di contatto per gli "interessati"**, in merito a qualunque problematica connessa al trattamento dei loro dati nonché all'esercizio dei loro diritti;
- fungere da **punto di contatto per il Garante** per la protezione dei dati personali oppure, eventualmente, per consultare il Garante di propria iniziativa.

Attenzione: la figura del DPO non va confusa con quella di un responsabile *privacy ex* art. 29 del nostro Codice Privacy. Elemento cruciale che differenzia le due figure: mentre il primo deve essere indipendente ed autonomo, il secondo deve agire seguendo soltanto le istruzioni del titolare del trattamento

Gli strumenti del trattamento: il Registro dei trattamenti

*Il **Registro delle attività di trattamento svolte dal Titolare del trattamento**, deve recare le seguenti informazioni:*

a) il nome ed i dati di contatto del Titolare del trattamento, eventualmente del Contitolare del trattamento, del DPO;

b) le finalità del trattamento;

c) la sintetica descrizione delle categorie di interessati (cittadini, residenti, utenti, dipendenti, amministratori, parti, altro), nonché le categorie di dati personali (dati identificativi, dati genetici, dati biometrici, dati relativi alla salute);

Gli strumenti del trattamento: il Registro dei trattamenti

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati: persona fisica o giuridica; autorità pubblica; altro organismo destinatario;

e) l'eventuale trasferimento di dati personali verso un paese terzo od organizzazione internazionale;

f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Gli strumenti del trattamento: il Registro dei trattamenti

REGISTRO ATTIVITA' DI TRATTAMENTO (art.30, c.1, GDPR)

TITOLARE DEL TRATTAMENTO		DATA PROTECTION OFFICER	
Indirizzo		Indirizzo	
N. Telefono		N. Telefono	
Mail		Mail	
PEC		PEC	
DELEGATO/RAPPRESENTANTE DAL TITOLARE (eventuale)		Registro Tenuto Da	
Indirizzo		Data Creazione	
N. Telefono		Ultimo Aggiornamento	
Mail		N. Schede Compilate	
PEC		Prossima Revisione	

	DATI PERSONALI								INTERESSATI			DESTINATARI			SICUREZZA
Prog.	Descrizione	Categoria	Dati particolari SI/NO	Finalità del trattamento	Modalità	Base giuridica del trattamento	Luogo di conservazione (cartaceo/digitale)	Tempi di conservazione	Categoria	Consenso (SI/NO)	Informativa (SI/NO)	Categoria	Resp. Esterno (eventuale) SI/NO	Paesi terzi, org.ni int.li (eventuale) SI/NO	Misure Tecniche ed organizzative adottate (e rimandi ad eventuali allegati di dettaglio)

Gli strumenti del trattamento: il Registro dei trattamenti

ESEMPI DI MISURE DI SICUREZZA (ORGANIZZATIVE)

- Selezionare personale moralmente integro.
- Introdurre codice disciplinare e sanzioni
- Segregare l'archivio cartaceo con accesso ristretto
- Non lasciare documenti incustoditi nelle postazioni di lavoro.
- Sala di attesa separata da zona uffici.
- Ufficio Segreteria sempre presente durante orario ufficio
- Formazione del personale

Gli strumenti del trattamento: il Registro dei trattamenti

ESEMPI DI MISURE DI SICUREZZA (TECNICHE)

- Sistema antifurto.
- Sistema di videosorveglianza.
- Identity e Access management (password, accesso selezionato alla rete, etc.)
- Firewall
- Antivirus e Antispyware
- Back-up sistematico dei dati informatici
- Businness continuity
- Provider internet

DPIA - *Valutazione di impatto sulla protezione dei dati*

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve effettuare una valutazione dell'impatto del medesimo trattamento ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.

DPIA - *Valutazione di impatto sulla protezione dei dati*

Una valutazione di impatto sulla protezione dei dati (di seguito indicata con "DPIA") consiste in una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali e permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

DPIA - *Valutazione di impatto sulla protezione dei dati*

E' richiesto in relazione

a) ai trattamenti automatizzati, ivi compresa la profilazione,

b) ai trattamenti su larga scala di categorie particolari di dati (sensibili), nonché relativamente ai dati ottenuti dalla sorveglianza sistematica, sempre su larga scala, di zone accessibili al pubblico.

Sarà ad ogni modo il Garante Privacy (per quanto riguarda l'Italia) a redigere e rendere pubblico l'elenco delle tipologie di trattamenti soggetti al requisito della "valutazione di impatto sulla protezione dei dati".

Data breach - **La notifica delle violazioni dei dati**

- Sulla base della normativa europea, il Garante per la protezione dei dati personali ha adottato negli ultimi anni una serie di provvedimenti che introducono in determinati settori **l'obbligo di comunicare eventuali violazioni di dati personali** ("*data breach*") all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati. Il mancato o ritardato adempimento della comunicazione espone alla possibilità di sanzioni amministrative.

Data breach - **La notifica delle violazioni dei dati**

- Mentre per la **notifica all'autorità** di controllo è richiesto "*un **rischio per i diritti e le libertà degli individui***", per la **notifica al diretto interessato** è necessario che il **rischio** sia "***elevato***": in quest'ultimo caso, è richiesta una soglia di pericolo maggiore anche per evitare inutili allarmismi da parte dei soggetti interessati.

REGOLE DEONTOLOGICHE

Le regole deontologiche hanno una natura prettamente giuridica, sono elaborate direttamente dal Garante privacy e fissano le condizioni di liceità dei trattamenti dei dati alle quali si riferiscono con la conseguenza che il rispetto di tali regole è condizione essenziale di liceità e correttezza del trattamento.

INFATTI ai sensi dell'ART. **40 GDPR:** I Codici di condotta sono destinati a contribuire alla corretta applicazione del Regolamento in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

REGOLE DEONTOLOGICHE

In attuazione dell'art. 40 GDPR e dell'art. 2 quater del D.lgs 196/2003 come modificato dal D.lgs. 101/2018 il Garante privacy italiano ha verificato la **conformità, dei codici di deontologia e di buona condotta** esistenti per i trattamenti di dati personali, con il Regolamento UE 2016/679 sulla protezione dei dati personali..

Più precisamente il Garante ha verificato la conformità al GDPR delle disposizioni contenute nei codici riportati negli allegati A.1, A.2, A.3, A.4, A.5, A.6 e A.7 del D.lgs. 196/2003, modificandoli o adottandone dei nuovi laddove non adeguati, così sono stati pubblicati:

REGOLE DEONTOLOGICHE

- **Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica** (G.U. del 4 gennaio 2019, n. 3);
- **Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica** (G.U. del 15 gennaio 2019, n. 12);
- **Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale** (G.U. del 14 gennaio 2019, n. 11);
- **Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica** (G.U. del 14 gennaio 2019, n. 11);
- **Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria** (G.U. del 15 gennaio 2019, n. 12).

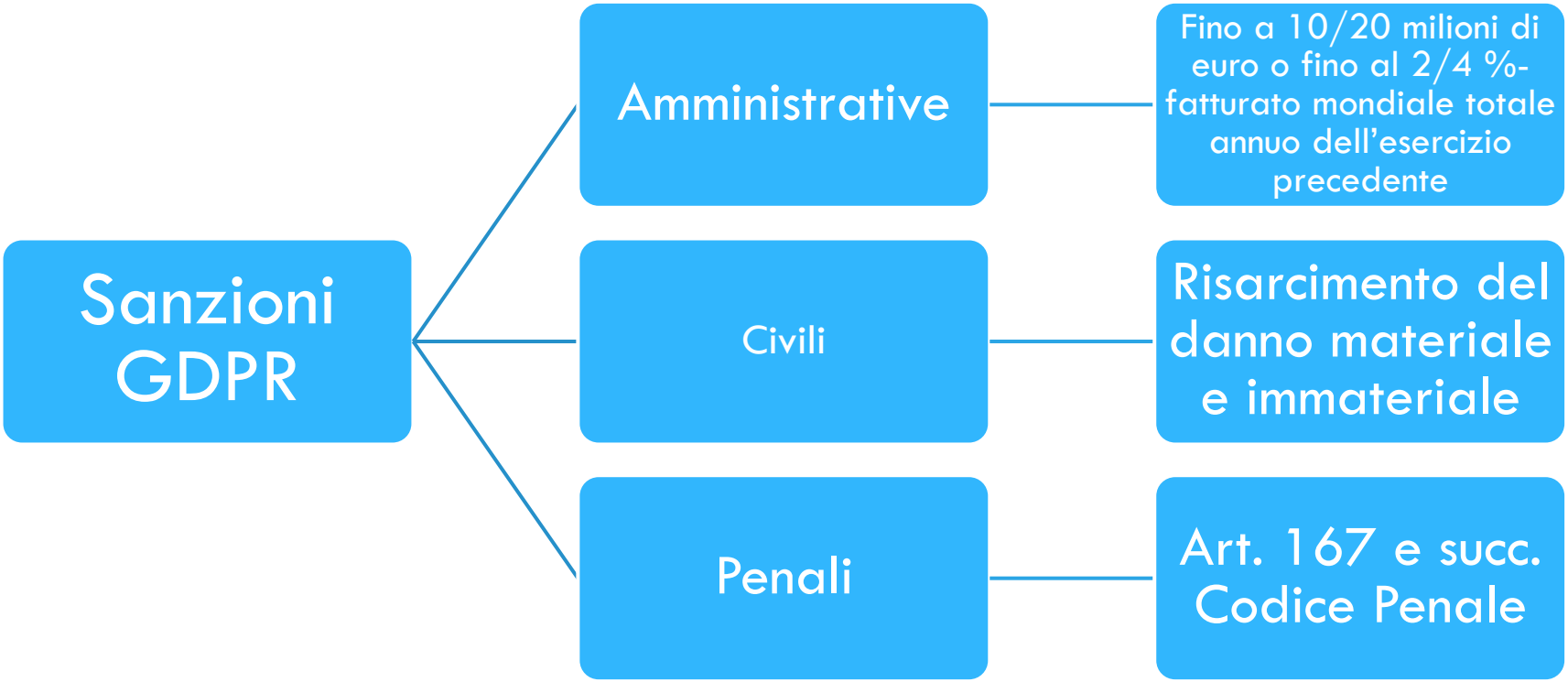
REGOLE DEONTOLOGICHE

Dalla data di pubblicazione di tali "Regole deontologiche", hanno cessato di trovare applicazione i corrispondenti codici di deontologia riportati negli allegati A1, A2, A3, A4 e A6 del Codice. Mentre Le disposizioni dei codici di deontologia e di buona condotta di cui agli allegati A5 e A7 continueranno a produrre effetti fino al completamento delle procedure di revisione previste dal comma 1 del medesimo articolo 20.

Si tratta di

- **A7. Codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale**
- **A.5. Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti**

Responsabilità e sistema sanzionatorio



Sanzioni amministrative pecuniarie

1. Le violazioni agli obblighi in capo alle imprese (20 articoli su 49) sono punite **fino a 10 milioni di euro o fino al 2% del fatturato mondiale annuo**.

Ad esempio:

- la violazione dell'obbligo di tenuta del registro dei trattamenti;
- la mancata valutazione d'impatto DPIA;
- l'omessa consultazione preventiva dell'Autorità;
- l'omessa notifica di data breach;
- l'omessa nomina del DPO;
- l'omessa adozione di misure di sicurezza adeguate.

Sanzioni amministrative pecuniarie

2. Gli altri 29 articoli puniscono **fino a 20 milioni di euro o fino al 4 % del fatturato mondiale annuo** la violazione dei principi del regolamento e dei diritti degli interessati.

Ad esempio:

- i principi di base del trattamento, comprese le condizioni relative al consenso;
- i diritti degli interessati;
- i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale;
- l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo.

Responsabilità civile e risarcimento danni

Art. 82 Regolamento: chiunque subisce un danno materiale o immateriale (patrimoniale o non patrimoniale) causato da una violazione del regolamento, ha diritto ad ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento

Il Legislatore Italiano, come quello comunitario, considera il trattamento di dati personali come attività pericolosa (vedi **art. 2050 Codice Civile**).

Chi ritenga di essere stato leso da un trattamento dati che lo riguardano può ottenere il risarcimento danni **senza dover provare la colpa del Titolare**. Deve provare solo gli eventuali danni derivati dal trattamento. Il nesso di causalità è pertanto che:

– Il danno si sia realizzato;

– Dipenda dall'attività di trattamento dati;

Responsabilità civile e risarcimento danni

Chi ha effettuato il trattamento, per sottrarsi all'obbligo di risarcimento, ha l'onere di provare di aver adottato tutte le misure idonee ad evitare il danno (***inversione dell'onere della prova***).

Solidarietà: Qualora più titolari o responsabili del trattamento siano coinvolti nello stesso trattamento, ogni titolare o responsabile dovrebbe rispondere per la totalità del danno.

In ogni caso:

Responsabilità Titolare: risponde quando è coinvolto nel trattamento che, violando il regolamento, ha cagionato il danno;

Responsabilità Responsabile: risponde per il danno cagionato solo se non ha adempiuto agli obblighi del regolamento che siano specificamente diretti nei suoi confronti, o ha agito in modo difforme o addirittura contrario rispetto alle legittime istruzioni impartitegli dal titolare del trattamento.

Responsabilità penale

La responsabilità penale è prevista dagli articoli 167 e seg. del codice privacy, così come modificati dal decreto 101 del 2018:

- **Art. 167:** Trattamento Illecito di dati;
- **Art. 167- bis:** Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala;
- **Art. 167- ter:** Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala;
- **Art. 168:** Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante;
- **Art. 170**: Inosservanza di provvedimenti del Garante;
- **Art. 171**: Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori.

Mezzi a tutela dell'interessato

Istanza al titolare del trattamento

L'interessato al trattamento che ritiene di aver subito una violazione dei suoi diritti può rivolgersi direttamente al titolare del trattamento (o al responsabile o anche attraverso un incaricato) per la sua tutela, senza particolari formalità (per lettera, mail, fax, ecc...).

L'interessato deve ricevere una risposta entro 30 giorni, termine che può essere esteso a 60 giorni, nel qual caso il titolare deve darne comunicazione all'interessato nei primi 30 giorni. In mancanza di risposta, o in caso di risposta non soddisfacente, l'interessato può rivolgersi all'Autorità di controllo (Garante) o a quella giudiziaria.

Mezzi a tutela dell'interessato

Dinanzi al **Garante:**

- **SEGNALAZIONE** (per sollecitare un controllo quando non si hanno dati per effettuare un reclamo)
- **RECLAMO CIRCOSTANZIATO**: col quale rappresenta una violazione della normativa in materia di protezione dei dati personali. Il reclamo, regolamentato dall'articolo 77 del GDPR, deve contenere una serie di elementi, in particolare l'indicazione dettagliata dei fatti e delle circostanze, delle norme del GDPR che si presumono violate e delle misure richieste.

Mezzi a tutela dell'interessato

In sede giudiziaria: dinanzi a **Giudice Ordinario**

- **RICORSO** per esercitare i diritti dell'interessato ed ottenere la immediata sospensione del trattamento e la cessazione del comportamento illegittimo ed il risarcimento del danno.

Alternativo al reclamo al Garante (no ambedue, la proposizione dell'uno esclude l'altro), ad eccezione dei casi di:

- Opposizione verso provvedimento che conclude reclamo (entro 30 giorni dal ricevimento);
- Richiesta risarcimento dopo reclamo.

Il processo di compliance Privacy al GDPR

Le attività da svolgere possono sinteticamente essere così individuate (in successione temporale):

- Definizione delle categorie di dati personali trattati e adozione del Registro dei trattamenti di dati personali;
- mappatura dei processi per individuare quelli collegati al trattamento dei dati personali;
- individuazione, nell'ambito della suddetta mappatura, delle minacce e prima valutazione dei rischi;

Il processo di compliance Privacy al GDPR

- Identificazione e valutazione dei principali gaps da colmare per essere conformi al GDPR (gap analysis);
- definizione, alla luce dei divari evidenziati, di un piano di adeguamento complessivo (action plan), con le proposte di miglioramento dei processi ed eventualmente della regolamentazione interna;
- interventi formativi per il personale.
- implementazione e conseguente monitoraggio degli interventi previsti.

L'implementazione del modello Privacy

1. **struttura organizzativa**: definizione, formalizzazione e implementazione della struttura organizzativa del sistema di data protection, ruoli e responsabilità;

2. soggetti coinvolti: sensibilizzazione e **formazione** dei soggetti chiamati a ricoprire un ruolo attivo nell'ambito del modello di funzionamento della data protection (incaricati del trattamento, responsabili, etc.;

3. **processi**: definizione, formalizzazione e implementazione di processi e regole connessi alla protezione dei dati personali, sia in modo diretto (ad esempio la gestione dei diritti degli interessati) sia in modo indiretto (ad esempio la gestione delle misure di sicurezza tecnico-organizzative);

L'implementazione del modello Privacy

4. **documentazione**: stesura ex novo della documentazione o modifica della documentazione esistente (ad esempio informative, moduli di consenso, clausole contrattuali) e avvio della relativa adozione, anche verso l'esterno;

5. **controlli interni**: definizione e implementazione di un sistema di controlli interni per la protezione dei dati personali (ad esempio il sistema di deleghe), ivi compresa la realizzazione di internal audit volti a evidenziare eventuali non conformità.

A valle dell'intero processo di adeguamento deve essere quindi effettuato un controllo periodico in merito alla corretta adozione del modello di funzionamento della data protection ed elaborazione di eventuali **azioni correttive**, con conseguente **aggiornamento** del modello stesso.

Norma UNI 11697:2017

- **Titolo:** Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza
- **Data entrata in vigore:** 30 novembre 2017
- La norma definisce i profili professionali relativi al trattamento e alla protezione dei dati personali coerentemente con le definizioni fornite dall'EQF e utilizzando gli strumenti messi a disposizione dalla UNI 11621-1 "Attività professionali non regolamentate - Profili professionali per l'ICT - Parte 1: Metodologia per la costruzione di profili professionali basati sul sistema e-CF".

Norma UNI 11697:2017

- La norma fa riferimento ai profili professionali relativi al trattamento ed alla protezione dei dati personali ed è stata sviluppata secondo l'ormai ben noto schema europeo chiamato EQF-European Qualification framework, che rappresenta la linea guida per sviluppare norme applicabili ad attività professionali non regolamentate e non ordinistiche.
- Le **figure professionali** delineate dalla norma UNI sono le seguenti:

Data Protection Officer (DPO)

- supporta il titolare o il responsabile del trattamento nell'applicazione e nell'osservanza del Regolamento (UE) 2016/679 ("Regolamento"), in conformità all' art. 37 (Designazione del Responsabile della protezione dei dati) ha il compito principale di garantire, in maniera indipendente, l'applicazione interna delle disposizioni del Regolamento da parte del Titolare del trattamento.
- Il DPO è inoltre tenuto a tenere un registro di tutte le operazioni di trattamento che coinvolgono dati personali effettuato da parte dell'istituzione. Il registro, che deve contenere le informazioni circa lo scopo e le condizioni delle operazioni di trattamento, dovrebbe essere accessibile a tutti gli interessati.

Manager Privacy

- assiste il titolare nelle attività di coordinamento di tutti i soggetti che – nell'organizzazione – sono coinvolti nel trattamento di dati personali (responsabili, incaricati, amministratori di sistema, ecc.), garantendo il rispetto delle norme in materia di privacy e il mantenimento di un adeguato livello di protezione dei dati personali.

Specialista Privacy

- figura di supporto appositamente formato egli collabora con il Manager Privacy e cura la corretta attuazione del trattamento dei dati personali all'interno dell'organizzazione, svolgendo le attività operative che, di volta in volta, si rendono necessarie durante tutto il ciclo di vita di un trattamento di dati personali. Tale figura è richiesta soprattutto all'interno di grandi organizzazioni aziendali (che incide su più uffici e/o stabilimenti con una diversa collocazione territoriale) ove si rende necessario creare più "presidi" privacy;

Valutatore Privacy

- figura dotata di una apposita formazione che si caratterizza per la sua terzietà sia nei confronti del Manager che dello Specialista Privacy; egli esercita una attività di monitoraggio (audit) andando ad esaminare periodicamente il trattamento dei dati personali e valutando il rispetto delle normative di settore emanate a livello nazionale, comunitario e internazionale. Egli, inoltre, approva le misure necessarie per l'eliminazione di eventuali non conformità alla disciplina prescritta.

GRAZIE DELL'ATTENZIONE

Pride29 Srl

Avv. Sabrina Primavera

Via Nomentana 909

00137 Roma

Tel. 068276766

www.pride29.it