MILANO
LODI
MONZA BRIANZA

F.I.M.A.A.

PRIVACY: GDPR e adempimenti in tempo di COVID
Tutela dei dati personali: raccolta, trattamento e conservazione

Avv. Matteo Alessandro Pagani

SOMMARIO

- **Introduzione**
- **Ambito di applicazione materiale**
- **Ambito di applicazione territoriale**
- **Principali definizioni**
- **I soggetti del trattamento**: Titolare; Contitolare; Responsabile; Sub-Responsabile; Autorizzato
- **Principi fondamentali del trattamento**: il Principio di Accountability
- **Dati oggetto di trattamento**: Categorie particolari di dati personali; FOCUS: trattamento dei dati genetici, biometrici e relativi alla salute; Dati penali
- **Diritti degli interessati**: Informazioni, comunicazioni e modalità; Informativa sul trattamento dei dati; Diritto di accesso; Diritto di rettifica; Diritto alla cancellazione; Diritto alla limitazione del trattamento; Diritto di portabilità; Diritto di opposizione; Processo decisionale automatizzato
- **Registro dei trattamenti**: del Titolare; del Responsabile
- **Sicurezza dei dati e valutazione dei rischi**
- **Data Breach**
- **Data Protection Impact Assessment** (DPIA)
- **Data Protection Off**icer (DPO)
- **Trasferimento dei dati extra UE-SEE**
- **Sanzioni**: Sanzioni amministrative previste dal GDPR; Sanzioni penali previste dal Codice Privacy; Riepilogo sanzioni 2020; tipologie di infrazioni; Alcuni casi reali

Ambito di applicazione materiale

Il Regolamento si applica **unicamente** nel caso di **dati personali riferiti a una persona fisica** (c.d. interessato). Le disposizioni del Regolamento trovano applicazione **sia nell'ambito dei trattamenti automatizzati** (ovvero realizzati con il supporto di strumenti informatici) di dati personali **sia per i trattamenti manuali** di dati personali destinati in un archivio

Ambito di applicazione territoriale

Dal **punto di vista territoriale**, il Regolamento UE si applica ai **soggetti** (Titolare o Responsabile del trattamento che sia) **stabiliti all'interno del territorio dell'UE**, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'UE.

Il Regolamento trova **altresì** applicazione e quindi garantisce la tutela a **tutte le persone fisiche che si trovano all'interno dell'UE – SSE (Fil-Nor-Lic)** destinatarie di:

- offerta di beni o prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento
- attività di monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Il **Regolamento** si applica, quindi, integralmente ai **soggetti**, in qualsiasi parte del mondo siano situati e quindi anche se fuori dall'UE **che offrono servizi o prodotti a persone fisiche situate all'interno dell'UE**

Principali definizioni

- **Dato personale:** ex art. 4, (1) GDPR, 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 ad un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online ovvero uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

- **Trattamento:** ex art. 4, (2) GDPR, qualsiasi operazione ovvero insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati ed applicata a Dati personali o insieme 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

Principali definizioni

- **Titolare del trattamento:** ex art. 4, (7) GDPR la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di Dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri

- **Interessato al trattamento dei dati:** è la persona fisica cui si riferiscono i Dati personali oggetto di trattamento. Più precisamente, l'interessato è una persona fisica identificata o identificabile, che può essere identificata in modo diretto o indiretto facendo riferimento, ad esempio, ad informazioni come: il nome, un numero di identificazione, dati riguardanti l'ubicazione, un identificativo on-line oppure uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

- **Consenso dell'interessato**: ex artt. 4, (11) e 7 GDPR qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i Dati personali che lo riguardano siano oggetto di trattamento

Principali definizioni

- **Responsabile del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio ovvero altro organismo che tratta Dati personali per conto del Titolare, ai sensi dell'art. 28 del Regolamento (UE) 2016/679, previo accordo giuridico o altro atto equivalente

- **Violazione dei dati personali:** ex art. 4, (12) GDPR, la violazione di sicurezza che comporta accidentalmente ovvero in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati personali trasmessi, conservati o comunque trattati

- **Dati particolari:** ex art. 9 GDPR, tutti quei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, i dati biometrici, i dati relativi alla salute e i dati relativi alla vita sessuale o all'orientamento sessuale della persona

- **Dati relativi alla salute:** dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute

- **Dati relativi a condanne penali e reati**: sono dati personali relativi a condanne penali e areati connessi a misure di sicurezza, quali ad esempio casellario giudiziale e carichi pendenti. Tali dati possono essere trattati solamente sotto il controllo della autorità pubblica ovvero previa autorizzazione proveniente da norme dell'Unione Europea e del singolo Stato membro

I soggetti del trattamento

Data Protection Officer

Persona fisica incaricata di fornire consulenza in merito al GDPR, sorvegliarne la corretta applicazione, cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità e gli interessati.

Titolare

Persona fisica, giuridica o altro organismo che, singolarmente o insieme ad altri contitolari, determina le finalità e i mezzi del trattamento di dati personali.

Contitolare

Contitolari del trattamento sono due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento.

Autorizzato al trattamento

Persona fisica che tratta dati personali e dovrà essere istruito a riguardo dal Titolare.

Responsabile del trattamento

Persona fisica, giuridica o altro organismo - esterno rispetto al Titolare - che tratta dati personali per conto del Titolare del trattamento.

Sub-Responsabile del trattamento

Persona fisica, giuridica o altro organismo, individuato dal Responsabile, che tratta dati personali previa autorizzazione scritta da parte del Titolare. È soggetto agli stessi obblighi previsti per il Responsabile.

Contitolari del trattamento

Contitolare del trattamento: Art. 26 paragrafo 1 – «*Allorché due o più titolari del trattamento determinano congiuntamente le **finalità** e i **mezzi del trattamento**, essi sono **contitolari del trattamento**. Tale accordo può designare un punto di contatto per gli interessati*»

Essi **determinano** tale attività **mediante un accordo interno**

Responsabile del trattamento (1 di 3)

Responsabile del trattamento: ai sensi dell'art. 28 paragrafo 1: la persona fisica o giuridica, l'autorità pubblica, il servizio ovvero altro organismo che tratta Dati personali per conto del Titolare, ai sensi dell'art. 28 del Regolamento (UE) 2016/679, previo accordo giuridico o altro atto equivalente.

I Responsabili esterni sono, quindi, coloro i quali **prestano attività ovvero erogano servizi**, da intendersi nella eccezione più ampia, **per il Titolare** che **implicano il trattamento di Dati Personali di quest'ultimo**, regolamentando tale attività per il tramite di rapporti giuridici quali contratti, ordini di servizio e richieste formali. Alcuni esempi di responsabili esterni possono essere:

- studi e società di consulenza,
- commercialisti,
- società di formazione,
- RSPP e consulenti per la sicurezza sul lavoro,
- società IT,
- software house,
- consulenti e società di marketing.

Sub-Responsabile del trattamento

Sub-Responsabile del trattamento: persona giuridica, ditta individuale o libero professionista incaricato dal Responsabile Esterno, per conto del Titolare, di eseguire delle attività che comportano il Trattamento dei Dati Personali, come previsto dall'art. 28, § 2 e 4 GDPR, in qualità di ulteriore responsabile

Il **Responsabile** del trattamento **può ricorrere a un sub-Responsabile solo dopo autorizzazione scritta da parte del Titolare del trattamento**.

NOTA BENE: Il Responsabile del trattamento impone al sub-Responsabile **gli stessi obblighi contenuti nel contratto o in altro atto giuridico tra il Titolare del trattamento e il Responsabile del trattamento**.

Autorizzato al trattamento (1 di 2)

Autorizzato al trattamento: qualsivoglia soggetto (dipendente/collaboratore), incaricati al trattamento dei dati personali sotto l'autorità diretta del Titolare.

Ai sensi **dell'art 2 *quaterdecies* co.1 del Nuovo Codice della Privacy** (dlgs. 196/2003 aggiornato al dlgs. 101/2018): «*Il* ***titolare*** *o il* ***responsabile*** *del trattamento* possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo*, che* ***specifici compiti e funzioni connessi al trattamento di dati personali*** *siano* ***attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità***».

Inoltre, il **Considerando (29) del Regolamento** prevede che il titolare del trattamento **deve indicare le persone autorizzate all'interno della propria realtà**, mentre tra i compiti del Responsabile del trattamento (che può per delega del titolare "istruire" tali persone autorizzate) da definirsi con il "contratto" vi è la previsione che lo stesso "garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza".

Gli autorizzati al trattamento possono essere i dipendenti, i collaboratori, gli agenti, gli stagisti o i tirocinanti dell'azienda titolare del trattamento: sono **persone fisiche che operano sotto l'autorità del titolare** (o responsabile) **che per poter compiere operazioni di trattamento devono essere state a ciò designate** (cioè autorizzate) **e specificamente istruite**.

Principi fondamentali del trattamento ai sensi dell'art. 5 GDPR

ATTENZIONE!

Il Titolare del trattamento è competente per il rispetto di tutti i principi fondamentali e deve essere in grado di provarne il rispetto secondo il c.d. principio di accountability (responsabilizzazione)

I **principi fondamentali** applicabili al trattamento dei dati personali codificati dal Regolamento, da rispettare in ogni aspetto del trattamento dei dati personali, possono così riassumersi:

- **Principio di liceità**, ossia rispetto delle disposizioni normative
- **Principio di correttezza**, ossia garantire che il trattamento avvenga in modo corretto
- **Principio di trasparenza,** ossia assicurare la consapevolezza dell'interessato
- **Principio di limitazione delle finalità**, ossia assicurare gli scopi del trattamento devono essere determinati, espliciti e legittimi
- **Principio di minimizzazione dei dati**, ossia assicurare che il trattamento abbia ad oggetto dati personali adeguati, pertinenti e limitati a quanto necessario per il raggiungimento della specifica finalità di trattamento
- **Principio di esattezza**, ossia garantire che siano predisposte le misure di trattamento adeguate e che i dati siano esatti e aggiornati e ove necessario sia cancellati o rettificati dati inesatti
- **Principio di limitazione della conservazione**, ossia assicurare che i dati siano conservati in modo da consentire l'identificazione dell'interessato solo per il periodo di tempo necessario per il raggiungimento della specifica finalità per cui sono oggetto di trattamento
- **Principio di integrità e riservatezza**, ossia garantire che i dati siano protetti mediante adozione di misure di sicurezza tecniche e organizzative adeguate da trattamenti non autorizzati o illeciti, dalla perdita, distruzione o danno accidentali.

Il «principio di accountability»

Il Regolamento richiama l'applicazione del **principio di accountability** attraverso una serie di adempimenti richiesti al Titolare del trattamento, **tra i quali**:

- **Rispetto dei diritti degli interessati**
- **Privacy by design** -> ossia la privacy è da tenere in considerazione sin dalla fase di progettazione di ogni nuovo progetto, attività, contratto, documento: occorre sempre porsi la domanda: «*Tratterò dei dati personali*
- **Privacy by default ->** ossia privacy come impostazione predefinita
- **Nomina Responsabile del trattamento**
- **Istruzioni agli autorizzati al trattamento**
- **Registro dei trattamenti**
- **Adozione di misure di sicurezza adeguate**
- **Notifica e comunicazione degli eventi di Data Breach**
- **Esecuzione del Data Privacy Impact Assessment (DPIA)**
- **Nomina del Data Protection Officer (DPO)**
- **Trasferimento dei dati in territorio extra-UE**

Il principio di limitazione della conservazione dei dati (tempi / periodi connessi)

In base a quanto previsto dalla **lett. e) del paragrafo 1, dall'art. 5 GDPR**

I dati **possono essere trattati solamente**

- **per il tempo necessario a conseguire o realizzare le finalità per cui sono trattati** e, quindi,
- per il **periodo minimo necessario al conseguimento delle suddette finalità.**

Presupposti di liceità del trattamento

Affinché il **trattamento dei dati personali** possa essere **considerato lecito, deve essere presente una base giuridica** che ne legittimi l'esecuzione

BASI GIURIDICHE DEL TRATTAMENTO

- **Consenso espresso da parte dell'interessato a una o più specifiche finalità di trattamento**
- **Necessità di esecuzione di un contratto o esecuzione di attività precontrattuali**
- **Necessità di adempiere a un obbligo legale cui il Titolare del trattamento è soggetto**
- **Necessità per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica**
- **Necessità di esecuzione di funzioni istituzionali da parte di un'autorità pubblica**
- **Legittimo interesse del Titolare del trattamento**

- **Trattamento dei dati personali strettamente necessari ai fini di prevenzione delle frodi**
- **Trattamento di dati personali nell'ambito di gruppi imprenditoriali, per l'adempimento di finalità amministrative**

Categorie particolari di dati personali

Il **GDPR** definisce, poi, all'**art. 9, paragrafo 1** le «**categorie particolari di dati personali**» (comunemente noti anche come «dati sensibili») come quei «**dati personali che rivelino**»:

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

Dati penali: Ipotesi di trattamento previste dal codice privacy (art. *2octies D.lgs. 196/2003 come modificato ed integrato dal D.lgs. 101/2018*)

- Adempimento di obblighi ed esercizio di diritti da parte del titolare o dell'interessato in **materia di diritto del lavoro** o comunque nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi
- Adempimento degli obblighi previsti **da disposizioni di legge o di regolamento** in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali
- **Verifica o accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti**
- Accertamento di **responsabilità in relazione a sinistri o eventi attinenti alla vita umana**, nonché la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia
- Accertamento, **l'esercizio o la difesa di un diritto in sede giudiziaria**
- **Esercizio del diritto di accesso ai dati e ai documenti amministrativi**, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia

Diritti degli interessati (artt.12-22) - Principi generali

DIRITTI DEGLI INTERESSATI

- Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti
  - Art. 12
- Informativa da fornire qualora i dati personali siano raccolti presso l'interessato
  - Art.13
- Informativa da fornire qualora i dati personali non siano raccolti presso l'interessato
  - Art. 14
- **Diritto di accesso dell'interessato**
  - Art. 15
- **Diritto di rettifica (dei dati personali inesatti)**
  - Art. 16

Diritti degli interessati (artt.12-22) - Principi generali

DIRITTI DEGLI INTERESSATI

- **Diritto alla cancellazione (c.d. diritto all'oblio)**
  - Art. 17
- **Diritto di limitazione del trattamento**
  - Art. 18
- **Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento**
  - Art. 19
- **Diritto alla portabilità dei dati (in un formato strutturato, di uso comune e leggibile da dispositivo automatico)**
  - Art. 20
- **Diritto opposizione al trattamento (dei dati personali, che hanno come base giuridica il legittimo interesse)**
  - Art. 21
- **Diritto a non essere sottoposto a processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione**
  - Art. 22

Informativa da fornire qualora i dati personali siano raccolti presso l'interessato - Art. 13

INFORMATIVA PER DATI PERSONALI RACCOLTI PRESSO GLI INTERESSATI

- Identità e dati di contatto del Titolare del trattamento (di suo eventuale rappresentante) e di eventuale DPO
- Finalità di trattamento cui sono destinati i dati personali
- Destinatari o categorie di destinatari dei dati personali
- L'intenzione del Titolare di effettuare trasferimenti di dati personali verso Paesi terzi od organizzazioni internazionali e, nel caso, l'esistenza o l'assenza di decisioni di adeguante dalla Commissione o il riferimento a garanzie adeguate o opportune o ad altre condizioni di liceità e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili
- Periodi di conservazione dei dati personali o i criteri utilizzati per determinare questo periodo
- I legittimi interessi perseguiti dal Titolare o da terzi, qualora il trattamento dei dati personali sia basato su un legittimo interesse
- L'esistenza dei diritti dell'interessato a poter richiedere al Titolare l'accesso, rettifica, cancellazione o la limitazione del trattamento o l'opposizione al trattamento oltre che il diritto alla portabilità dei dati
- Qualora il trattamento si basi sul consenso, l'esistenza del diritto di poter revocare il consenso in qualsiasi momento senza pregiudizio sulla liceità del trattamento fino a quel momento effettuato
- Il diritto di proporre reclamo all'Autorità Garante
- Se la comunicazione di dati personali è un obbligo legale o contrattuale o precontrattuale, e se l'interessato ha l'obbligo di fornire i dati, nonché le conseguenze della mancata comunicazione di tali dati
- L'esistenza di un processo decisionale automatizzato, compresa la profilazione, e indicazioni della logica utilizzata e delle conseguenze per l'interessato previste da tale tipologia di trattamento

Registro dei trattamenti: principi generali

REGISTRO dei TRATTAMENTI

Documento che contiene la **mappatura di tutte le caratteristiche dei trattamenti dei dati personali effettuati dal Titolare** del trattamento **e** dal **Responsabile** del trattamento

Ha una **funzione descrittiva** e **deve rappresentare la situazione reale** in cui sono eseguite le attività di trattamento e, su richiesta, è messo a disposizione dell'Autorità Garante

Possono essere tenuti in forma scritta, anche in formato elettronico.

La tenuta del Registro è **obbligatoria**

- **per le organizzazioni con più di 250 dipendenti**
- **se i trattamenti effettuati possano presentare un rischio per i diritti e le libertà dell'interessato**
- **i trattamenti effettuati non siano occasionali**
- **se i trattamenti di categorie particolari di o ai dati personali relativi a condanne penali e a reati**

Al di la dell'obbligatorietà la tenuta del Registro dei trattamenti è **un'occasione** per verificare il rispetto dei principi fondamentali, per la liceità del trattamento, per la verifica del rispetto dei principi di *privacy by design* e **privacy di default.**

Il Registro deve essere **regolarmente aggiornato** per dare evidenza del fatto che ciascun trattamento dati è indicato ed analizzato all'interno del Registro stesso.

Data Breach

Violazione di Dati personali o «Data Breach»: ex art. 4, (12) GDPR, la violazione di sicurezza che comporta accidentalmente ovvero in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati personali trasmessi, conservati o comunque trattati.

Quando si parla di «**Violazione dei Dati personali**» (art. 4, par. 12 GDPR) occorre considerare:

- **natura della violazione**:
  - accidentale o volontario;
  - illecita;
- **conseguenza sui dati:**
  - distruzione;
  - perdita;
  - modifica;
  - divulgazione non autorizzata;
  - accesso ai dati da parte di soggetti non autorizzati;
- **conseguenze sugli interessati**:
  - danni morali o immateriali;
  - perdita del controllo dei dati e conseguenti perdite economiche;
  - discriminazioni;
  - furto d'identità e frode;
  - danno reputazionale;
  - ulteriori conseguenze negative.

Data Breach

In caso di Data Breach
il Titolare dovrà valutare

- la **natura** e **l'entità** della potenziale violazione/ violazione dei Dati personali;
- **l'impatto** della violazione dati dei Dati personali;
- le **misure da adottare** per **arginare** gli effetti dannosi della violazione medesima;
- la **necessità di notifica al Garante**;
- la **necessità della notifica agli interessati**.

Data Breach

CONTENUTO MINIMO DELLA COMUNICAZIONE AGLI INTERESSATI

- **dati di contatto cui rivolgersi per avere più informazioni**
- **descrizione possibili conseguenze**
- **descrizione delle contromisure adottate/che si intende adottare**

Non è richiesta la comunicazione all'interessato in presenza di una delle seguenti condizioni:

- **il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai Dati personali oggetto della violazione**, in particolare quelle destinate a rendere i Dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- **il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato** per i diritti e le libertà degli interessati;
- **detta comunicazione richiederebbe sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Data Protection Impact Assessment (DPIA) - Principi generali

In caso di **trattamenti** che, alla luce dell'**uso di nuove tecnologie, della natura, dell'oggetto, del contesto e delle finalità del trattamento**, possono presentare **rischi elevati per i diritti e le libertà delle persone fisiche**, il **Titolare** del trattamento, **prima di procedere al trattamento**, **deve effettuare** una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. In particolare, il **paragrafo 3 dell'art. 35** del GDPR individua **tre ipotesi esplicite e specifiche**, che richiederebbero lo svolgimento di una DPIA.

- **in caso di valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche**
- **nei trattamenti su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali e a reati**
- **in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico.**

L'**Autorità Garante**, nel **provvedimento n. 467 dell'11 ottobre 2018**, ha redatto un **ulteriore elenco** delle tipologie di trattamenti soggetti al requisito del Privacy Impact Assessment*.

Ulteriori casistiche sono individuate dal **WP29, oggi EDPB** - Comitato Europeo per la protezione dei dati - nelle linee guida WP248 del 2017.
*

Data Protection Impact Assessment
Alcuni esempi di trattamenti che richiedono o meno una DPIA (secondo il WP29)

Esempi di trattamento	Criteri pertinenti	DPIA
Ospedale che tratta dati genetici e sanitari relativi ai pazienti (sistema informativo ospedaliero)	▪Dati sensibili o dati di natura estremamente personale ▪Dati relativi a interessati vulnerabili ▪Dati trattati su larga scala	▪**SI**
Utilizzo di un sistema di videosorveglianza per il controllo del traffico autostradale. Il Titolare prevede di utilizzare un sistema intelligente di analisi delle immagini per l'individuazione dei veicoli e il riconoscimento automatico delle targhe	▪Monitoraggio sistematico ▪Utilizzi innovativi o applicazione di soluzioni tecnologiche o organizzative	▪**SI**
Azienda che controlla sistematicamente le attività dei dipendenti, compreso l'utilizzo dei terminali informatici, la navigazione su Internet, ecc	▪Monitoraggio sistematico ▪Dati relativi a interessati vulnerabili	▪**SI**
Un'istituzione che crei un database nazionale di valutazioni creditizie o per finalità antifrode	▪Valutazione o scoring ▪Decisioni automatizzate che producono effetti giuridici o incidono in misura significativa sull'interessato ▪Impedimenti all'esercizio di un diritto o all'utilizzo di un servizio o di un contratto da parte dell'interessato ▪Dati sensibili o dati di natura estremamente personale	▪**SI**
Trattamento di «dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato"	▪Dati sensibili o dati di natura estremamente personale ▪Dati relativi a interessati vulnerabili	▪**NO**

Data Protection Officer

Il **Data Protection Officer, noto anche come «Responsabile della Protezione dei Dati Personali»** è una figura prevista dal Regolamento e che può essere riportata e rileva nell'ambito del c.d. Organigramma Privacy.

Il GDPR prevede che il Titolare del trattamento e il Responsabile del trattamento **debbano designare** un Data Protection Officer quando:

- **il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali**
- **le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;**
- **le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati.**

La **nomina del Data Protection Officer** però

- può essere può essere prevista anche in casi ulteriori in base alla legge nazionale o al diritto dell'UE o
- può essere effettuata anche su base volontaria.

Trasferimento dei dati extra UE-SEE

Trasferimenti sulla base di una decisione di adeguatezza (art. 45) o di garanzie adeguate (art. 46)

Casistiche di trasferimento extra UE-SEE ammesse – DECISIONE DI ADEGUATEZZA E GARANZIE (1)

- **Decisioni di adeguatezza** della Commissioni UE (Andorra, Argentina, Australia solo per alcune limitatissime ipotesi, Canada, Faer Oer, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera, Uruguay, Giappone)*.

Relativamente ai Paesi che non sono compresi o dovessero essere eliminati dall'elenco sopra riportato*, il trasferimento di dati fuori dal SEE è ammesso solo nei seguenti casi sotto riportati.

- **Clausole contrattuali standard (SCC)** adottate dalla Commissione UE, integrate, se necessario con le misure supplementari suggerite dall'EDPB (Comitato Europeo per la Protezione dei Dati)
- **BCR** (**Binding Corporate Rules** o **Norme Vincolanti di Impresa**), approvate dall'autorità di controllo competente (ad esempio il Garante Privacy), ovvero un accordo contenente una serie di clausole che fissano i principi vincolanti per il trattamento dei dati personali a cui sono tenute tutte le società appartenenti ad uno stesso gruppo, integrate, se necessario con le misure supplementari suggerite dall'EDPB
- Adozione di **codici di condotta** o **meccanismi di certificazione**, approvati secondo le norme del GDPR, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel Paese terzo ad applicare le garanzie adeguate, integrati, se necessario con le misure supplementari suggerite dall'EDPB.

***NOTA BENE**: l'elenco dei Paesi adeguati è costantemente aggiornato dalla Commissione UE in caso di variazioni (sia con l'inserimento di ulteriori nuovi Paesi, sia con riferimento alla cancellazione dei Paesi che non assicurassero più adeguate garanzie) ed è disponibile al seguente indirizzo internet *https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en*

Trasferimento dei dati extra UE-SEE (4 di 6)

Trasferimenti in virtù di deroghe per situazioni specifiche (art. 49)

Casistiche di trasferimento extra UE-SEE ammesse dal GDPR - DEROGHE

In assenza di una decisione di adeguatezza ai sensi dell'articolo 45, **o di appropriate garanzie ai sensi dell'articolo 46**, comprese le BCR (disciplinate anche dall'art. 47), un trasferimento o una serie di **trasferimenti** dati verso Paesi terzi o un'organizzazione internazionale **deve essere effettuato nel rispetto di una delle seguenti condizioni**.

- ❑ L'interessato ha dato il **proprio consenso**, dopo essere stato informato dei possibili rischi derivanti dalla mancanza di una decisione di adeguatezza e di garanzie adeguate
- ❑ Il trasferimento è **necessario all'esecuzione di un contratto** concluso **tra l'interessato e il titolare** del trattamento ovvero **all'esecuzione di misure precontrattuali** adottate **su istanza dell'interessato**
- ❑ Il trasferimento è necessario per la **conclusione o l'esecuzione di un contratto** stipulato **tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato**
- ❑ Il trasferimento è **necessario per importanti motivi di interesse pubblico**
- ❑ Il trasferimento è **necessario per accertare, esercitare o difendere un diritto in sede giudiziaria**
- ❑ Il trasferimento è **necessario per tutelare gli interessi vitali dell'interessato o di altre persone**, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso
- ❑ Il trasferimento sia **effettuato a partire da un registro** che, a norma del diritto dell'Unione o degli Stati membri**, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse**, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.

SANZIONI AMMINISTRATIVE previste dal GDPR

Il **Regolamento** ha introdotto un **profondo cambiamento** nel sistema sanzionatorio: oggi caratterizzato da un notevole aumento del massimo edittale. In particolare, la **recente normativa** prevede **due livelli di sanzioni**:

Fino a ***€ 10.000.000*** o (per le imprese) fino al ***2%*** del fatturato mondiale totale annuo dell'esercizio precedente, se superiore

Articolo 83, paragrafo 4 GDPR

Fino a ***€ 20.000.000*** o (per le imprese) fino al ***4%*** del fatturato mondiale totale annuo dell'esercizio precedente, se superiore

Articolo 83, paragrafi 5 e 6 GDPR

SANZIONI PENALI previste dal CODICE PRIVACY
Cosa prevede la norma (1 di 6)

Il **Codice Privacy italiano**
(D.Lgs. 196/2003 come integrato e modificato dal D.lgs 101/2018)

Art. 167 - *Trattamento illecito di dati*

Sanziona il **trattamento** di dati personali **non conforme alla Normativa Privacy** vigente in tema di

- dati relativi al **traffico su internet**,
- dati relativi all'**ubicazione geografica dell'interessato** (diversi da quelli desumibili dalla navigazione),
- di **comunicazioni commerciali e per finalità di marketing** (effettuate tramite emai e altri mezzi di comunicazione elettronica),
- di **dati particolari trattati per motivi di interesse pubblico**
- di **dati penali**, anche in considerazione dell'eventuale inosservanza delle specifiche disposizioni del Codice Privacy,
- in tema di **trasferimenti di dati personali in paesi extra UE-SEE**.

SANZIONI PENALI previste dal CODICE PRIVACY - Cosa prevede la norma (2 di 6)

Il **Codice Privacy italiano**
(D.Lgs. 196/2003 come integrato e modificato dal D.lgs 101/2018)

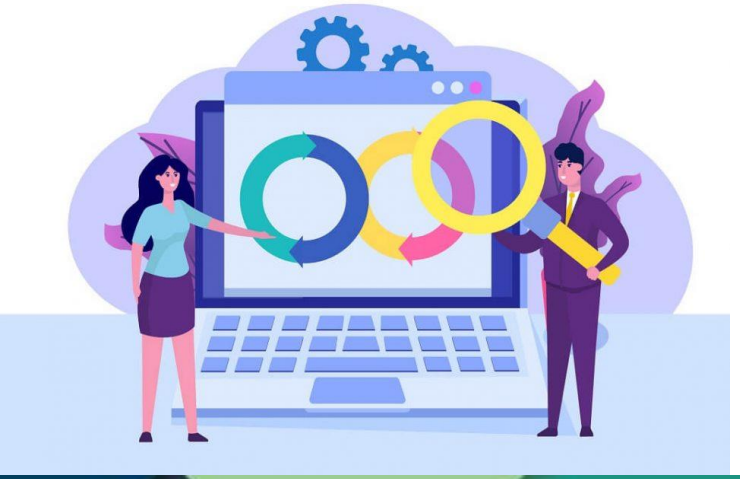
Art. 167 bis - *Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala*

Sanziona chiunque comunica o diffonde, al fine di trarre profitto per sé o per altri ovvero al fine di arrecare danno, **un archivio automatizzato o una parte sostanziale di esso** contenente dati personali oggetto di trattamento **su larga scala senza consenso dell'interessato** (qualora il consenso sia richiesto) **oppure in violazione delle disposizioni** del Codice Privacy in tema di dati particolari trattati per motivi di interesse pubblico e in tema di dati penali.

SANZIONI PENALI previste dal CODICE PRIVACY - Cosa prevede la norma (3 di 6)

Il **Codice Privacy italiano**
(D.Lgs. 196/2003 come integrato e modificato dal D.lgs 101/2018)

Art. 167 ter - *Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala*



Sanziona chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, **acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso** contenente dati personali oggetto di trattamento su larga scala.

SANZIONI PENALI previste dal CODICE PRIVACY - Cosa prevede la norma (4 di 6)

Il **Codice Privacy italiano**
(D.Lgs. 196/2003 come integrato e modificato dal D.lgs 101/2018)

Art. 168 - *Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante*

Sanziona chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, **dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi**, oppure **intenzionalmente cagiona** un'**interruzione** o **turba la regolarità** di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.

SANZIONI PENALI previste dal CODICE PRIVACY - Cosa prevede la norma (5 di 6)

Il **Codice Privacy italiano**
(D.Lgs. 196/2003 come integrato e modificato dal D.lgs 101/2018)

Art. 170 - *Inosservanza dei provvedimenti del Garante*

Sanziona chiunque, essendovi tenuto, **non osserva il provvedimento generale** relativo al **trattamento di categorie particolari** di dati e i **provvedimenti speciali**, che prevedano la limitazione provvisoria o definitiva di trattamenti di dati, **adottati dal Garante**.

SANZIONI PENALI previste dal CODICE PRIVACY - Cosa prevede la norma (6 di 6)

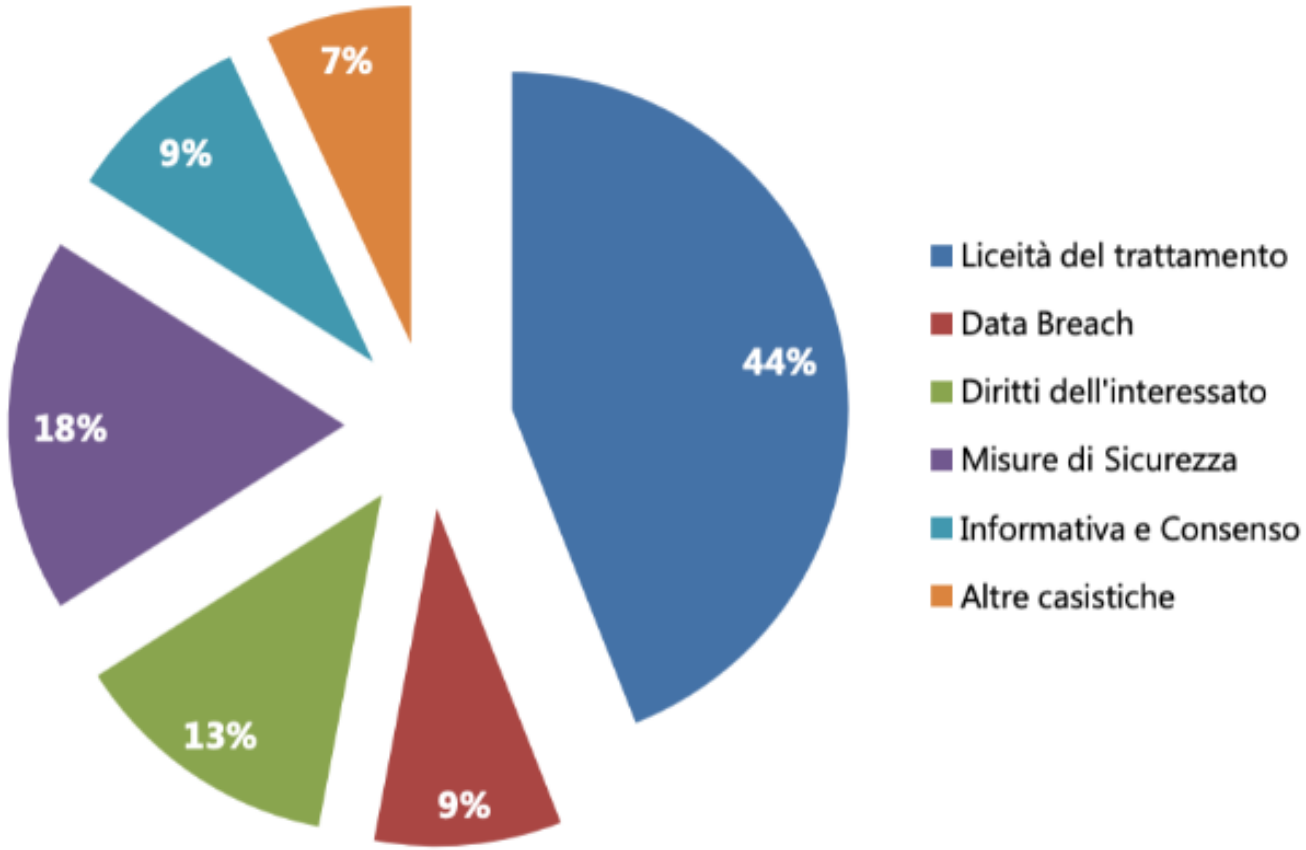
Il **Codice Privacy italiano**
(D.Lgs. 196/2003 come integrato e modificato dal D.lgs 101/2018)

Art. 171 - *Violazione delle disposizioni in materia di controllo a distanza e indagini sulle opinioni dei lavoratori*

Sanziona chi **violi le disposizioni in materia di controllo a distanza previste dall'art. 4 Statuto dei Lavoratori** (a mero titolo esemplificativo e non esaustivo, l'installazione di impianti di videosorveglianza in assenza di previo accordo sindacale oppure di autorizzazione amministrativa da parte dell'Ispettorato del Lavoro).

Sanzioni in ambito GDPR: tipologie di infrazioni principali

fig .8 – Tipologie di infrazione



(fonte: Grafico elaborato da Federprivacy)

SANZIONI in ambito GDPR - Alcuni casi reali

Garante Privacy
Provvedimento nei confronti di TIM S.p.A.
(n. 7 del 15 gennaio 2020)

Il **Garante** Privacy ha irrogato una **sanzione di € 27.802.946** euro a TIM S.p.A. per **numerosi trattamenti illeciti** di dati legati all'**attività di marketing** del provider di telecomunicazione (tra cui contatti avvenuti in assenza di consenso da parte degli interessati).

A seguito di numerose segnalazioni da parte degli utenti, il Garante avviava un'attività istruttoria lunga e complessa che si è avvalsa del contributo del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza.
Al termine sono emerse numerose e gravi violazioni della disciplina in materia di protezione dei dati personali che hanno interessato nel complesso **alcuni milioni di persone**.

Il Garante ha **numerosi comportamenti in violazione dei principi imposti** dalla normativa vigente e, per tale ragione ha ritenuto di applicare una **sanzione amministrativa pari allo 0,2% del fatturato** corrispondente a €27.802.946.

SANZIONI in ambito GDPR - Alcuni casi reali

Garante Privacy
Provvedimento nei confronti di Facebook Ireland Ltd e Facebook Italy s.r.l.
(n. 134 del 14 giugno 2019)

Il **Garante** per la protezione dei dati personali ha applicato a Facebook una sanzione di **€ 1 milione** per gli **illeciti compiuti** nell'ambito del caso "Cambridge Analytica" (la società che attraverso un app per test psicologici aveva avuto accesso ai dati di 87 milioni di utenti e li aveva usati per tentare di influenzare le presidenziali americane del 2016).

La sanzione, comminata sulla base del vecchio Codice Privacy, fa seguito ad un precedente Provvedimento del Garante (del gennaio 2019) con il quale l'Autorità aveva vietato a Facebook di continuare a trattare i dati degli utenti italiani.

Il Garante aveva infatti accertato che 57 italiani avevano scaricato l'app Thisisyourdigitallife attraverso la funzione Facebook login e che, in base alla possibilità consentita da questa funzione di condividere i dati degli "amici", **l'applicazione aveva poi acquisito i dati di ulteriori 214.077 utenti italiani**, **senza che questi l'avessero scaricata, fossero stati informati della cessione dei loro dati e avessero espresso il proprio consenso a questa cessione**.
La **comunicazione** da parte di FB dei dati alla app Thisisyourdigitallife era dunque **avvenuta in maniera non conforme alla normativa sulla privacy**.

I dati non erano comunque stati trasmessi a Cambridge Analytica.

Avv. Matteo Alessandro Pagani

PLS SRL

Via Turati 26 – 2021 Milano

Via Corsica 10 – 25125 Brescia

MILANO
LODI
MONZA BRIANZA

F.I.M.A.A.

COLLEGIO AGENTI D'AFFARI IN MEDIAZIONE DI MILANO, LODI, MONZA BRIANZA E PROVINCE DAL 1945