Progetto «PartecipAzione»

La gestione della privacy

16 ottobre 2024

Building a better working world

Obiettivi dell'incontro

La presente sessione di formazione mira a richiamare gli **aspetti chiave** della normativa contenuta nel Regolamento UE 2016/679 (GDPR) e nel d.lgs. 196/2003 ss.mm.ii. (Codice Privacy).

In particolare andremo a vedere:

- cosa sono i dati personali;
- quali sono i soggetti a cui sono attribuiti dei compiti dalla normativa;
- quali sono i principali adempimenti richiesti.

Il Regolamento UE 2016/679 («GDPR»)

EU General Data Protection Regulation

- Efficace dal **25 maggio 2018**.
- A differenza di una direttiva comunitaria, il Regolamento è **direttamente applicabile** negli Stati membri e non richiede alcuna normativa di recepimento.
- Resta salva la normativa nazionale che non contrasta con i principi del Regolamento. A tal proposito il **d.lgs. 101/2018** ha novellato il «Codice della Privacy» ovvero il **d.lgs. 196/2003** armonizzandolo con le disposizioni previste dal Regolamento.

Il GDPR in numeri:

173 considerando	99 articoli	112 pagine

Il GDPR stabilisce norme volte a garantire da un lato la protezione delle persone fisiche con riguardo al trattamento dei loro dati personali, dall'altro norme relative alla libera circolazione di tali dati.

Cosa si intende per trattamento di dato personale?

Cos'è un **trattamento di dati personali?** Una 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.

Dato personale

«Qualsiasi informazione riguardante una persona fisica **identificata** o **identificabile** (Interessato)»

Categorie particolari di dati personali (art.9 GDPR)

«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».

Dati relativi a condanne penali o reati e misure di sicurezza (art. 10 GDPR)

Il GDPR **si applica** ai trattamenti:

- effettuati da titolari o responsabili del trattamento stabiliti in un Paese UE
- di dati personali di interessati che si trovano nell'Unione effettuati da titolari non stabiliti nell'Unione
- di dati personali effettuati da un titolare che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico

Il GDPR **non si applica** ai trattamenti:

- di dati riferibili a persone giuridiche
- di dati anonimi
- di dati per scopi esclusivamente personali

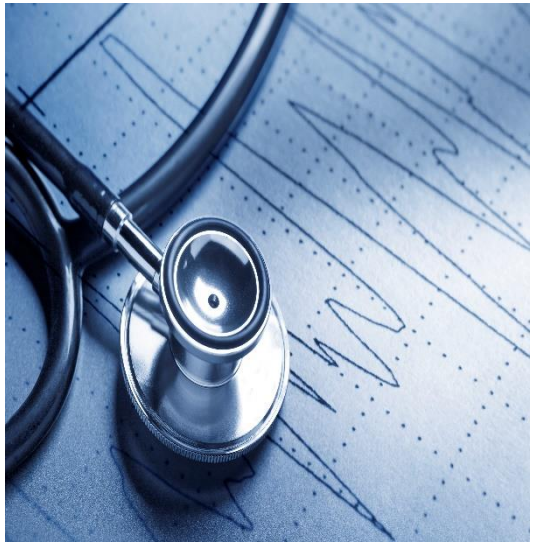
Focus: dati particolari art. 9 del GDPR

Dati genetici

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

Dati 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 biometrici

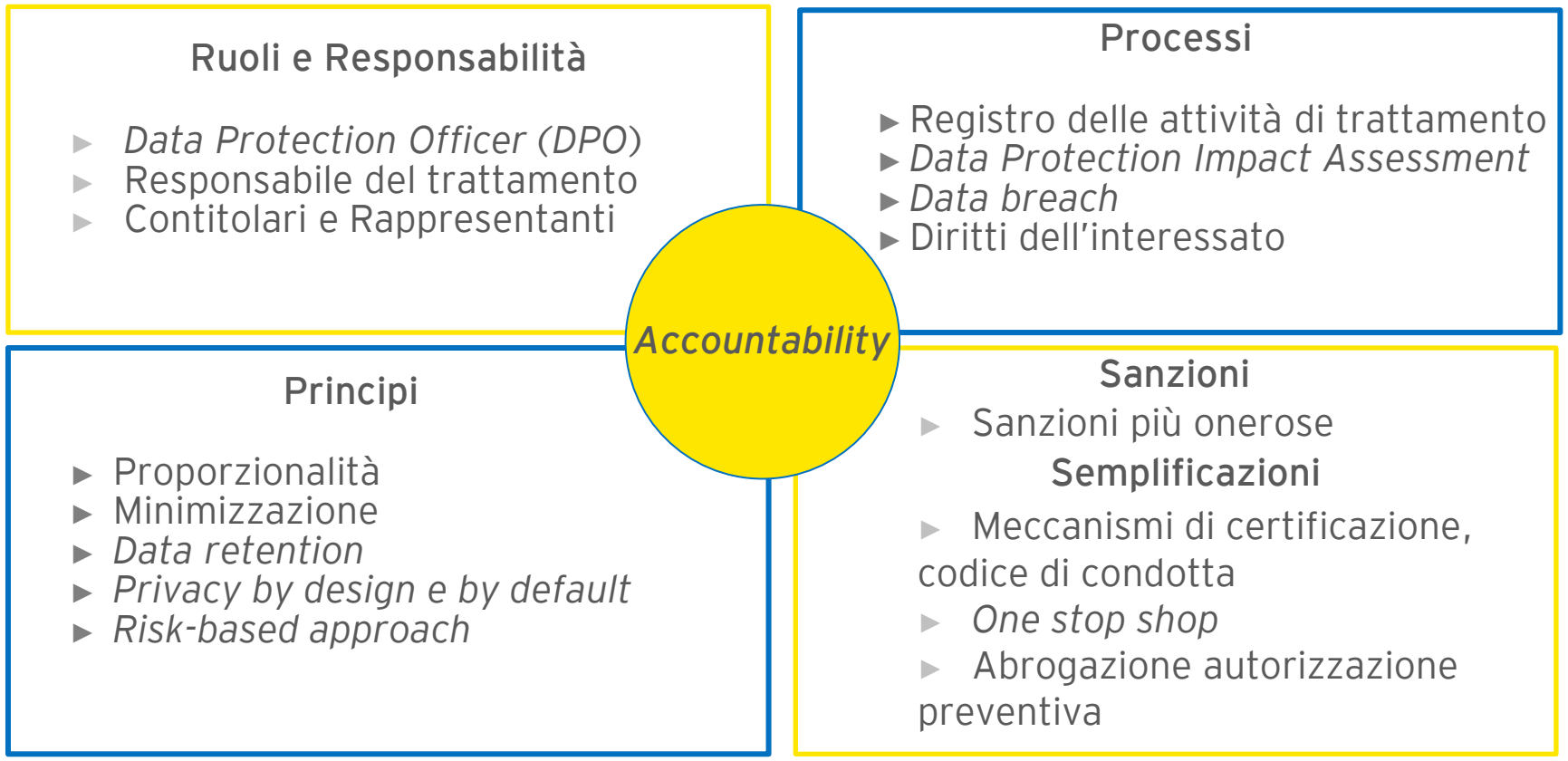
Dati personali ottenuti da un **trattamento tecnico specifico** relativi alle **caratteristiche fisiche, fisiologiche o comportamentali** di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Altre tipologie di dati particolari

Dati relativi ad **opinioni politiche, fede religiosa** o **orgine etnica**. Ad esempio, vi rientrano i dati che esprimono l'appartenenza sindacale o il credo.

L'approccio del GDPR

Il GDPR pone l'accento sulla tutela dei diritti dell'interessato ed introduce diversi nuovi aspetti. Fulcro centrale è rappresentato dal **principio di *accountability*** (ovvero di «responsabilizzazione»).



Ruoli e responsabilità: i principali attori

Titolare del trattamento

- È il soggetto (persona fisica o giuridica) che determina le **finalità e i mezzi** del trattamento.
- Nomina il ***Data Protection Officer,*** ove necessario**.**
- Agevola l'esercizio dei **diritti da parte degli interessati**
- **Adotta misure tecniche e organizzative** adeguate.
- Notifica i ***data breach*.**
- Valuta e gestisce i **rischi** associati al trattamento dei dati.

Responsabile del trattamento

- È l'entità legale che tratta dati personali **per conto** del titolare del trattamento.
- I trattamenti del responsabile sono disciplinati da un contratto/altro atto giuridico **(DPA)** ex art. 28 del GDPR.
- È responsabile dell'**attuazione delle istruzioni** fornite dal Titolare (incluse le misure di sicurezza).
- Non ricorre ad **altro responsabile** senza previa autorizzazione del Titolare.

Data Protection Officer

- Può o deve essere nominato dal Titolare del trattamento
- Rispetta il requisito dell'indipendenza e dell'assenza di conflitti di interessi.
- Coopera con l'Autorità di controllo e funge da punto di contatto.
- Ha un ruolo di indirizzo e controllo e fornisce ***consulenza*** al titolare riportando al suo vertice gerarchico.
- Sorveglia l'osservanza del GDPR e contribuisce alla consapevolezza aziendale nelle tematiche privacy.

Autorizzato al trattamento

- È la **persona fisica** che effettua materialmente le operazioni di trattamento sui dati personali all'interno dell'azienda.
- Può operare alle **dipendenze** del titolare e/o del responsabile.
- È necessario che riceva le **istruzioni operative**, compreso di obblighi inerenti le misure di sicurezza e la formazione.

I principi essenziali della normativa privacy

Accountability

Il GDPR prevede che il Titolare del trattamento metta in atto misure tecniche e organizzative **adeguate** per garantire ed **essere in grado di dimostrare** che le operazioni di trattamento siano conformi al Regolamento stesso.

Privacy by design e by default

Il GDPR disciplina l'obbligo di assicurare che le misure adottate attuino efficacemente i **principi di *privacy by design*** (protezione dei dati fin dalla progettazione) e ***privacy by default*** (impostazione predefinita che prevede il trattamento dei soli dati necessari al perseguimento delle finalità).

Proporzionalità

Deve essere rispettato il principio di **proporzionalità**: i dati devono essere adeguati, pertinenti e **limitati a quanto necessario rispetto alle finalità** per le quali sono trattati.

Risk-based approach

Il GDPR prevede un **approccio *risk-based***.

È definita la necessità di effettuare un ***Data Protection Impact Assessment***, ovvero una valutazione dei rischi per i trattamenti previsti.

L'implementazione delle misure di sicurezza adottate terrà conto dell'analisi dei rischi e dei **costi** di attuazione. Il GDPR indica, a titolo esemplificativo e non esaustivo, quali misure di sicurezza sono appropriate per ridurre i rischi: la **pseudonimizzazione**, la crittografia, la **resilienza dei sistemi**.

La liceità del trattamento: le basi giurdiche del trattamento

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni (c.d. basi giuridiche).

1. L'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità.
2. Il trattamento è necessario all'**esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.
3. Il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento.
4. Il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento.
5. Il trattamento è necessario per l'esecuzione di un compito di **interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
6. Il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato.

Attenzione particolare è dovuta nell'individuazione della base giuridica rispetto al trattamento di **categorie particolari** di dati (art. 9 del GDPR) e dei **dati relativi a condanne penali e reati e misure di sicurezza** (art. 10 del GDPR).

Focus: base giuridica il consenso art. 7 del GDPR

Ogni trattamento deve trovare fondamento in **un'idonea base giuridica**: il consenso costituisce uno dei **fondamenti di liceità** del trattamento

Cosa cambia

- La **forma scritta** è la modalità idonea a configurare **l'inequivocabilità del consenso**.
- Il consenso **deve essere esplicito**:
  - per le categorie particolari di dati personali (art. 9 GDPR);
  - per le decisioni basate su trattamenti automatizzati, compresa la profilazione (art. 22 GDPR).
- Negli altri casi, **non deve essere necessariamente** documentato per iscritto, né è richiesta la forma scritta.
- Il consenso dei **minori** è valido **a partire dai 16 anni**; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Cosa non cambia

- Il consenso deve essere, in tutti i casi, **libero, specifico, informato e inequivocabile**.
- Non è ammesso il consenso tacito o presunto (es. caselle prespuntate in un modulo).
- Il consenso deve essere manifestato attraverso **«dichiarazione o azione positiva inequivocabile».**

Obblighi di informativa artt. 13 e 14 del GDPR

Caratteristiche dell'informativa

- **Concisa**, **trasparente**, **intellegibile** per l'interessato e **facilmente accessibile.**
- Linguaggio **chiaro** e **semplice** (per i minori deve essere predisposta informativa idonea).
- In linea di principio, fornita per **iscritto.**
- E' ammesso l'utilizzo di **icone** predisposte dalla Commissione Europea ma solo se «in combinazione» con l'informativa estesa.

Tempistiche

Se i dati personali sono raccolti presso l'interessato (art. 13 del GDPR), l'informativa va fornita **contestualmente** all'ottenimento dei dati personali che lo riguardano.

Se i dati personali sono raccolti presso altre fonti (art. 14 del GDPR), l'informativa va:

- entro un **termine ragionevole** dall'ottenimento dei dati personali (massimo entro un mese);
- nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento del **primo contatto** con l'interessato;
- se prevista la comunicazione ad altro destinatario, **non oltre la prima comunicazione** dei dati personali.

Principali informazioni da rendere all'interessato

- l'identità e i dati di contatto del titolare del trattamento;
- i dati di contatto del responsabile della protezione dei dati;
- le finalità del trattamento, nonché la base giuridica del trattamento;
- l'eventuale legittimo interesse qualora sia questa la base giuridica individuata;
- gli eventuali destinatari o le categorie di destinatari;
- l'intenzione di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e le misure garanzie appropriate;
- il periodo di conservazione dei dati personali;
- l'esistenza dei diritti incluso il diritto di revocare il consenso eventualmente prestato e di proporre reclamo a un'autorità di controllo;
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se il conferimento è obbligatorio le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione con informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

I diritti dell'interessato artt. 15 e ss. del GDPR 1/2

Diritto di accesso

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali.

Diritto di rettifica

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.

Diritto di limitazione al trattamento

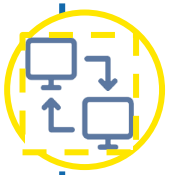
L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento (ad esempio, nei casi di trattamento illecito o quando i dati personali siano necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria).

Diritto all'oblio

Il Titolare del trattamento deve garantire all'interessato la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo (Right to be forgotten).

Diritto di opposizione

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni.



Diritto alla portabilità dei dati

L'interessato ha il diritto di

- ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti ad un Titolare;
- trasmettere tali dati ad un altro Titolare senza impedimenti da parte del Titolare al quale li aveva forniti.

I diritti dell'interessato artt. 15 e ss. del GDPR 2/2

Quali sono i principali step della gestione delle **richieste di esercizio dei diritti degli interessati ex artt. 15 – 22 del GDPR?**

Il termine per fornire riscontro all'interessato **è pari ad un mese**, periodo questo estendibile **fino a tre mesi** in casi di particolare complessità. Il titolare è tenuto a fornire un riscontro anche in caso di diniego.

La violazione dei dati personali (*data breach) 1/2*

Un ***data breach*** è una **violazione di sicurezza** che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. La violazione non attiene solo i trattamenti effettuati in modalità digitale ma può concretizzarsi anche in trattamenti che avvengono con modalità cartacee.

Art. 33

Obbligo del titolare di:

(i) notifica e comunicazione del titolare all'Autorità di controllo della violazione senza ingiustificato ritardo e, ove possibile, **entro 72 ore** dal momento in cui ne è venuto a conoscenza;

(ii) documentare le violazioni di dati personali subite, anche se non notificate all'Autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati.

Art. 34

Quando la violazione dei dati personali è suscettibile di presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento **comunica la violazione all'interessato** senza ingiustificato ritardo.

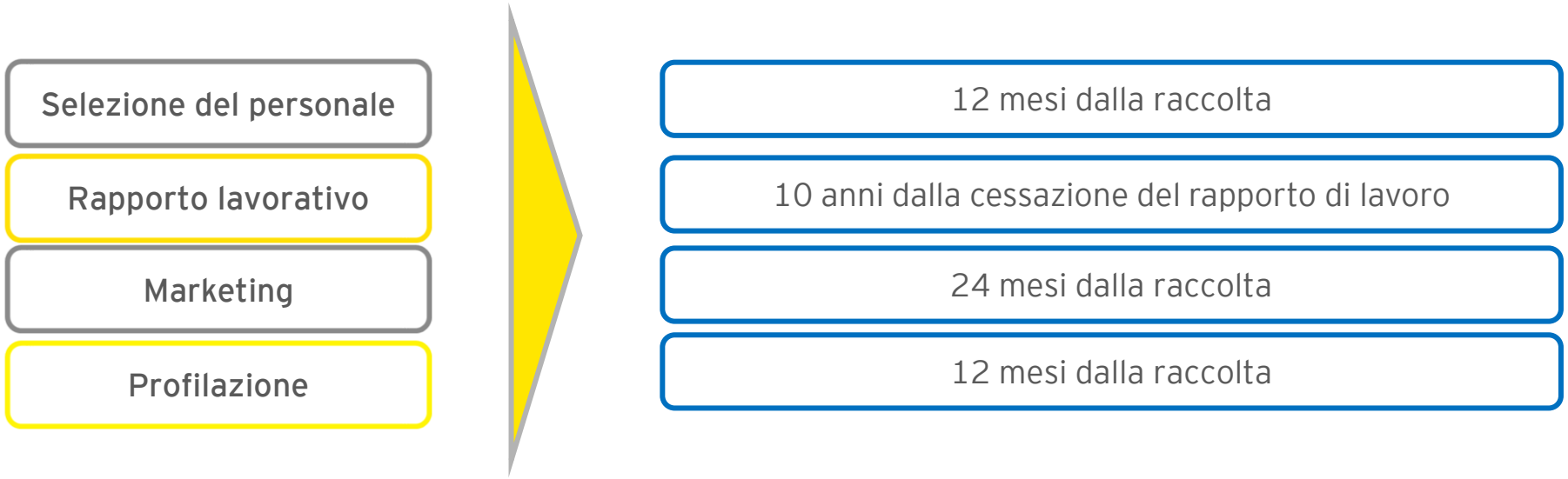
La violazione dei dati personali (*data breach) 2/2*

Quali sono i principali step di una sospetta violazione di dati personali?

L'incidente di sicurezza può riguardare non solo un trattamento che avviene in modalità informatica, ma anche in modalità cartacea.

La data retention

Il titolare deve assicurare che i dati personali siano trattati per un determinato periodo di tempo per poi essere cancellati o anonimizzati.
Di seguito alcuni esempi:



I principi di *privacy by design e by default*

La pianificazione di una nuova iniziativa, sin dalla sua progettazione, deve porre al centro la persona, ed essere quindi ideata secondo un approccio "*privacy oriented*", volto a valutare se ciò che si sta progettando avrà un impatto sui dati personali.

Art. 25 del GDPR

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento [...] il titolare del trattamento mette in ***atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione****, volte ad attuare in modo efficace i principi di protezione dei dati, quali la* ***minimizzazione****, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati,* ***per impostazione predefinita,*** *solo i* ***dati personali necessari*** *per ogni specifica finalità del trattamento.*

I titolari e i responsabili del trattamento devono:

- tenere in considerazione, sin dalla **ideazione e progettazione** delle attività di trattamento (che intende porre in essere), **la protezione della riservatezza dei dati personali degli interessati** cui il trattamento si riferisce. Pertanto, ogni progetto ad impatto privacy deve nascere ed essere costruito nel **rispetto della disciplina di protezione dei dati personali** (*by design*);
- effettuare il trattamento dei soli dati personali degli interessati **nella misura e per il tempo necessari a raggiungere le finalità del trattamento**, implementando le **misure tecniche adeguate a proteggere i dati personali degli interessati** (*by default*).

La Data Protection Impact Assessment

La **DPIA (art. 35 GDPR)** consiste in una procedura finalizzata a valutare il rischio del trattamento rispetto ai diritti e le libertà degli interessati. La DPIA è uno strumento che aiuta il titolare non soltanto a rispettare le prescrizioni del GDPR, ma anche a dimostrare l'adozione di misure idonee a garantire il rispetto di tali prescrizioni.

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

*2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il **responsabile della protezione dei dati**, qualora ne sia designato uno.*

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

*a) una **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;*

*b) il trattamento, su **larga scala**, di categorie particolari di dati personali di cui all'articolo9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo10; o*

*c) la **sorveglianza sistematica** su larga scala di una zona accessibile al pubblico».*

Il Registro delle attività di trattamento

Il **registro delle attività di trattamento (art. 30 del GDPR)** costituisce il censimento dei trattamenti di dati personali effettuati da un soggetto sia in qualità di titolare sia in qualità di responsabile qualora tratti i dati per conto di altri titolari del trattamento.

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta dell'Autorità di controllo.

Il registro dei trattamenti di un **titolare** richiede informazioni in merito:

- il nome e i dati di contatto del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- la descrizione generale delle misure di sicurezza tecniche e organizzative.

Il registro dei trattamenti di un **responsabile** richiede informazioni in merito:

- il nome e i dati di contatto del responsabile o dei responsabili del trattamento, e del responsabile della protezione dei dati;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Il Registro delle attività di trattamento

Registro del trattamento lato titolare

Descrizione del trattamento

Esempio

- Finalità del trattamento
- Operazioni di trattamento
- Categorie di interessati
- Categorie dati personali

Comunicazione

- Destinatari dei dati o categorie di destinatari

Trasferimento dei dati verso paesi extra UE

- Paese terzo
- Misura di garanzia o decisione di adeguatezza

Periodo di conservazione

- Termini ultimi per la cancellazione dei dati

Titolare del trattamento

- Titolare del Trattamento
- Dati di contatto del Titolare
- Contitolarità del Trattamento
- Data Protection Officer

Responsabile del trattamento

- Responsabile del trattamento

Misure di sicurezza

- Misure tecniche
- Misure organizzative
- Sistema informatico
- Archivio cartaceo

Il registro lato responsabile ha una struttura più semplice e riporta i diversi trattamenti effettuati per conto di altri titolari.

Inoltre per le aziende con determinate caratteristiche (es. meno di 250 dipendenti) lo stesso ha una struttura più semplice

La gestione dei fornitori che trattano dati personali per conto del titolare

Il *Data Processing Agreement* (DPA) - disciplinato dall'articolo 28 del GDPR - è un accordo scritto tra il **titolare** del trattamento dei dati e il **responsabile del trattamento** dei dati che stabilisce le obbligazioni e le responsabilità tra le parti rispetto al trattamento dei dati personali oggetto di affidamento.

Cosa deve prevedere un DPA?

1. Materia disciplinata, durata del trattamento, finalità il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.
2. Istruzioni anche in tema di trasferimenti verso paesi terzi
3. Obbligo di riservatezza in capo alle persone autorizzate
4. Autorizzazione (specifica o generale) alla nomina di altri responsabili
5. Misure tecniche e organizzative richieste ai sensi dell'art. 32 del GDPR
6. Cancellazione/Restituzione dei dati
7. Assistenza in caso di esercizio dei diritti, data breach, valutazione d'impatto privacy e ispezioni.

Misure di sicurezza di tipo tecnico ed organizzativo

E' obbligo del titolare e del responsabile del trattamento mettere in atto **misure di sicurezza tecniche ed organizzative adeguate** per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'art. 32 del GDPR.

Minacce

- Violazione, perdita e distruzione dei dati
- Trattamento non conforme alle finalità dichiarate
- Furti d'identità
- Modifica non autorizzata dei dati
- Condivisione non autorizzata con terze parti
- *Malware* e *ransomware*

Quali potrebbero essere le **misure di sicurezza di tipo tecnico ed organizzativo** da adottare al fine di prevenire l'accesso non autorizzato, la perdita o la violazione dei dati stessi, identificare vulnerabilità e comportamenti anomali? Facciamo qualche esempio:

Cifratura di dispositivi	Tecniche che non consentono di decifrare le informazioni su *computer* e dispositivi mobili o *smartphone*, anche in caso di perdita dei dispositivi
Antivirus e *Antimalware*	Prevenzione dai *malware*, rilevazione e blocco di attività malevoli
***Firewall* e sicurezza della rete**	Protezione perimetrale della sicurezza informatica mediante il controllo dell'accesso alla rete e il monitoraggio del traffico

Profili sanzionatori

Quali sono le potenziali sanzioni previste dalla normativa vigente qualora dovesse esserci una violazione delle disposizioni?

Sanzioni pecuniarie

Le sanzioni previste dal GDPR possono raggiungere, per le imprese il cui fatturato supera **20.000.000€,** un importo fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente.

Sanzioni penali

Il GDPR demanda agli Stati Membri la disciplina relativa alle sanzioni di natura penale. Pertanto, il Codice Privacy disciplina gli illeciti penali e le relative sanzioni al Capo II – Artt. 167 e seguenti.

Ai fini della valutazione dell'applicabilità della sanzione, **le Autorità valutano:**

- **natura, gravità e durata della violazione** (tenendo in considerazione la natura, l'oggetto o la finalità del trattamento, nonché il numero di interessati lesi dal danno e il livello del danno da essi subito);
- il carattere **doloso o colposo** della violazione;
- le **misure adottate** dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
- il **grado di responsabilità** del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto;
- eventuali **precedenti violazioni** pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
- il **grado di cooperazione** con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
- le **categorie di dati personali interessate** dalla violazione.

"Before I write my name on the board, I'll need to know how you're planning to use that data."

Grazie per l'attenzione!