CONTENUTI

Principi generali, concetti e definizioni
Ambiti di applicazione territoriale e materiale
Accountability, Privacy by design e Privacy by default
I ruoli:
- Titolare del trattamento
- Responsabile del trattamento
- Soggetti Autorizzati al trattamento

Liceità del trattamento dati personali e categorie particolari di dati (sensibili e giudiziari) e dati dei minori
Informative
Diritti degli interessati
Sicurezza: misure adeguate, valutazione del rischio
Registri attività di trattamento
Data Protection Impact Assessment (DPIA) e Consultazione preventiva
Data Breach | Violazione dei dati personali: concetto e procedure
DPO (cenni)
Certificazione Privacy e Codici di condotta
Trasferimenti dati all'estero e garanzie
Autorità di controllo (Garanti Privacy) | competenza
One stop shop e cooperazione fra DPA
EDPB Comitato Europeo protezione dei dati
Sanzioni - Tutele e danno risarcibile

CONCETTO DI PRIVACY

COSA SONO I DATI PER UN'AZIENDA

IL QUADRO NORMATIVO APPLICABILE IN ITALIA

Regolamento 2016/679	in vigore, pienamente applicabile dal 25 maggio 2018
Direttiva 1995/46	è decaduta il 24 maggio 2018
Codice D.Lgs. 196/2003	in vigore, è stato adeguato alla nuova normativa europea dal D.Lgs 101/2018
Provvedimenti Autorità Garante	in vigore, non decadono, fino a quando non vengono modificati, sostituiti, abrogati
Accordi Internazionali su Trasferimento dati	In vigore, non decadono, fino a quando non verranno modificati, sostituiti, abrogati
Decisioni Commissioni UE	in vigore, non decadono, fino a quando non verranno modificate, sostituite, abrogate

CHE COS'E' IL GENERAL DATA PROTECTION REGULATION ?

GDPR

- è stato approvato 27 aprile 2016 dopo 4 anni di preparazione e dibattito
- decorre dal 25 maggio 2018
- si compone di 99 articoli e 173 considerando
- riscrive la disciplina della Privacy a livello europeo.
- nasce in seguito alla continua evoluzione degli stessi concetti di privacy e protezione dei dati personali e quindi dalla conseguente necessità di aggiornare gli strumenti di tutela dovuta principalmente alla diffusione del progresso tecnologico.
- riguarda i dati relativi alle Persone Fisiche

AMBITO DI APPLICAZIONE

SI APPLICA ai trattamenti

- **di soli dati personali** di persone fisiche
- interamente o parzialmente automatizzati o non automatizzati se i dati personali sono contenuti in un archivio o sono destinati a confluirvi
- effettuati da un Titolare o Responsabile stabilito nell'UE, anche se il trattamento è effettuato fuori dall'UE
- effettuati da un Titolare o Responsabile non stabilito nell'UE se il trattamento ha ad oggetto dati personali di interessati che si trovano nell'UE quando le attività di trattamento riguardano
  - l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato
  - il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione
- effettuati da un Titolare stabilito in uno Stato extra UE soggetto al diritto di uno Stato UE in virtù del diritto internazionale

AMBITO DI APPLICAZIONE

NON SI APPLICA ai trattamenti

- effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico
- di informazioni anonime o dati personali anonimizzati
- per attività che non rientrano nel diritto dell'Unione (es. sicurezza nazionale)
- per attività di speciale rilevanza pubblica (es. politica estera e di difesa comune)
- effettuati da autorità ai fini di prevenzione, accertamento e repressione reati e ai fini di sicurezza pubblica

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

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

Limitazione di Trattamento

il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro

Profilazione

qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica

DEFINIZIONI

Titolare del Trattamento

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri

Responsabile del Trattamento

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

DEFINIZIONI

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

Archivio

qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico

DEFINIZIONI

Terzo

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile

Consenso dell'interessato

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

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

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

DEFINIZIONI

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

Dati relativi alla Salute

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

DEFINIZIONI

Non più DATI SENSIBILI E GIUDIZIARI

Nel GDPR

DATI PARTICOLARI (ex dati sensibili)

- relativi a razza, religione, appartenenza sindacale, vita o orientamento sessuale
- Dati relativi alla salute = dati sanitari
- Dati genetici
- Dati biometrici

DATI RELATIVI A CONDANNE PENALI E REATI (ex dati giudiziari)

ATTORI E RUOLI

ATTORI E RUOLI

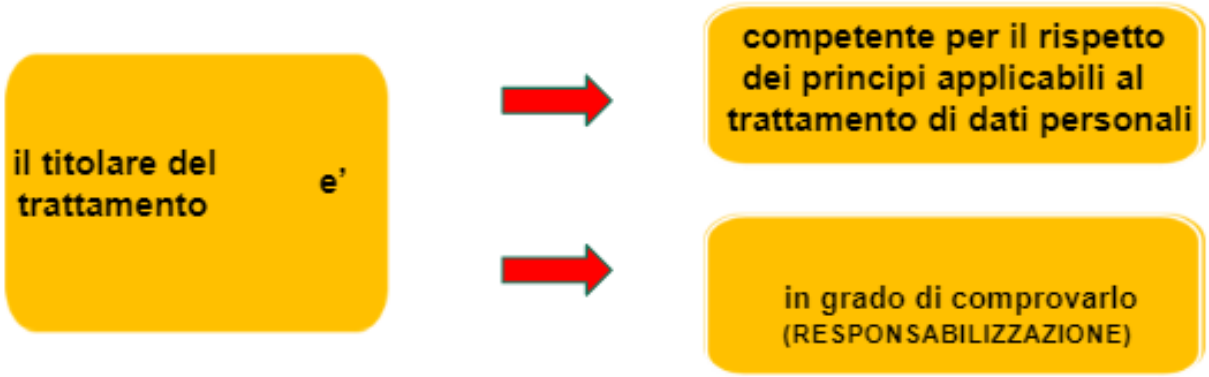
Chi è il titolare…

La persona fisica o giuridica, l'autorità pubblica, il servizio che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali (art. 4, § 7)

….e il contitolare

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari trattamento (art. 26)

ATTORI E RUOLI - TITOLARE



Dimostrare: provare una verità con un ragionamento logico o con prove di fatto

ATTORI E RUOLI – RAPPRESENTANTE DEL TITOLARE

Persona fisica o giuridica stabilita nell'Unione che, espressamente designato per iscritto, dal Titolare o dal Responsabile del trattamento extra UE li rappresenta per quanto riguarda gli obblighi del GDPR

Il rappresentante è un mandatario, stabilito in uno stato dell'Unione Europea, di un'organizzazione stabilità extra UE, che tratta dati di interesse UE non occasionalmente e le attività di trattamento riguardano

Offerta di beni o servizi ai suddetti interessati nell'Unione

Il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione

ATTORI E RUOLI – RESPONSABILE DEL TRATTAMENTO

Il responsabile

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (artt. 4, § 8-28)

Può nominare sub responsabili per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e **responsabile primario**

Il **responsabile primario** risponde dinanzi al titolare dell'inadempimento del sub responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento

ATTORI E RUOLI – RESPONSABILE DEL TRATTAMENTO

ATTORI E RUOLI – RESPONSABILE DEL TRATTAMENTO

In base al contratto il responsabile si impegna a:

trattare dati soltanto su istruzione documentata del Titolare

consentire i trattamenti solo a persone autorizzate con impegno alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza

adottate tutte le misure di Sicurezza (es. cifratura, recupero da backup)

rispettare le condizioni per ricorrere a un subresponsabile del trattamento

assistere il titolare per dare seguito alle richieste per l'esercizio dei diritti dell'interessato

cancellare o restituire tutti i dati e cancellare le copie esistenti

mettere a disposizione del titolare informazioni per dimostrare il rispetto di tali obblighi o consentire ispezioni

ATTORI E RUOLI – RESPONSABILE DEL TRATTAMENTO

L'adesione da parte del Responsabile del trattamento ad un codice di condotta approvato o ad un meccanismo di certificazione può essere utilizzato come elemento per dimostrare le garanzie sufficienti

Se un Responsabile del trattamento viola il Regolamento, determinando le finalità e i mezzi del trattamento, è considerato un Titolare del trattamento in questione

ATTORI E RUOLI – AUTORIZZATO AL TRATTAMENTO

Personale operativo di supporto all'attività del titolare e del responsabile

il GDPR

- non utilizza il termine incaricato ma fa riferimento a **chiunque sia sotto l'autorità diretta del Titolare o del Responsabile** (art. 29)
- prevede che tali soggetti siano istruiti dal titolare o dal responsabile

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri

DATA PROTECTION BY DEFAULT AND BY DESIGN

PRIVACY BY DESIGN

Vi è l'obbligo di avviare qualsiasi progetto introducendo fin dall'inizio gli strumenti a tutela dei dati personali

PRIVACY BY DEFAULT

Per impostazione predefinita i titolari dovrebbero trattare solo i dati personali nella misura necessaria per le finalità previste e per il periodo strettamente necessario a tali fini

DATA PROTECTION BY DEFAULT AND BY DESIGN

IN SINTESI

- **prevenire** non correggere, cioè i problemi vanno valutati nella fase di progettazione
- privacy **incorporata** nel progetto
- privacy come impostazione di **default**
- massima **funzionalità**, in modo da rispettare tutte le esigenze
- **sicurezza** durante tutto il ciclo del prodotto o servizio
- **trasparenza**
- **centralità** dell'utente

APPROCCIO BASATO SUL RISCHIO

Art. 32 para. 1 e 2

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio,.....

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

VALUTAZIONE DEI RISCHI

analisi dei rischi

- L'analisi dei rischi è un insieme di processi ben individuati in imprese strutturate con scopo di individuare, valutare e gestire le minacce per l'organizzazione
- Per GDPR il rischio inerente al trattamento è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati
- **Analisi** deve essere effettuata **non in ottica Titolare (Organizzazione) ma in ottica INTERESSATO**
- **Analisi va aggiornata** con introduzione **nuovi trattamenti** o se ci sono **variazioni sostanziali su quelli in essere**

MISURE DI SICUREZZA

la pseudonimizzazione e la cifratura dei dati personali

la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento

la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico

una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

PRINCIPI GENERALI DEL GDPR

Modalità di raccolta e requisiti dei dati personali

I dati personali devono essere

- Trattati in modo lecito corretto e trasparente (**principio correttezza e trasparenza**)
- Raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo NON incompatibile con tali finalità (**principio limitazione delle finalità**)
- Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità (**principio della minimizzazione dati**)
- Esatti e se necessario aggiornati (**principio esattezza**)
- Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (**principio limitazione della conservazione**)
- Trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, con misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (**principio dell'integrità e riservatezza)**

LICEITÀ DEL TRATTAMENTO

il trattamento di dati personali deve trovare fondamento in una idonea base giuridica

I 6 elementi di leicità del trattamento

- **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 a 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;
- **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 titolare/responsabile del trattamento;
- **INTERESSE LEGITTIMO:** il trattamento è necessario ai fini degli interessi legittimi perseguiti dal responsabile del trattamento o da una terza parte

LICEITÀ DEL TRATTAMENTO DATI PARTICOLARI

- Consenso esplicito dell'interessato per più finalità;
- Trattamento necessario per assolvere obblighi e diritti del Titolare del trattamento o dell'interessato (es. diritto del lavoro, Legge, etc…
- Dati resi manifestatamente pubblici dall'interessato (es. social network);
- Per accertare, esercitare o difendere un diritto in sede giudiziaria
- Tutela di un interesse vitale (es. incapacità fisica o giuridica di prestare il proprio consenso);

LICEITÀ DEL TRATTAMENTO DATI PARTICOLARI

- Trattamento di dati di membri anche passati di fondazioni, associazioni, organismi senza scopo di lucro con finalità legate ai dati «sensibili» con divieto di comunicazione esterna senza consenso;
- Trattamento necessario per motivi di interesse pubblico;
- Trattamento necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale, ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto di un professionista della sanità;
- Trattamento necessario per motivi di interesse pubblico nel settore della sanità pubblica (es. gravi minacce alla salute);
- Trattamento necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;

LICEITÀ DEL TRATTAMENTO DATI RELATIVO A CONDANNE PENALI E REATI

Il trattamento dati relativo a condanne penali e reati può avvenire:

Se autorizzato dal diritto dell'Unione o degli Stati membri

Un eventuale registro completo delle condanne penali (es. il casellario giudiziale) deve essere tenuto soltanto sotto il controllo dell'Autorità pubblica

CONSENSO

CARATTERISTICHE DEL CONSENSO

LIBERO

Nei contratti il consenso per finalità di marketing non deve essere obbligatorio

---

Il consenso non deve essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera

---

Il consenso non deve essere considerato liberamente espresso quando vi è squilibrio fa Titolare ed interessato

SPECIFICO E INFORMATO

Un consenso per ogni finalità

Conoscenza del Titolare del trattamento e delle finalità

DIMOSTRABILE

Il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha espresso il proprio consenso al trattamento dei propri dati personali

Qualora il trattamento abbia più finalità, il consenso deve essere prestato per tutte queste

CONSENSO

Trattamento dati di minori relativamente **all'offerta di servizi della società dell'informazione**

Trattamento lecito solo il minore ha almeno **16 anni**

Il trattamento di dati personali di minori di **età inferiore ai 16 anni** è lecito se il consenso è prestato o autorizzato dal **titolare della responsabilità genitoriale**

I DIRITTI DELL'INTERESSATO

- ad essere informato (artt. 12-13-14);
- di accesso ai dati (art. 15);
- di rettifica (art. 16);
- alla cancellazione dei dati, o «diritto all'oblio» (art. 17);
- alla limitazione del trattamento (art. 18);
- alla portabilità dei dati (art. 20);
- ad opporsi a determinate forme di trattamento (art. 21)
- a non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato dei dati che lo riguardano (art. 22)

I DIRITTI DELL'INTERESSATO

INFORMAZIONI E COMUNICAZIONI PER ESERCIZIO DIRITTI DELL'INTERESSATO

- Titolare del trattamento **adotta misure appropriate per fornire** →
  - adeguate informative
  - comunicazioni in materia di diritti degli Interessati e di notifica di violazioni di dati personali all'interessato

- **risposta** all'interessato **in un mese**, anche in caso di diniego, estendibili **fino a tre mesi** in caso di particolare complessità
- Una risposta deve essere fornita **in ogni caso** (anche se negativa o interlocutoria):artt. 12.3 + 12.4

- Le **informative ed i riscontri** all'interessato sono **gratuiti**
- **richieste manifestamente infondate o eccessive** (art.12.5) il titolare può stabilire se, e quanto, chiedere, come **contributo** ovvero se sono chieste più copie dei dati personali nel caso del diritto di accesso (art. 15.3), tenendo conto dei costi amministrativi sostenuti
- **contributo spese** deve essere **ragionevole** (art. 12.5)

DIRITTO ALL'INFORMAZIONE - INFORMATIVA

DUE TIPI DI INFORMATIVE →
- Dati personali raccolti presso l'interessato
- Dati personali NON raccolti presso l'interessato

Informazioni necessarie da inserire

- esistenza di trattamenti di dati personali che lo riguardano;
- finalità di tali trattamenti;
- identità dei soggetti che svolgono il trattamento (titolari) e dei loro rappresentanti
- i dati di contatto del responsabile della protezione dei dati, ove nominato
- Identità dei soggetti terzi a cui i dati potrebbero essere comunicati (destinatari) e possibilità che i dati siano trasmessi in un paese extra UE
- periodo di conservazione dei dati
- eventuale obbligo di comunicare i propri dati e conseguente della mancata comunicazione
- eventuale automatizzazione dei processi di trattamento, logiche utilizzate in tali processi e possibili conseguenze
- diritti che l'interessato può esercitare in relazione al trattamento

DIRITTO ALL'INFORMAZIONE - INFORMATIVA

- deve essere fornita all'interessato sempre e **prima di effettuare la raccolta dei dati**
- deve essere **concisa, trasparente, intelligibile e facilmente accessibile**
- deve essere **formulata con linguaggio semplice e chiaro** (soprattutto quelle rivolte a minori)
- deve essere fornita per iscritto «o con altri mezzi» (elettronici o oralmente se lo chiede l'interessato)
- se i dati non sono raccolti direttamente presso l'interessato *(art. 14 del regolamento)*, l'informativa deve comprendere anche le **categorie** dei dati personali oggetto di trattamento e la **fonte** da cui hanno origine i dati personali
- **deve essere anche specificato il diritto di proporre reclamo ad un 'autorità di controllo e** se esiste un **responsabile della protezione dati e il modo per contattarlo**
- ogni volta che le finalità cambiano l'interessato deve essere informato prima di procedere al trattamento ulteriore. Occorre quindi verificare se le informative rese in precedenza sono in linea con il Regolamento Europeo

REGISTRI ATTIVITA' TRATTAMENTO

REGISTRI ATTIVITA' TRATTAMENTO

REGISTRI ATTIVITA' TRATTAMENTO

INFORMAZIONI MINIME

da inserire nel

REGISTRO DEL TITOLARE

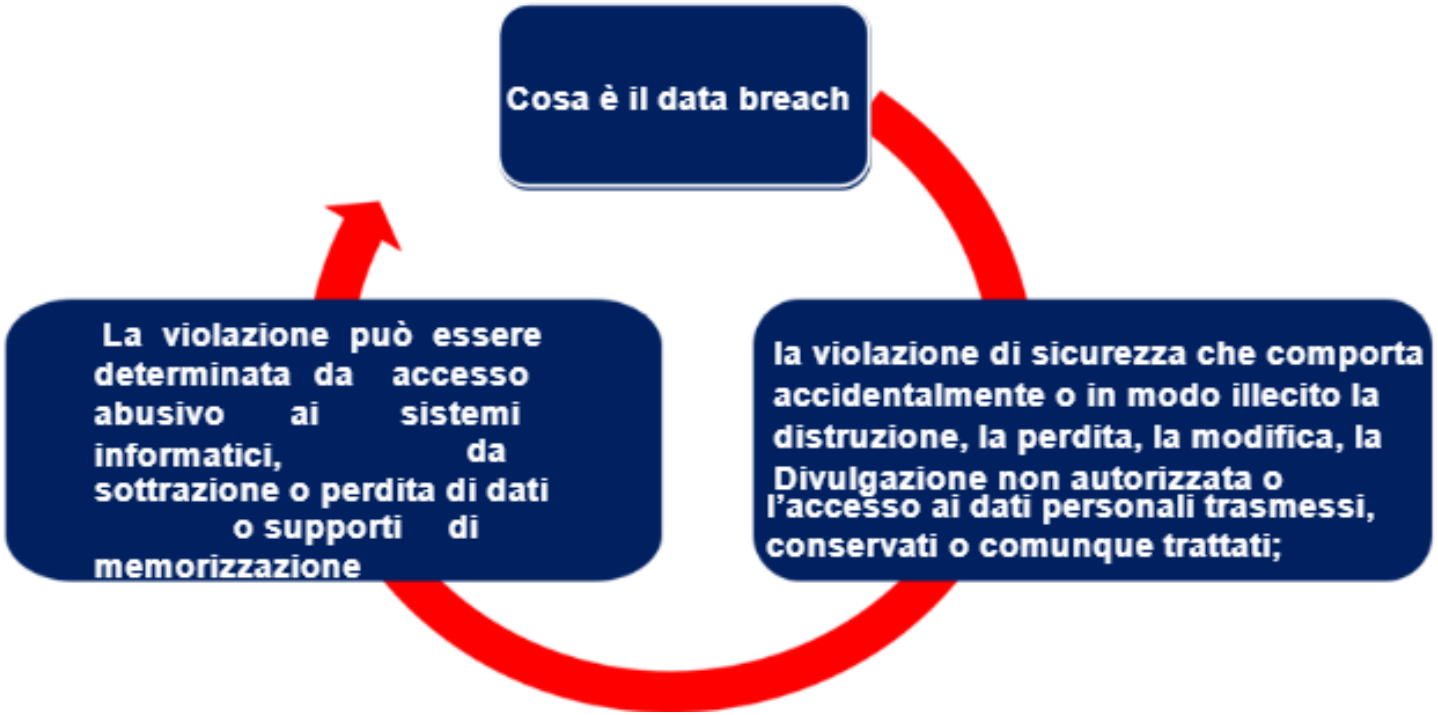
- ✓il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati
- ✓le finalità del trattamento
- ✓una descrizione delle categorie di interessati e delle categorie di dati personali
- ✓le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali
- ✓ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate
- ✓ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati
- ✓ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative

REGISTRI ATTIVITA' TRATTAMENTO

INFORMAZIONI MINIME da inserire nel REGISTRO DEL RESPONSABILE DEL TRATTAMENTO	✓il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, 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 o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
	✓ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

REGISTRI ATTIVITA' TRATTAMENTO

DATA BREACH


Cosa è il data breach
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;
La violazione può essere determinata da accesso abusivo ai sistemi informatici, da sottrazione o perdita di dati o supporti di memorizzazione

DATA BREACH

Perché il regolamento (art. 33) ha posto attenzione al DATA BREACH

una violazione dei dati personali può, se non affrontata in modo tempestivo ed adeguato, provocare danni fisici, materiali e immateriali alle persone fisiche (es. discriminazione – furto o usurpazione d'identità – perdite finanziarie – pregiudizio alla reputazione ecc.)

In caso di Data Breach OBBLIGO DI NOTIFICAZIONE

- **in caso di rischi per i diritti e le libertà delle persone fisiche**, dell'avvenuta violazione al Garante **ENTRO 72 ORE** E COMUNQUE "SENZA INGIUSTIFICATO RITARDO"
- **nei casi di violazioni con rischi elevati** anche nei confronti degli interessati, sempre **"SENZA INGIUSTIFICATO RITARDO"**
- **ESCLUSO SE È IMPROBABILE CHE LA VIOLAZIONE DEI DATI PRESENTI RISCHI** per i diritti e le libertà delle persone fisiche

DATA BREACH

Il Titolare del trattamento documenta qualsiasi violazione dei dati personali comprese le circostanze a esse relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio

Il Responsabile del trattamento informa il Titolare senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione, nel caso in cui tratti dati personali in nome e per conto suo

DATA BREACH

Contenuti della notifica	a.descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione
	a.comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni
	a.descrizione delle probabili conseguenze della violazione dei dati personali
	descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi

DATA BREACH

Comunicazione all'interessato

Se 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.

Contenuti della comunicazione all'interessato (usare linguaggio semplice e chiaro)	natura della violazione dei dati personali violati;
	nome e dati di contatto del DPO;
	probabili conseguenze della violazione dei dati personali;
	misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione

DATA BREACH

Non è richiesta la comunicazione all'interessato se

Il Titolare ha messo in atto misure tecniche e organizzative adeguate di protezione, quali la cifratura

Il Titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e libertà degli interessati

Detta comunicazione richiederebbe sforzi sproporzionati. In tal caso si procede ad una comunicazione pubblica

VALUTAZIONE D'IMPATTO - DPIA

Chi la effettua e quando

Il titolare del trattamento

prima di procedere a **trattamenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche**

allorché si prevede in particolare l'uso di nuove tecnologie

Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi

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

VALUTAZIONE D'IMPATTO - DPIA

Gruppo Art. 29

Per **rischio** si intendo uno **scenario descrittivo di un evento e delle relative conseguenze** , che sono **stimate in termini di gravità e probabilità**

IL RISCHIO

E' la potenzialità che un'azione o un'attività possano portare a un evento indesiderabile

EVENTUALITA' DI SUBIRE UN DANNO

ERRORI DA NON COMMETTERE

1. Non bisogna confondere o esaurire il problema della gestione dei rischi con il tema delle misure di sicurezza
2. Il rischio non è del titolare ma del soggetto interessato

VALUTAZIONE D'IMPATTO - DPIA

Casi in cui la valutazione d'impatto sulla protezione dei dati è obbligatoria

Valutazione sistematica e globale di aspetti personali basata su trattamento automatizzato sulla quale si fondano decisione che hanno effetti giuridici o incidono significativamente sulle persone fisiche

Esempio: PROFILAZIONE

Sorveglianza sistematica su larga scala

su una zona accessibile al pubblico

Trattamento su larga scala di categorie di dati particolari e di dati relativi a condanne penali e reati

CONSULTAZIONE PREVENTIVA

Titolare del trattamento , prima di procedere al trattamento, consulta l'Autorità di controllo (DPA) qualora la valutazione d'impatto sulla protezione dei dati (DPIA) indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio

trattamenti da sottoporre a consultazione preventiva, dopo la DPIA, sono quelli che comportano l'utilizzo di nuove tecnologie o di nuovo tipo

La DPA darà riscontro al Titolare in caso di violazione del GDPR entro 8 settimane dal ricevimento della richiesta con un parere scritto, prorogabile di 6 settimane nei casi più complessi

I termini potranno essere sospesi se la DPA fa richieste di informazioni al Titolare al fine della completezza della documentazione

Il GDPR ha abolito l'obbligo generale di notificazione presente nella legislazione italiana (D.Lgs. 196/03)

RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI - DPO

Figura che riflette l'approccio responsabilizzante che è proprio del Regolamento

Il ruolo può essere affidato a una figura: **interna** (rapporto di lavoro subordinato – dipendente) o **esterna** (contratto di servizi)

Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un RPD quando:

- Amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;
- L'attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati SU LARGA SCALA;
- L'attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici o di dati relativi a condanne penali.

IL DPO IN SINTESI

Competente
Indipendente
Autonomo
Raggiungibile

a) sorveglia l'osservanza del regolamento,

b) collabora con il titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);

c) informa e sensibilizza

d) coopera con il Garante e funge da punto di contatto

e) supporta il titolare o il responsabile in ogni attività connessa al trattamento di dati personali.

NON HA COMPITI OPERATIVI E DECISIONALI

CERTIFICAZIONE PRIVACY

Gli Stati membri, le Autorità di controllo, il Comitato e la Commissione incoraggiano l'istituzione di meccanismi di certificazione, sigilli e marchi standardizzati di protezione dei dati che consentano di dimostrare la conformità al GDPR dei trattamenti effettuati ai Titolari e dai Responsabili del trattamento, anche con sede al di fuori dell'UE.

La certificazione è volontaria e accessibile tramite una procedura trasparente, non riduce la responsabilità del Titolare o del Responsabile riguardo alla conformità al GDPR e lascia impregiudicati i compiti e i poteri delle DPA competenti

CERTIFICAZIONE PRIVACY

La certificazione è rilasciata dagli organismi di certificazione o dall'Autorità di controllo competente in base ai criteri approvati da tale Autorità di controllo competente

volontario, il meccanismo di certificazione viene richiamato come **elemento per dimostrare la conformità al GDPR** da parte dei Titolare o Responsabili,

è previsto fra le **attenuanti in caso di sanzione**, è anche un valido strumento per permettere agli interessati di valutare il livello di protezione dei dati, dei prodotti e servizi acquisiti

La certificazione dovrà avere una revisione periodica ogni 3 anni

CODICE DI CONDOTTA

CODICE DI CONDOTTA

✓ codici di condotta 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

✓Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente regolamento

✓Le associazioni e gli altri organismi che intendono elaborare un codice di condotta o modificare o prorogare un codice esistente sottopongono il progetto alla DPA competente. La DPA esprime un parere sulla conformità al regolamento del progetto di codice, della modifica o della proroga e lo approva , se ritiene che offra in misura sufficiente garanzie adeguate

✓Qualora il progetto di codice, la modifica o la proroga siano approvati, e se il codice di condotta in questione non si riferisce alle attività di trattamento in vari Stati membri, l'autorità di controllo registra e pubblica il codice

TRASFERIMENTI DATI ALL'ESTERO E CONDIZIONI DI ADEGUATEZZA

I trasferimenti di dati personali verso Paesi non appartenenti allo Spazio Economico Europeo (SEE, ossia UE + Norvegia, Liechtenstein, Islanda) o verso un'organizzazione internazionale sono consentiti a condizione che l'adeguatezza del Paese terzo o dell'organizzazione sia riconosciuta tramite decisione della Commissione europea (art. 45 del Regolamento UE 2016/679).

AUTORITÀ DI CONTROLLO COMPETENTE (DPA)

Anche il Regolamento Privacy UE prevede che ogni Stato dell'Unione Europea abbia una o più Autorità di controllo (DPA) autonome e indipendenti, incaricate di sorvegliare l'applicazione del GPDR.

Il fine è quello di tutelare i diritti e le libertà fondamentali delle persone fisiche interessate, con riguardo al trattamento dati e di agevolare la libera circolazione dei dati personali all'interno dell'Unione

Le DPA godono di indipendenza dagli altri Organi degli Stati UE con compiti e poteri propri. Il membro o i membri di ogni Autorità di controllo non devono subire pressioni esterne, né dirette, né indirette e non sollecitano né accettano istruzioni da alcuno

Ogni Stato membro provvede affinché ogni DPA sia dotata delle risorse umane, tecniche e finanziarie, dei locali e delle infrastrutture necessari per l'effettivo adempimento dei suoi compiti l'esercizio dei propri poteri

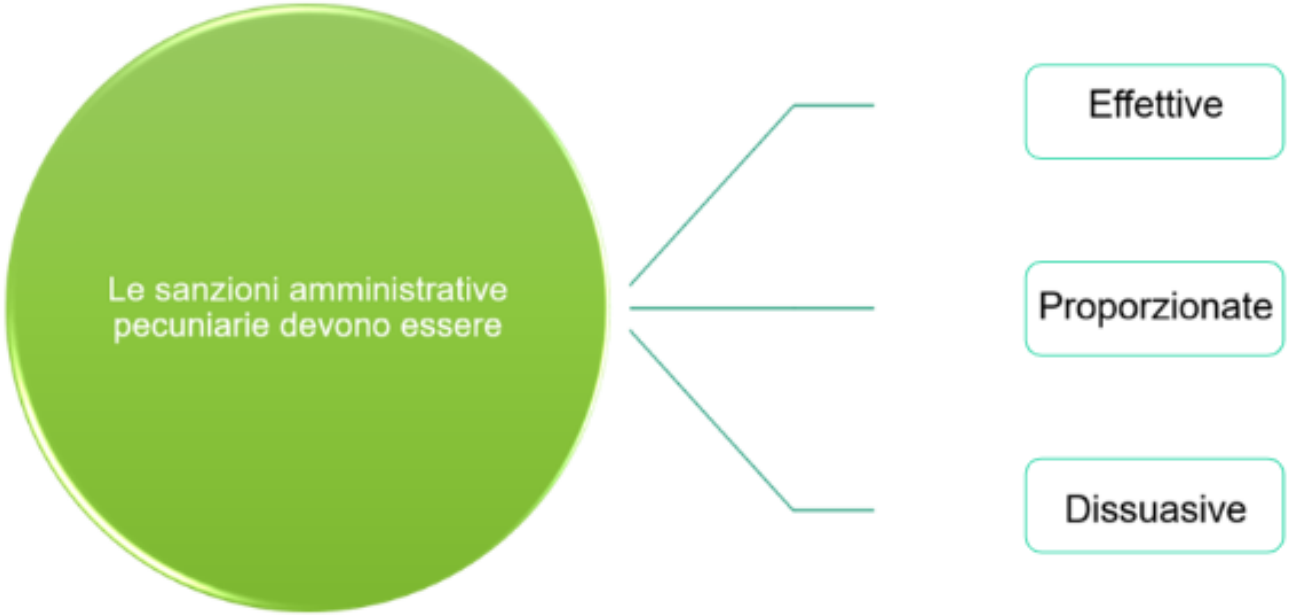
AUTORITÀ DI CONTROLLO COMPETENTE (DPA)

COMPITI

- controllare che i trattamenti di dati personali siano conformi al Regolamento nonché a leggi e regolamenti nazionali
- collaborare con le altre autorità di controllo
- esaminare reclami
- adottare i provvedimenti previsti dalla normativa in materia di protezione dei dati personali
- formulare pareri su proposte di atti normativi e amministrativi
- partecipare alla discussione su iniziative normative con audizioni presso il Parlamento
- partecipare alle attività dell'Unione europea ed internazionali di settore
- curare l'informazione e sviluppare la consapevolezza in materia di protezione dei dati personali, con particolare attenzione alla tutela dei minori

AUTORITÀ DI CONTROLLO COMPETENTE (DPA)

SANZIONI


Le sanzioni amministrative pecuniarie devono essere
Effettive
Proporzionate
Dissuasive

SANZIONI

Elementi di valutazione per infliggere una sanzione amministrativa pecuniaria e per fissarne l'ammontare

- La natura, la gravità e la durata della violazione.
- Il carattere doloso o colposo.
- Il tipo di violazione.
- Le misure di sicurezza adottate dal Titolare.
- L'adesione ad un codice di condotta.
- La tipologia di dato coinvolto.
- Eventuali precedenti violazioni.
- Il grado di cooperazione con l'Autorità di controllo.

SANZIONI

Sanzioni amministrative pecuniarie fino a € 10.000.00 o il 2% del fatturato mondiale annuo

Violazione degli obblighi del titolare e del responsabile secondo gli articoli 8, 11, da 25 a 39, 42 e 43 del regolamento

Violazione degli obblighi dell'organismo di certificazione secondo gli articoli 42 e 43 del regolamento

Violazione degli obblighi dell'organismo di controllo l'articolo 41, comma 4, del regolamento. secondo

SANZIONI

Sanzioni amministrative pecuniarie fino a € 20.000.00 o il 4% del fatturato mondiale annuo

Violazione dei principi di base del trattamento, comprese le condizioni relative al consenso, secondo gli articoli 5, 6, 7 e 9 del regolamento.

Violazione dei diritti degli interessati secondo gli articoli da 12 a 22 del regolamento

Violazione dei trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale secondo gli articoli da 44 a 49 del regolamento

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 secondo l'articolo 58, comma2, o il negato accesso in violazione dell'articolo 58, comma 2, del regolamento