Il Regolamento (UE) 2016/679 e la disciplina sulla privacy

Prof. Avv. Stefano Aterno

Il Regolamento UE n.2016/679 (GDPR)

- Il **GDPR** è stato approvato dal Parlamento e dal Consiglio europei il 14 aprile 2016 ed è divenuto pienamente applicabile negli Stati membri dell'Ue a decorrere da 25 maggio 2018.

- Il **Codice Privacy** italiano (D.Lgs. 196/2003) è stato quindi integrato e adeguato al GDPR attraverso il D.Lgs. 101/2018.

Regolamento UE n. 679/2016 relativo alla **protezione** delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla **libera circolazione** di tali dati

- Si applica ai **trattamenti aventi ad oggetto dati personali**:
  - di persone che si trovano nell'Unione europea; oppure
  - eseguiti da un Titolare o un Responsabile del trattamento stabiliti in UE (o altro luogo soggetto al diritto di uno Stato membro UE); oppure
  - eseguiti da un Titolare o un Responsabile del trattamento stabiliti non in UE per specifici trattamenti di dati personali di persone che si trovano nell'UE.
- Tra gli altri casi, il GDPR **non si applica**:
  - ai trattamenti di dati anonimi;
  - ai trattamenti svolti da una persona per attività personali/domestiche (es. vita privata e familiare dei singoli, la corrispondenza e gli indirizzari o l'uso dei social network).

Dati personali e categorie

Dato personale: qualsiasi informazione relativa a un Interessato identificato o identificabile, ad esempio il nome, il numero di telefono, dati relativi all'ubicazione, un identificativo *online*, uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati comuni

Dati particolari («dati sensibili»)

Dati giudiziari

Dati particolari

Dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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 «giudiziari»

Dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

N.B. Il Regolamento non trova applicazione nel caso di trattamento dei dati personali da parte delle autorità competenti laddove sia finalizzato alla prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. Il trattamento per queste finalità è oggetto di tutela della direttiva (UE) 2016/680.

Trattamento di dati personali

Trattamento di dati personali

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate ai dati personali o a insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, la modifica, l'estrazione, la consultazione, l'uso, la trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, raffronto, cancellazione o distruzione.

Princìpi fondamentali del GDPR

Ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati all'art. 5 del GDPR:

- liceità, correttezza e trasparenza: in modo lecito, corretto e trasparente («autodeterminazione informativa»);
- limitazione delle finalità: raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità;
- minimizzazione dei dati: adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esattezza: esatti e, se necessario, aggiornati;
- limitazione della conservazione: conservati in forma identificativa per un arco di tempo non superiore al conseguimento delle finalità;
- integrità e riservatezza: in modo da garantire adeguata sicurezza.

Minimizzazione dei dati

- Il trattamento dei dati deve essere limitato a quanto **strettamente necessario** a perseguire una finalità legittima.
- I dati personali dovrebbero essere trattati **solo se** la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi.
- Il trattamento dei dati non deve interferire in modo sproporzionato con gli interessati, i diritti e le libertà in gioco (altrimenti non lo tratto).

Principio di responsabilizzazione (cd. principio di accountability) (art. 5, co. 2)

Il principio di «accountability»

La responsabilizzazione richiede da parte dei titolari e dei responsabili del trattamento di:

- ✓ **adottare** attivamente e in modo permanente misure finalizzate alla promozione e alla salvaguardia della protezione dei dati nelle attività di trattamento (prestazione di risultato, no obblighi specifici).
- ✓ **garantire** la conformità (*compliance*) alla normativa in materia di protezione dei dati nell'ambito delle operazioni di trattamento e dei rispettivi obblighi.
- ✓ **dimostrare/rendicontare** in qualsiasi momento agli interessati, al pubblico in generale e alle autorità di controllo che essi operano in conformità delle disposizioni sulla protezione dei dati. I titolari e responsabili del trattamento devono altresì rispettare alcuni obblighi strettamente legati alla responsabilità (ad esempio, tenere un registro delle attività di trattamento e designare il responsabile della protezione dei dati).

Responsabilità per violazione del GDPR

Art. 82 GDPR: Diritto al risarcimento e responsabilità

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.
2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.
3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

[…]

Responsabilità e responsabilizzazione l'art. 82 conferma il criterio soggettivo della responsabilità per esercizio di attività pericolosa

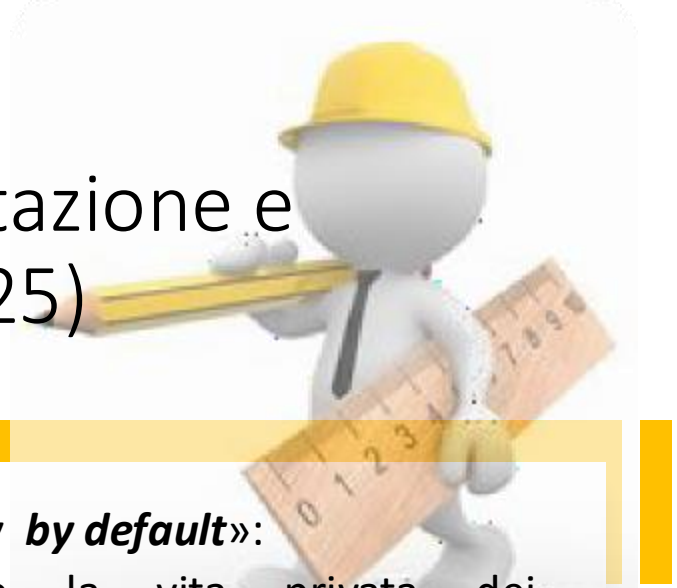
Il titolare e tutti coloro che sono coinvolti nel trattamento dei dati personali (responsabile del trattamento e incaricati):

✓ **sono obbligati a fare tutto il possibile per evitare il danno**
(eventuale, possibile, caso fortuito, forza maggiore)
e

✓ sono tenuti a dimostrarlo
(rendicontazione)

Inversione onere della prova

Principio di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (art. 25)



Principio della «***Privacy by design***»:

la protezione dei dati debba avvenire fin dalla progettazione di un prodotto/servizio/processo conformemente alle tutele imposte dal GDPR (approccio preventivo).

Ad esempio:

1. processi di autenticazione sicura;

2. limitazione alla raccolta dei dati (personali) strettamente necessari all'attività di trattamento sulla base delle finalità e basi giuridiche identificate;

3. cifratura del database;

4. utilizzo di tecniche di pseudonimizzazione o anonimizzazione (più o meno sofisticate);

Principio della «***Privacy by default***»:

necessità di tutelare la vita privata dei cittadini di *Default*, ovvero come impostazione predefinita.

Ad esempio:

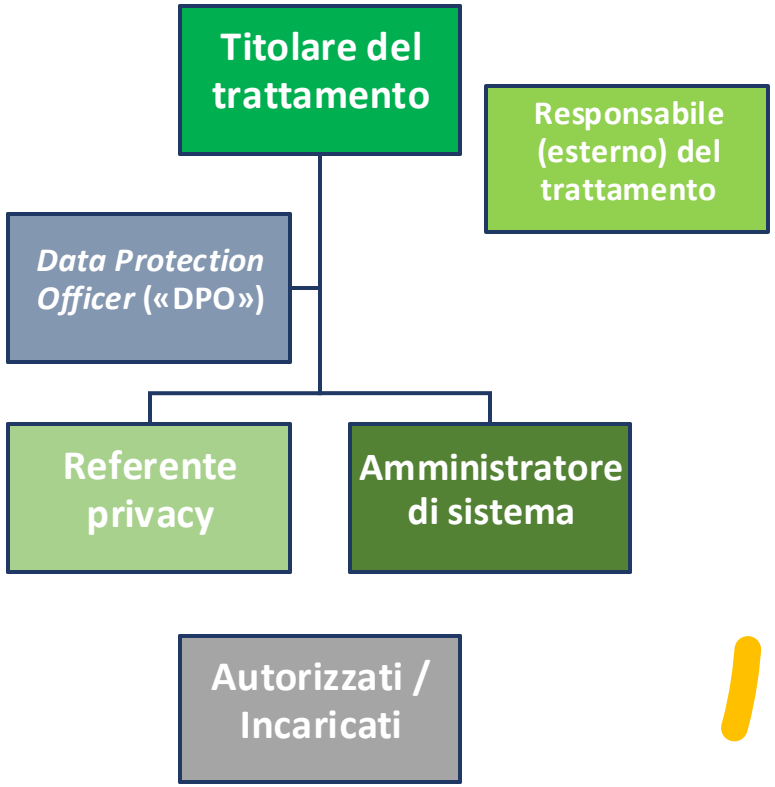
1. prevedere una richiesta di autorizzazione all'accesso delle risorse del device adoperato limitatamente alla necessità di raccolta dati (come l'accesso alla memoria, alla geo localizzazione, ecc.) con la negazione del consenso preimpostata;

2. adeguate informative relative al trattamento dei dati.

I principali «ruoli» privacy

Il soggetto che determina le finalità e i mezzi del trattamento di dati è il **Titolare del trattamento**. Talvolta, i Titolari possono essere due o più in merito al medesimo trattamento. Nel caso in cui i diversi titolari determinano congiuntamente le finalità e i mezzi del trattamento sono definiti **Contitolari del trattamento**.

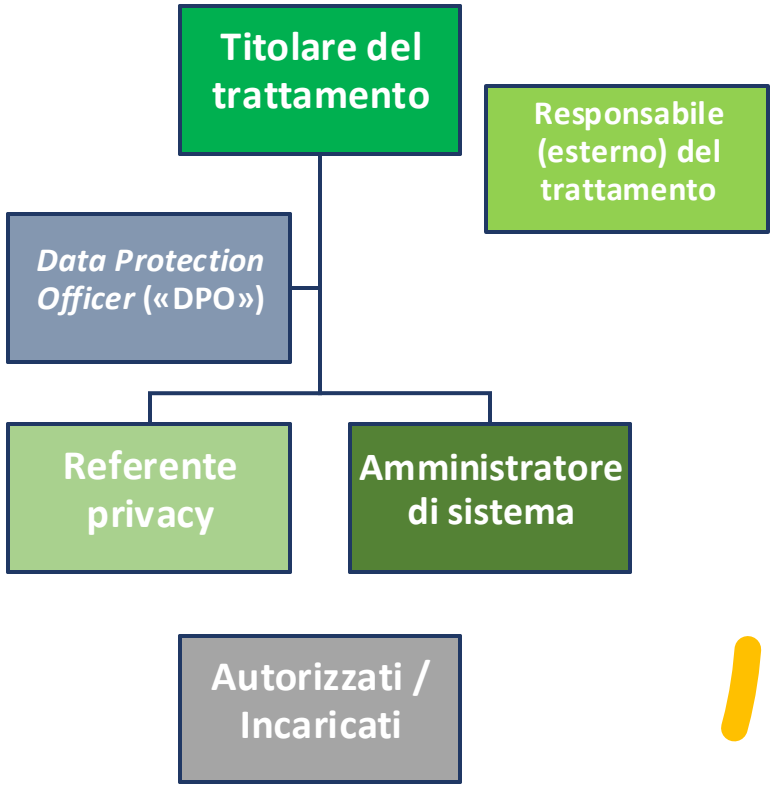
Il soggetto (esterno) che compie operazioni di trattamento per conto del Titolare è **Responsabile del trattamento**.



I principali «ruoli» privacy

I soggetti interni alla struttura organizzativa del Titolare, che trattano dati personali su sue indicazioni e istruzioni, e sotto la sua autorità/supervisione diretta, sono **Incaricati del trattamento** (o persone autorizzate).

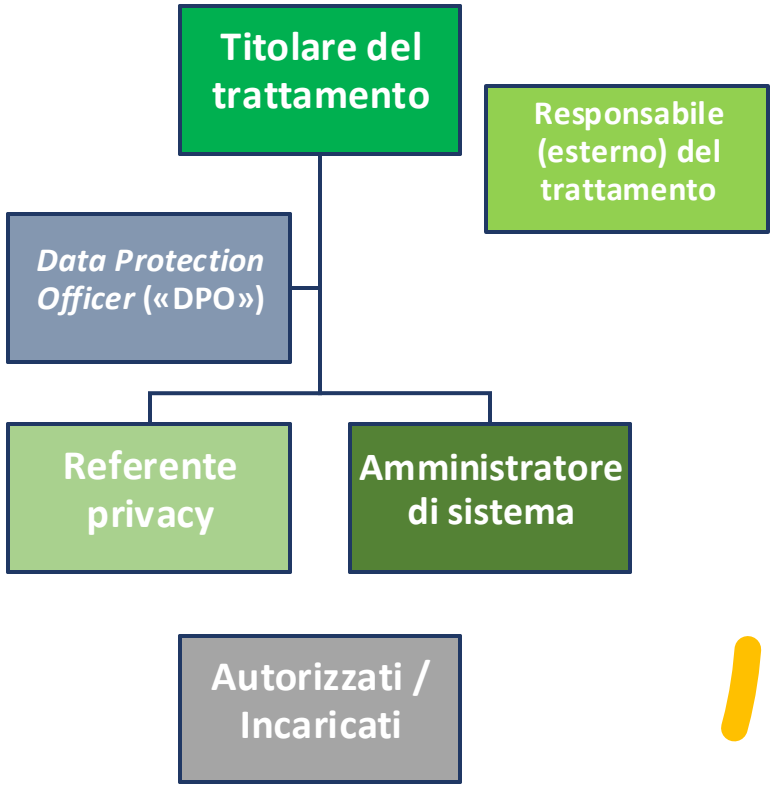
Il Titolare potrebbe inoltre individuare un ufficio / una funzione / una persona preposta a tutte le questioni di protezione dei dati («Referente privacy»).



I principali «ruoli» privacy

Se il trattamento di dati avviene con sistemi informatici, potrebbero essere nominati uno o più **Amministratori di sistema**, i quali, svolgendo le loro funzioni, possono accedere ai dati personali trattati. Per questo motivo, devono essere istruiti in maniera specifica.

In alcuni casi, è necessario (od opportuno) nominare un **Responsabile della protezione dei dati** (in inglese, *Data Protection Officer* o **DPO**).



Condizioni di liceità o «basi giuridiche»

La base giuridica è il fondamento di liceità del trattamento. Affinché i dati siano trattati in modo lecito, il trattamento deve essere conforme ad uno dei legittimi presupposti (basi giuridiche) elencati dai seguenti articoli del Regolamento Europeo n. 679/2016:

- Art. 6: dati comuni;
- Art. 9: dati particolari;
- Art. 10: dati giudiziari.

Liceità del trattamento (art. 6 GDPR)

Condizioni o «basi giuridiche» per i dati personali comuni:

- ✓ **Consenso** dell'Interessato
- ✓ Esecuzione di un **contratto** o misure precontrattuali
- ✓ Adempimento di un **obbligo di legge**
- ✓ Salvaguardia di **interessi vitali**
- ✓ Esecuzione di un compito di **interesse pubblico** o connesso all'esercizio di pubblici poteri
- ✓ Perseguimento di un **interesse legittimo** del Titolare

Liceità del trattamento (art. 9 GDPR)

È vietato trattare dati personali particolari salvo ricorra una delle seguenti condizioni o «basi giuridiche»:

- ✓ **Consenso** dell'Interessato
- ✓ Adempimento di obblighi di legge in materia di diritto del lavoro
- ✓ Salvaguardia di **interessi vitali**
- ✓ **Esercizio del diritto di difesa** in sede giudiziaria
- ✓ Riguardo dati personali resi **manifestamente pubblici** dall'interessato
- ✓ Esecuzione di un compito di **interesse pubblico** rilevante
- ✓ Finalità di medici preventiva o del lavoro
- ✓ Perseguimento di interesse pubblico nel settore della **sanità pubblica**
- ✓ **Archiviazione**, **ricerca scientifica** o **fini statistici**.

Liceità del trattamento (art. 10 GDPR)

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire:

- ✓ soltanto sotto il controllo dell'autorità pubblica; o
- ✓ se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Nuovi diritti riconosciuti dal GDPR

***Diritto alla cancellazione dei dati* (cd. "diritto all'oblio") (art. 17):**
Ricorrendo determinate condizioni, per diritto all'oblio si intende la **possibilità per l'interessato di ottenere dal Titolare del trattamento la cancellazione dei dati personali** che lo riguardano senza ingiustificato ritardo. Declinazione del diritto all'oblio su Internet è la deindicizzazione.

Diritto alla portabilità dei dati (art. 20):
Diritto di ricevere, da chi li tratta, i propri dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico, nonché il diritto di **trasmettere tali dati a un altro Titolare del trattamento senza impedimenti**, qualora l'interessato abbia fornito il proprio consenso al trattamento o se questo sia necessario per l'esecuzione di un contratto (evitare il lock-in tecnologico).

Se una persona chiede di esercitare uno dei diritti che il GDPR conferisce, il Titolare deve dare riscontro alla richiesta **entro 30 giorni dal ricevimento**.

Nel gestire l’istanza, è necessario **identificare il richiedente** (anche chiedendogli documenti di riconoscimento) e valutare se la richiesta è legittima. Tranne in casi particolari, è opportuno riscontrare positivamente e quanto prima la richiesta.

Per queste ragioni, al ricevimento (in qualunque forma) di una richiesta, **occorre informare** senza ritardo il Titolare e il DPO, che si occuperanno di dare riscontro.

Informativa sul trattamento dei dati personali (art. 13 GDPR)

- Identità e contatti del Titolare del trattamento
- Finalità e base giuridica del trattamento
- Eventuale interesse legittimo perseguito
- Periodo di conservazione dei dati
- Eventuali destinatari dei dati
- Eventuali trasferimenti extra-UE
- Diritti dell'interessato previsti dal GDPR
- Dati di contatto del DPO

Diritti dell'interessato

Interessato: la persona fisica cui si riferiscono i dati.

- **Accesso.** Diritto a ottenere conferma che sia in corso un trattamento dei propri dati e, in tal caso, di accedere a tali dati (da non confondere con il diritto di accesso agli atti della P.A. in materia di trasparenza).
- **Rettifica.** Diritto di ottenere rettifica dei dati personali inesatti, nonché il loro aggiornamento.
- **Cancellazione («Oblio»).** Diritto di ottenere la cancellazione dei propri dati trattati, al ricorrere di specifiche condizioni (talvolta esistono tempi di conservazione obbligatori: es. cartella clinica, conto corrente, tabulati telefonici).
- **Limitazione.** Diritto di ottenere che il trattamento dei propri dati sia limitato, al ricorrere di specifiche condizioni.
- **Portabilità.** Diritto di ricevere, da chi li tratta, i propri dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico.
- **Opposizione e revoca.** Diritto di opporsi in qualsiasi momento al trattamento dei propri dati, oppure di revocare in qualsiasi momento il consenso prestato.
- **Processo decisionale automatizzato e profilazione.** Diritto di non essere sottoposti a una decisione basata unicamente su trattamenti automatizzati, inclusa la profilazione, che incida in modo significativo sulla persona dell'Interessato.

Responsabile della protezione dei dati “DPO”

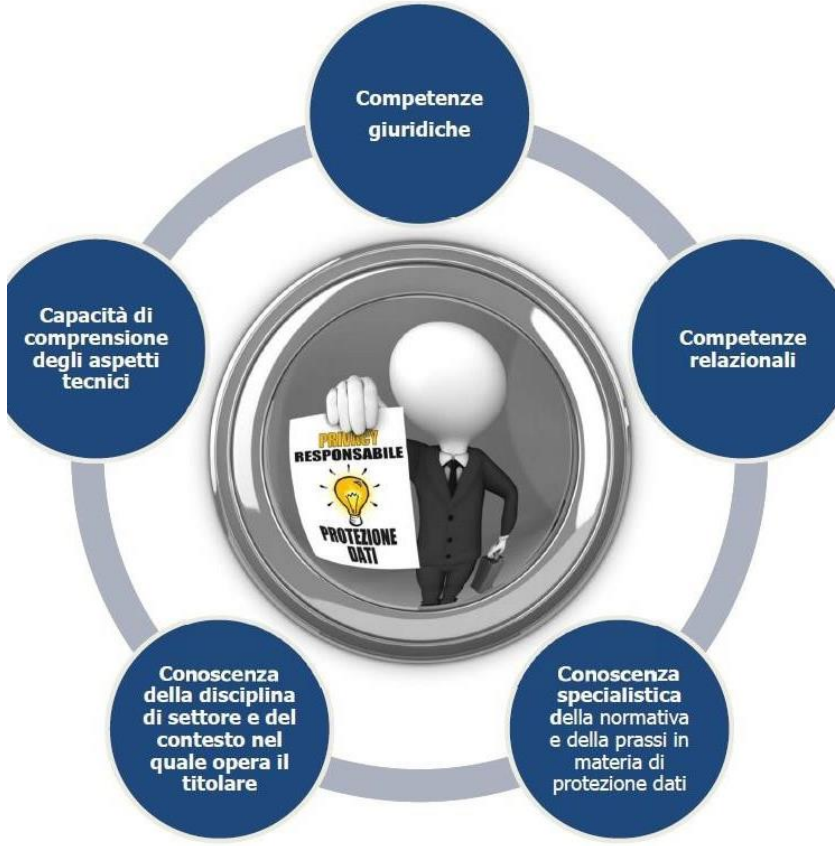
- **Considerando 97**
- **Art. 37** — *Designazione del responsabile della protezione dei dati*
- **Art. 38** — *Posizione del responsabile della protezione dei dati*
- **Art. 39** — *Compiti del responsabile della protezione dei dati*
- **Gruppo di lavoro art. 29** — *Linee guida sui Responsabili della Protezione dei Dati del 13 dicembre 2016*

Nuova figura di Garanzia

Chi è il «DPO»?

- Il DPO (Data Protection Officer) o RTD (Responsabile della Protezione dei Dati) è un soggetto che deve essere designato dai titolari di più grandi dimensioni (obbligatorio per **un'autorità pubblica o un organismo pubblico)** con i seguenti compiti:
- **informare e fornire consulenza** al titolare e ai suoi dipendenti in merito agli obblighi derivanti dalle norme sulle protezione dei dati;
- **sorvegliare** l'osservanza delle norme sulla protezione dei dati, delle politiche del titolare in tale materia;
- **cooperare** con il Garante e fungere da punto di contatto per il Garante per questioni connesse al trattamento.

Ha competenze trasversali.



Misure di sicurezza (art. 32 GDPR)

Al fine di garantire la sicurezza dei dati trattati, il GDPR impone a Titolari e Responsabili di approntare le **misure tecniche** e **organizzative** ritenute adeguate per il caso concreto, tali da proteggere i dati stessi da trattamenti non autorizzati o illeciti e dalla perdita, distruzione e danno accidentali. Importanza del criterio di privacy by design. Ad esempio:

a) la **pseudonimizzazione** e la **cifratura** dei dati personali

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

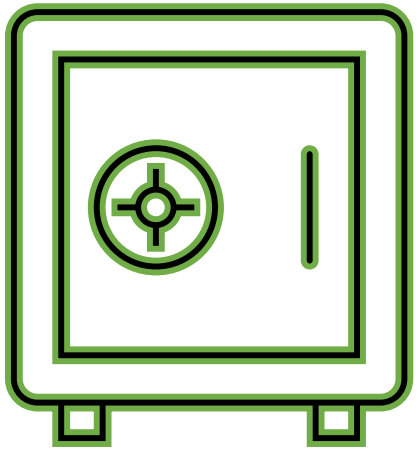
c) la capacità di **ripristinare tempestivamente la disponibilità e l'accesso dei dati** personali in caso di incidente fisico o tecnico

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

Misure organizzative

Complesso di **regolamenti, politiche e procedure** interni, idonei a ottenere un livello di sicurezza e protezione delle informazioni coerente con gli obiettivi e con le strategie del Titolare. Ad es.:

- Procedure per la gestione degli strumenti informatici e dei sistemi di rete;
- Procedura per il riscontro alle richieste di esercizio dei diritti degli Interessati;
- Procedura per Data Breach.



Misure tecniche

Complesso delle misure tecnologiche approntate per garantire la sicurezza dei dati trattati e la resilienza dei sistemi IT utilizzati. Ad es.:

- Procedure e programmi di *backup* e *restore*;
- Crittografia;
- Antivirus, firewall;
- Sistemi di autenticazione ai portali web;
- Disaster Recovery.

Focus (1): Le Password

- dati personali quali nomi o date di nascita propri o di familiari o di persone care, numeri di telefono, targa auto o cose simili
- sequenze prevedibili (tipo «password», «123456», «ciao»,)
- parole di uso comune
- nomi e personaggi famosi o di fumetti
- tutto o parte del nome utente

- Meglio utilizzare almeno otto caratteri e inserire :
- sia LETTERE sia NUMERI,
- Sia MINUSCOLE sia MAIUSCOLE,
- Sia SIMBOLI @ !*[^ « /

Suggerimenti:

- Non lasciare la password su post-it
- Non comunicare la password ad amici e parenti, tantomeno a persone appena conosciute.
- Se avete bisogno di comunicare la password a chiunque per qualunque motivo provvedere a cambiarla subito dopo.
- Nei servizi in rete cambiare la password subito dopo il primo accesso
- Cercare di trovare un vostro sistema personalissimo di generazione delle password

Curiosità : il tempo medio utilizzato per craccare una password

un programma di ricerca delle password /attacco a dizionario utilizzato con un computer di buona potenza consente di provare 10 milioni di password al secondo:

MARIA → 0 secondi

06285439 → 10 secondi

topolini → 6 minuti

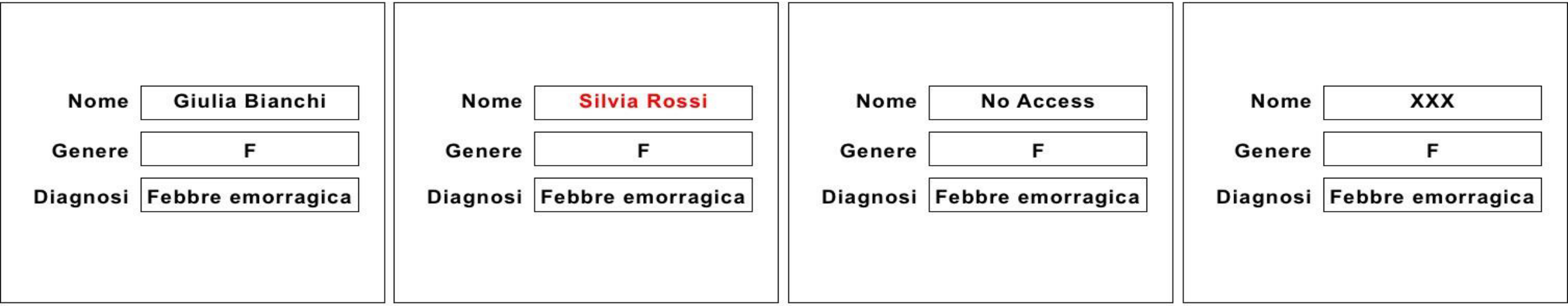
Mari7ns → 4 giorni

Pa69*Cto → 23 anni

Focus(2): pseudonimizzazione dei dati personali

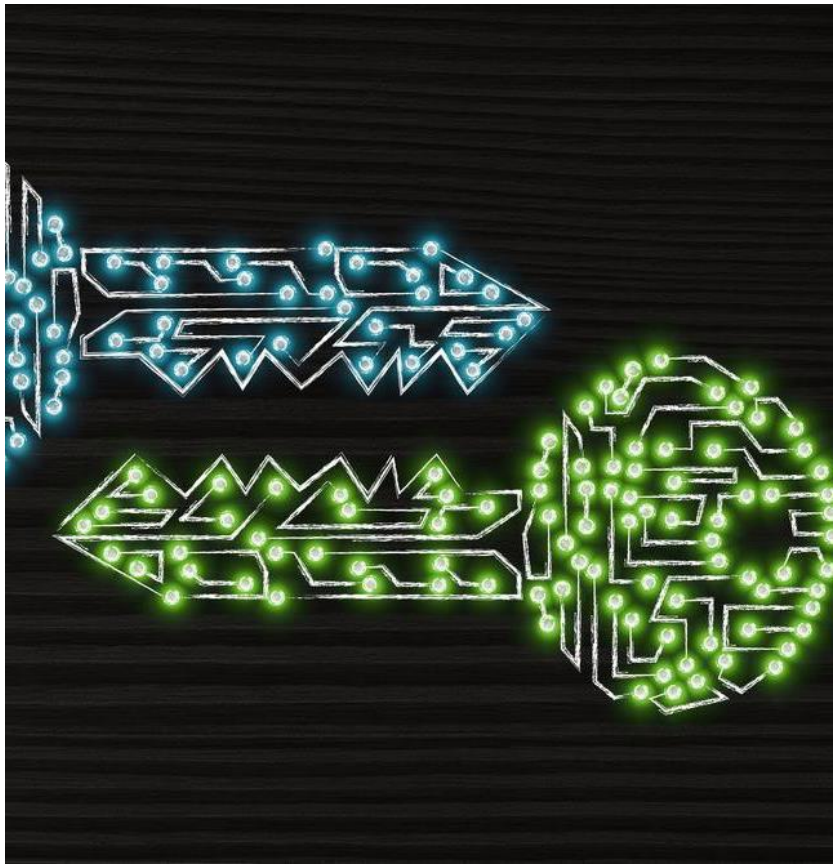
La **pseudonimizzazione** è una tecnica che consiste "nel trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di **informazioni aggiuntive**, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile" (art. 4 punto 5 del GDPR)

I dati pseudonimizzati **NON** sono dati anonimi.



Focus(3): Cifratura

- **Pseudonimizzazione simmetrica:** nella pseudonimizzazione simmetrica si utilizza la stessa chiave per cifrare, o mascherare, il dato e per renderlo nuovamente leggibile. Con questa tecnica c'è però il problema di come condividere la chiave senza che questa venga scoperta.
- **Pseudonimizzazione asimmetrica:** nella pseudonimizzazione asimmetrica si utilizzano due chiavi distinte: la prima per cifrare il dato, la seconda per decifrarlo. In questo modo è possibile facilitare la condivisione poiché si utilizza una chiave per crittografare, visibile a chiunque, e una chiave per decifrare che conosce solo il destinatario rendendo quindi non necessaria la sua condivisione.



Rischio elevato? ➡ V.i.p.

Considerando 78 (art. 25)

Per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio.

Valutazione d'impatto sulla protezione dei dati personali.

L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per DIMOSTRARE che il trattamento dei dati personali rispetta il presente regolamento.

Valutazione d'impatto sulla protezione dei dati (cd. PIA) (art. 35) …

quando un tipo di trattamento

può presentare <u>un rischio elevato</u> per i diritti e le libertà delle persone fisiche

il Titolare **prima di procedere al trattamento** dei dati deve effettuare

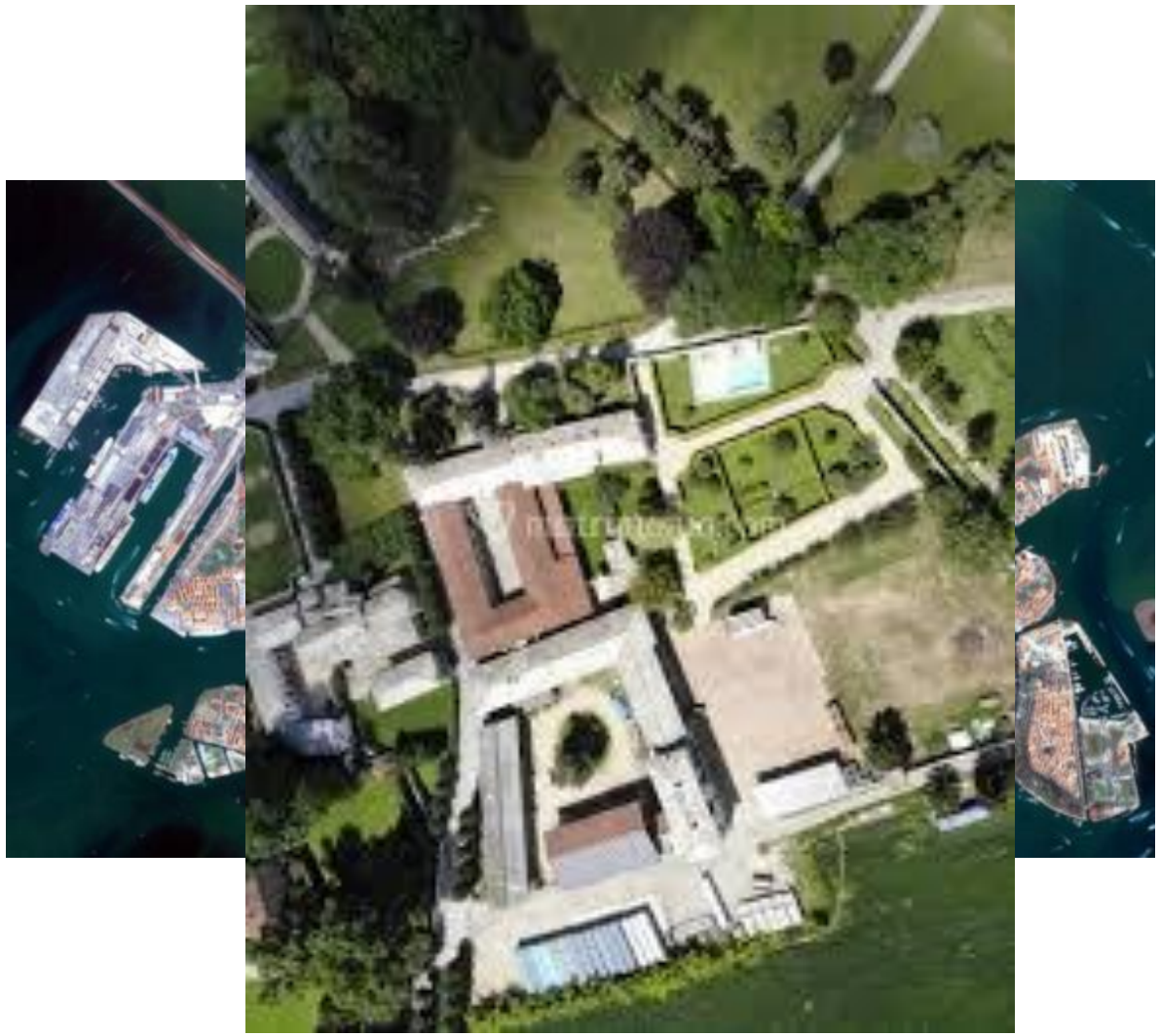
una **valutazione dell'impatto** dei trattamenti ("**Privacy Impact Assessment**" cd. **PIA**)

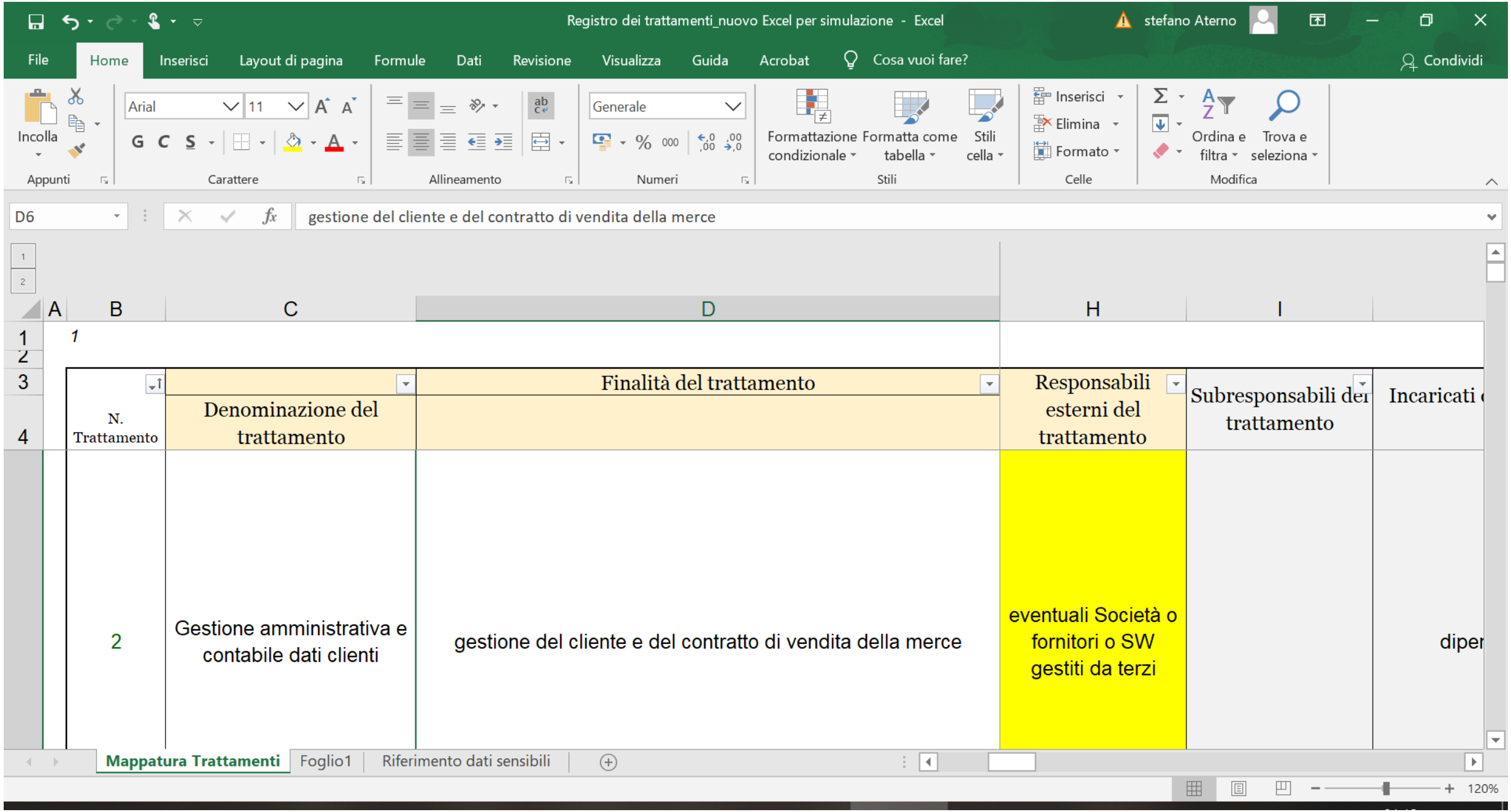
Se la valutazione d'impatto sulla protezione dei dati indica che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione,

prima del trattamento si dovrebbe consultare l'autorità di controllo.

Il Titolare del trattamento nel svolgere la PIA si consulta con il Responsabile della protezione dei dati, se designato.

Registro delle attività di trattamento (art. 30)




Registro dei trattamenti_nuovo Excel per simulazione - Excel
stefano Aterno
File
Home
Inserisci
Layout di pagina
Formule
Dati
Revisione
Visualizza
Guida
Acrobat
Cosa vuoi fare?
Condividi
Incolla
Arial
11
Generale
Formattazione condizionale
Formatta come tabella
Stili cella
Inserisci
Elimina
Formato
Ordina e filtra
Trova e seleziona
Appunti
Carattere
Allineamento
Numeri
Stili
Celle
Modifica
D6
gestione del cliente e del contratto di vendita della merce
1
Finalità del trattamento
N. Trattamento
Denominazione del trattamento
Responsabili esterni del trattamento
Subresponsabili del trattamento
Incaricati
2
Gestione amministrativa e contabile dati clienti
gestione del cliente e del contratto di vendita della merce
eventuali Società o fornitori o SW gestiti da terzi
Mappatura Trattamenti
Foglio1
Riferimento dati sensibili
120%

Registri delle attività di trattamento (art. 30)

Ogni Titolare del trattamento (e anche ogni responsabile esterno del trattamento) tiene un registro delle attività di trattamento svolte sotto la propria responsabilità.

Il Registro deve riportare:

-gli estremi del **Titolare** o del **Responsabile** del trattamento e, ove presente, del **Responsabile della protezione dei dati;**

-le **finalità** del trattamento;

-una descrizione delle categorie di **interessati** e di **dati** oggetto del trattamento e delle categorie di **destinatari cui i dati vengono comunicati;**

-ove applicabile, i **trasferimenti di dati** personali verso un paese terzo o un'organizzazione internazionale:

-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.**

Violazione dei dati personali («data breach»)

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.

N.B. ciò vale sia per i sistemi informatici, sia per documenti cartacei in cui sono contenuti dati personali.

Data breach non solo informatici!

Il Data Breach può essere costituito, a titolo esemplificativo e non esaustivo, da:

- accesso o acquisizione dei Dati Personali da parte di terzi non autorizzati;
- furto o perdita di dispositivi informatici contenenti Dati Personali;
- deliberata alterazione di Dati Personali;
- impossibilità di accedere ai Dati Personali per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- perdita o distruzione di Dati Personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- divulgazione non autorizzata dei Dati Personali.

Violazione dei dati personali («data breach»)

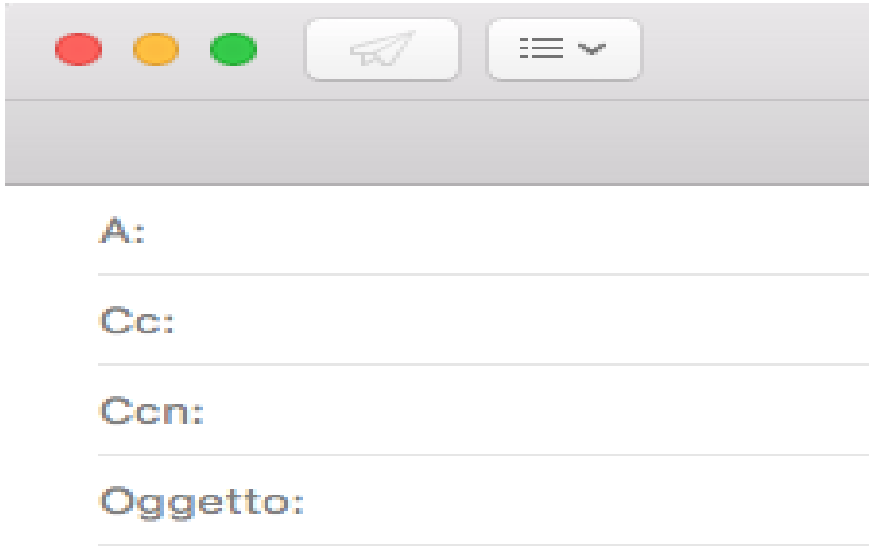
In ogni caso in cui c'è un rischio relativo ai dati personali trattati per conto del Titolare, occorre **informare tempestivamente il Titolare** dell'accaduto.

Il DPO valuterà la gravità dell'evento. Se del caso, il Titolare sarà tenuto a **notificare la violazione al Garante** privacy entro 72 ore dalla notizia. Nei casi più estremi, occorrerà anche **comunicare la violazione ai soggetti interessati**.

Invio di e-mail

L'invio di un'e-mail contenente dati personali di un interessato al destinatario sbagliato è un data breach!

- Verificare preliminarmente se il **contenuto e allegati** dell'email contengono dati particolari e/o giudiziari (es. permessi per malattia, certificati medici). Se ricorrono queste condizioni alzare il livello di attenzione e verificare soprattutto che il destinatario dell'email sia correttamente indicato.
- In caso di e-mail con **più destinatari**, verificare che tutti i destinatari siano legittimati a conoscere le informazioni contenute nell'email.
- In caso di e-mail con destinatari esterni al gruppo di lavoro, valutare se mettere **in copia conoscenza nascosta** gli altri destinatari.



Sanzioni amministrative pecuniarie (art. 83 - 84)

- Il Regolamento ha aumentato l'ammontare delle sanzioni amministrative pecuniarie, che potranno arrivare fino ad un massimo di 20 milioni di Euro o fino al 4% del fatturato mondiale totale annuo, lasciando peraltro ciascuno Stato membro libero di adottare norme relative ad altre sanzioni.

- Sanzioni equivalenti per le violazioni negli Stati membri. Tali sanzioni devono essere effettive, proporzionate e dissuasive.

- Gli Stati membri dovranno stabilire disposizioni ad hoc relative a **sanzioni penali** per le violazioni del presente regolamento

- La mancata previsione di minimi edittali consente di valutare, nella dosimetria della pena da infliggere, una pena anche nel minimo molto bassa nei **casi di lieve rilevanza**. Il vecchio codice prevedendo invece delle pene minime talvolta eccessivamente alte obbligava al pagamento di importi spropositati rispetto al fatto concreto.

- Il comma 4 dell'art. 83 fissa una serie di disposizioni in violazione delle quali le sanzioni amministrative pecuniarie possono **essere irrogate fino a 10 000 000 EUR**, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.
- Le disposizioni sono relative agli obblighi del titolare del trattamento e del responsabile del trattamento in materia di:

- consenso ai minori in relazione ai servizi della società di informazione (articolo 8);
- trattamento che non richiede l'identificazione (articolo 11);
- privacy by design e privacy by default, (articolo 25);
- contitolari del trattamento (art. 26);
- rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione (art. 27);
- Responsabile del trattamento e obblighi derivanti dalla sua qualifica ex lege(art. 28);
- trattamento e istruzione al trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento (art. 29)
- registro delle attività di trattamento con i diversi criteri, limiti e obblighi (art. 30)
- gli adempimenti derivanti dagli obblighi di cooperazione con l'autorità di controllo (art. 31);

- di obblighi previsti per mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (art. 32);
- obblighi di notifica di una violazione dei dati personali all'autorità di controllo, cd data breach(art. 33);
- comunicazione di una violazione dei dati personali all'interessato (art.34);
- valutazione d'impatto sulla protezione dei dati art. 35
- consultazione preventiva (art. 36);
- designazione del responsabile della protezione dei dati (art. 37);
- posizione del responsabile della protezione dei dati (art.38);
- compiti del responsabile della protezione dei dati (art. 39);
- ed inoltre, in relazione:
- agli adempimenti e gli obblighi per chi si certifica (art. 42);
- agli organismi di certificazione (art. 43);
- alla violazione degli obblighi in campo all'organismo di controllo dei codici di condotta approvati.

Ai sensi del comma 5, invece la violazione di altre disposizioni è soggetta a sanzioni amministrative pecuniarie punibili **fino a 20 000 000 EUR,** o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Queste disposizioni, la cui violazione comporta **sanzioni più gravi** rispetto alle precedenti sono relative a :

- violazioni dei principi base del trattamento,
- comprese le condizioni relative al consenso,
- quelle a norma degli articoli sui principi fondamentali (art.5),
- liceità del trattamento (art.6), condizioni per il consenso (art. 7),
- e per il trattamento di categorie particolari di dati personali, ovvero per il trattamento dei dati sensibili (art. 9).

- Altre disposizioni punite con queste sanzioni così alte **sono quelle che riguardano i diritti degli interessati** come quelle relative:
- alle informative, alle comunicazioni e alle modalità trasparenti per l'esercizio dei diritti dell'interessato (art.12);
- alle informative da fornire qualora i dati personali siano raccolti presso l'interessato (art.13);
- alle informative da fornire qualora i dati personali non siano stati ottenuti presso l'interessato (art.14);
- al diritto di accesso dell'interessato (art.15);
- al diritto di rettifica (art.16);
- al diritto alla cancellazione anche chiamato in certe situazioni «diritto all'oblio» (art.17);
- al diritto di limitazione del trattamento (art.18);
- all'obbligo di notifica in caso di rettifica o cancellazione dei dati personali o di limitazione del trattamento (art.19);
- al diritto alla portabilità dei dati (art.20);
- al diritto di opposizione (art.21).
- E' soggetta alla sanzione fino a 20.000.000 di euro anche la violazione delle disposizioni relative ai trasferimenti di dati personali a un destinatario in un paese terzo (o un'organizzazione internazionale) a norma degli articoli da 44 a 49;

PARAMETRI PER LA DOSIMETRIA DELLA PENA

Per decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

- a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
- b) il carattere doloso o colposo della violazione;
- c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
- d) 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 ai sensi degli articoli 25 e 32;
- e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
- f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
- g) le categorie di dati personali interessate dalla violazione;
- h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
- i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
- j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42;
- k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Grazie per l'attenzione!

resto a vostra disposizione per eventuali domande

Prof. Avv. Stefano Aterno

saterno@e-lex.it

www.e-lex.it

Grazie per l’attenzione
resto a vostra disposizione per eventuali domande

Prof. Avv. Stefano Aterno

stefano@aterno.it

www.e-lex.it