Regolamento europeo (EU) 2106/679
Documento aggiornato al 31 dicembre 2018

ATTENZIONE

Questa presentazione è in continuo aggiornamento attraverso un monitoraggio periodico anche in funzione di eventuali interventi del Legislatore europeo o del Garante italiano. La presentazione deve pertanto essere presa in considerazione con le dovute cautele, e quindi come indicazione di massima. Inoltre non deve essere presa in considerazione come documento ufficiale che sostituisce l'intervento di un Professionista della materia, al quale è comunque consigliato rivolgersi.

Potranno anche essere rilasciati nuovi aggiornamenti e/o revisioni.

Stefano Bertani


REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

(Testo rilevante ai fini del SEE)

186 pagine

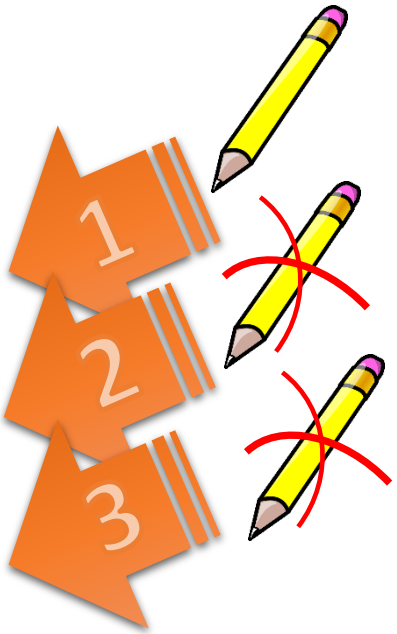
Introduzione

- Il Regolamento è in vigore dal maggio 2016 ma è obbligatorio a partire dal 25 maggio 2018 (Art.99): viene di conseguenza abrogato il D.Lgs 196/2003.
- Si applica per il trattamento interamente o parzialmente automatizzato di dati personali (anche destinati a figurarvi) ma non si applica ai trattamenti di dati personali effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico. (Art.2)
- Si applica pertanto per il trattamento dei dati personali effettuato nell'ambito delle attività professionali da parte di un Titolare del trattamento o di un Responsabile del trattamento, e per dati personali di interessati che si trovano nell'Unione. (Art.3)

Gestione dei dati personali

- E’ importante sottolineare come i dati personali devono essere trattati (Art. 5) in modo lecito, corretto e trasparente nei confronti dell’interessato («liceità, correttezza e trasparenza»).
- Ovviamente raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.
- I dati devono pertanto essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»).
- Devono essere esatti e, se necessario, aggiornati.
- Devono essere 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.

Quando è possibile trattarli



Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni (Art.6):

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 la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
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 che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

16 anni

Art.9

È vietato trattare dati personali che rivelino 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. (C51)

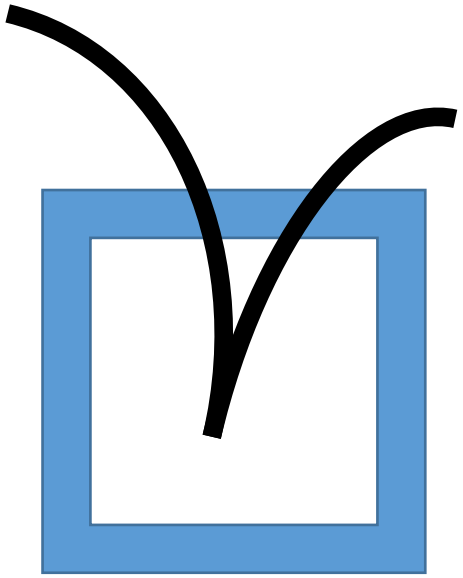
2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: (C51, C52)

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

Come tutelarci?

Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali. (Art. 7)



Come gestire il consenso

Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento e con la stessa facilità con cui è stato precedentemente accordato.

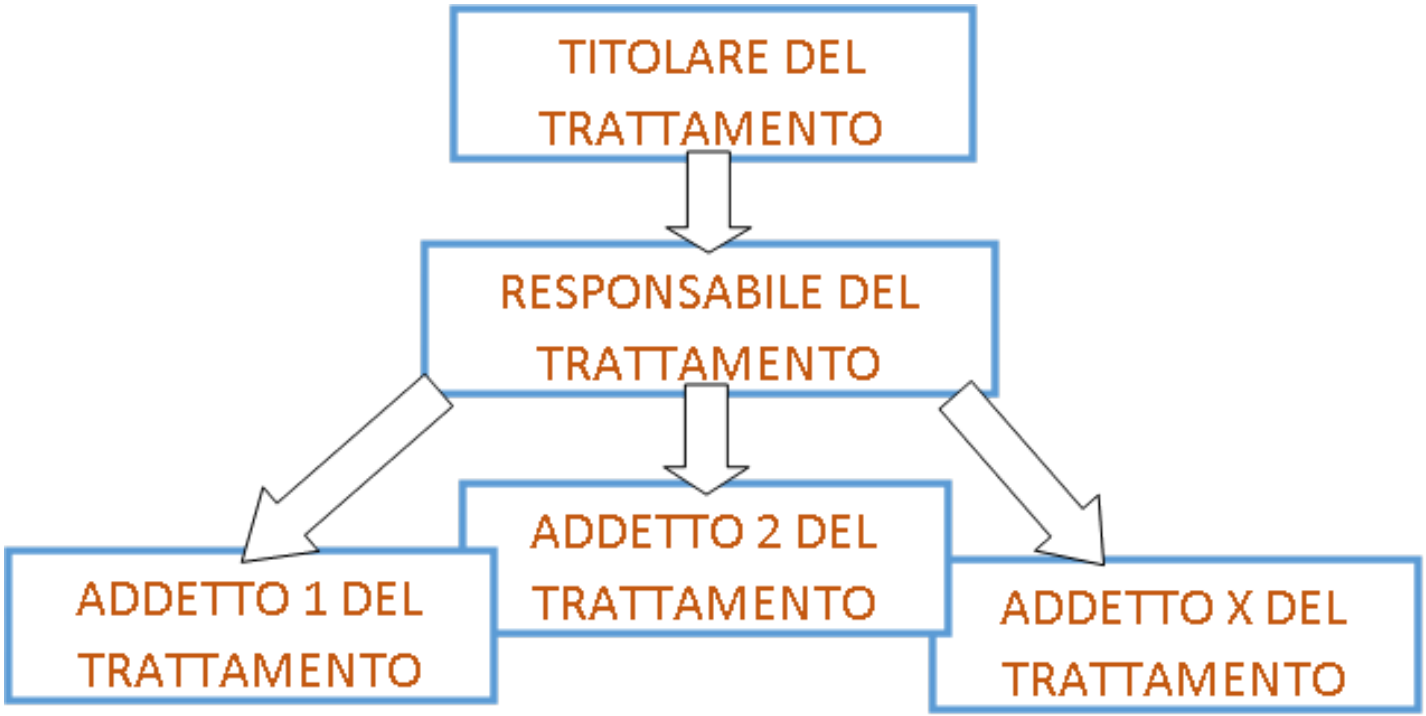
Quattro macro argomenti da conoscere

Per comprendere al meglio il nuovo Regolamento privacy, ed applicarlo operativamente, è necessario concentrarsi su quattro macro argomenti:

- Titolare del Trattamento ed organizzazione interna;
- Valutazione del rischio e relative Misure di adeguamento Privacy;
- Informative privacy ed eventuale Consenso;
- Registro dei trattamenti.

L'osservanza degli adempimenti descritti nei punti sopra riportati permette di risultare "conformi" alla normativa GDPR.

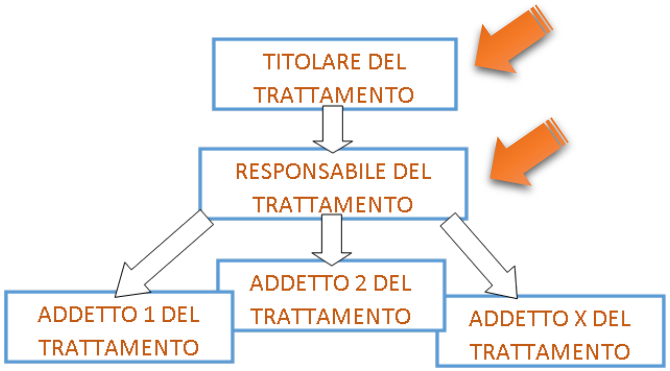
Titolare del trattamento e organizzazione



Titolare del trattamento

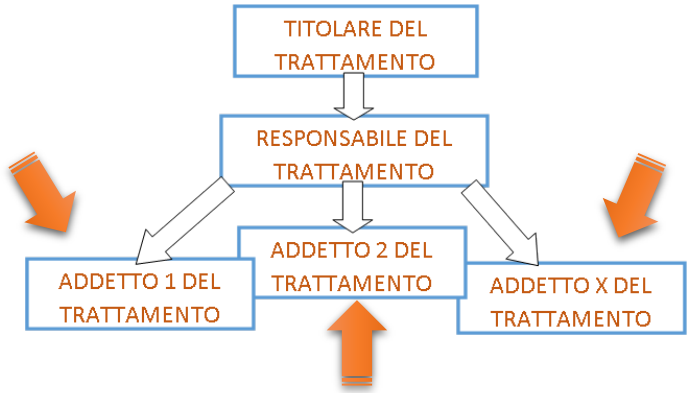
- Il Titolare del trattamento è **individuato** e non è nominato. In effetti è il titolare/responsabile dell'impresa. E' una persona fisica, ma può essere anche una figura giuridica, ente o associazione che determina modalità e le finalità del Trattamento ed i relativi profili di sicurezza.
- Il **Titolare del trattamento** mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. (art.24)

Il Titolare del trattamento può pertanto affidare i propri dati a responsabili interni per raggiungere al meglio gli obiettivi imposti dalla normativa (Principio di «Accountability»)



Incaricato del trattamento

- Ogni Responsabile (o Titolare nel caso di mancanza del Responsabile) potrà poi avvalersi di **Incaricati al trattamento** (solo persone fisiche) che dovranno essere formalmente nominate per iscritto e quindi debitamente formate a garanzia del rispetto delle procedure previste a livello organizzativo, e quindi coerenti con il dettato normativo.
- La nomina deve ovviamente individuare l'ambito di trattamento consentito.



Procedure e Formazione

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 pertanto 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. (Art. 29)

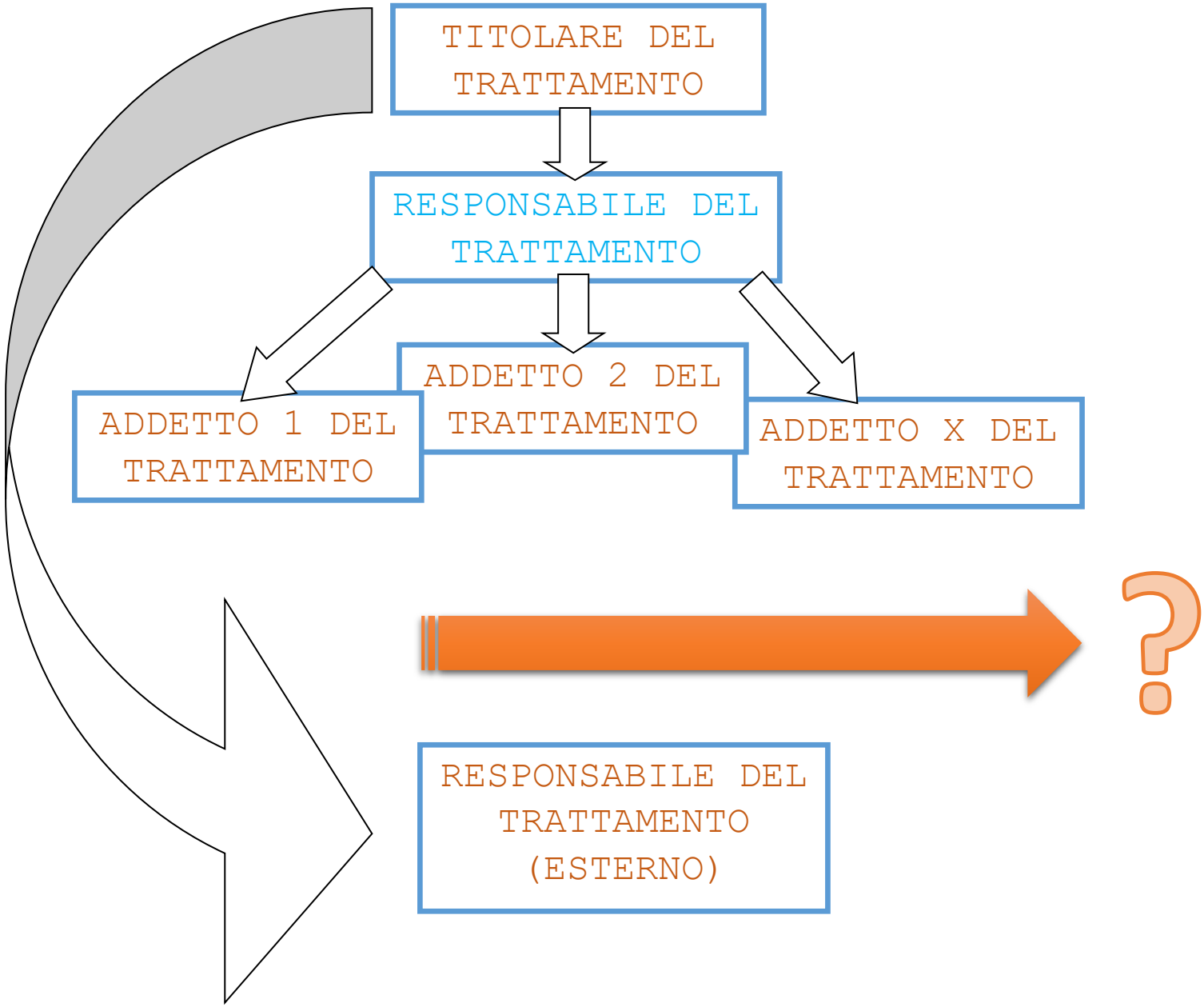
*Si consiglia di riportare sulla lettera di incarico i riferimenti di eventuali documento sulla sicurezza dei dati personali con le istruzioni operative (o relativi riferimenti), documenti che diventano parti integranti del Registro dei trattamenti. La stesura di un **Disciplinare tecnico** e consigliato anche per regolare il rapporto con la propria forza lavoro anche per quanto riguarda il lavoro stesso.*

Responsabile del trattamento esterno

- Il Titolare del trattamento può nominare un **Responsabile del trattamento**, soggetto al quale affida il trattamento dei dati (Art. 28) e che può essere persona giuridica o fisica.
- Risponde in solido con il Titolare nel caso di violazioni e il suo operato deve essere garantito sulla base di uno specifico contratto o atto giuridico che deve risultare pertanto vincolante per il Responsabile rispetto al Titolare. Deve pertanto risultare definita la durata, la natura e le finalità del trattamento affidato, il tipo di dati personali e le categorie dei soggetti interessati e risulti altresì definiti gli obblighi e i diritti del Titolare del trattamento.

Il Titolare del trattamento può pertanto affidare i propri dati a responsabili che presentino garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti previsti dal Regolamento e garantisca la tutela dell'interessato.

Es. Commercialisti, tecnici, strutture terze, eccetera.


TITOLARE DEL TRATTAMENTO
RESPONSABILE DEL TRATTAMENTO
ADDETTO 1 DEL TRATTAMENTO
ADDETTO 2 DEL TRATTAMENTO
ADDETTO X DEL TRATTAMENTO
?
RESPONSABILE DEL TRATTAMENTO (ESTERNO)

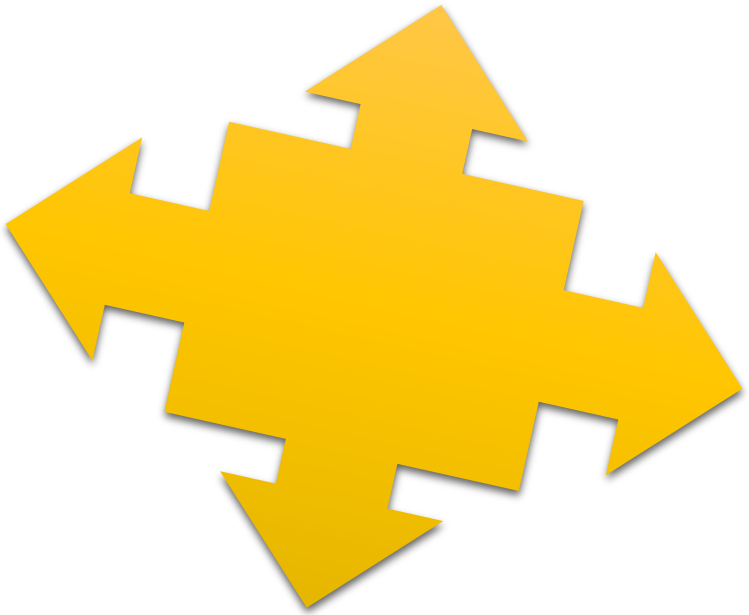
Come raggiungere la «compliance» GDPR

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. (Art.32)

9 passi per la «compliance» GDPR

1) *CONOSCERE IL PROPRIO BUSINESS*

In base al principio di “Accountability” (Responsabilizzazione), i Titolari del trattamento devono mettere in atto tutte le misure tecniche e organizzative necessarie per assicurare, ed essere in grado di dimostrare, che la raccolta e l’utilizzo dei dati siano conformi alle nuove regole.



9 passi per la «compliance» GDPR

2) *MAPPATURA DEI TRATTAMENTI*

La mappatura avviene attraverso un'analisi del proprio modello organizzativo, verificando come all'interno della propria organizzazione vengono gestiti i dati.

- *Che TIPI di dati raccolgo?*
- *PERCHÈ li raccolgo?*
- *DOVE archivio i dati?*
- *CHI ha accesso a questi dati della mia organizzazione o soggetti terzi?*
- *Posso MINIMIZZARE l'uso e/o la raccolta?*
- *Per QUANTO TEMPO vengono conservati presso la mia organizzazione?*
- *Vengono rispettati i diritti privacy degli interessati?*

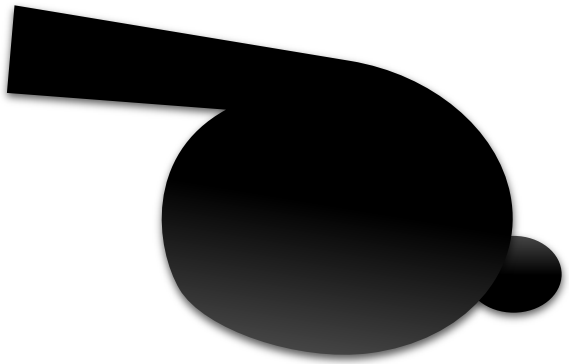
Alcuni esempi di attività:

- Effettuare la mappatura delle banche dati: dovrò analizzare quali dati sono presenti e quali banche dati sono conservate e dove (in pc locali, tablet o in rete);
- Quali dati vengono trattati a livello informatico e quali a livello cartaceo;
- Quali dati sono raccolti obbligatoriamente per motivi di legge e quali per attività di marketing;

9 passi per la «compliance» GDPR

3) ANALISI DEI RISCHI

Una volta mappati i dati è necessario individuare COSA MANCA (GAP ANALYSYS) per colmare eventuali mancanze e rendere adeguate le procedure operative con le disposizioni previste dal Regolamento in termini di trattamento, sicurezza e protezione, che non prevede il concetto di “misure minime previste”.



9 passi per la «compliance» GDPR

4) ADOZIONE MISURE IDONEE

Il Regolamento non fornisce indicazioni precise su quali siano le misure pratiche e minime da adottare (a differenza del precedente Codice della Privacy): l'approccio dovrà essere valutato caso per caso, tenendo in considerazione la natura, l'ambito di applicazione, il contesto e le finalità del trattamento.

Alcuni esempi:

- 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;
- Predisporre procedure serie di backup
- eccetera eccetera.

SIA A LIVELLO INFORMATICO SIA TRADIZIONALE

Art.32

*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, che comprendono, tra le altre, **se del caso**:*

- *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.*

9 passi per la «compliance» GDPR

5) PORTABILITA' DEI DATI, DIRITTO DI MODIFICA E DI CANCELLAZIONE

Il diritto alla portabilità dei dati, che consente all'interessato di richiedere al titolare i propri dati in formato strutturato e leggibile da un elaboratore automatico, dovrà essere gestito e quindi messo a disposizione degli interessanti. Anche in questo caso è necessario dotarsi di una procedura per la "Portability".

Analogamente anche il diritto di modifica e di cancellazione deve essere garantito all'interessato attraverso una procedura specifica.

9 passi per la «compliance» GDPR

6) ADOZIONE DI PROCEDURE DI DATA BREACH (PERDINA DEI DATI)

L'Analisi dei rischi non è sufficiente ad evitare il verificarsi di una violazione dei dati personali: nel caso di perdita dei dati il Titolare del trattamento ha il dovere di comunicare la violazione all'autorità di controllo (il Garante della privacy nazionale) entro 72 ore dal momento in cui ne è venuto a conoscenza.

Per questo è necessario dotarsi di una specifica procedura per la gestione del "Data Breach" da riportare nel Registro dei trattamenti.

9 passi per la «compliance» GDPR

7) AGGIORNAMENTO DELLE INFORMATIVE

L'aggiornamento delle informative è una fase cruciale in quanto regola il rapporto con gli interessati e permette l'acquisizione dei dati.

E' importante ricordare la differenza tra i dati personali raccolti necessariamente per lo svolgimento del proprio lavoro o per legge, e quelli raccolti per attività di profilazione e marketing.

Inoltre ai dipendenti dovrà essere consegnata la relativa informativa sul trattamento dei loro dati.

Informativa standard

Nel momento in cui i dati personali sono ottenuti, il Titolare fornisce all'interessato, in particolare, le seguenti informazioni (Art.13):

- l'identità e i dati di contatto del Titolare del trattamento;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- qualora il trattamento sia basato sul consenso, l'esistenza del diritto di revocare il consenso in qualsiasi momento;
- il diritto 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 l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati.

9 passi per la «compliance» GDPR

8) LETTERE DI INCARICO PER DIPENDENTI, CONSULENTI E SOGGETTI TERZI

Eventuali Responsabili del trattamento e Incaricati del trattamento dovranno essere incaricati con specifica "lettera" con riportate tutte le necessarie indicazioni per il corretto svolgimento del proprio lavoro, garantendo così che il trattamento, la protezione e la conservazione dei dati possa avvenire seguendo i dettami indicati dal Titolare del trattamento a norma di Regolamento.

I dipendenti o i coadiuvanti (soci, familiari o altri che hanno accesso ai dati) sono:

- soggetti che trattano i dati per conto del Titolare;
- persone fisiche di cui i dati sono trattati dal Titolare tratta i dati.

9 passi per la «compliance» GDPR

9) COMPLETAMENTO DEL REGISTRO DEI TRATTAMENTI

Il documento deve riportare tutte le azioni da eseguire, da chi (definizione ruoli e competenze), in che modo e in che tempi, la documentazione da produrre, le comunicazioni interne ed esterne, gli interventi infrastrutturali sia a livello informatico che di sicurezza tradizionale, ed infine la formazione e la consulenza ai responsabili ed al personale.

Cartaceo o Digitale

Registro dei trattamenti

Ogni **Titolare del trattamento** deve conservare ed aggiornare un registro delle attività di trattamento svolte sotto la propria responsabilità (Art.30). Tale registro deve contiene tutte le seguenti informazioni:

- il nome e i dati di contatto del Titolare del trattamento;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

Ogni **Responsabile del trattamento** deve conservare ed aggiornare un registro di tutte le categorie di attività relative al trattamento svolte per conto del Titolare, contenente:

- il nome e i dati di contatto del Responsabile e di ogni Titolare per conto del quale agisce;
- le categorie dei trattamenti effettuati per conto del Titolare del trattamento;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Art.24

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ***ed essere in grado di dimostrare****, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.*

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del Titolare del trattamento.

Documentazione per la «compliance»

Il Registro dei trattamenti fa parte di una più complessa e completa documentazione che comprende:

- INFORMAZIONI GENERALI del Titolare dei trattamenti
- REGISTRO DEI RESPONSABILI E INCARICATI
- REGISTRO INTERVENTI FORMATIVI
- MAPPATURA DEI TRATTAMENTI (REGISTRO DEI TRATTAMENTI VERO E PROPRIO)
- ANALISI DEI RISCHI CHE INCOMBONO SUI DATI
- MISURE DI SICUREZZA ADOTTATE
- PROCEDURE OPERATIVE GDPR (PORTABILITA', MODIFICA E CANCELLAZIONE)
- DATA BREACH E RIPRISTINO DEI DATI

- DISCIPLINARE OPERATIVO
- ELENCO DOCUMENTAZIONE PRIVACY (INFORMATIVE, NOMINE eccetera)

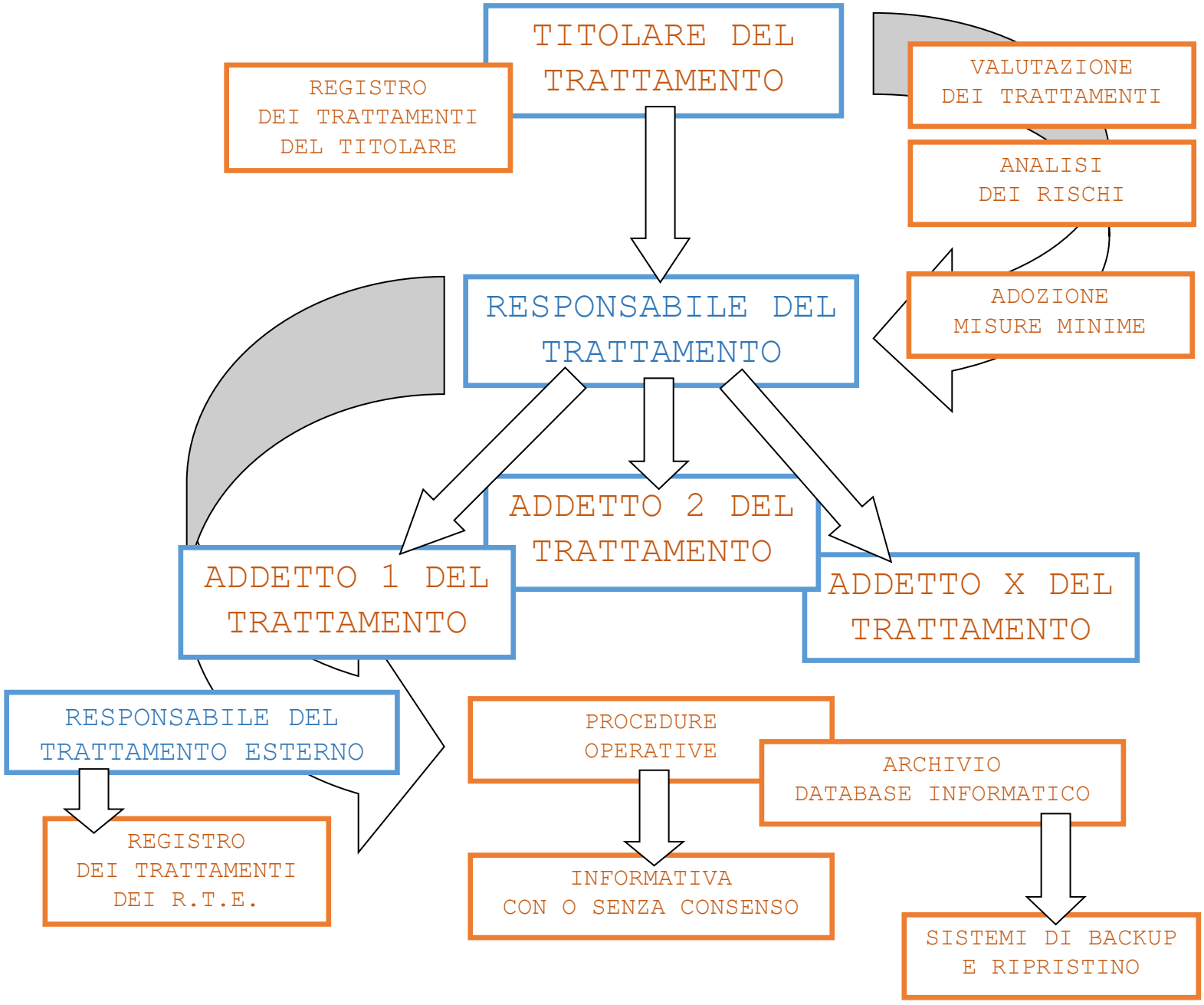
Misure di sicurezza «consigliate»

TRATTAMENTO DATI A LIVELLO DIGITALE:

- crittografia
- procedure di autenticazione
- utilizzo di password «serie» con scadenza ogni tre mesi
- attivazione di account diversificati
- integrazione di sistemi hardware di protezioni di rete (firewall)
- politiche di aggiornamento delle applicazioni
- installazione protezioni software (anti virus, anti malware)
- esecuzione di backup programmati
- limitazione utilizzo internet, social ed email

TRATTAMENTO DOCUMENTALE CARTACEO:

- chiusura a chiave delle porte
- organizzare la documentazione in archivi non accessibili da terzi
- evitare di lasciare documenti incustoditi
- regolamentare l'utilizzo di sistemi hardware trasportabili


TITOLARE DEL TRATTAMENTO
REGISTRO DEI TRATTAMENTI DEL TITOLARE
VALUTAZIONE DEI TRATTAMENTI
ANALISI DEI RISCHI
ADOZIONE MISURE MINIME
RESPONSABILE DEL TRATTAMENTO
ADDETTO 1 DEL TRATTAMENTO
ADDETTO 2 DEL TRATTAMENTO
ADDETTO X DEL TRATTAMENTO
RESPONSABILE DEL TRATTAMENTO ESTERNO
REGISTRO DEI TRATTAMENTI DEI R.T.E.
PROCEDURE OPERATIVE
ARCHIVIO DATABASE INFORMATICO
INFORMATIVA CON O SENZA CONSENSO
SISTEMI DI BACKUP E RIPRISTINO

Per saperne di più

- Regolamento europeo (EU) 2106/679
  https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679
- https://www.garanteprivacy.it/

Grazie

Stefano Bertani

Regolamento europeo (EU) 2106/679
Documento aggiornato al 31 dicembre 2018