Claudia Carimini
Manager Privacy – AGM – GRC Team

La nuova privacy:
dal Codice

Panoramica del Regolamento: le novità rilevanti ai fini della compliance

- Ambito di applicazione territoriale
- Accountability del titolare
- Data protection by design e by default
- Conservazione dei dati - Diritto all'oblio - Portabilità dei dati
- Ridefinizione dei ruoli organizzativi e della responsabilità tra ruoli
- I Registri delle attività di trattamento
- Sicurezza addizionale di misure tecniche e organizzative adeguate
- Valutazione d'impatto sulla protezione dei dati
- Obbligo di notifica di una violazione dei dati personali
- Codici di condotta e meccanismi di certificazione dei trattamenti
- Responsabilità solidale di titolare e responsabile
- Entità delle sanzioni

Le tre tappe della
Data Protection

1. La Direttiva comunitaria 95/46/CE, principi generali e normative nazionali (c.d. "Direttiva madre")
2. Le Direttive comunitarie 2002/58/CE e 2009/136/UE relative al trattamento dei dati personali nel settore delle comunicazioni elettroniche (cookie law e email marketing)
3. Il Regolamento UE 2016/679 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/GDPR): un **regolamento** e non una direttiva.

Il Quadro normativo

Regolamento 2016/679	**IN VIGORE,** pienamente applicabile dal 25 maggio 2018
Direttiva 1995/46	**IN VIGORE,** decade il 24 maggio 2018
Codice D.Lgs. 196/2003	**A OGGI IN VIGORE,** dovrebbe essere ABROGATO
Provvedimenti Autorità Garante	**IN VIGORE, NON DECADONO,** fino a quando non verranno 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

Oggetto e finalità

Il Regolamento stabilisce norme

1. relative alla protezione delle **persone fisiche** con riguardo al trattamento dei loro **dati personali**
2. per la libera circolazione di tali dati (Art.1)

Non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome, la forma e i suoi dati contatto (c. 14)

Ai fini del regolamento per "**dato personale**" si intende 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**.

Ambito di applicazione materiale

Il Regolamento si applica:

- al **trattamento automatizzato** di dati personali
- al **trattamento NON automatizzato** di dati personali contenuti in un **archivio**

In particolare per il caso di "trattamenti non automatizzati" il c.15 specifica che non rientrano nell'ambito di applicazione del GDPR i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine.

ES.: Gli appunti presi su una agenda cartacea non suddivisa per criteri specifici, non destinata ad archiviazione, non rientrano nell'applicazione della norma.

Nuovo ambito di applicazione territoriale

1. Il regolamento si applica al trattamento di dati personali effettuato da un **Titolare** o da un **Responsabile stabilito** nell'Unione anche se il trattamento è effettuato **fuori dall'Unione**
2. Il regolamento si applica al trattamento dei dati personali di residenti nell'Unione Europea effettuato da un **Titolare** o da un **Responsabile anche non stabilito nell'Unione Europea**, quando le attività di trattamento riguardano:
   a. l'offerta di beni o la prestazione di servizi ai cittadini residenti nell'Unione Europea
   b. il controllo del loro comportamento nell'Unione

E' un grande cambiamento rispetto alla regola precedente in base alla quale la normativa applicabile è quella del luogo in cui ha sede il titolare del trattamento

I tre pilastri della Data Protection

1. Il principio di "**accountability**"
2. Il criterio della "**privacy by design e by default**"
3. L'approccio basato sul **rischio**

ACCOUNTABILITY

Il principio di **accountability** – "responsabilizzazione" è inserito all'interno dell'art. 5 del regolamento "Principi applicabili al trattamento di dati personali"

Vengono richiamati i **principi generali**, che hanno valenza per ogni aspetto della disciplina e devono essere rispettati in ogni fase del trattamento. Sono sostanzialmente i principi già elencati all'art. 11 del Codice

- Liceità correttezza e trasparenza
- Limitazione delle finalità
- Minimizzazione dei dati
- Esattezza
- Limitazione della conservazione
- Integrità e riservatezza

"Il Titolare del trattamento è competente per il rispetto del paragrafo 1 ed in grado di dimostrarlo"

(art. 5.2)

ACCOUNTABILITY

E ancora

"Il Titolare del trattamento mette in atto misure tecniche ed organizzative **adeguate** per **garantire** ed **essere in grado di dimostrare** che il trattamento è effettuato conformemente al presente regolamento" (art. 24)

Deve essere dimostrata la **sostanza** degli adempimenti non il rispetto formale

Inoltre **non basta aver adempiuto** alle richieste normative, ma **occorre essere in grado di dimostrarlo**

ACCOUNTABILITY

=

RESPONSABILIZZAZIONE

"adozione di **comportamenti proattivi** e tali da dimostrare la **concreta attuazione** di misure finalizzate ad assicurare l'applicazione del Regolamento" (Guida all'applicazione del Regolamento UE)

PRIVACY BY DESIGN E PRIVACY BY DEFAULT

Al fine di poter dimostrare la **conformità** con il presente regolamento il titolare adotta **politiche interne** e attua **misure** che soddisfano in particolare i principi della **protezione dei dati fin dalla progettazione** e della **protezione dei dati di default.**

Questo implica la necessità di configurare il trattamento prevedendo **fin dall'inizio** le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, **tenendo conto del contesto complessivo** ove il trattamento si colloca **e dei rischi** per i diritti e le libertà degli interessati.

Tali misure potrebbero consistere, **tra l'altro**, nel:

- **ridurre al minimo** il trattamento dei dati personali
- **pseudonimizzare** i dati il più presto possibile
- offrire **trasparenza** sul trattamento
- consentire all'interessato di **controllare** i suoi dati
- migliorare le condizioni di **sicurezza**

RISK BASED APPROACH

Il rischio inerente al trattamento è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.

All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

Nuova forma e contenuto dell'informativa

In base al principio di **trasparenza**, va resa in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

Le informazioni sono fornite **per iscritto** o con altri mezzi, se del caso in formato elettronico.

Dovrà essere precisato il **periodo di conservazione** dei dati personali oppure, se non possibile, i criteri utilizzati per determinare questo periodo.

Dovrà essere indicata l'esistenza di un processo decisionale automatizzato, compresa la **profilazione**.

Se i dati non sono stati raccolti presso l'interessato dovrà essere indicata **l'origine** del dato.

Specificare i dati di contatto del DPO (se nominato)

Specificare sei dati personali vengono trasferiti in **paesi terzi**

Nuova forma e contenuto del consenso

- **Specifico e informato**

  Un consenso per ogni finalità

  Preceduto dall'informativa

- **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 (onere della prova)

- **Esplicito**

  Solo per il trattamento dei dati particolari e per la profilazione

  All'interno di un contratto scritto la richiesta di consenso deve essere presentata in modo chiaramente distinguibile e con un linguaggio semplice e chiaro

- **Facilità di revoca**

Nuovi diritti riconosciuti all'interessato

Vengono ampliati istituti già noti (accesso, rettifica, opposizione) ed introdotti nuovi diritti, con il chiaro obiettivo di rafforzare i diritti dell'interessato fondati sul principio di trasparenza. In particolare:

- Diritto alla **cancellazione** (diritto all'oblio) inteso come il diritto dell'interessato di ottenere dal titolare la cancellazione dei dati personali che lo riguardano in presenza di particolari condizioni

- Diritto di **limitazione di trattamento**, con cui l'interessato può chiedere una restrizione del trattamento (ad es. la sola conservazione dei dati con esclusione di qualsiasi altro utilizzo)

- Diritto alla **portabilità** dei dati, definito "il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e di trasmettere tali dati a un altro titolare senza impedimenti"

Nuovi diritti riconosciuti all'interessato

Richieste del regolamento

- Il titolare adotta misure appropriate per fornire all'interessato tutte le informazioni
- in forma concisa, trasparente, chiara, facilmente accessibile
- senza ingiustificato ritardo e al più tardi entro un mese
- il titolare agevola l'esercizio dei diritti dell'interessato, anche per via elettronica
- se possibile, fornisce l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali

Il Garante raccomanda che i titolari adottino le **misure tecniche e organizzative** necessarie per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati, che – a differenza di quanto attualmente previsto – dovrà avere per impostazione predefinita forma scritta (anche elettronica).

Ridefinizione dei **ruoli organizzativi** e della **responsabilità** tra ruoli

I ruoli privacy previsti: Il Titolare (Data Controller)
Il Responsabile (Data Processor)
Le persone autorizzate: incaricati e responsabili

I Contitolari del trattamento (Joint controllers) → **accordo interno**

Maggior enfasi su ruolo e responsabilità del Responsabile:

- criteri di scelta (responsabilità in eligendo)
- **contratto scritto**
- istruzioni documentate da seguire («titolare» se non rispetta)
- **la possibilità di nomina di sub-responsabili**
- il dovere di informazione del responsabile (responsabile in solido)
- aiutare il titolare ad evadere le richieste degli interessati

Il Responsabile della Protezione dei Dati – DPO

IL Titolare del Trattamento Dati
art. 24

- ✓ Regolamentazione contrattuale dei ruoli e delle responsabilità per i soggetti coinvolti nel trattamento (Contitolari, Responsabili; DPO)
- ✓ Nomina di un Data Protection Officer (Obbligatoria solo in alcuni casi)
- ✓ Attuazione di politiche adeguate in materia di protezione dei dati
- ✓ Informativa privacy da fornire agli interessati e gestione corretta dei consensi
- ✓ Adeguato riscontro ai soggetti interessati che esercitano i propri diritti

IL Titolare del Trattamento Dati

Protezione dei dati in base ai rischi

- ✓ Rispetto dei principi **Privacy by Design e Privacy by Default**
- ✓ Valutazione d'impatto, obbligatoria per i trattamenti che comportano rischi
- ✓ Implementazione di adeguate misure di sicurezza atte a ridurre i rischi
- ✓ Consultazione preventiva all'Autorità di Controllo, ove necessario
- ✓ Notificazione delle violazioni di dati personali (**Data Breach**) all'Autorità ed agli interessati

IL Titolare del Trattamento Dati

Principio di ACCOUNTABILITY

- ✓ Obbligo di dimostrare il rispetto a tutti i requisisti posti dal Regolamento, di rendere conto delle azioni svolte in materia di trattamento dei dati personali e di rispondere delle conseguenze
- ✓ Mantenere aggiornato un Registro delle Attività Svolte
- ✓ Attestazione della corretta raccolta dei consensi degli interessati
- ✓ Ricorso facoltativo a codici deontologici e a meccanismi di certificazioni
- ✓ Responsabilità diretta in caso di richiesta di risarcimento del danno

IL Responsabile del Trattamento Dati
art. 28

- Tenere i dati personali eseguendo le istruzioni fornite dal Titolare
- Assicurare che le persone autorizzate a trattare i dati personali si siano impegnate a rispettare vincoli di riservatezza
- Implementare e mantenere tutte le misure tecniche ed organizzative adeguate
- Rendersi disponibile ad audit di verifica da parte del titolare del trattamento
- Assistere il titolare del trattamento per la gestione delle richieste di diritto d'accesso e per gli altri obblighi imposti dal Regolamento
- Su richiesta del titolare cancellare o restituire i dati personali al termine del trattamento

IL Responsabile del Trattamento Dati

- Fornire al titolare qualsiasi informazione necessaria per dimostrare il rispetto del Regolamento
- Tenere un registro delle categorie di attività di trattamento dei dati personali svolte per conto del titolare del Trattamento
- Avvertire il Titolare del Trattamento immediatamente dopo aver riscontrato il verificarsi di una violazione dei dati
- Cooperare con l'Autorità di Vigilanza
- Designare un Responsabile della Protezione dei Dati (DPO), nei casi in cui è richiesto

Il DPO – Responsabile della protezione dei dati

Gli obblighi di nomina

a) amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;

b) tutti i soggetti la cui 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;

c) tutti i soggetti la cui 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.

Un gruppo di imprese o più soggetti pubblici possono nominare un unico Responsabile della protezione dei dati.

Un titolare del trattamento o un responsabile del trattamento possono comunque designare un Responsabile della protezione dei dati personali anche in casi diversi da quelli sopra indicati.

Il DPO – Responsabile della protezione dei dati

Non un semplice responsabile del trattamento ma il "vigilante" del trattamento dei dati

I requisiti

Il Responsabile della protezione dei dati personali, nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:

1. possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;
2. adempiere alle sue funzioni in piena indipendenza ed in assenza di conflitti di interesse;
3. operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio.

Il titolare o il responsabile è tenuto a pubblicare i dati di contatto del responsabile della protezione dei dati ed a comunicarli all'autorità di controllo.

Il DPO – Responsabile della protezione dei dati

Il responsabile della protezione dei dati personali dovrà:

I compiti

a) **informare** e **consigliare** il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) **verificare** l'attuazione e l'applicazione del Regolamento nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle **responsabilità**, la **formazione** del personale coinvolto nelle operazioni di trattamento, e gli **audit** relativi;
c) **fornire**, se richiesto, **pareri** in merito alla valutazione d'impatto sulla protezione dei dati e **sorvegliare** i relativi adempimenti;
d) fungere da **punto di contatto** per gli **interessati**;
e) cooperare e fungere da **punto di contatto** per l'Autorità di controllo

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento.

Obbligo di tenuta di nuove documentazioni

Il titolare ed il responsabile devono tenere i **registri delle attività di trattamento** effettuate

I registri sono richiamati nel contenuto minimo delle valutazioni d'impatto e sono funzionali alla definizione delle misure di sicurezza

Devono essere in forma scritta, anche in formato elettronico, e devono essere messi a disposizione dell'autorità di controllo

Il registro del Titolare

- Nome e dati di contatto del titolare, del contitolare, del rappresentante, del DPO
- Finalità del trattamento
- Descrizione delle categorie di interessati e delle categorie di dati
- Le categorie di destinatari cui i dati sono o saranno comunicati
- Eventuali trasferimenti di dati all'estero e garanzie adottate
- Tempi di cancellazione dei dati (termini ultimi previsti)
- Descrizione generale delle misure di sicurezza tecniche e organizzative adottate

Obbligo di tenuta di nuove documentazioni

Il responsabile tiene un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare

Registro del Responsabile

- Nome e dati di contatto del responsabile, di ogni titolare per conto del quale agisce, del rappresentante, del DPO
- Le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento
- Eventuali trasferimenti di dati all'estero e garanzie adottate
- Descrizione generale delle misure di sicurezza tecniche e organizzative adottate

Gli obblighi di tenuta del registro **non si applicano** alle imprese con **meno di 250 dipendenti**, fatta salva l'effettuazione di trattamenti rischiosi per i diritti e le libertà dell'interessato o di trattamenti relativi a categorie particolari di dati o dati personali relativi a condanne penali e a reati.
Le **raccomandazioni** del Garante nella Guida applicativa del 28 aprile 2017

Nuove misure di sicurezza dei dati (art.32)

"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"

Stato dell'arte e
costi di attuazione

Natura, oggetto, contesto e finalità del trattamento
Rischio per i diritti e le libertà dell'interessato

Adozione di misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio

Nuove misure di sicurezza dei dati (art.32)

Tali misure "adeguate" comprendono, **tra le altre**, **se del caso**:

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.

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 d'impatto DPIA e consultazione preventiva

Quando un **tipo di trattamento**, in base alla natura, l'oggetto, il contesto e le finalità del trattamento, **presenta un rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento effettua, prima di procedere al trattamento, una **valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.**

La valutazione d'impatto unitamente all'obbligo di tenuta dei registri sostituisce l'obbligo in generale di effettuare la notificazione all'autorità di controllo e si inserisce nel principio di accountability.

Si riconferma la scelta del regolamento di strategie di tutela sostanziale e non formale.

Se a seguito della valutazione d'impatto permangono rischi elevati il titolare deve richiedere una **verifica preliminare** all'autorità.

Obbligo di notifica di una violazione dei dati personali

Il regolamento generalizza l'obbligo di effettuare la notifica di una violazione dei dati personali, nel nostro ordinamento già prevista solo in alcuni settori

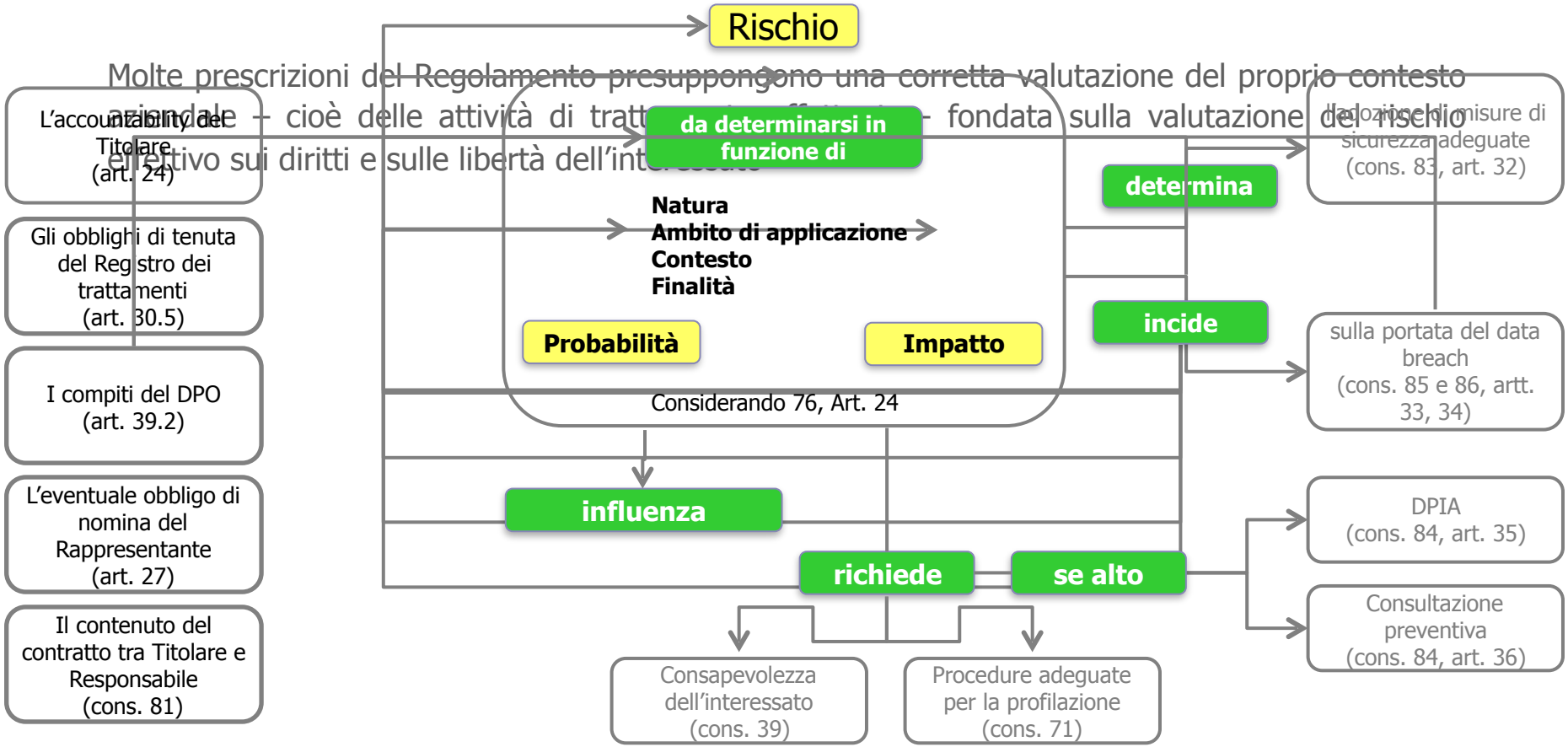
Si stabilisce l'obbligo per tutti i Titolari del trattamento di effettuare la notifica della violazione all'autorità di controllo entro 72 ore ma **soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati**

Tutti i titolari di trattamento dovranno in ogni caso **documentare le violazioni** di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati.

Obbligo di tenere un inventario delle violazioni

Cosa significa Risk based approach

Molte prescrizioni del Regolamento presuppongono una corretta valutazione del proprio contesto aziendale – cioè delle attività di trattamento effettuate – fondata sulla valutazione del rischio effettivo sui diritti e sulle libertà dell'interessato



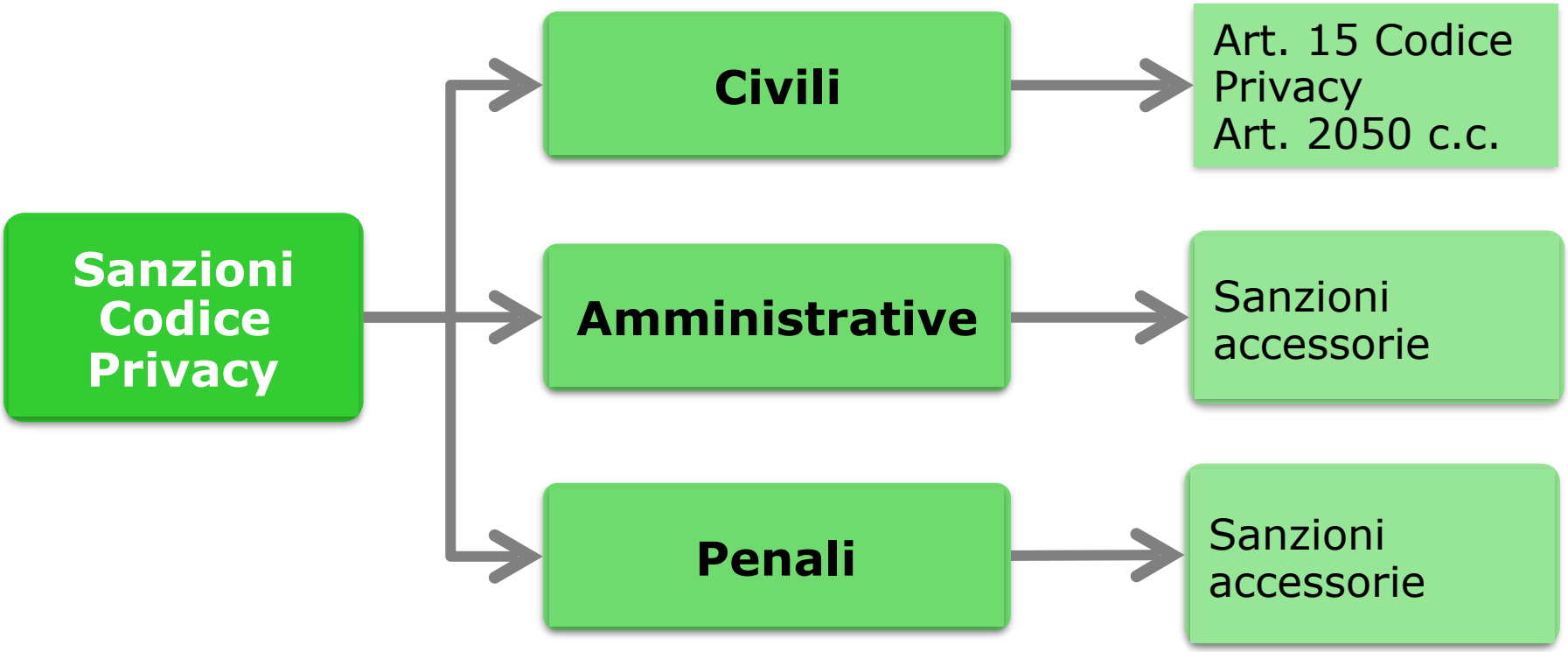
Codici di condotta e certificazioni

Altra novità introdotta dal regolamento: la possibilità di dimostrare il rispetto degli obblighi, la validità delle procedure e la solidità delle regole attraverso strumenti di "soft law" la cui adesione è volontaria:
codici di condotta, **meccanismi di certificazione**, **marchi di protezione dei dati**.

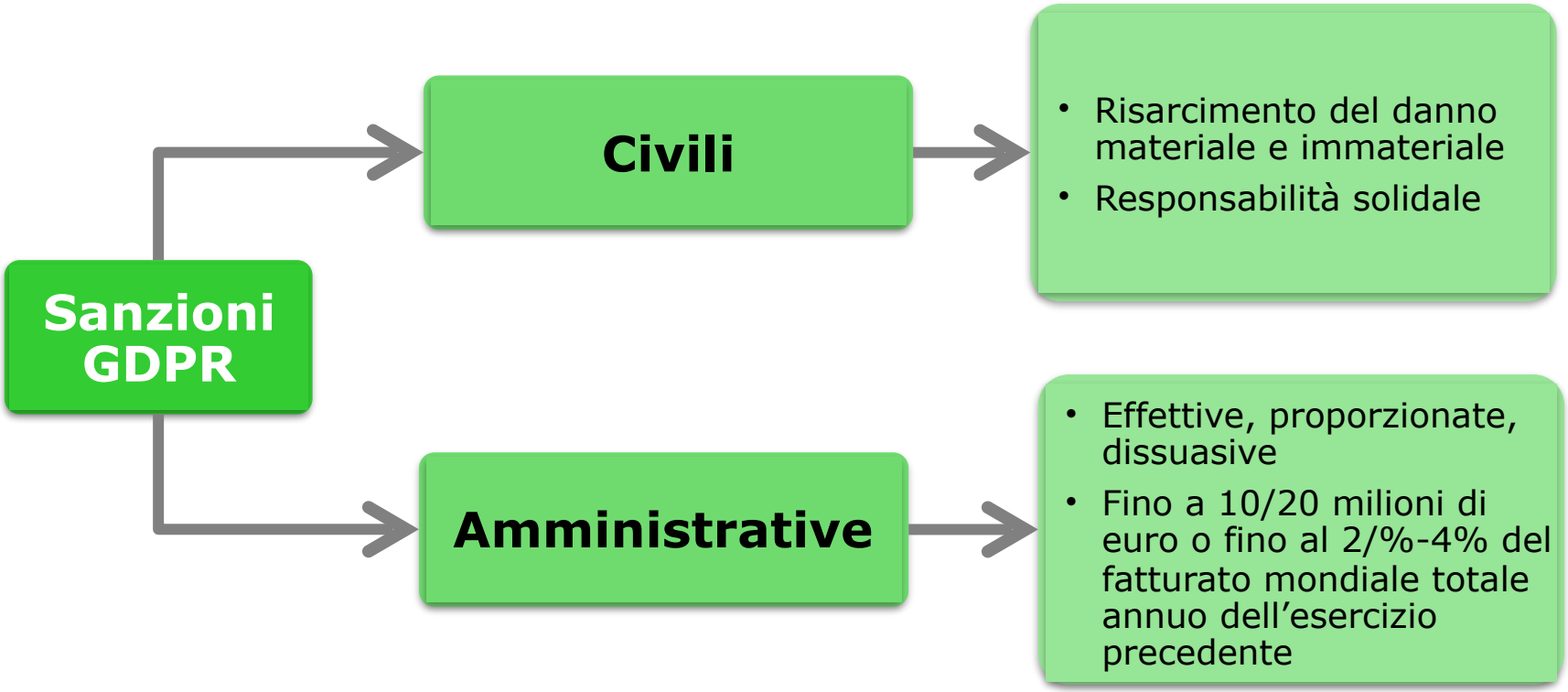
Sono intesi come mezzo per dimostrare l'affidabilità e la conformità del sistema privacy ai requisiti richiesti: valutazione d'impatto, privacy by design e by default, sicurezza del trattamento, qualità ed esattezza dei dati

Certificazioni e adesione a codici di condotta approvati non manlevano da responsabilità, ma forniscono un valido strumento di accountability

Attuale impianto sanzionatorio



Nuovo impianto sanzionatorio



Le **sanzioni** amministrative pecuniarie

1. Le violazioni agli obblighi in capo alle imprese (20 articoli su 49) sono punite **fino a 10 milioni di euro o fino al 2% del fatturato mondiale annuo**.

Ad esempio:

- la violazione dell'obbligo di tenuta del registro dei trattamenti;
- la mancata valutazione d'impatto DPIA;
- l'omessa consultazione preventiva dell'Autorità;
- l'omessa notifica di data breach;
- l'omessa nomina del DPO;
- l'omessa adozione di misure di sicurezza adeguate.

Le **sanzioni** amministrative pecuniarie

2. Gli altri 29 articoli puniscono **fino a 20 milioni di euro o fino al 4 % del fatturato mondiale annuo** la violazione dei principi del regolamento e dei diritti degli interessati.

Ad esempio:

- i principi di base del trattamento, comprese le condizioni relative al consenso;
- i diritti degli interessati;
- i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale;
- 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.

Quindi ?

Cosa fare **?**

Come **gestire la transizione** dalla vecchia alla nuova normativa **?**

Come strutturare il **progetto di adeguamento** al nuovo Regolamento**?**

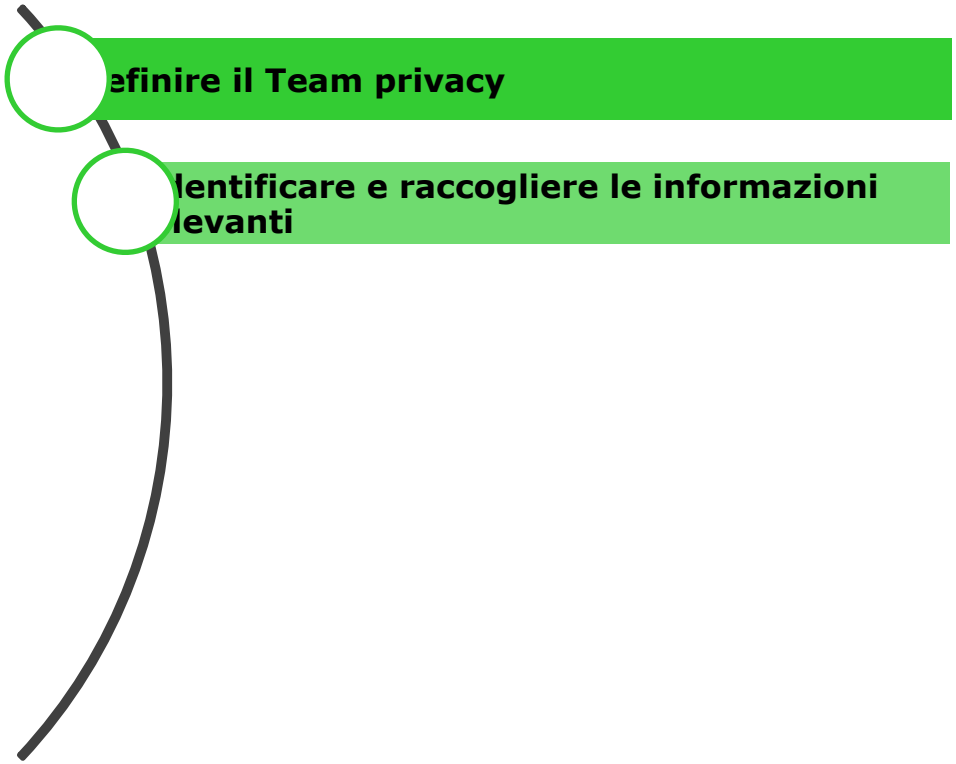
Il progetto GDPR

efinire il Team privacy

Creare il "Team privacy" per definire i criteri di trattamento dei dati e diffondere la cultura del dato in azienda.

Le nuove disposizioni delineano un quadro di cambiamento che impatta su più attori e richiede l'attivazione di un programma organico e trasversale, un vero Sistema di Governo della Privacy

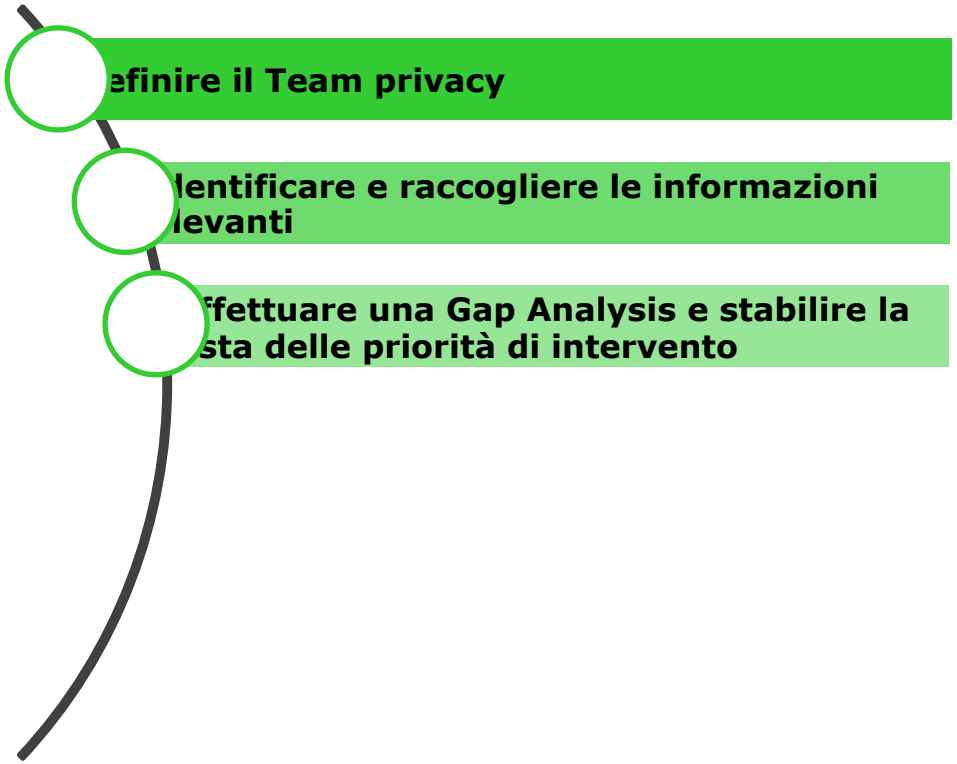
Il progetto GDPR



Occorre ripartire dalla mappatura dei trattamenti, identificando:

- Le tipologie di trattamenti effettuati;
- Le categorie di dati personali trattati;
- Le finalità di trattamento;
- I soggetti (interni e esterni) che trattano i dati, con particolare attenzione ai Data Processor;
- L'ambito di circolazione dei dati durante l'intero ciclo di vita dei dei trattamenti, per identificare e governare anche eventuali trasferimenti di dati al di fuori della UE.

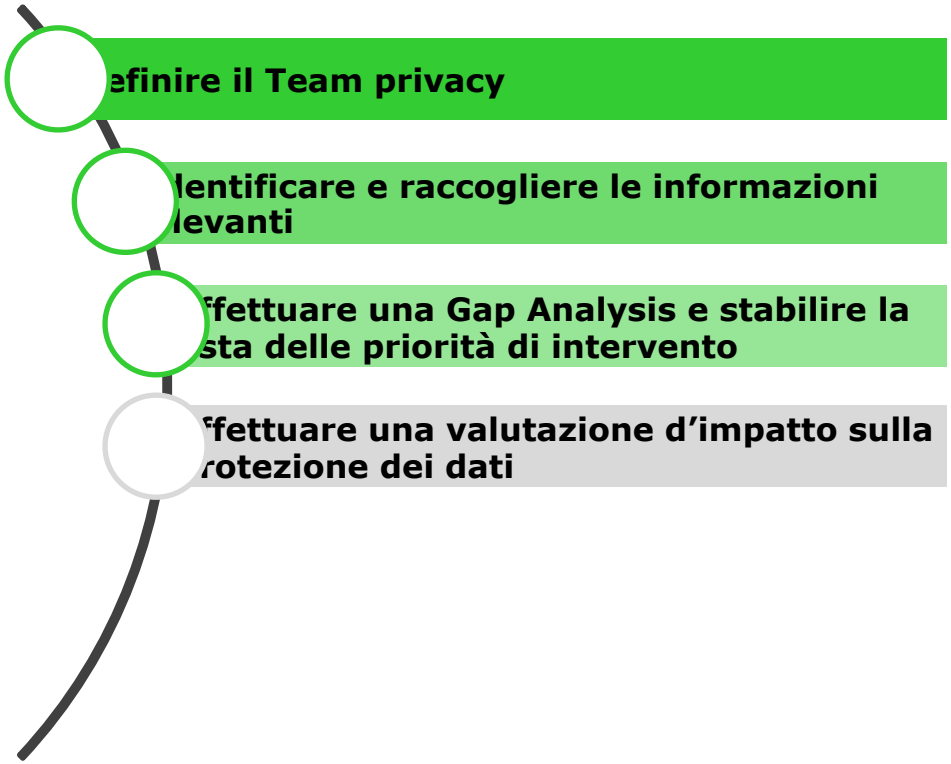
Il progetto GDPR



Gap Analysis e prioritizzazione degli interventi.

Occorre procedere ad un'autovalutazione della propria situazione aziendale rispetto alle previsioni della nuova normativa" (c.d. "gap analysis"), individuando le misure da adottare secondo un ordine di priorità degli interventi, da stabilire in funzione del livello di rischio sui diritti e sulle libertà degli interessati.

Il progetto GDPR

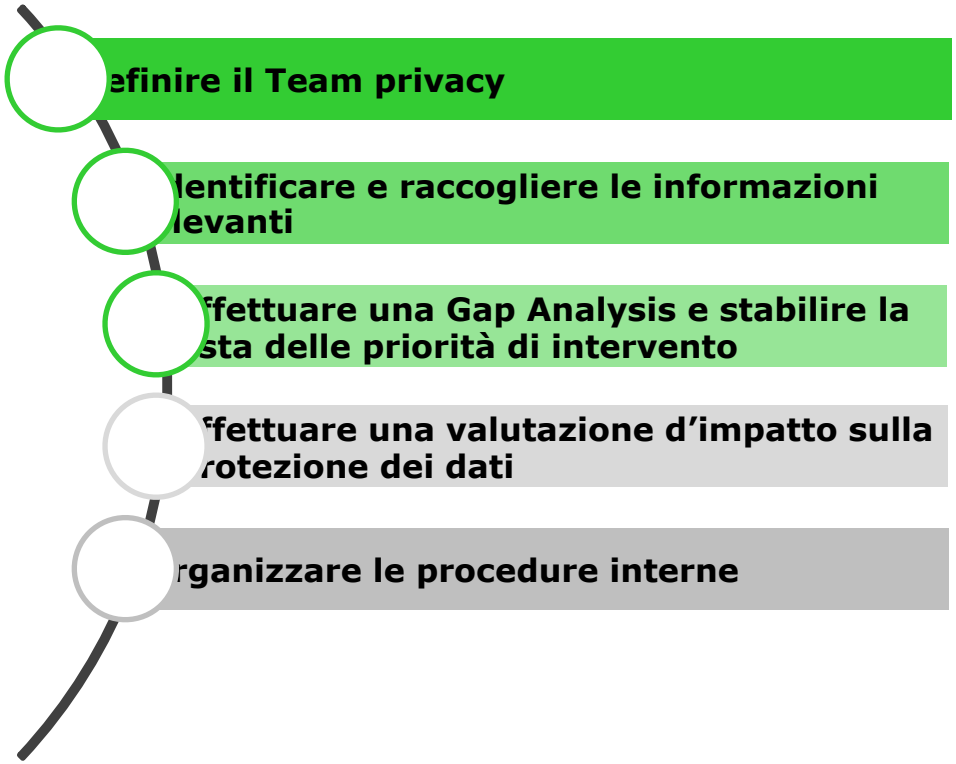


Fare (se richiesto) la DPIA, contenente

- una descrizione sistematica del trattamento e delle sue finalità,
- una valutazione della necessità e della proporzionalità del trattamento,
- una valutazione dei rischi per i diritti e le libertà delle persone,
- le misure previste per affrontare i rischi e dimostrare la conformità al regolamento

Prevedere un'attività di monitoraggio e verifica

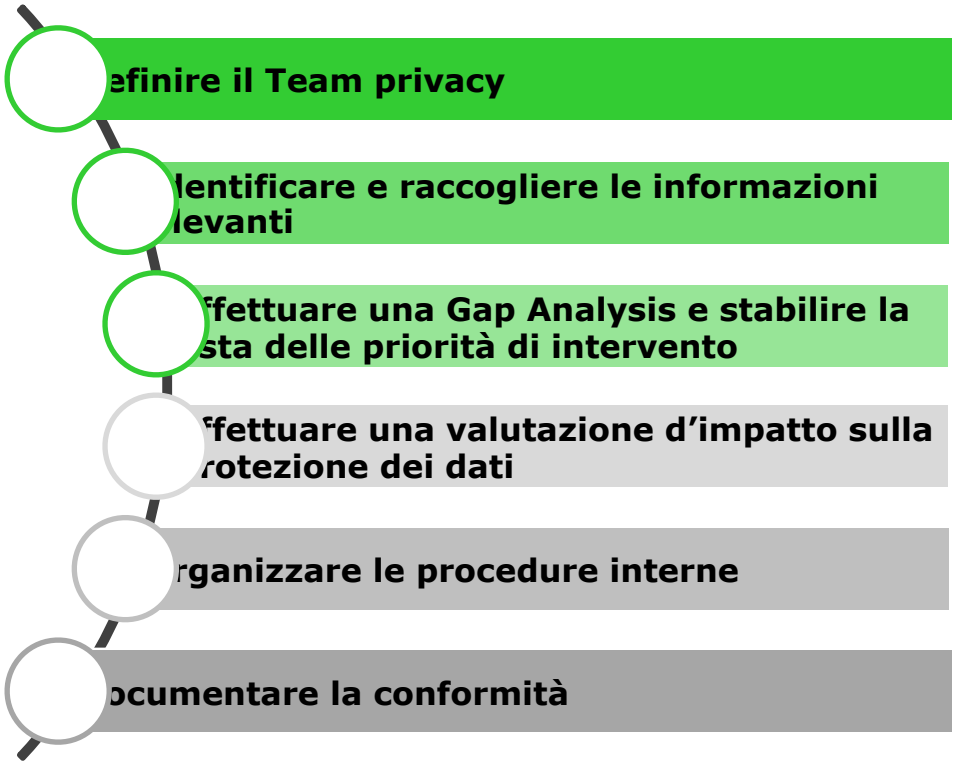
Il progetto GDPR



Organizzare le procedure interne in ottica PbD:

- procedure per rendere l'informativa agli interessati
- procedure per la raccolta del consenso
- procedure di risposta all'esercizio dei diritti degli interessati
- procedure di gestione dei data breach
- procedure per integrare la privacy nei prodotti e nei servizi aziendali (minimizzazione dei dati, policy di data retention)
- Procedure di formazione delle persone autorizzate al trattamento
- …

Il progetto GDPR

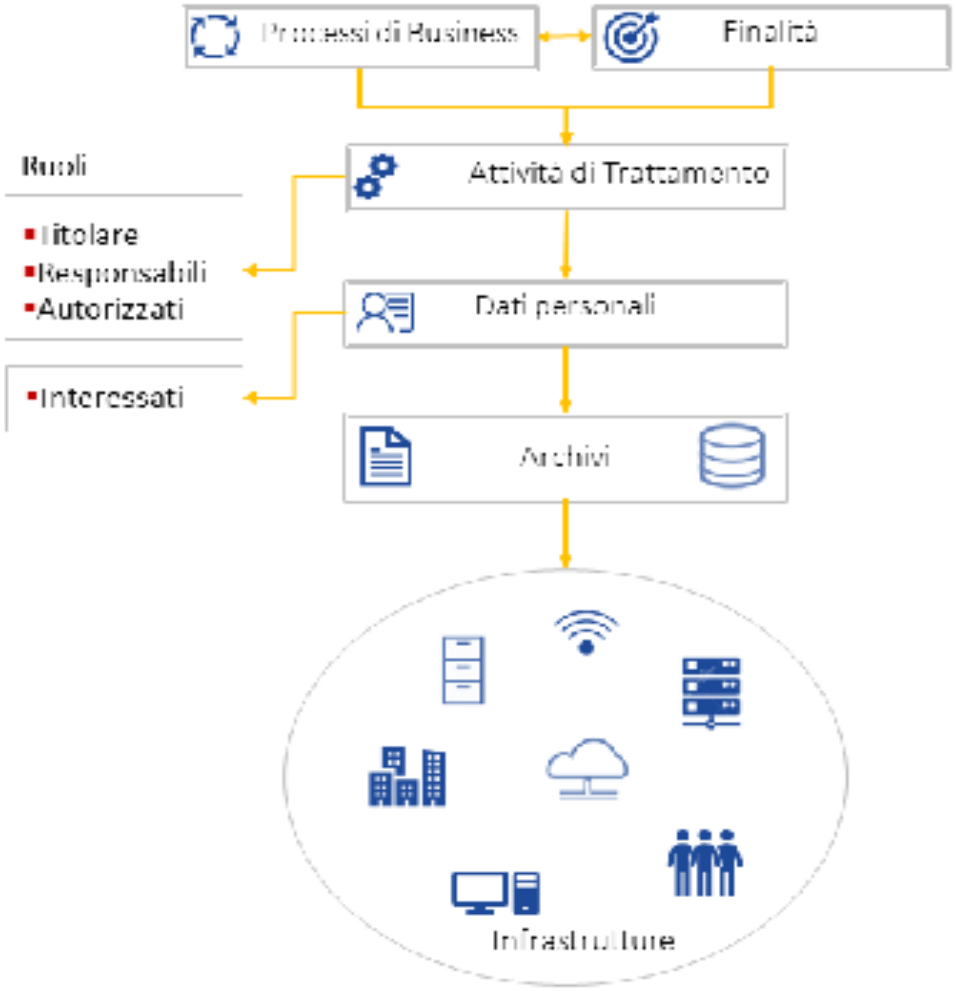


Documentare la conformità

Il Titolare "deve essere in grado di dimostrare in ogni momento la propria conformità al Regolamento".

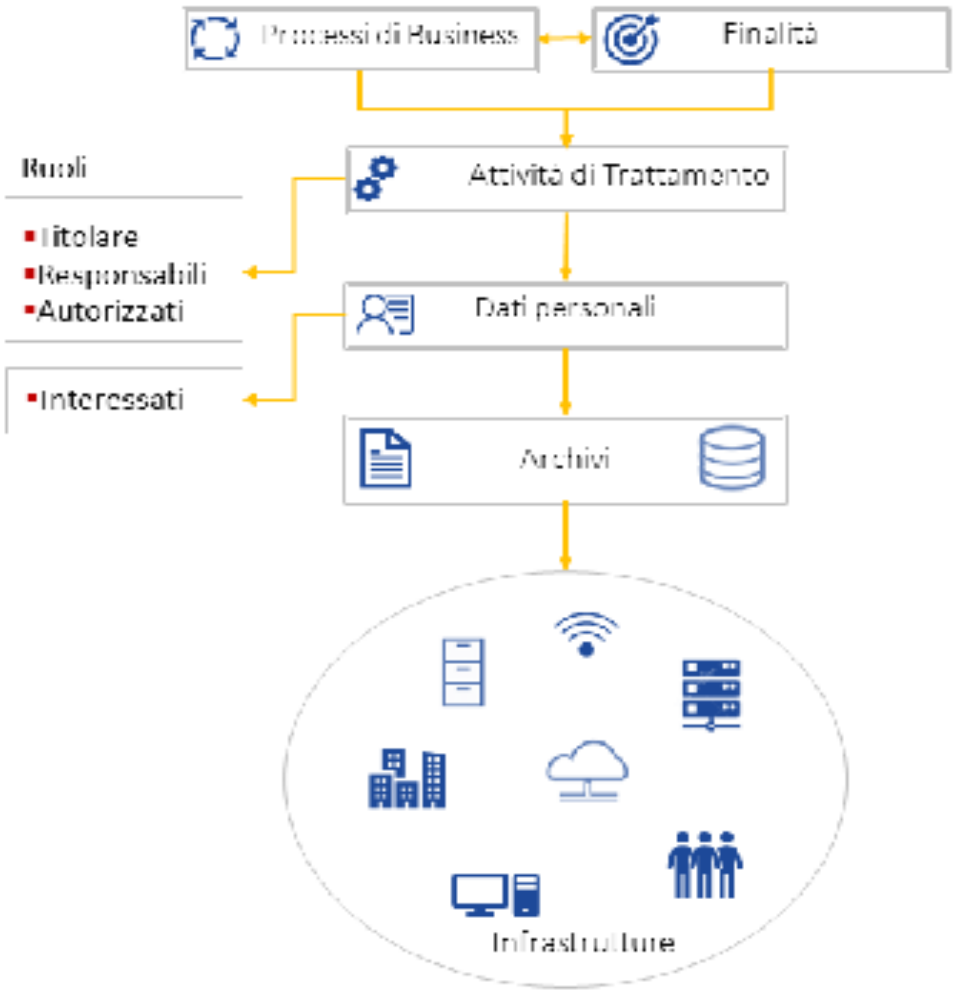
Occorre quindi creare e organizzare un apparato documentale che consenta questa **dimostrabilità**, prevedendo delle verifiche e degli aggiornamenti sistematici per essere in grado di dimostrare una protezione costante (dynamic compliance)

Processi aziendali – Finalità



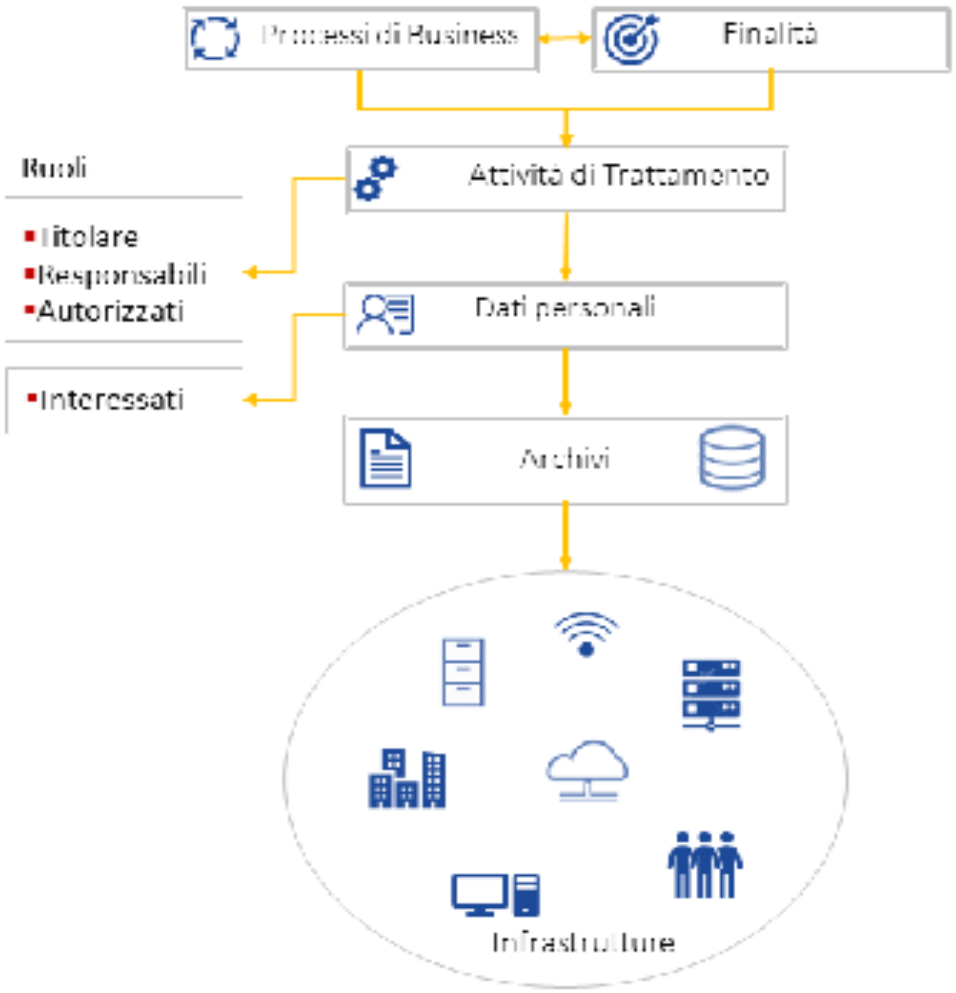
- Identificazione dei processi aziendali e delle finalità
- Verifica documentale: Organigramma dettagliato; eventuale DPS o altri documenti generali realizzati per gestire il sistema privacy in conformità al D.Lgs. 196/2003

Trattamenti



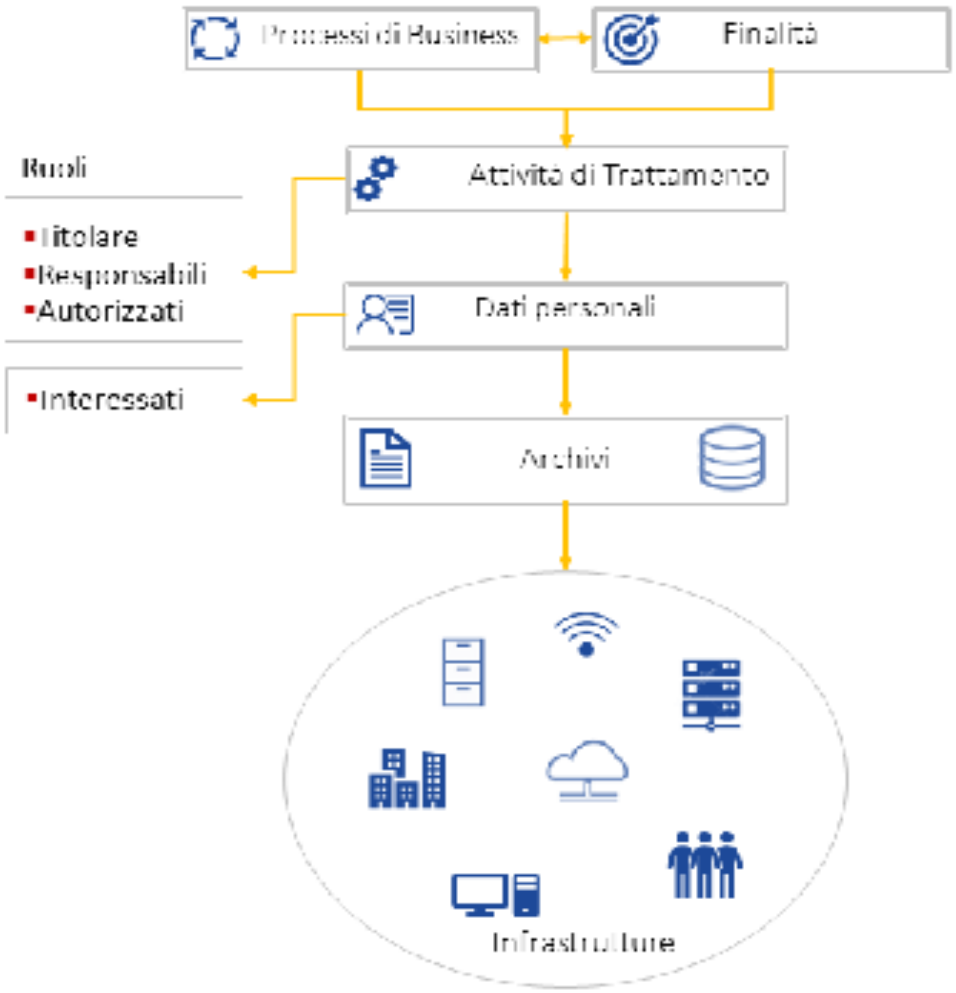
- Identificazione dei trattamenti:
  - quali trattamenti sono svolti nell'ambito di un processo aziendale?
  - Chi sono i soggetti coinvolti (titolare, responsabili interni e esterni, autorizzati)?
- Verifica documentale: nomine e incarichi a responsabili e autorizzati

Dati personali



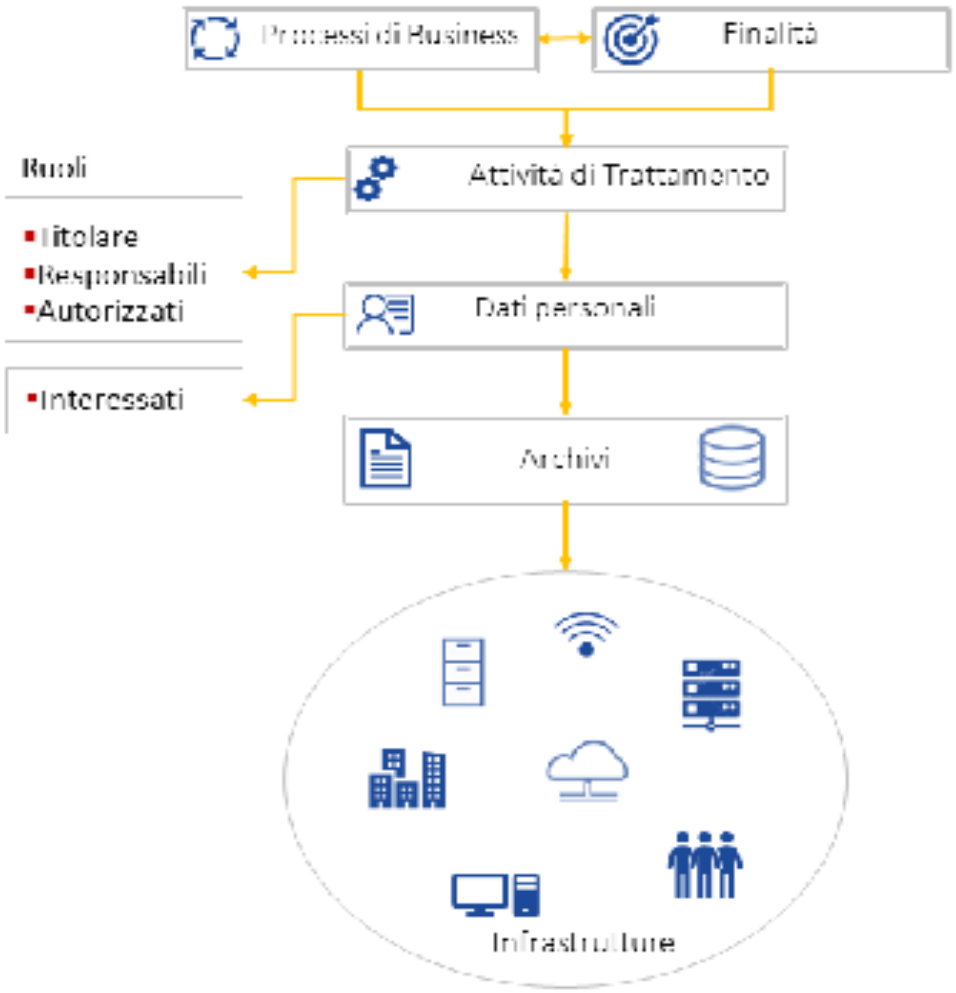
- Identificazione dei dati personali:
  - Che tipologie di dati personali vengono trattati (anagrafici, di contatto, bancari, fiscali, ecc.)?
  - Sono trattati dati particolari / giudiziari?
  - Chi sono gli interessati (dipendenti, fornitori, clienti, ecc.)
  - Come sono raccolti i dati (presso gli interessati, acquisizione con altre modalità)?
  - Per quanto tempo sono conservati?
- Verifica documentale: informative e acquisizioni del consenso dagli interessati

Archivi



- Identificazione degli archivi:
  - In che formato sono conservati i dati personali (digitale o analogico)?
  - In quali database/archivi/ strumenti/applicazioni sono elaborati e conservati i dati?

Infrastruttura



- Valutazione dell'infrastruttura:
  - Che caratteristiche hanno i database/archivi/ strumenti/ applicazioni su cui sono conservati e elaborati i dati?
  - Dove si trovano fisicamente?
  - Quali soggetti vi possono accedere?
  - Quali misure di sicurezza tecniche e organizzative sono applicate all'infrastruttura?

grc team
Governance, Risk Management
& Compliance

Grazie per l'attenzione

Claudia Carimini
Manager Privacy – AGM – GRC Team