OIBA
ORDINE DEGLI INGEGNERI della Provincia di Bari

«La normativa privacy nell'esercizio della professione»

Avv. Antonio Matarrese

LAW//APP
Consulenza Legale Applicata

Seminario di Deontologia Professionale
Bari, 16 dicembre 2022

Privacy, definizione

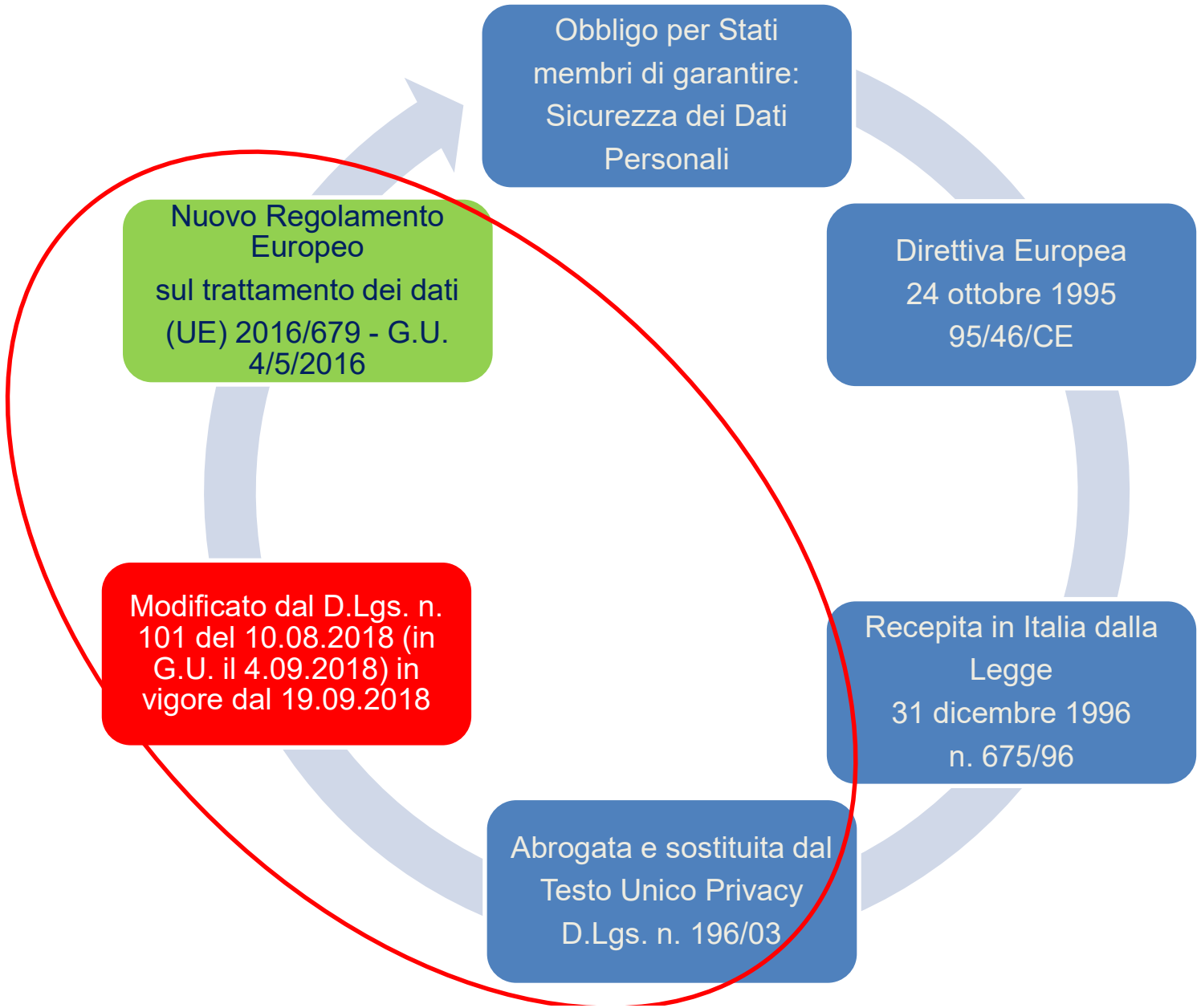
il significato di «privacy»

La **privacy**, termine inglese equivalente a **privatezza o solitudine**, è **il diritto alla riservatezza della propria vita privata**: *the right to be let alone* (lett. **"il diritto di essere lasciati in pace"**), secondo la formulazione del giurista statunitense Louis Brandeis.

Il significato di *privacy,* nel tempo, si è evoluto, arrivando ad indicare **il diritto al controllo sui propri dati personali**.

Il significato odierno di *privacy* è comunemente riconducibile al relativo **diritto della persona di controllare che le informazioni che la riguardano vengano «trattate» o «controllate» da altri solo in caso di necessità.**

Evoluzione normativa

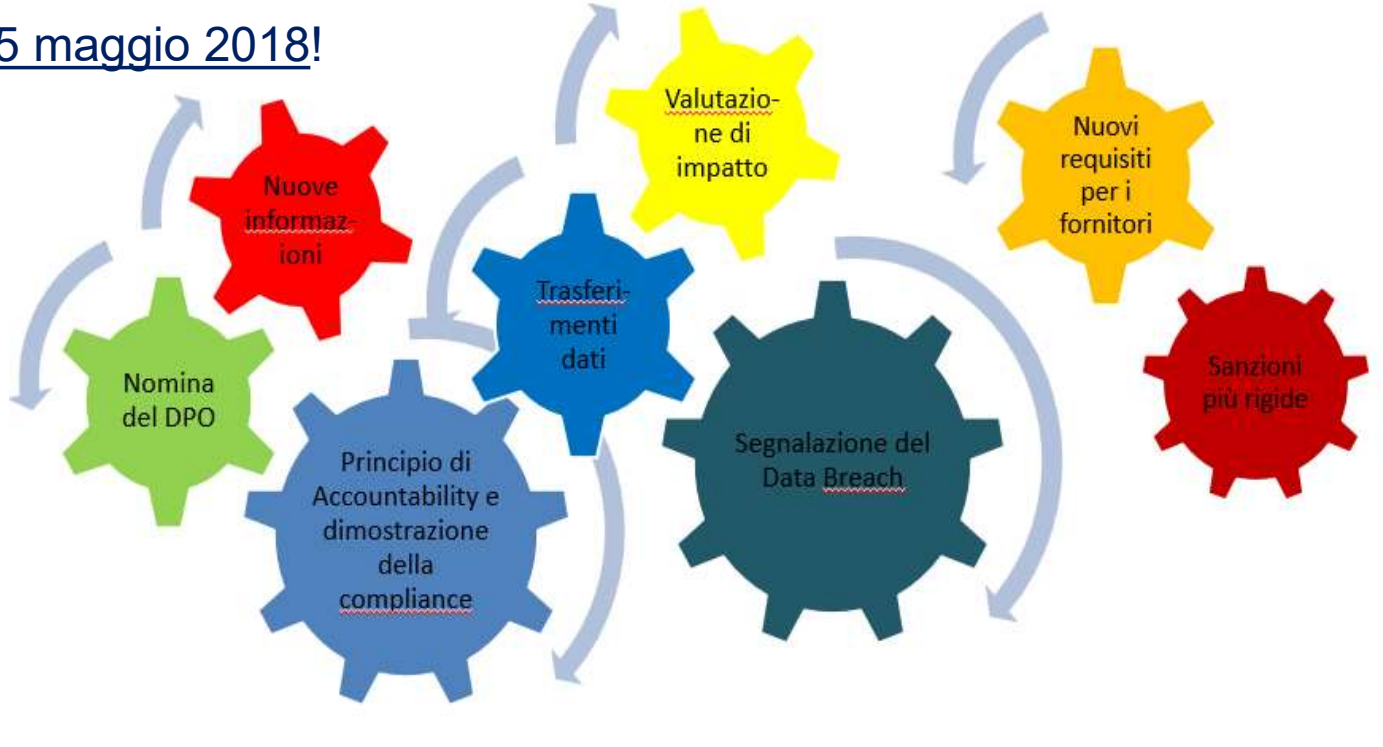


General Data Protection Regulation

Il GDPR

Regolamento Europeo (UE 2016/679) relativo alla "*protezione delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati*", volto a disciplinare i trattamenti di dati personali, sia nel settore privato, sia nel settore pubblico.

Entrato in vigore il 25 maggio 2018!



Quali sono gli obblighi per i professionisti?

1. effettuare delle verifiche preliminari e **mappare i trattamenti** effettuati nell'ambito dell'attività professionale;
2. individuare **ruoli** e responsabilità all'interno dello studio professionale e predisporre precise procedure interne;
3. individuare i **soggetti esterni** che trattano dati per conto del professionista;
4. redigere le **informative** sul trattamento dei dati personali;
5. analizzare i **rischi** e definire le misure di sicurezza necessarie a limitare tali rischi;
6. predisporre precise **procedure** interne per garantire l'esercizio dei diritti degli interessati;
7. predisporre il **registro dei trattamenti**.

Quali sono gli obblighi per i professionisti?

Il principio di accountability, introdotto dal GDPR, comporta per qualsiasi organizzazione - compresi gli Studi Professionali – una necessaria e approfondita auto-analisi riguardante:

- la modalità di circolazione (interna ed esterna) dei dati personali, e quindi delle procedure adottate per ritenere tali trattamenti conformi alla normativa,
- le specifiche misure di sicurezza tecniche e organizzative messe in atto.

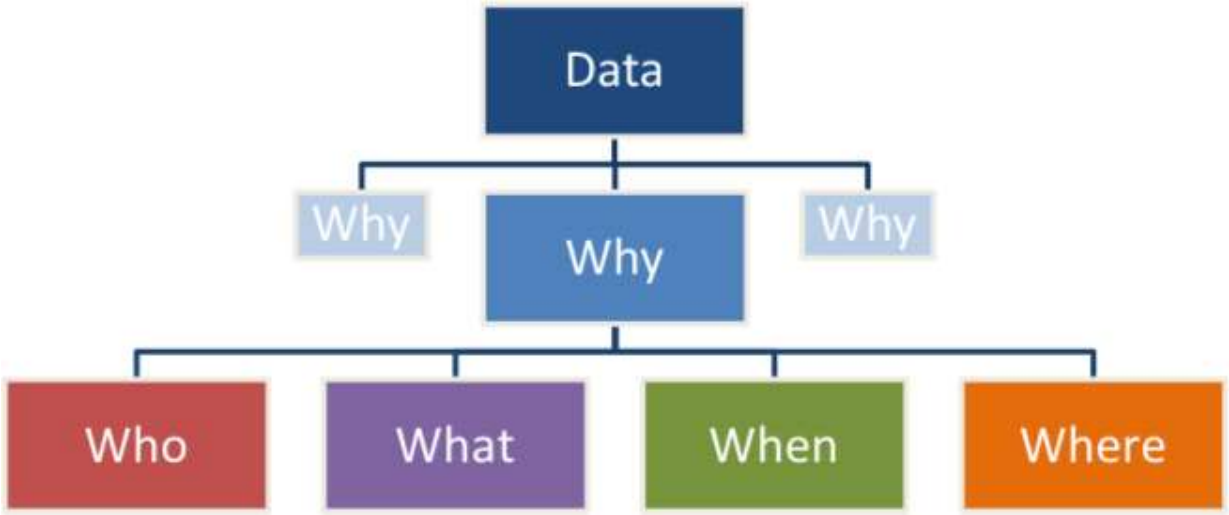
È inoltre necessario monitorare la correttezza delle procedure di trattamento e protezione dei dati personali, sia sotto il profilo giuridico, oltre che tecnico-informatico.

Quali sono gli obblighi per i professionisti?

In particolare, occorre considerare che gli Studi professionali detengono e gestiscono un **ingente volume di informazioni** di natura personale relativa non solo ai clienti, ma anche a collaboratori, dipendenti, fornitori, controparti, ecc.

Ciò rende queste realtà, piccoli o grandi che siano, un potenziale obiettivo dei cybercriminali. Una **violazione della sicurezza dei dati** può avere degli effetti legali, economici e reputazionali devastanti sia per i clienti, sia per gli stessi studi professionali. Per questo è fondamentale che i titolari del trattamento si dotino di misure di sicurezza efficaci, al fine di preservare la riservatezza, l'integrità e la disponibilità dei dati persor

Mappatura del «dato»



Mappatura degli «strumenti»

- mappare gli strumenti e le risorse informatiche interne (gestionali, sistemi operativi, account, ecc.)

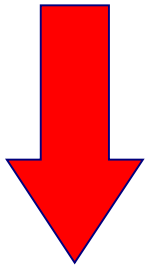
- mappare eventuali trattamenti elettronici particolari (videosorveglianza, sistemi con riconoscimento facciale o impronta digitale, ecc.)

- mappare i *data base* elettronici e cartacei (archivio documenti dipendenti, data base clienti, elenco fornitori, cartelle di documenti relativi alla fatturazione elettronica, archivio pratiche e progetti, ecc.)

- mappare gli strumenti e le risorse fisiche interne (sistemi di allarme, zone ad accesso riservato, ecc.)

Trattamento dei dati personali

TRATTAMENTO: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, 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



Qualsiasi operazione compiuta nei confronti dei dati personali costituisce "trattamento"

Definizione di dato personale

- ***«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.

Definizione di dato personale

I codici identificativi, sia quelli ricavati da dati anagrafici (ad esempio il **codice fiscale**), che i codici univoci attribuiti a una persona in base a criteri predefiniti (ad esempio **i codici cliente**) sono dati personali.

Dato personale è quindi **qualsiasi informazione riferita** (**o** anche semplicemente **riferibile** tramite un codice) **a una persona**: anche il numero di targa di una vettura riferita a un proprietario o il numero di una polizza riferita a un assicurato.

Definizioni e loro ambito di applicazione

dato personale potrebbe essere

UNA IMMAGINE

UN SUONO

<u>e qualunque notizia o informazione che sia riferibile a un soggetto fisico determinato o determinabile</u>

Definizioni e loro ambito di applicazione

«Particolari categorie di dati» sono:

informazioni relative a una persona fisica identificata o identificabile, idonee a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale; sono, altresì, dati personali appartenenti a categorie particolari i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale.
I dati personali appartenenti a categorie particolari devono essere protetti con attenzione, poiché il loro trattamento espone a molteplici rischi i diritti e le libertà degli interessati.

Definizioni e loro ambito di applicazione

«Particolari categorie di dati» sono i dati giudiziari (art. 10 del Nuovo Regolamento):

«Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'art. 6.1, 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»

I soggetti individuati dal regolamento

- Titolare del trattamento
- Responsabile del trattamento
- L’interessato
- Il Responsabile della protezione dei dati (DPO)

Il titolare del trattamento

DEFINIZIONE

Può essere una persona fisica o giuridica, pubblica o privata, riconosciuta o no.
Il titolare è il centro d'imputazione delle decisioni e **determina le finalità e i mezzi del trattamento**.

Finalità: perché del trattamento?
Obiettivo al servizio del quale viene effettuato il trattamento (es: il trattamento per finalità di marketing, è funzionale allo svolgimento dell'attività di promozione)

Mezzi: come avviene il trattamento?
Non si riferisci solo ai mezzi tecnici (es. hardware, software), ma anche quali sono i dati, come e quando raccoglierli, quali terzi avranno accesso ai dati, ecc. (profilo organizzativo)

Il ruolo concretamente dipende dall'**effettivo potere decisorio esercitato**.
E' una figura apicale nella gerarchia della privacy.

Chi è il titolare del trattamento nello studio?
Il professionista !

Obblighi e adempimenti :

- Il titolare **decide** e **programma** le misure di sicurezza;
- il titolare **attua** le misure di sicurezza. Predispone misure tecniche e organizzative adeguate, curando di verificarle e aggiornarle periodicamente. Deve dotarsi di policy interne;
- si **attiene** ai doveri di correttezza per l'intera durata del trattamento; si conformai ai principi di trasparenza e responsabilizzazione;
- **sceglie** i soggetti che ricoprono i ruoli subalterni e li istruisce;
- ha l'obbligo di **designare**, nei casi previsti dalla legge, il DPO;
- **fornisce** istruzioni adeguate al personale che tratta i dati;
- nel caso di violazioni dei dati deve porre in essere contromisure effettive e tempestive e procedere alla notificazione al Garante e alla comunicazione all'interessato;

Il responsabile del trattamento

DEFINIZIONE
Il responsabile è il soggetto che svolge attività di trattamento per conto del titolare.

Può essere una persona fisica o giuridica, pubblica o privata, riconosciuta o no.

Il responsabile deve presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate. E' importantissima la sua scelta (selezione).

In base all'atto di nomina il responsabile si impegna a:

- ✓ Ha il dovere di agire secondo le istruzioni di trattamento fornite dal titolare e di impartirle ai suoi dipendenti e collaboratori.
- ✓ consentire i trattamenti solo a persone autorizzate con impegno alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza;
- ✓ adottare tutte le misure di sicurezza (es. cifratura, pseudonimizzazione, recupero da back up);
- ✓ 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;

L’incaricato al trattamento: dipendenti e collaboratori

Pur non prevedendo espressamente la figura dell’«incaricato» del trattamento, il regolamento non ne esclude la presenza in quanto fa riferimento a **«persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile».**

L’Incaricato del trattamento è una figura di primissima rilevanza nell’organigramma di privacy di qualsiasi struttura poiché, sotto la diretta autorità del titolare e del responsabile (se nominato), egli è colui il quale, dietro apposita autorizzazione, **effettua materialmente le operazioni di trattamento sui dati personali**.

Il Data Protection Officer - Art. 37, considerando 97

Quale è il ruolo del DPO?

«SORVEGLIA L'OSSERVANZA DEL REGOLAMENTO»

Il DPO costituisce un punto di riferimento interno alle aziende e degli enti, in quanto è coinvolto in tutte le questioni attinenti alla privacy, è un punto di contatto per gli interessati, le divisioni operative interne di aziende o enti, le autorità di controllo.

Nell'ottica del principio di trasparenza, l'identità ed i dati di contatto del DPO devono essere riportati nell'informativa privacy; devono essere pubblicati sul sito internet dell'ente e contenuti anche nel registro dei trattamenti.

Quando deve essere nominato?

Secondo l'art. 37 del Regolamento, devono nominare obbligatoriamente un Responsabile della protezione dei dati:

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.

Il Data Protection Officer: compiti

Il **DPO** ha il compito di:

- **raccoglie le informazioni per individuare i trattamenti svolti e verifica che essi siano conformi alla legge**;
- **sorvegliare l'osservanza del regolamento**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
- **informare e sensibilizzare** il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento Europeo, dalla normativa e dalla prassi interna;
- **verificare** che la normativa vigente e le policy interne del titolare siano correttamente attuate ed applicate, incluse le attribuzioni delle responsabilità, la sensibilizzazione e la formazione del personale, ed i relativi **audit**;
- collaborare con il titolare/responsabile, laddove necessario, nel condurre una **valutazione di impatto sulla protezione dei dati (DPIA);**
- **fungere da collegamento** sia con il Garante della Privacy che con gli interessati, che potranno rivolgersi a lui anche per l'esercizio dei loro diritti.

L’interessato

DEFINIZIONE

L’interessato è la persona fisica indentificata o identificabile.
Non c’è una definizione nel Regolamento, ma la si desume da quella di dato personale: ovvero qualsiasi informazione riguardante una persona fisica.

La figura **dell’interessato** è costruita sul concetto di **dato personale**, per cui ne subisce la forza espansiva.

L’interessato: i suoi diritti

I **diritti dell’interessato** possono essere considerati declinazioni particolari del più ampio diritto all’**autodeterminazione informativa** ovvero

«il potere di governare il flusso delle proprie informazioni»

dunque implica la pretesa, riconosciuta dall’ordinamento all’individuo, di avere conoscenza di quel flusso, di afferrarne la circolazione, la finalità e i soggetti che lo dirigono.
Comprende altresì il riconoscimento in capo alla persona di un potere di controllo, nel **doppio senso di «verifica» e di «intervento»**.

L’interessato: i suoi diritti

I diritti dell’interessato, appartengono a due macro categorie: nella prima rientrano i **diritti di natura «conoscitiva»**, nella seconda rientrano i **diritti di «controllo»**.

- I **diritti conoscitivi** sono quelli di:

- ricevere informazioni sul trattamento ossia il diritto all’informativa (artt. 13 e14)
- richiedere/ottenere informazioni sul trattamento e sui dati trattati, vale a dire il diritto di accesso (art. 15)
- ricevere informazioni su gravi anomalie incorse nel trattamento, ossia il diritto alla comunicazione di una violazione dei dati (art. 34)

- I **diritti di controllo** possono avere ad oggetto o il trattamento o i dati trattati.

Hanno ad oggetto il **trattamento** i diritti di:

- autorizzare il trattamento, ossia il diritto al consenso (artt. 6.1 a) e 9.2 a))
- modificare il trattamento, ossia il diritto di limitazione (art. 18)
- far cessare il trattamento, ossia il diritto di revoca del consenso (art. 7.3) e il diritto di opposizione (art. 21)

Hanno ad oggetto i **dati**, i diritti di:

- spostare complessi strutturati di dati, ossia il diritto alla portabilità (art. 20)
- modificare i dati, ossia i diritti di rettifica e di integrazione (art. 16)
- eliminare i dati personali, ossia il diritto di cancellazione/oblio (art. 17).

Presupposti di liceità del trattamento dati personali

Il Regolamento conferma che ogni trattamento deve trovare fondamento in **un'idonea base giuridica**; i fondamenti di liceità del trattamento sono indicati all'art. 6 del Regolamento.

Consenso	**Contratto**	**Obbligo legale**	**Salvaguardia interessi vitali**	**Compito di interesse pubblico connesso all'esercizio di pubblici poteri**	**Legittimo interesse del titolare**
Per una o più specifiche finalità	Necessità di esecuzione di contratto o misure precontrattuali	Possibilità di integrazione da parte della legislazione nazionale	Dell'interessato o di altra persona fisica	Possibilità di integrazione da parte della legislazione nazionale	Se non prevalgono interessi, diritti e libertà fondamentali dell'interessato specie se minore

Fonte della tabella: *Privacy e Regolamento Europeo 2016/679, Ipsoa*

Il Registro delle attività di trattamento

Ogni **titolare del trattamento** e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.
Il Registro deve essere istituito e tenuto sempre aggiornato; può essere in forma scritta o in formato elettronico.

Il Registro delle attività di trattamento

Nel Registro tenuto dal Titolare devono essere obbligatoriamente descritte almeno le seguenti informazioni:

1. estremi identificativi e di contatto del titolare del trattamento e degli eventuali contitolari del trattamento;
2. estremi identificativi e di contatto del responsabile del trattamento e degli eventuali responsabili del trattamento di secondo livello;
3. estremi identificativi e di contatto del rappresentante del titolare o del responsabile;
4. estremi identificativi e di contatto del DPO;
5. finalità del trattamento; (*)
6. descrizione delle categorie di interessati; (*)
7. descrizione delle categorie di dati personali;
8. categorie di destinatari a cui i dati personali sono comunicati (*);
9. eventuali trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale con documentazione delle garanzie in materia di privacy;
10. termine ultimo previsto per la cancellazione dei dati (*);
11. descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

La valutazione del rischio

Cosa si intende per rischio?

DEFINIZIONE

«Per "rischio" si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità» per i diritti e le libertà

(Linee guida del Gruppo di lavoro Articolo 29 WP248rev.1)

Sicurezza dei dati e analisi dei rischi

ATTENZIONE!

Non bisogna confondere la **gestione dei rischi** con le **misure di sicurezza**, anche se sono argomenti con una certa correlazione

Il «rischio» non si riferisce al titolare, ma all'**interessato**.

La valutazione del rischio deve riguardare:

- la sicurezza del trattamento (come)
- gli effetti del trattamento (conseguenze): **danni economici, danni per la reputazione, discriminazione, furto di identità, perdite finanziarie, danni fisici o psicologici, perdita di controllo dei dati, impossibilità di esercitare diritti**, ecc.

L’analisi dei rischi

- L’analisi dei rischi è un processo che **va svolto all’inizio** dell’adeguamento al Regolamento.

- Va rifatto con una certa **frequenza** perché cambiano gli elementi di contesto e quindi cambiando il contesto cambiano le norme, i provvedimenti, cambiano le tecnologie, cambiano i rischi.

  Ad esempio se un professionista introduce un nuovo tipo di trattamento, introduce anche un nuovo tipo di rischio.

- L’analisi dei rischi, quindi, non si fa una sola volta nella vita ma si fa periodicamente e successivamente si aggiorna.

GDPR in pochi passi…

ISFORM
Istituto per la Formazione Manageriale

1) Assessment

Effettuare una valutazione a livello:
- organizzativo;
- Policy;
- Processi;
- Tecnologici.

2) Analisi del rischio

Analizzare le vulnerabilità e determinare i possibili rischi a livello:
- Organizzativo;
- Policy;
- Processi;
- Tecnologico.

3) Valutazione del rischio

Valutare quali **MISURE ADEGUATE** sono idonee alla riduzione del rischio identificato (non ci sono più le misure minime).

4) Attuazione misure adeguate

Attuare le misure di sicurezza a livello:
- organizzativo;
- policy;
- processi;
- tecnologico

5) Implementazione delle misure adeguate

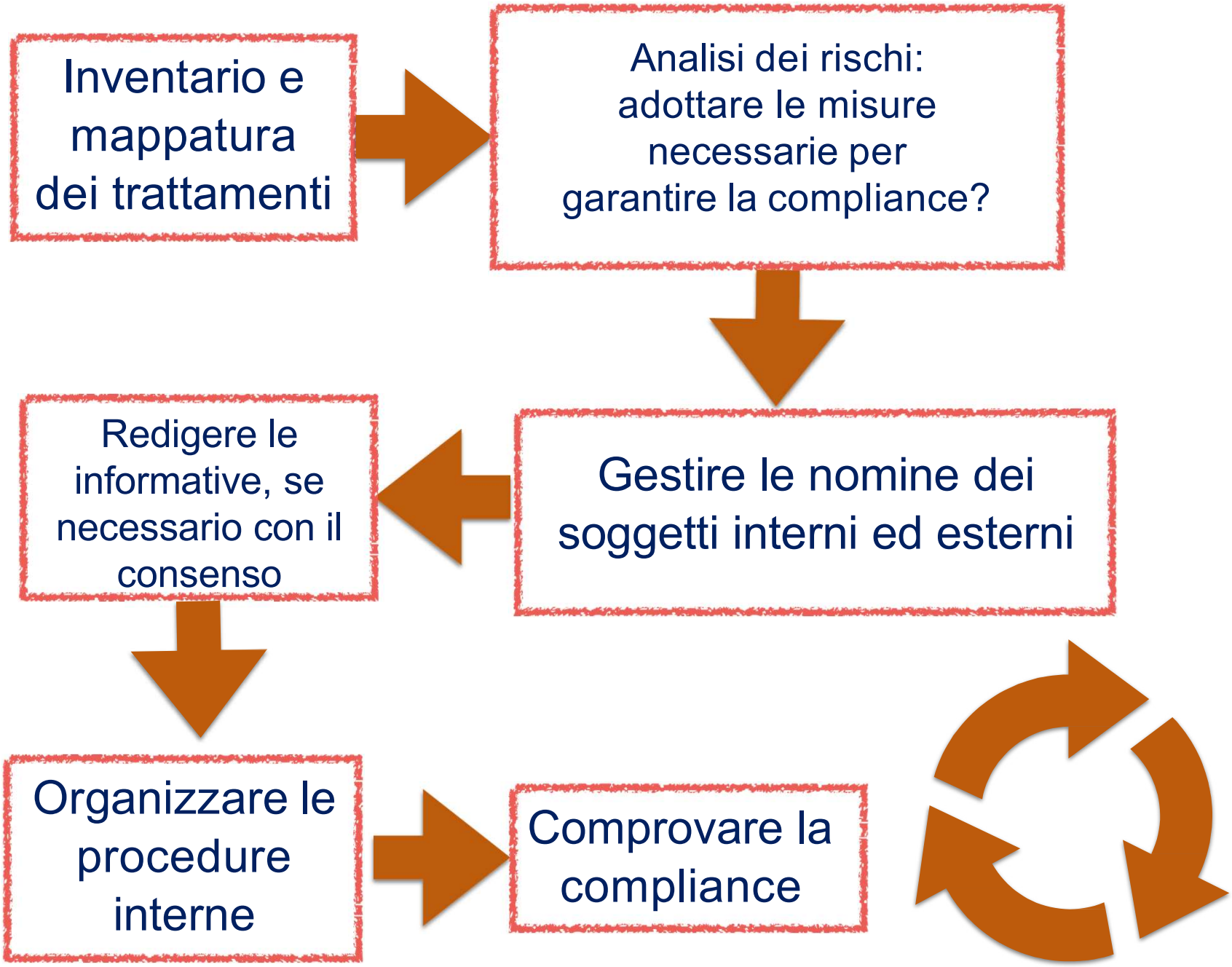
Implementare le misure di sicurezza a livello:
- organizzativo;
- policy;
- processi:
- tecnol

6) Aggiornamento periodico

Le attività indicate dal punto 1 al punto 5 devono essere effettuate periodicamente su base annuale.

Dasa-Rägister
UNI EN ISO 9001:2015
IQ-0119-01

CEPAS


Inventario e mappatura dei trattamenti
Analisi dei rischi: adottare le misure necessarie per garantire la compliance?
Gestire le nomine dei soggetti interni ed esterni
Redigere le informative, se necessario con il consenso
Organizzare le procedure interne
Comprovare la compliance

L’Accountability

Il **principio di Accountability** è uno delle novità fondamentali del Regolamento europeo in materia di protezione dei dati personali, noto anche come il **principio di responsabilizzazione** (art. 24).

Esso favorisce l’adozione di comportamenti proattivi e tali da <u>dimostrare</u> la concreta adozione di misure finalizzate ad assicurare l’attuazione del regolamento

Il presupposto del principio, risiede nel fatto che al titolare è affidato il compito di **<u>decidere autonomamente</u>** le **modalità**, le **garanzie** e i **limiti** del trattamento dei dati.

Accountability

QUINDI: tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità 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 dei dati personali è effettuato conformemente al Regolamento**.

Dette misure sono riesaminate e aggiornate qualora necessario.

ADOZIONE DI MISURE ADEGUATE ED EFFICACI

CAPACITA' DI COMPROVARE L'ADEGUATEZZA

Privacy by design e *Privacy by default*

Privacy by design significa protezione dei dati fin dalla fase della «**progettazione**».

Quindi in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, di servizi e di prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni devono tenere conto del diritto alla protezione dei dati, in modo da assicurarsi **che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati**.

Privacy by design e *Privacy by default*

Privacy by default **significa che la tutela della protezione del dato deve diventare una «impostazione predefinita».**

Il Titolare del trattamento, infatti, deve adottare **misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.**

Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

Il **responsabile del trattamento** garantisce che siano trattati, di *default*, solo i dati personali **necessari** per ciascuna finalità specifica del trattamento; e che, in particolare, la **quantità** dei dati raccolti e la **durata** della loro conservazione non vadano oltre il minimo necessario per le finalità perseguite.

Detti meccanismi garantiscono che, di *default*, non siano resi accessibili dati personali a un numero indefinito di persone e che gli interessati siano in grado di controllare la distribuzione dei propri dati personali.

OIBA
ORDINE DEGLI INGEGNERI della Provincia di Bari

Grazie per l'attenzione!

Avv. Antonio Matarrese

LAW//APP
Consulenza Legale Applicata

Milano
Via A. M. Ampère, 121
Tel.: 02.87157748

Bari
Via Emanuele Mola, 34
Tel.: 080.887592

www.lawapp.it - segreteria@lawapp.it