G.D.P.R. Parte Prima

Regolamento generale sulla protezione dei dati personali

Regolamento UE 2016/679

GDPR (General Data Protection Regulation)

RGDP (Regolamento Generale sulla Protezione Dati)

Entrata in vigore 25/05/2016

Vigenza in via definitiva 25/05/2018

DIRETTIVA 95/46

L'unione europea ha introdotto un sistema di regole volte a governare i trattamenti di dati personali

LEGGE 675/96

La direttiva è stata recepita in Italia dalla Legge n.675 del 1996, la prima legge sulla protezione dei dati personali a livello nazionale.

D. LGS. 196/2003

Il c.d. Codice della privacy ha abrogato la precedente legge in materia di protezione dei dati personali.

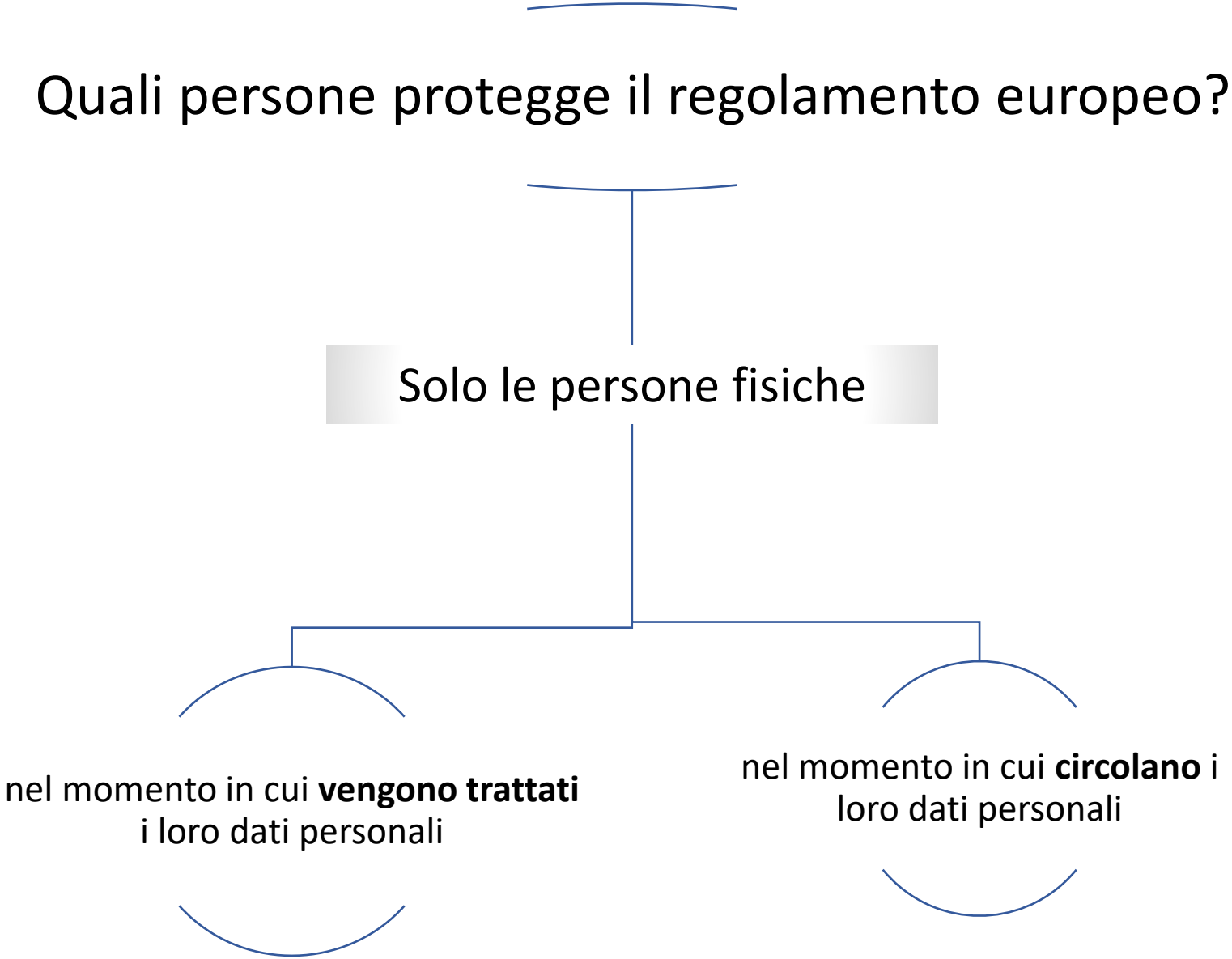
REG. UE 679/2016

È entrato in vigore il 24 maggio 2016 e diventato direttamente applicabile in tutti gli stati dell'Unione europea a partire dal 25 maggio 2018.

D. LGS. 101/2018

C.d. «Decreto di armonizzazione» entrato in vigore il 19 settembre 2018 integra il D. LGS. 196/2003 in ottica di conformità al REG. UE

Quali persone protegge il regolamento europeo?

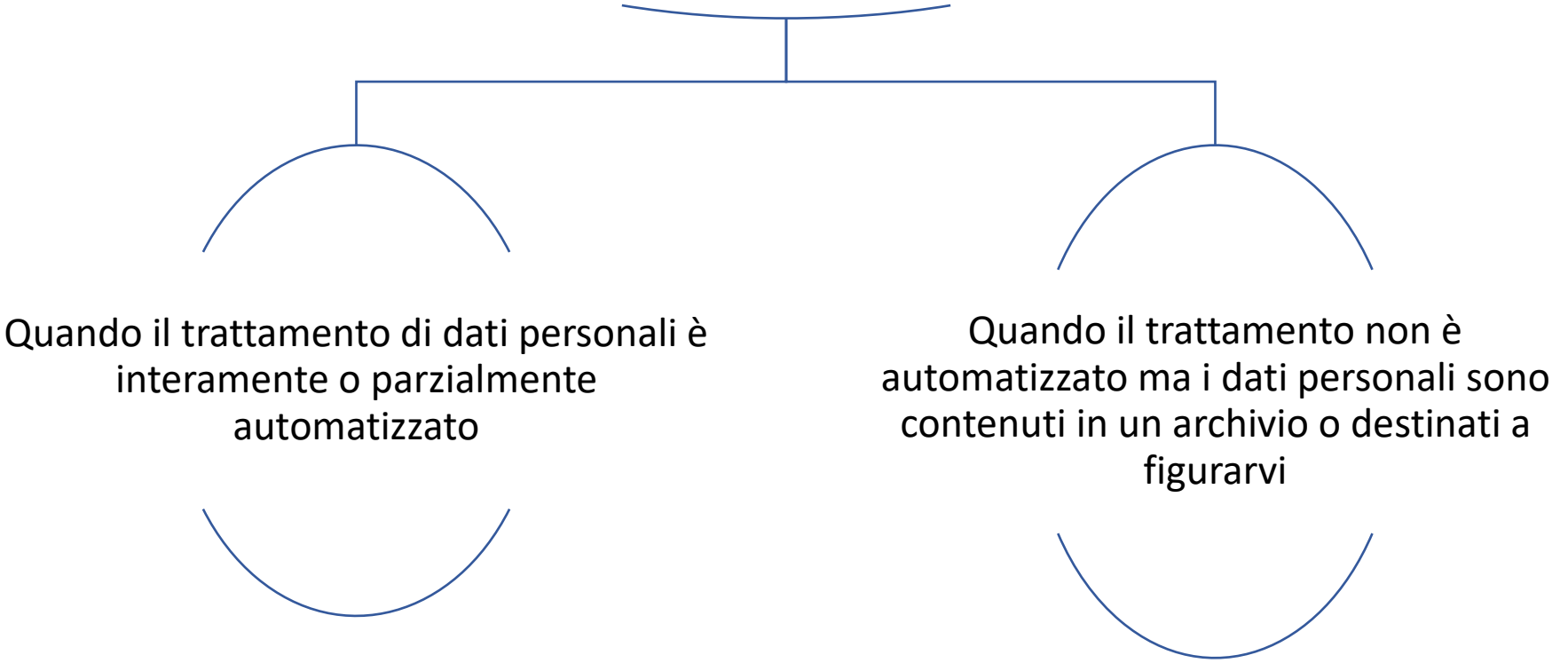


A chi si applica il nuovo regolamento europeo ?

A tutti i titolari di trattamenti con sede nell’ UE

A tutti i titolari fuori UE ma che forniscono beni e servizi o svolgono monitoraggio dei comportamenti nell’UE

Quando si applica il nuovo regolamento europeo?



Quando non si applica il nuovo regolamento europeo?

attività a carattere esclusivamente personale o domestico

trattamento di dati interamente manuale in un contesto non strutturato

Il trattamento riguarda informazioni che non sono, o non sono più, dati personali: persone decedute o dati anonimi o anonimizzati.

Sottrazione al regolamento per materie specifiche: politica estera e sicurezza comune; repressione reati: prevenzione, indagine, accertamento o perseguimento di reati, esecuzione di sanzioni penali, salvaguardia sicurezza pubblica; attività che non rientrano nell'ambito di applicazione del diritto dell'unione: sicurezza nazionale.

Corte di giustizia UE

Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività.

Il riferimento al **carattere personale e domestico** del trattamento è stato **escluso** in alcune sentenze della corte:

Videosorveglianza che si estende ad uno spazio pubblico;

Social network, forum di discussione, chat, qualora la condivisione di dati non sia ristretta ad amici ma accessibile a chiunque.

D. Lgs. 196/2003 (come modificato dal D. Lgs. 101/2018)
Art. 2-terdecies (Diritti riguardanti le persone decedute)

1- I diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.

2- L'esercizio dei diritti di cui al comma 1 non è ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della società dell'informazione, l'interessato lo ha espressamente vietato con dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata.

3- In ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difendere in giudizio i propri interessi.

COSA NON CAMBIA

- Definizione dato personale
- Definizione trattamento
- Titolare del trattamento
- Principi relativi al trattamento
- Liceità del trattamento
- Obbligo di informativa
- Obbligo di consenso (nei casi previsti)
- Protezione delle sole persone fisiche

Definizioni art. 4
REG. UE 679/2016

Cos’è un dato personale?

Qualsiasi informazione riguardante una **persona fisica** identificata o identificabile («**interessato**»);

si considera identificabile la persona che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Definizioni art. 4
REG. UE 679/2016

Categorie particolari di dati

Dati genetici: dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona che forniscono informazioni uniche sulla fisiologia o sulla salute di detta persona, in particolare dall'analisi di un campione biologico.

Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

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

Dati sensibili: origine etnica e razziale, opinioni politiche, convinzioni filosofiche e religiose, l'appartenenza sindacale, dati relativi alla vita sessuale o orientamento sessuale.

Definizioni art. 4
REG. UE 679/2016

Cos’è un trattamento di dati personali?

Qualsiasi attività svolta su dati personali, anche di tipo non trasformativo, quale ad esempio un mero accesso.

Il Garante italiano ha considerato pacificamente la videosorveglianza senza registrazione come una tipologia di trattamento, prescrivendo di conseguenza modalità e attenzioni per la sua effettuazione.

Definizioni art. 4
REG. UE 679/2016

Titolare del trattamento

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina **le finalità e i mezzi del trattamento** di dati personali.

Responsabile del trattamento

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

Contitolari, Responsabili e subresponsabili

Il **Contitolare del trattamento** è colui che partecipa congiuntamente ad altri soggetti alla determinazione delle finalità e delle modalità di un trattamento di dati personali. Un criterio importante da considerate per individuare i casi di contitolarità, è che il trattamento non sarebbe possibile senza la partecipazione di entrambe le parti.

Il regolamento:

- disciplina la **contitolarità del trattamento** *(art. 26)* e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti **con particolare riguardo all'esercizio dei diritti degli interessati**, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente;

Contitolari, Responsabili e subresponsabili

- fissa più dettagliatamente (rispetto al Codice) **le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento** attribuendogli specifici compiti: deve trattarsi, infatti, di un **contratto** (o altro atto giuridico conforme al diritto nazionale) e deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28 al fine di dimostrare che **il responsabile fornisce "garanzie sufficienti"** – quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento;

Contitolari, Responsabili e subresponsabili

- consente la **nomina di sub-responsabili del trattamento** da parte di un responsabile (si veda art. 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli **stessi obblighi contrattuali che legano titolare e responsabile primario**; quest'ultimo **risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile**, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (si veda art. 82, paragrafo 1 e paragrafo 3);

Contitolari, Responsabili e subresponsabili

- prevede **obblighi specifici in capo ai responsabili del trattamento**, in quanto distinti da quelli pertinenti ai rispettivi titolari.

Ciò riguarda, in particolare, la tenuta del **registro dei trattamenti** svolti (ex art. 30, paragrafo 2); l'adozione di idonee **misure tecniche e organizzative per garantire la sicurezza dei trattamenti** (ex art. 32 regolamento); **la designazione di un RPD-DPO**, nei casi previsti dal regolamento o dal diritto nazionale.

Si ricorda, inoltre, che anche il responsabile non stabilito nell'Ue dovrà designare un rappresentante in Italia quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del regolamento – diversamente da quanto prevedeva l'art. 5, comma 2, del Codice.

Definizioni art. 29
REG. UE 679/2016

Autorizzato al trattamento

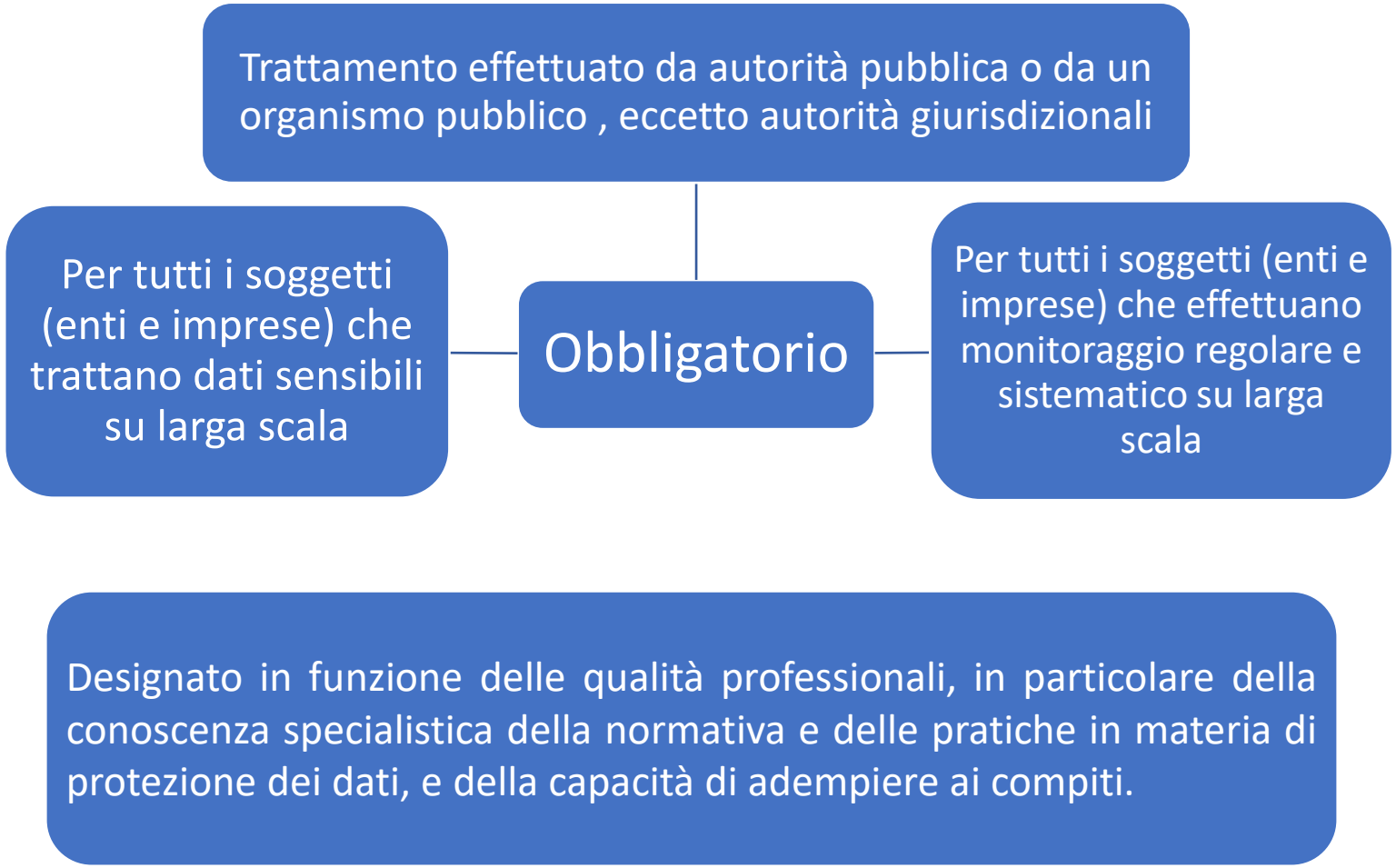
Chiunque agisca sotto l'autorità del titolare o del responsabile del trattamento non può trattare i dati se non è istruito in tal senso.

Designati*

Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

*Art. 2-quaterdecies D. Lgs. 196/2003

DPO (Data Protection Officer) Art. 37 - 38 - 39




CONSULENZA
Informare e consigliare il titolare, il responsabile e i dipendenti in merito agli obblighi del GDPR
COOPERAZIONE
con l'autorità di controllo
VIGILANZA
Sorvegliare l'osservanza del GDPR
DPO
FORNIRE UN PARERE
in merito alla DPIA e sorvegliare lo svolgimento
CONTATTO
con l'autorità di vigilanza

Come devono essere trattati i dati personali?

ART. 5 REG. UE 679/2016
PRINCIPI DEL TRATTAMENTO

- in modo **lecito, corretto e trasparente** nei confronti dell'interessato;
- raccolti per **finalità determinate, esplicite e legittime;**
- **adeguati, pertinenti e limitati** a quanto necessario;
- **esatti** e, se necessario, **aggiornati**;
- **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;
- **trattati in maniera da garantire un'adeguata sicurezza** dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Quando è lecito un trattamento?

ART. 6 REG. UE 679/2016
LICEITA' DEL TRATTAMENTO

- L'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più finalità.
- Il trattamento è necessario **all'esecuzione di un contratto** di cui l'interessato è parte […];
- è necessario per adempiere un **obbligo legale** del titolare;
- è necessario per la **salvaguardia di interessi vitali** di una persona fisica;
- è necessario per l'esecuzione di un compito di **interesse pubblico** o connesso con **l'esercizio di pubblici poteri**;
- è necessario per il perseguimento di un **legittimo interesse** del titolare o di terzi, a condizione che non prevalgano sui diritti/libertà dell'interessato.

Contratto e consenso

L’adesione ad un servizio di posta elettronica non prevede per l’interessato che ne faccia richiesta l’espressione di un consenso al trattamento dei dati personali necessari per il funzionamento del servizio stesso.

Per esempio, nome, cognome, codice fiscale, indirizzo di fatturazione, ecc.

Tuttavia, se il fornitore del servizio, intenda usare le coordinate di posta elettronica per l’invio di una *newsletter* informativa periodica all’interessato, avrà bisogno di acquisire preventivo consenso al trattamento.

Quando è lecito un trattamento di dati particolari?

ART. 9 REG. UE 679/2016
TRATTAMENTO DI DATI PARTICOLARI

- Consenso esplicito per finalità specifiche;
- necessità di osservare obblighi in materia di diritto del lavoro, sicurezza e protezione sociale;
- trattamento di interesse vitale dell'interessato o di altra persona;
- trattamento effettuato da organismo non lucrativo con finalità politiche, filosofiche , religiose, sindacali;
- Dati resi manifestamente pubblici dall'interessato;
- Necessità di accertare, esercitare, difendere un diritto in sede giudiziaria;
- Interesse pubblico sulla base dell'ordinamento europeo o interno; trattamenti sanitari, ricerca scientifica e storica, statistica.

D. Lgs. 196/2003 (come modificato dal D. Lgs. 101/2018)
Art. 2-sexies (Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante)

I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

LINEE GUIDA WP29 (EDPB)
SUL CONSENSO

Il consenso come base di legittimità

Il consenso può costituire la base legittima appropriata solo se all'interessato vengono offerti il controllo e l'effettiva possibilità di scegliere se **accettare o meno i termini proposti o rifiutarli senza subire pregiudizio**.

Quando richiede il consenso, il titolare del trattamento deve valutare se soddisferà tutti i requisiti per essere valido.

Se ottenuto nel pieno rispetto del regolamento, il consenso è uno strumento che **fornisce all'interessato il controllo sul trattamento dei dati personali che lo riguardano**.

In caso contrario, il controllo diventa illusorio e il consenso non costituirà una base valida per il trattamento, **rendendo illecita l'attività di trattamento.**

LINEE GUIDA WP29 (EDPB)
SUL CONSENSO

Il consenso come base di legittimità

L' ottenimento del consenso non fa venir meno né diminuisce in alcun modo **l'obbligo del titolare** del trattamento di rispettare i principi applicabili al trattamento per quanto concerne **la correttezza, la necessità e la proporzionalità, nonché la qualità dei dati**.

Il fatto che il trattamento dei dati personali si basi sul consenso dell'interessato non legittima **la raccolta di dati non necessari** a una finalità specifica di trattamento, che sarebbe fondamentalmente iniqua.

In termini generali, qualsiasi azione di **pressione o influenza inappropriata** sull'interessato che impedisca a quest'ultimo di esercitare il suo libero arbitrio, rende il consenso invalido.

LINEE GUIDA WP29 (EDPB)
SUL CONSENSO

Il consenso come base di legittimità

Quando il trattamento si fonda sul consenso dell'interessato, il titolare **deve sempre essere in grado di dimostrare** (articolo 7.1 del Regolamento) che l'interessato ha prestato il proprio consenso, che è valido se:

- all'interessato **è stata resa l'informazione** sul trattamento dei dati personali (articoli 13 o 14 del Regolamento);

- è stato espresso dall'interessato **liberamente**, in modo **inequivocabile** e, se il trattamento persegue più finalità, **specificamente** con riguardo a ciascuna di esse. Il consenso deve essere **sempre revocabile**.

Occorre verificare che la richiesta di consenso sia **chiaramente distinguibile da altre richieste** o dichiarazioni rivolte all'interessato (articolo 7.2), per esempio all'interno della modulistica.

Non è ammesso il **consenso tacito o presunto** (per esempio, presentando caselle già spuntate su un modulo).

Condizioni per il consenso
art. 7 REG. UE 679/2016

Come deve essere il consenso?

Quando il trattamento riguarda le "categorie particolari di dati personali" (articolo 9 Regolamento) il consenso deve essere "**esplicito**"; lo stesso vale per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – articolo 22).

La "forma scritta" è la modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito".

Il consenso dei minori è valido a partire dai 16 anni*; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

L'interessato deve essere informato che può revocare il consenso in ogni momento senza pregiudicare gli effetti già prodotti.

* 14 anni con il D. LGS. 101/2018

COSA CAMBIA

- Accountability del titolare
- Ruolo del responsabile del trattamento
- Privacy by design e by default
- Valutazione dei rischi
- Adozione misure tecniche ed organizzative adeguate
- Data breach
- Valutazione di impatto (DPIA)
- Data Protection Officer (DPO)
- Risposta all’esercizio dei diritti degli interessati
- Entità delle sanzioni


Registro dei trattamenti
Analisi dei rischi
Privacy by design e by default
Misure di sicurezza adeguate
Data Breach
DPO
DPIA
Diritti degli interessati
Accountability

Accountability
=
Responsabilità verificabile

Art. 24 REG. UE 679/2016

Il titolare del trattamento deve mettere in atto **misure tecniche e organizzative** adeguate per garantire, **ed essere in grado di dimostrare**, che il trattamento è effettuato conformemente al Regolamento, con l'onere di riesaminarle e aggiornarle qualora necessario.

Aiutano a dimostrare la conformità l'adesione ai codici di condotta o ad un meccanismo di certificazione.

Accountability

=

Dovere di documentazione

Il titolare pertanto deve NON SOLO precostituire un **apparato DOCUMENTALE** idoneo a garantire la protezione dai rischi dal punto di vista formale, ma anche un apparato di **misure FISICHE E ORGANIZZATIVE** che proteggano effettivamente gli individui e i loro dati.

L'adeguatezza delle misure si valuta in base alla natura, all'ambito, al contesto, alle finalità, probabilità e gravità dei rischi caratterizzanti l'ambito in cui si opera.

Obblighi del titolare del trattamento

Titolari e responsabili hanno l'obbligo di adottare comportamenti positivi tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.

Si tratta di un'assoluta novità circa l'autonomia e la possibilità di personalizzazione delle procedure in capo a ciascun titolare/responsabile.

Si parla del concetto di data protection BY DEFAULT and BY DESIGN: vi è la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e, al tempo stesso, tutelare i diritti degli interessati tenendo conto del contesto e dei rischi specifici. Assume importanza la specifica previsione dei rischi, che dovrà essere analizzata tramite la valutazione di impatto privacy (DPIA) e assicurata dalla tenuta di un registro dei trattamenti.

L'intervento dell'Autorità di controllo sarà ex post e si collocherà successivamente rispetto alle determinazioni assunte dal titolare: si assiste ad un'*abolizione della notifica preventiva dei trattamenti e del prior checking*.