Regolamento Generale sulla Protezione dei Dati

Ordine CdL di Napoli

Convegno Ramada 23 maggio 2018

Relatori: Francesco Capaccio e Pietro Di Nono

Regolamento Generale sulla Protezione dei Dati

G.D.P.R. è l'acronimo di

General

Data

Protection

Regulation

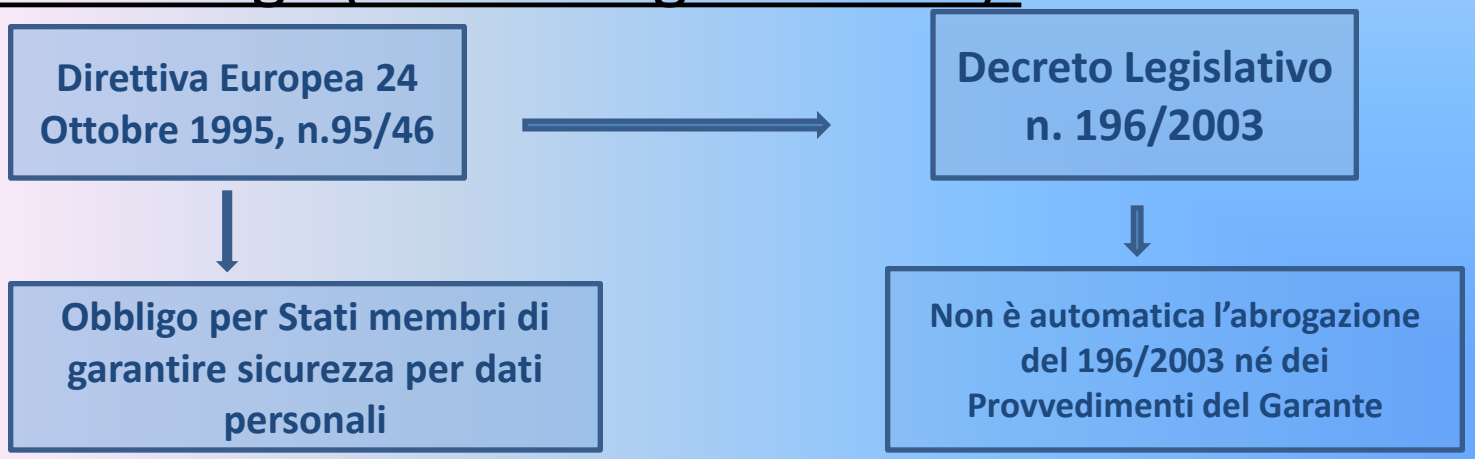
Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27.04.2016

Inquadramento Normativo

Non è un Regolamento nuovo, è stato adottato il 27 aprile 2016 e il 25 maggio 2018 troverà la sua applicazione.

E' una norma *self executing e* non avrà necessità di essere recepita perché entrerà direttamente in uso.

<u>Cosa abroga (art. 94 Regolamento):</u>



Inquadramento Normativo

E’ facoltà degli Stati membri attuare la normativa europea emanando specifiche normative nazionali.

“Gli Stati membri adottano e pubblicano, entro il 6 maggio 2018, le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva. Essi comunicano immediatamente alla Commissione il testo di tali disposizioni. Essi applicano tali disposizioni a decorrere dal 6 maggio 2018”

(Considerando 8)

Inquadramento Normativo

Articolo 13 della **Legge 25 ottobre 2017, n. 163, cd. Legge di "Delegazione Europea" (pubblicata in G.U. 6 novembre** 2017, n. 259, entrata in vigore il 21 novembre 2017).

Inquadramento Normativo

INCOMPATIBILITA'

IL D.LGS. 196/2003 LASCIA SPAZIO AL NUOVO REGOLAMENTO

COMPATIBILITA'

SULLE SINGOLE PRESCRIZIONI SI APPLICA IL PIU' RESTRITTIVO

Inquadramento Normativo

Impostazioni generali del GDPR

Composizione

99 Articoli

173 Considerando (spiegazioni/ considerazioni per comprendere gli articoli)

WP 29 Working Party 29

E' un organismo consultivo e indipendente composto da 1 rappresentante delle autorità garanti per ciascuno Stato .

Fornisce pareri e raccomandazioni

Cambiamento del modo di pensare

Operazione Trasparenza

Da Privacy a Data Protection

Privacy = Dati delle persone

Data protection = Protezione asset aziendali

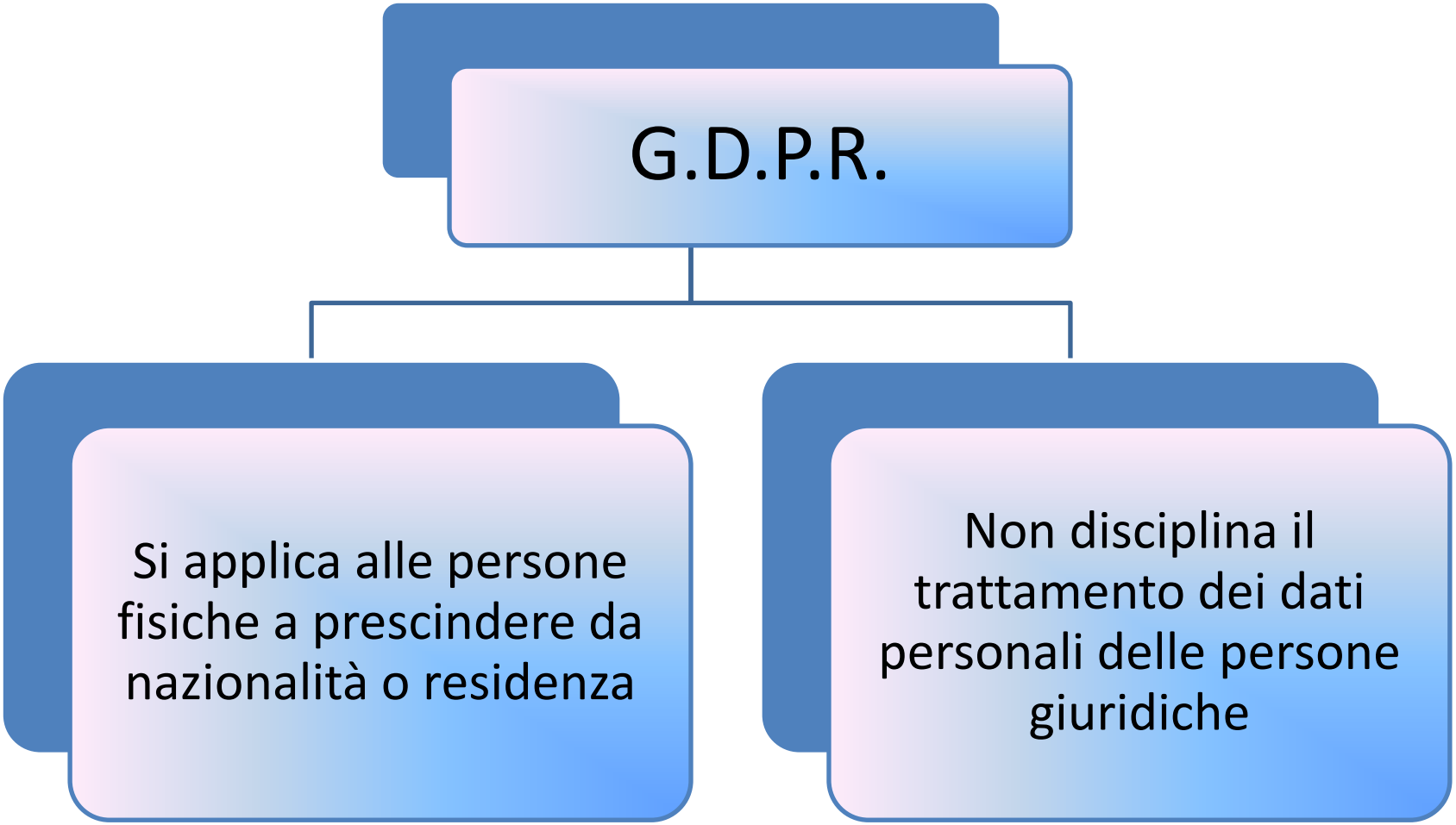

REQUIREMENTS
RULES
LAW
STANDARDS
COMPLIANCE
POLICIES
GOVERNANCE
TRANSPARENCY
REGULATIONS

Finalità del Regolamento – art.1

Aumentare la FIDUCIA delle persone nei confronti delle organizzazioni che trattano i loro dati personali.

Semplificare il LIBERO FLUSSO dei dati personali all'interno dell'UE con un sistema solido e coerente di protezione degli stessi.

Oggetto del Regolamento – art.1



Ambito di Applicazione – art.2 e 3

Materiale

- **Si applica al trattamento automatizzato e non automatizzato (cartaceo);**
- **Non si applica se effettuato da persone fisiche per l'esercizio di attività a carattere domestico (Considerando 18).**

Territoriale

- **Nell'ambito delle attività di uno stabilimento da parte di un Titolare/Responsabile del trattamento sito nell'UE;**
- **Nei confronti di interessati che si trovano nell'UE da parte di un Titolare/responsabile che non è stabilito nell'UE;**
- **Da un Titolare stabilito fuori dall'UE, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale.**

Ambito di Applicazione – art. 2 e 3

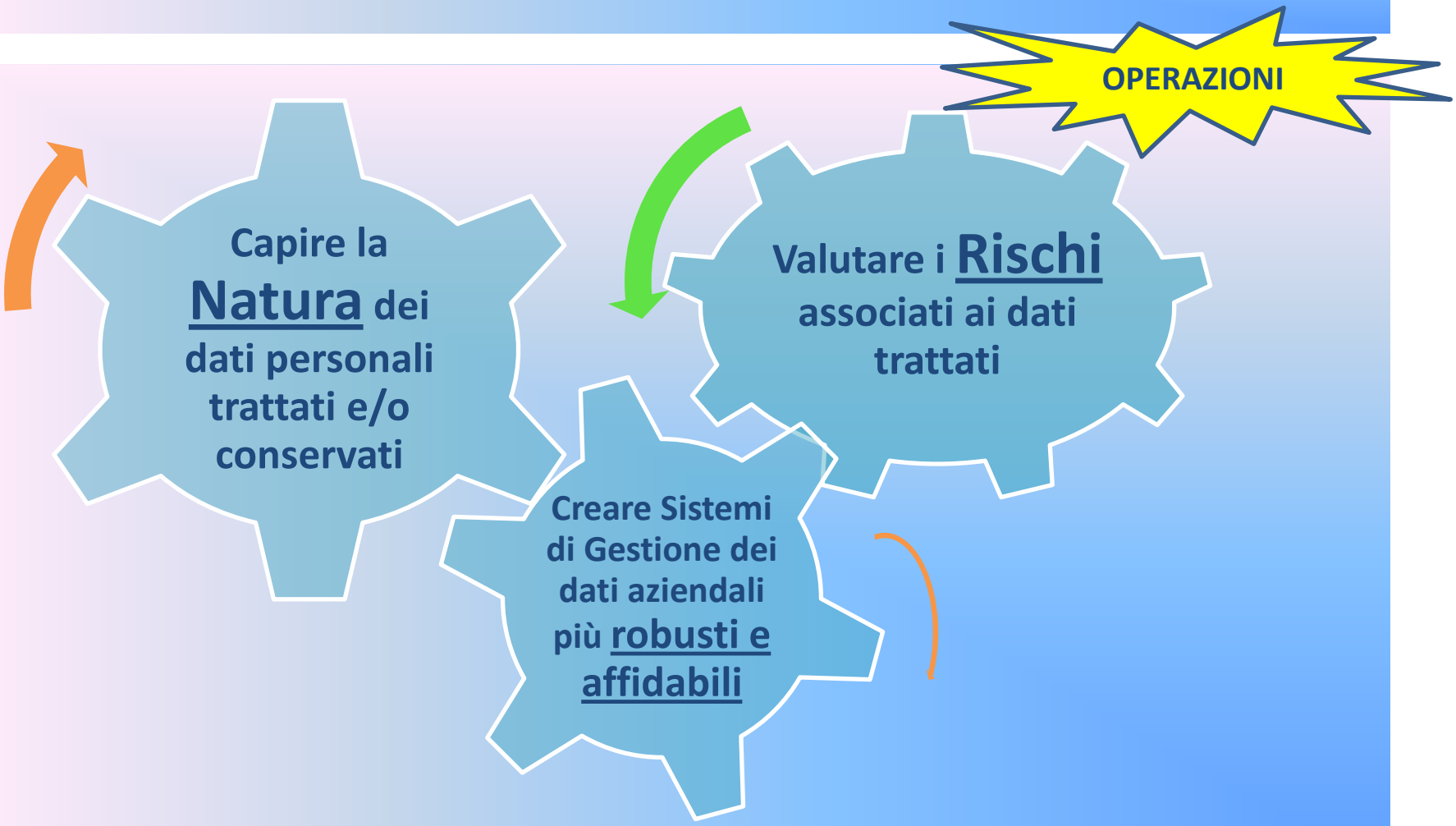
Il G.D.P.R stabilisce norme

Relative alla libera circolazione dei dati

A protezione di diritti e libertà fondamentali

Relative al trattamento dei dati personali

Il Dato nel Nuovo Regolamento



Il Dato nel Nuovo Regolamento

Art. 4 par. 1), 13),14),15) – Considerando 26,27,30,34,35,51

Il Regolamento Privacy all'**articolo 4, n. 1), definisce "dato personale" qualsiasi informazione riguardante una persona fisica identificata o identificabile (ovvero l'interessato).**

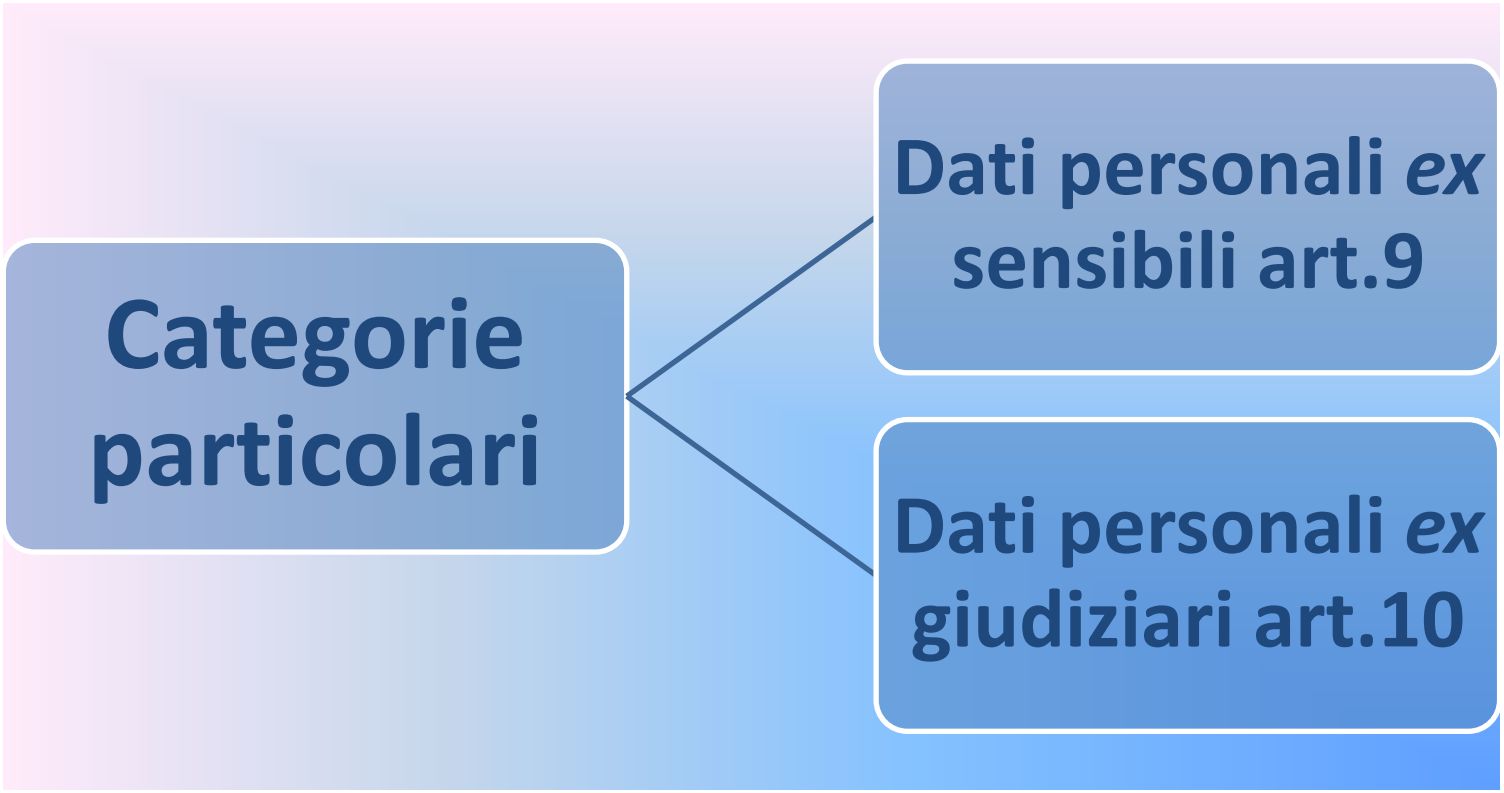
Si considera **identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare** riferimento a un identificativo come il **nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della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

Come evidenziato dal Considerando (30), le persone fisiche possono essere identificate anche mediante:

- **identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali**
- gli indirizzi IP,
- a **marcatori temporanei (cookies) o** identificativi di altro tipo, come i **tag di identificazione a radiofrequenza.**

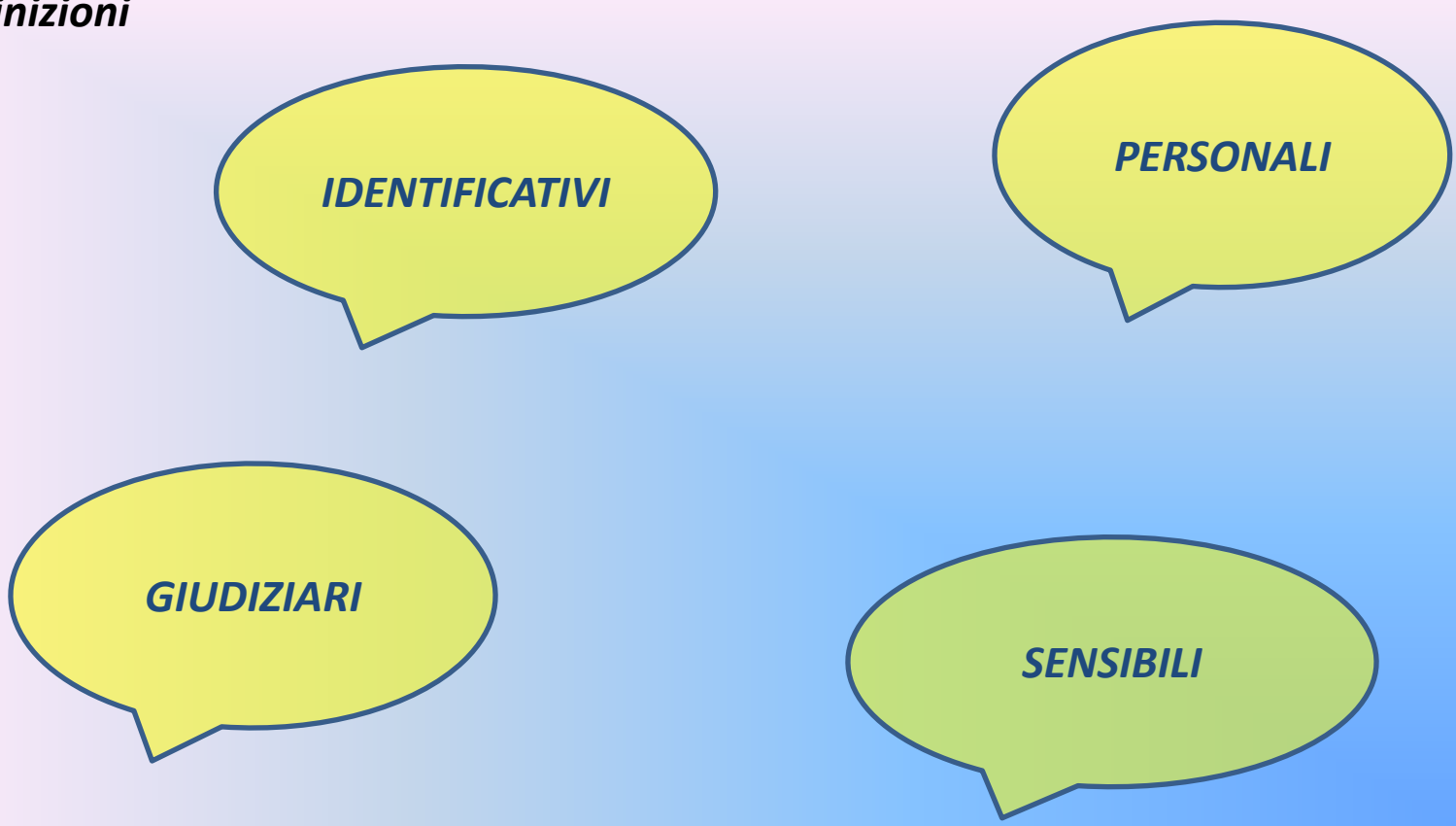
Il Dato nel Nuovo Regolamento

Il Dato personale su categorie particolari



Quadro attuale D.Lgs.196/2003

Definizioni



Quadro attuale D.Lgs.196/2003

DATI SENSIBILI

*"Dati personali idonei a **rivelare** l'origine razziale ed etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché lo stato di salute, e la vita sessuale."*

Quadro attuale D.Lgs.196/2003

DATI GIUDIZIARI

"Dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli Articoli 60 e 61 del codice di procedura penale.."

I Dati nella pratica aziendale

Personali	• Tutti i dati riferiti o riferibili ad un soggetto: nome, cognome, C.F., indirizzo, ecc. (es. clienti, dipendenti)
Sensibili	• Tutti i dati riguardanti l'origine razziale, la religione, le ideologie politiche, lo stato di salute e sessuale (es. dipendenti).
Giudiziari	• Tutti i dati relativi a provvedimenti in corso, carichi pendenti, sanzioni, imputazioni, ecc. (es. dipendenti)

Il Trattamento dei Dati

L'art. 4, n. 2) definisce il trattamento come qualsiasi **operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o insiemi di dati personali.**

Le **operazioni la cui effettuazione è considerata trattamento dei dati sono :**

Raccolta	Registrazione	Organizzazione
Strutturazione	Conservazione	Adattamento
Modifica	Estrazione	Consultazione
Comunicazione	Diffusione	Raffronto
Uso	Interconnessione	Limitazione
Cancellazione	Distruzione	

Limitazione del Trattamento

La limitazione di trattamento è definito dall'**art. 4, n. 3)** come il **contrassegno dei dati personali** **conservati con l'obiettivo di limitarne il trattamento in futuro.**

Tale possibilità è concessa all'interessato al ricorrere di una delle seguenti **ipotesi, elencate nell'art. 18 del Regolamento:**

- l'interessato contesti **l'esattezza dei dati personali**, **per il periodo necessario al titolare del trattamento per verificare** l'esattezza di tali dati personali;
- il **trattamento è illecito** **e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia** limitato l'utilizzo;
- benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per **l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria**;
- **l'interessato** **si è opposto al trattamento** **(articolo 21, paragrafo 1) in attesa della verifica in merito all'eventuale** prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Profilazione dei Dati

L'**art. 4, n. 4)** definisce **"profilazione" qualsiasi forma di trattamento automatizzato di dati personali mediante la** quale sono valutati determinati **aspetti personali relativi a una persona fisica, in particolare per analizzare o prevederne** i seguenti aspetti:

il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti.

*Secondo il **Considerando 71** l'interessato dovrebbe avere diritto di non essere sottoposto a profilazione se non per la sicurezza e affidabilità del servizio richiesto e/o per la conclusione del contratto e comunque solo in caso di consenso esplicito*

Principi Generali per il Trattamento dei Dati

L'articolo 5, Regolamento privacy prevede che i **dati personali devono essere trattati in base ai seguenti principi.**

Liceità, correttezza e trasparenza

un trattamento dei dati personali è lecito a condizione che rispetti almeno una delle seguenti condizioni (art.6):

a) l'**interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;**

b) 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;

c) il **trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;**

d) il **trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;**

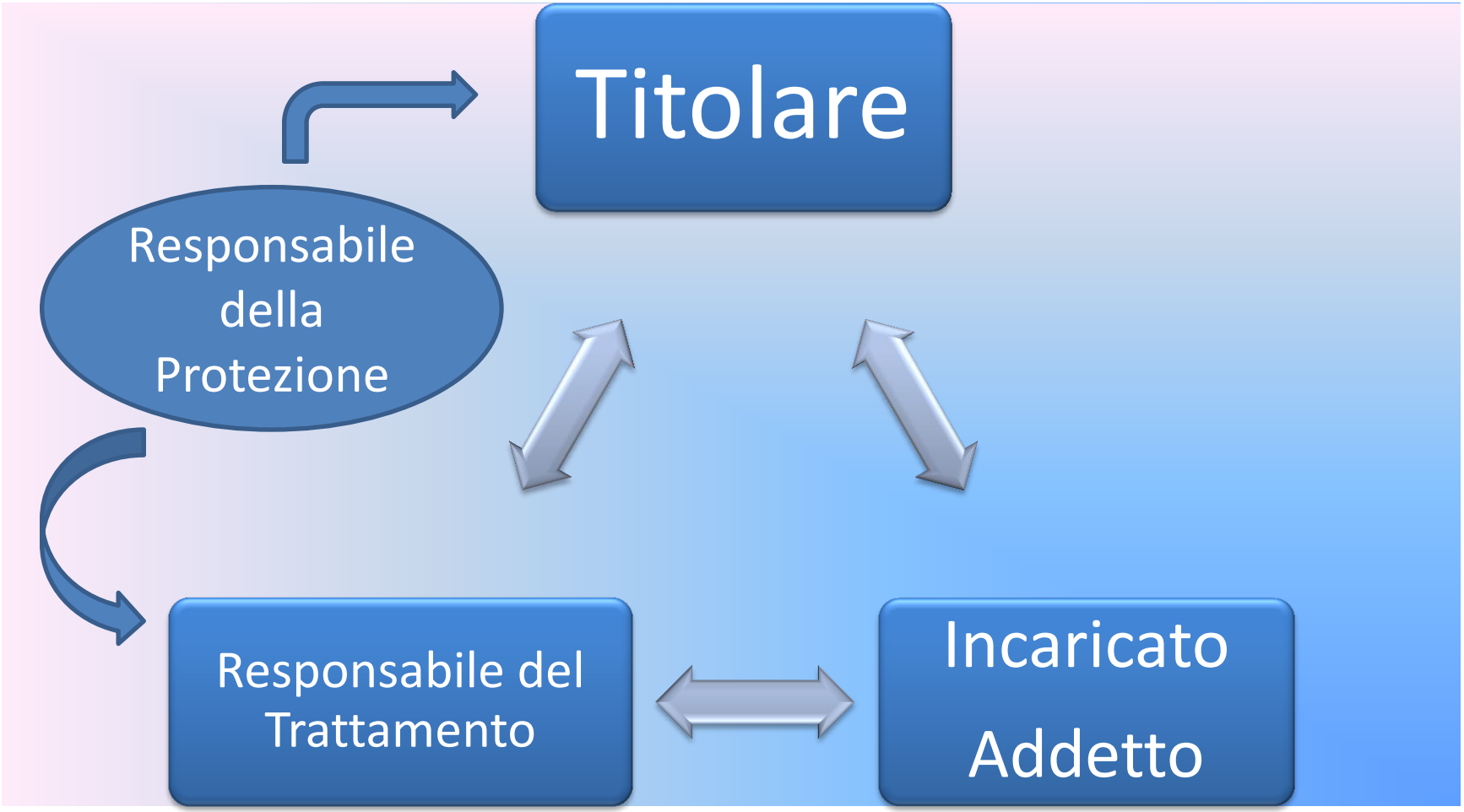
segue

Principi Generali per il Trattamento dei Dati

e) 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;

f) 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.

Le Figure del G.D.P.R

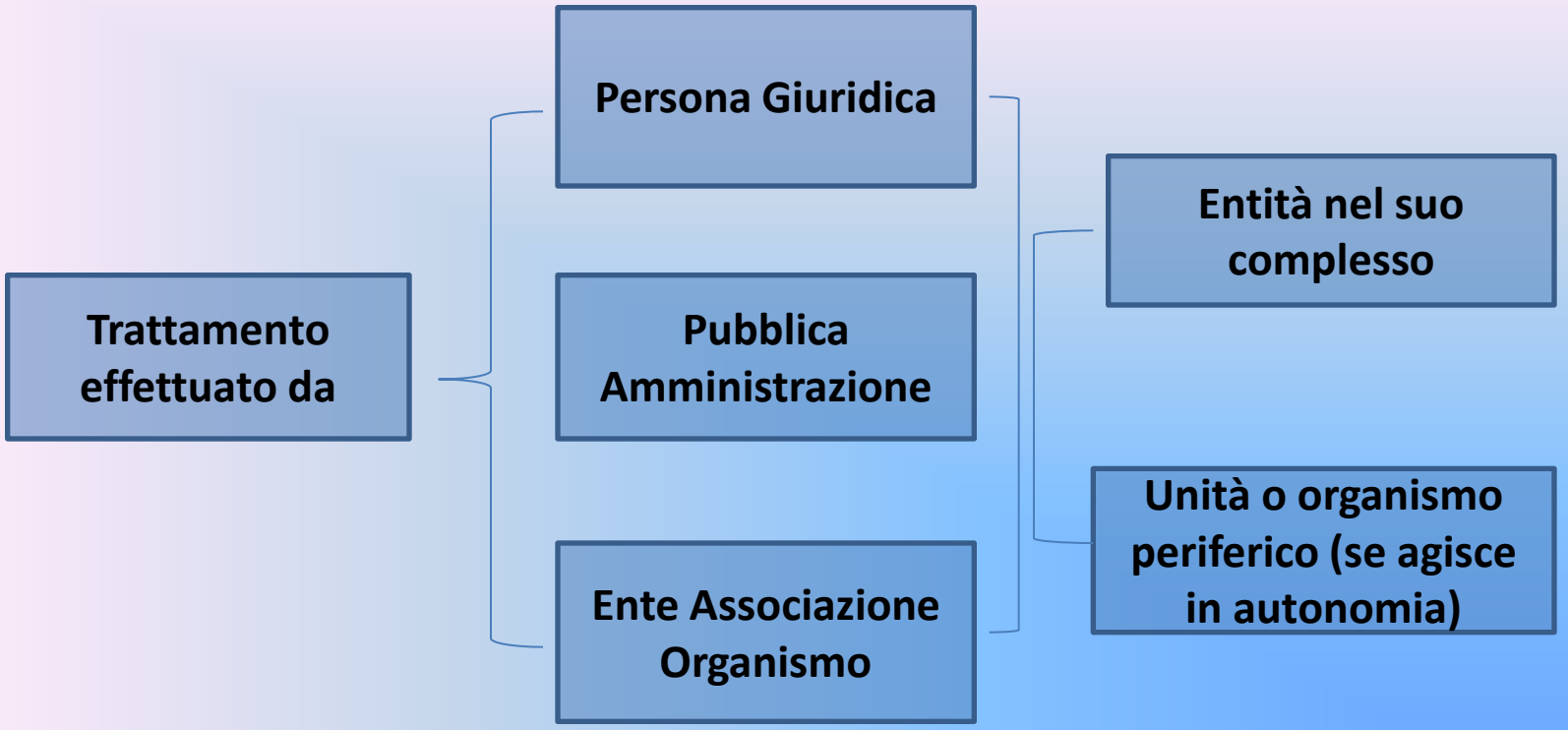


Titolare del Trattamento

Data Controller (Producer) – art. 4, 24, 25 (C.74-C.78)

"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****; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri"*

Titolare del Trattamento



Titolare del Trattamento

Data Controller (Producer) – art. 4, 24, 25 (C.74-C.78)

Il Titolare del Trattamento, oltre a definire le finalità e i mezzi del trattamento deve mettere in atto, ai sensi dell'art. 24, **misure tecniche organizzative adeguate** per garantire ed essere in grado di **dimostrare** che il trattamento è stato effettuato conformemente al Regolamento Privacy.

Titolare del Trattamento

Data Controller (Producer) – art. 4, 24, 25 (C.74-C.78)

Valutazione dei rischi per i diritti e le libertà degli interessati

Secondo il *Considerando* 75 il Titolare deve valutare se il trattamento di dati personali può causare all'interessato un danno fisico, materiale o immateriale.

IL TRATTAMENTO COMPORTA			
DISCRIMINAZIONI	***FURTO IDENTITA'***	***PERDITA RISERVATEZZA***	***MANCANZA CONTROLLO***
DATI EX SENSIBILI	***ASPETTI PERSONALI***	***PROFILI PERSONALI***	***PERSONE VULNERABILI***

Responsabile del Trattamento

Data Processor – art. 4, 28, 29 (C.81)

L'art. 4, n.8) del Regolamento definisce il 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"

"Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti". del presente Regolamento e garantisca la tutela dei diritti dell'interessato". (art. 28, par.1)

Responsabile del Trattamento

Data Processor – art. 4, 28, 29 (C.81)

Art. 28, par. 3

I trattamenti da parte di un Responsabile del Trattamento sono disciplinati da un contratto o da altro atto giuridico che vincoli il Responsabile al Titolare e definisca:

- ***La materia disciplinata***
- ***La durata del trattamento***
- ***La natura e la finalità del trattamento***
- ***Il tipo di dati personali e le categorie di interessati***
- ***Gli obblighi e i diritti del Titolare***

Responsabile del Trattamento

Data Processor – art. 4, 28, 29 (C.81)

Compiti

- E' obbligato alla **tenuta del Registro dei Trattamenti svolti** (*ex*. art.30, par. 2);
- Deve **adottare idonee misure** tecniche e organizzative **per garantire la sicurezza dei trattamenti** (ex art 32);
- Deve **designare un DPO nei casi** previsti dal regolamento o dal diritto nazionale (art. 37 del Regolamento);
- **Se non basato nell'UE dovrà designare un rappresentante in UE quando ricorrono le condizioni** di cui all' art. 27, par. 3 del Regolamento

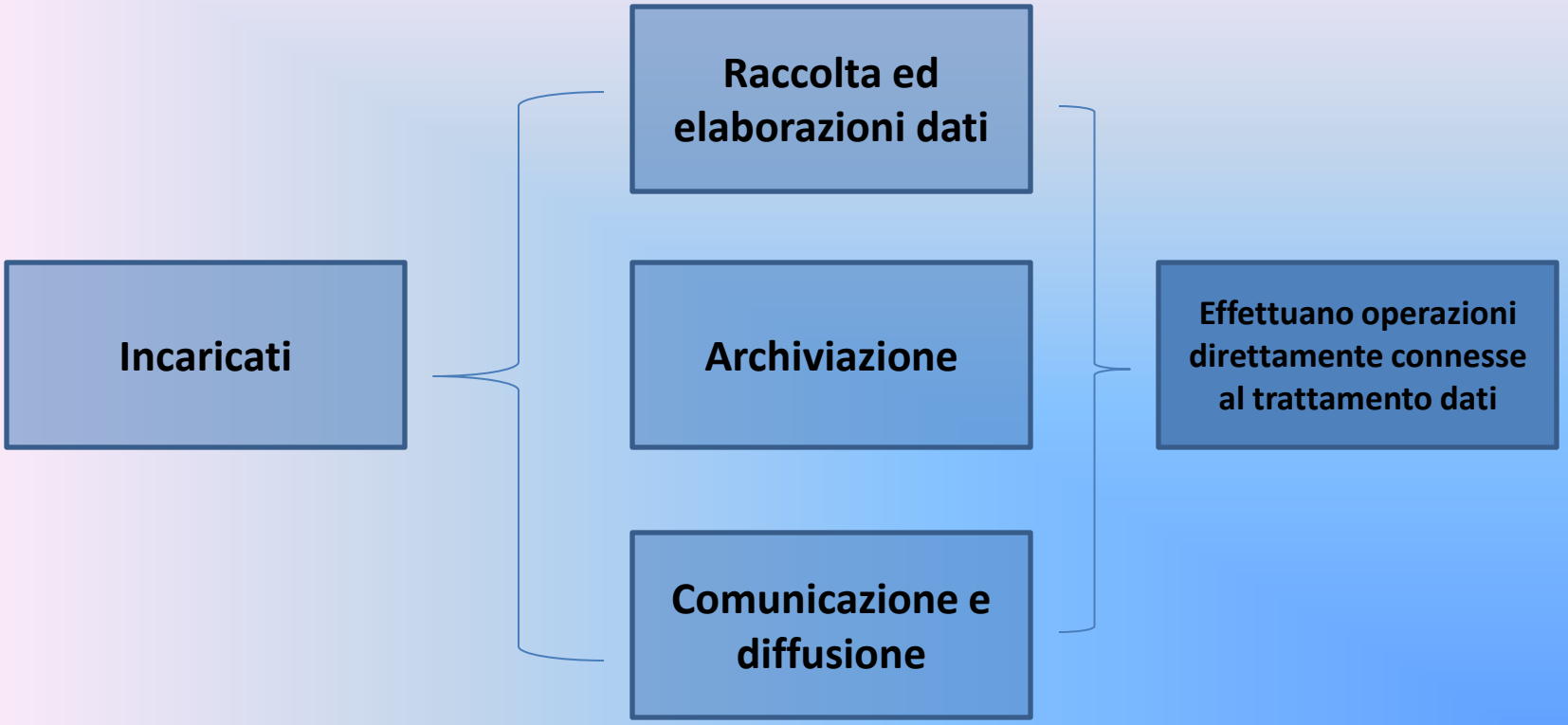
Responsabile del Trattamento

Sub Data Processor – art. 28, par. 4

Il Regolamento consente la nomina di **sub-responsabili** del trattamento da parte di un RTD per specifiche attività di trattamento, **nel rispetto degli stessi obblighi contrattali che legano il 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).

Incaricato del Trattamento

Person Authorised to Process – artt. 4, 29



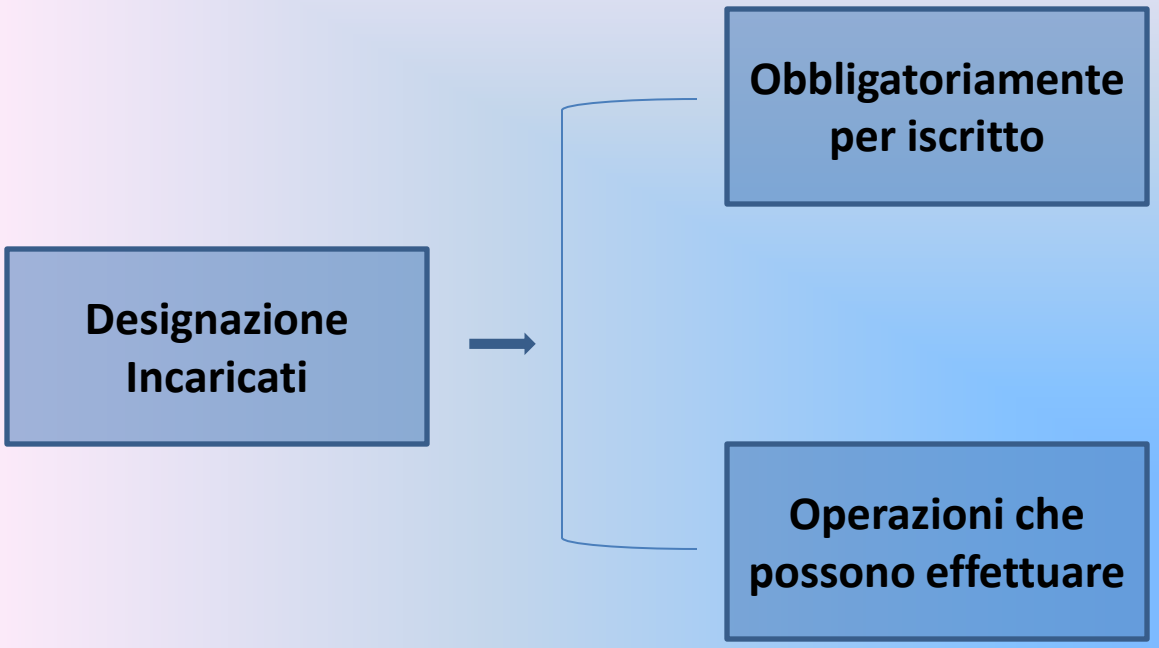
Incaricato del Trattamento

Diversamente a quanto previsto nel D.Lgs. n. 196/2003, nel Regolamento n. 679/2016 la figura dell'incaricato al trattamento **non è definita in maniera esplicita**: tuttavia, come si evince dalla lettura di vari articoli del Regolamento e come confermato dal Garante della privacy, detta figura è presente anche nella nuova disciplina privacy:

- **persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile (articolo** 4, n. 10) e art. e 28);
- **personale che esegue i trattamenti (art. 39);**
- **personale che ha accesso permanente o regolare ai dati personali (art. 47, par. 2).**

Incaricato del Trattamento

Person Authorised to Process – artt. 4, 29



Destinatario del Trattamento

Data Recipient – art. 4

"La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, **le autorità pubbliche** che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri **non sono considerate destinatari**; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento"

Responsabile della Protezione

Data Protection Officer – art. 37,38,39

"Il responsabile della protezione dei dati è una persona **esperta** nella protezione dei dati, il cui compito è **valutare e organizzare la gestione del trattamento** di dati personali, e dunque la loro protezione, all'interno di un'azienda, di un ente o di una associazione, affinché questi siano trattati in modo lecito e pertinente". **Può essere interno o esterno (DPO Team)**

E' nominato (per obbligo o facoltà) dal titolare del trattamento, è un **esperto in materia** che si pone **"interfaccia"** tra i vari soggetti coinvolti nella privacy, vigilando sulla corretta applicazione del Regolamento.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Scheda aggiornata in base alla versione delle Linee guida del WP29 emendata e adottata il 5 aprile 2017

Il Responsabile della protezione dei dati (RPD) o Data Protection Officer (DPO)

La scheda presenta la figura del Responsabile della protezione dei dati (RPD), o Data Protection Officer (DPO), in base a quanto previsto dal Regolamento (UE) 2016/679 e dalle Linee-guida del WP29

QUALI SONO I REQUISITI?

Il Responsabile della protezione dei dati, 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**, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze.
2. **adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse** . In linea di principio, ciò significa che il RPD non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali;
3. **operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio** (RPD/DPO esterno).

Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

IN QUALI CASI E' PREVISTO?

Dovranno designare obbligatoriamente un RPD:

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.

Anche per i casi in cui il regolamento non impone in modo specifico la designazione di un RPD, è comunque possibile una nomina su base volontaria.

Un gruppo di imprese o soggetti pubblici possono nominare un unico RPD.

QUALI SONO I COMPITI?

Il Responsabile della protezione dei dati dovrà, in particolare:

a) **sorvegliare l'osservanza del regolamento**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
b) collaborare con il titolare/responsabile, laddove necessario, nel condurre una **valutazione di impatto sulla protezione dei dati (DPIA);**
c) informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
d) cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;
e) supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un **registro delle attività di trattamento** .

La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento. Per un quadro completo: www.garanteprivacy.it/rpd

Quali sono i requisiti ?

In quali casi è previsto?

Quali sono i suoi compiti ?

Responsabile della Protezione

Data Protection Officer – art. 37,38,39

Il Titolare del Trattamento **pubblica i dati** di contatto e li comunica all'autorità di controllo;

E' designato (art.39) in base alle **qualità professionali**, alla **conoscenza specialistica**, alla prassi in materia di protezione dati e alla capacità di assolvere i compiti affidati;

Deve essere messo a conoscenza e **coinvolto** nelle questioni che riguardano la protezione dei dati personali

Responsabile della Protezione

Data Protection Officer – art. 37,38,39

NOMINA OBBLIGATORIA

- trattamento di un'**autorità pubblica o di un organismo pubblico;**
- le attività principali richiedono un **monitoraggio regolare e sistematico degli interessati su larga scala;**
- si effettua un trattamento su **larga scala di categorie particolari di dati (ex sensibili) e di dati penali (ex giudiziari)**

NOMINA FACOLTATIVA

negli altri casi.

Il WP 29 raccomanda di documentare le valutazioni compiute per la nomina di un DPO

Responsabile della Protezione

MONITORAGGIO (*C.24)-WP29*

Regolare **e** **Sistematico**

- **Che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;**
- **Ricorrente o ripetuto a intervalli costanti;**
- **Che avviene in modo costante o a intervalli periodici.**

- **Che avviene per sistema; predeterminato, organizzato o metodico;**
- **Che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;**
- **Che è svolto nell'ambito di una strategia.**

Responsabile della Protezione

Larga scala – WP 29

- ***il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;***
- ***il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;***
- ***la durata, ovvero la persistenza, dell'attività di trattamento;***
- ***la portata geografica dell'attività di trattamento.***

Interessato

artt. 4,15,16,17,18,20,21,22 – Capo III

“La persona fisica identificata o identificabile. 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”.

Diritti dell'Interessato

Diritti dell'Interessato	Articoli	Previsione
Diritto di accesso	15	L'**interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e** in tal caso, di **ottenere l'accesso ai dati personali e ad una serie di informazioni,** tra le quali: - le **finalità del trattamento;** - le **categorie di dati personali in questione;** - i **destinatari o le categorie di destinatari a cui i dati personali sono stati o** saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
Diritto di rettifica	16	**L'interessato ha il diritto di ottenere dal titolare del trattamento:** **- la rettifica dei dati personali inesatti che lo riguardano;** **- l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.**

Diritti dell'Interessato

Diritti dell'Interessato	Articoli	Previsione
Diritto alla cancellazione	17	**L'interessato ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano se sussiste uno degli specifici motivi indicati normativamente, tra i quali si ricordano i seguenti:** **- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;** **- l'interessato revoca il consenso su cui si basa il trattamento;** **- l'interessato si oppone al trattamento;**
Diritto alla limitazione di trattamento	18	**L'interessato ha il diritto di ottenere la limitazione del trattamento quando si verifica una delle ipotesi previste normativamente, tra le quali:** **- l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;** **- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo.**

Diritti dell'Interessato

Diritti dell'Interessato	Articoli	Previsione
Diritto alla portabilità dei dati	20	**L'interessato ha 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; - trasmettere tali dati a un altro titolare del trattamento.**
Diritto di opposizione	21	**L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali.**
Diritto di non essere sottoposto a trattamenti automatizzati	22	**L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.**

Diritti dell'Interessato

COSA CAMBIA

*Il **termine per la risposta** all'interessato è, per tutti i diritti (compreso il diritto di accesso), **1 mese (anche in caso negativo), estendibile fino a 3 mesi in casi di particolare complessità.***

Comunque entro 1 mese si deve dare **riscontro** della presa in carico.

Il TTD può valutare l'eventuale **contributo per la ricerca** **(per richieste manifestamente** infondate, eccessive o ripetitive)

Riscontro in **forma scritta / elettronica (a voce se richiesto dall'interessato)**

Risposta concisa, trasparente e facilmente accessibile, con **linguaggio semplice e chiaro**

INFORMATIVA DATI PERSONALI

Art 13 Par 1, Art 14 Par 1

"L'informativa è una dichiarazione che il titolare o il responsabile fa all'interessato circa l'utilizzo delle informazioni che lo riguardano"

CARATTERISTICHE

CONCISA	TRASPARENTE	INTELLEGIBILE
ACCESSIBILE	LINGUAGGIO SEMPLICE	RAFFORZATA PER I MINORI
INFORMATIVA STRATIFICATA		

INFORMATIVA DATI PERSONALI

Art 13 Par 1, Art 14 Par 1

INFORMAZIONI “DI BASE” DA FORNIRE ALL’INTERESSATO - ART. 13, PAR. 1

a) l’identità e **i dati di contatto del titolare del trattamento** e, ove applicabile, del suo rappresentante;

b) **i dati di contatto del responsabile della protezione dei dati**, ove applicabile;

c) le **finalità** del trattamento cui sono destinati i dati personali nonché la **base giuridica del trattamento;**

d) qualora il trattamento sia 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, i **legittimi interessi perseguiti** dal titolare del trattamento o da terzi;

e) gli **eventuali destinatari** o le eventuali categorie di destinatari dei dati personali;

f) ove applicabile, **l’intenzione** del titolare del trattamento **di trasferire dati** personali a un paese terzo o a un’organizzazione internazionale

ULTERIORI INFORMAZIONI DA FORNIRE ALL'INTERESSATO - ART. 13, PAR. 2

a) il **periodo di conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) 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;

c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di **revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il diritto di **proporre reclamo** a un'autorità di controllo;

segue

ULTERIORI INFORMAZIONI DA FORNIRE ALL'INTERESSATO - ART. 13, PAR. 2

e) 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;

f) l'esistenza di un **processo decisionale automatizzato**, compresa la **profilazione** e almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

INFORMATIVA DATI PERSONALI

Art 14 Par 1

Se i dati NON sono stati forniti dall'interessato:
La Fonte da cui hanno origine i dati personali e, se del caso, se provengano da fonti accessibili al pubblico

In questo caso l'Informativa è data ENTRO UN MESE o comunque entro un tempo ragionevole e prima della comunicazione dei dati

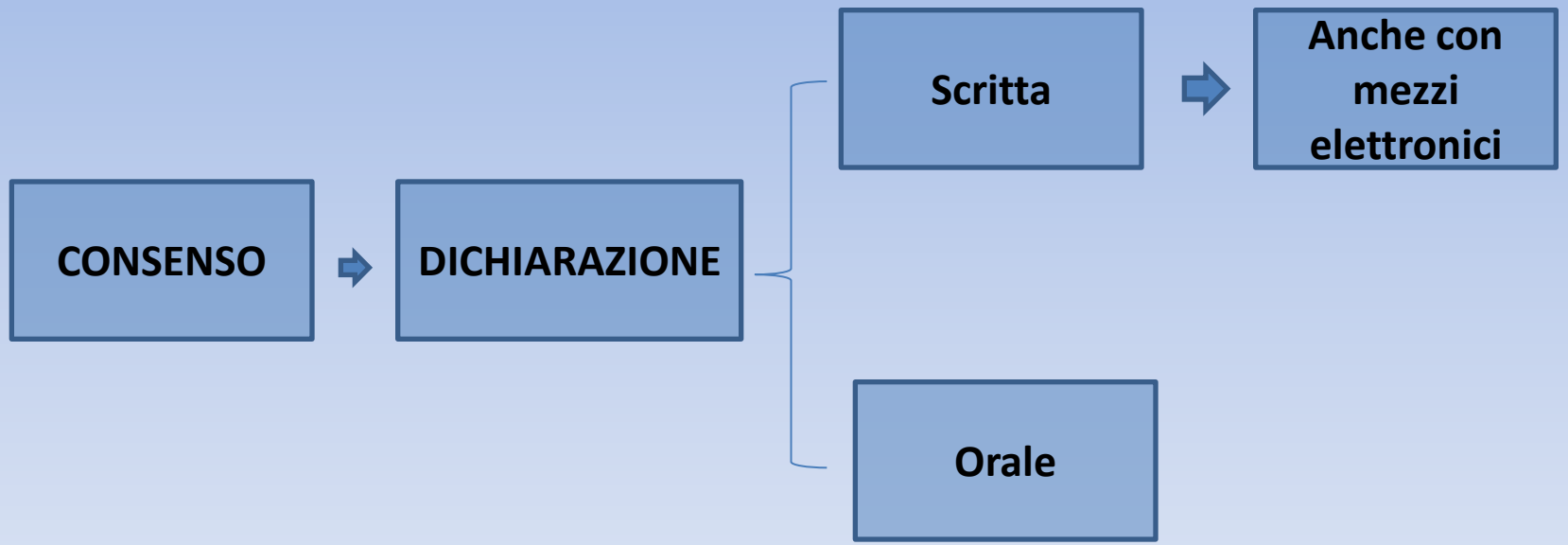
CONSENSO

Art. 4, 7 – C. 32, 42

"Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento"

NON PUO' PIU' ESSERE TACITO!

CONSENSO IN FORMA SCRITTA



Il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento

CONSENSO IN FORMA SCRITTA

E’ 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, **salvo che l’interessato abbia prestato il proprio consenso esplicito al trattamento (art.9).**

DATI PARTICOLARI → **CONSENSO IN FORMA SCRITTA** → **SOTTOSCRIZIONE INTERESSATO**

CONSENSO DEI MINORI

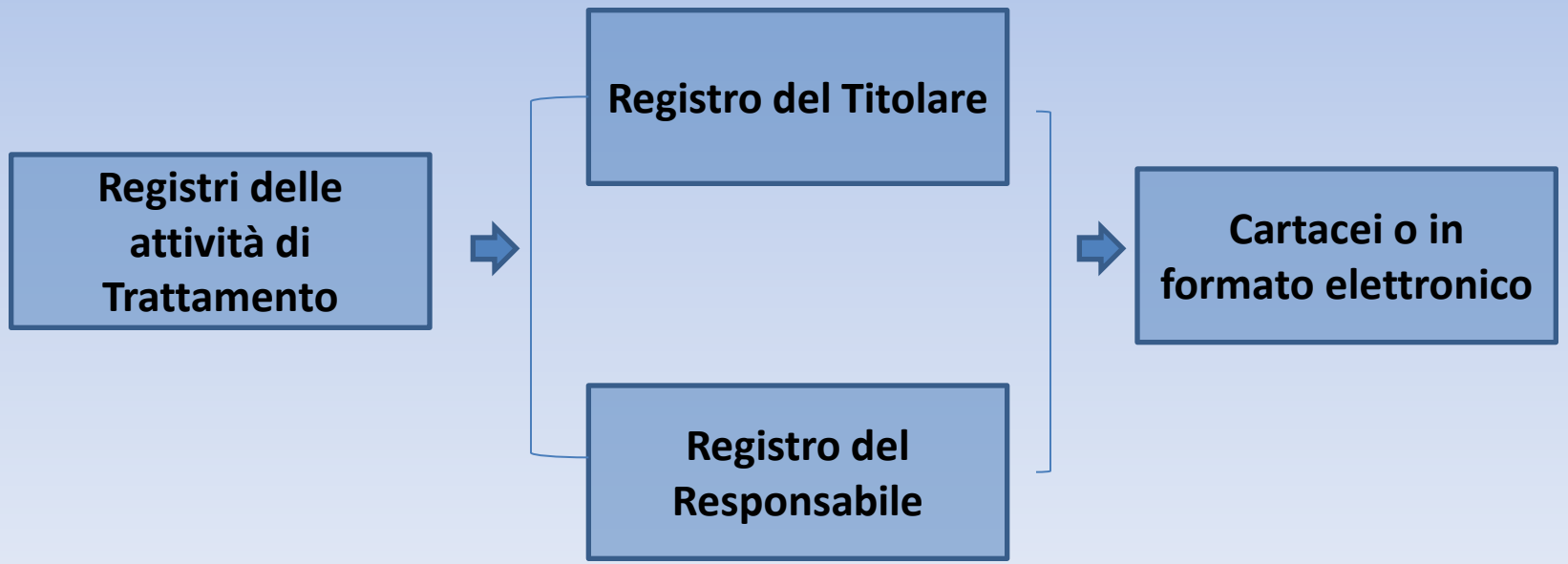
L'art. 8, Regolamento privacy, prevede inoltre che per quanto riguarda l'offerta diretta ai minori di servizi delle società di informazione, il **trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni.**

Gli Stati membri possono comunque stabilire per legge un'età inferiore a tali fini **purché non inferiore ai 13 anni.**

Se il **minore ha un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura** in cui il **consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.**

Registri delle Attività di Trattamento

L'art. 30, par. 1 e 2, prevede che ogni Titolare del trattamento e, ogni Responsabile del trattamento, tengono un registro delle attività di trattamento.



Registro del Titolare

Contenuto art.30, par.1:

il nome e i dati di contatto del titolare del trattamento	**le finalità del trattamento**	**descrizione delle categorie di interessati e delle categorie di dati personali**
categorie di destinatari a cui i dati personali sono stati o saranno comunicati	**trasferimenti di dati personali verso un paese terzo**	**termini ultimi previsti per la cancellazione**
descrizione generale delle misure di sicurezza tecniche e organizzative		

Registro del Responsabile

Contenuto art.30, par.2:

il nome e i dati di contatto del responsabile del trattamento e di ogni titolare del trattamento per conto del quale agisce e, ove applicabile, del responsabile della protezione dei dati	**le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento**
ove applicabile, i **trasferimenti di dati personali verso un paese terzo**	una **descrizione generale delle misure di sicurezza tecniche e organizzative**

Registri delle Attività di Trattamento

L'art. 30, par. 5, dispone che l'obbligo di tenuta dei **registri delle attività di trattamento** **non si applica alle imprese** o organizzazioni con **meno di 250 dipendenti, a meno che il trattamento**:

- possa presentare un **rischio per i diritti e le libertà dell'interessato,**
- **non sia occasionale;**
- includa **categorie particolari di dati di cui all'articolo 9, paragrafo 1, ovvero il trattamento** riguardi dati che possono rilevare l'origine razziale o etnica, l e opinioni politiche, l e convinzioni religiose o filosofiche; l'appartenenza sindacale, genetici, biometrici intesi a identificare in modo univoco una persona fisica, relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- preveda l'utilizzo di **categorie di dati personali relativi a condanne penali e a reati.**

Registri delle Attività di Trattamento

Il Garante della privacy evidenzia che il registro dei trattamenti è:

"...uno ***strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante,*** *ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico –* ***indispensabile per ogni valutazione e analisi del rischio".***

Per tale motivo, il Garante **invita tutti i titolari di trattamento e i responsabili, indipendentemente dalle dimensioni dell'organizzazione:**

- **dotarsi di tale registro e, in ogni caso,**
- **compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche.**

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

Data Protection Impact assessment (artt. 35-36)

Si tratta di una specifica analisi sullo stato dell'arte
che i TTD devono eseguire

Consiste nell'analisi dei rischi e nella stesura di un action plan per ridurre tali rischi.
E' necessario poi un controllo semestrale/annuale degli interventi eseguiti.

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

Gli esperti del WP 29 forniscono una **definizione di "valutazione di impatto" (non presente** nell'articolo 35, Regolamento n. 679/2016) da intendersi come la **procedura finalizzata a:**

- **descrivere il trattamento,**
- valutarne **necessità e proporzionalità,**
- facilitare la **gestione dei rischi (misure) per i diritti e le libertà delle persone fisiche,** che possono derivare dal trattamento dei loro dati

"...è uno strumento importante in termini di responsabilizzazione (accountability) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del GDPR, ma anche a dimostrare l'adozione di misure idonee a garantire il rispetto di tali prescrizioni [...]. In altri termini, la DPIA è una procedura che permette di realizzare e dimostrare la conformità con le norme".

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

Data Protection Impact assessment (artt. 35-36)

RISCHIO	MISURE
Non elevato	Adozione di misure idonee
Elevato	Prima dell'adozione delle misure idonee e del trattamento è necessario effettuare un **DPIA**
Elevato senza possibilità di attenuare il rischio	Consultazione del Garante Privacy

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

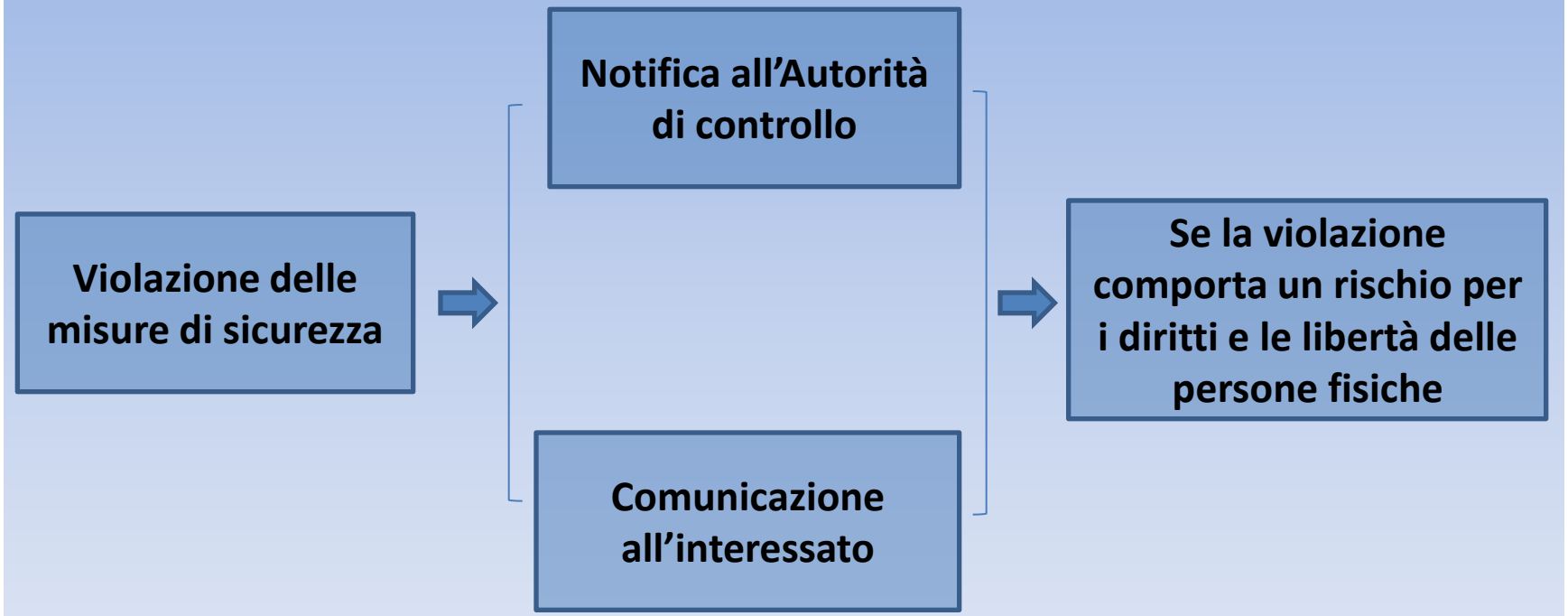
QUANDO È NECESSARIO CONDURRE UNA VALUTAZIONE DI IMPATTO

Se un trattamento soddisfa 2 dei seguenti criteri

Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive	**Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura**	**Monitoraggio Sistematico**
Dati sensibili o dati di natura estremamente personale	Trattamenti di dati su larga scala	Combinazione o raffronto di insiemi di dati
Dati relativi a interessi vulnerabili (considerando 75)	Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative	Impediscono di esercitare un diritto o di avvalersi di un servizio o di un contratto.

COMUNICAZIONI DI VIOLAZIONI

Data Breach (artt. 33,34)



COMUNICAZIONI DI VIOLAZIONI

La notifica (art.33) deve contenere:

- la **natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo** di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali;

- comunicare il nome e i **dati di contatto del responsabile della protezione dei dati** o di altro punto di contatto presso cui ottenere più informazioni;

- le **probabili conseguenze** della violazione dei dati personali;

- descrivere le **misure adottate** o di cui si propone l'adozione da parte del titolare del trattamento per **porre rimedio alla violazione** dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

COMUNICAZIONI DI VIOLAZIONI

La notifica deve essere inviata all'autorità competente senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui il titolare è venuto a conoscenza** della violazione, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, deve essere corredata dai motivi del ritardo.

SANZIONI AMMINISTRATIVE PECUNIARIE

Art. 83, C. 148,150-152

ELEMENTI DA CONSIDERARE PER DETERMINARE LA SANZIONE

La natura, la gravità e la durata della violazione	**Il carattere doloso o colposo**	**Le misure adottate per attenuare il danno subito**
Il grado di responsabilità del titolare	**Eventuali precedenti violazioni**	**Grado di cooperazione con l'autorità di controllo**
Categorie di dati personali interessate	**Modalità di conoscenza della violazione**	**L'adesione ai codici di condotta ai meccanismi di certificazione**

SANZIONI AMMINISTRATIVE PECUNIARIE

Tipologia di violazione	Articoli Regolamento	Sanzione
Obblighi del titolare e del responsabile del trattamento	**8,11 da 25 a 39, 42 e 43**	**Fino a 10 milioni di euro o per le imprese fino al 2% del fatturato totale dell'esercizio**
Principi di base del trattamento, comprese le condizioni relative al consenso	**5,6,7 e 9**	**Fino a 20 milioni di euro o per le imprese fino al 4% del fatturato totale dell'esercizio**
Diritti degli interessati	**da 12 a 22**	
Trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale	**da 44 a 49**	
Inosservanza di un ordine, di una limitazione dell'A.G.	**58, par. 1 e 2**	