

Il ruolo del Garante nell'applicazione della normativa in materia di protezione dei dati personali. Riflessioni sulla giurisprudenza nazionale e della Corte UE

Francesco MODAFFERI



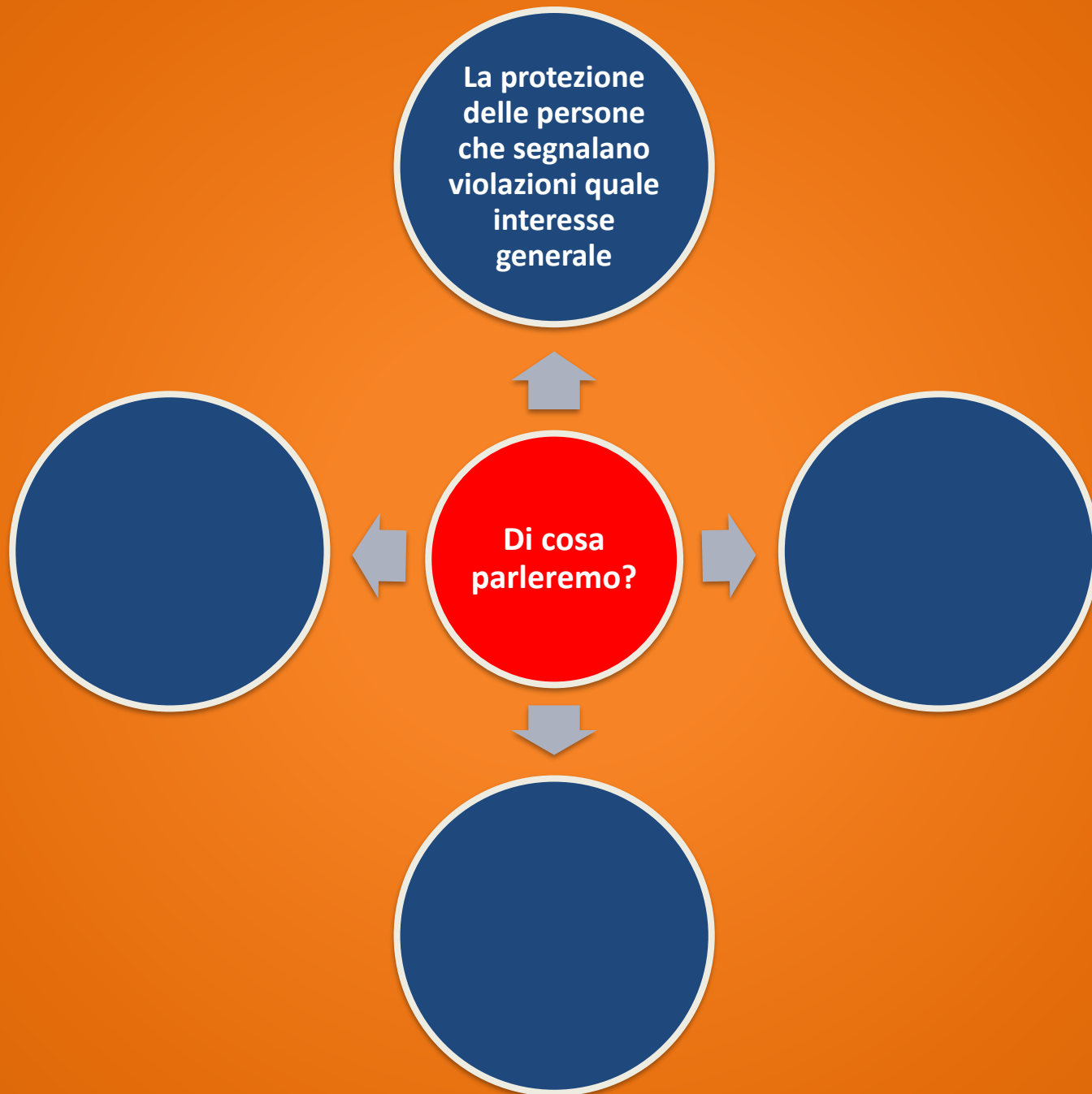
La protezione delle persone che segnalano violazioni quale interesse generale

Le indicazioni del Garante

La base giuridica del trattamento

Di cosa parleremo?

I principali temi di protezione dati e le disposizioni della nuova disciplina



La prevenzione delle violazioni quale interesse generale



Chi lavora per un'organizzazione pubblica o privata o è in contatto con essa nello svolgimento della propria attività professionale è spesso la prima persona a venire a conoscenza di minacce o pregiudizi al pubblico interesse sorti in tale ambito.

Nel segnalare violazioni del diritto unionale che ledono il pubblico interesse, tali persone (gli «informatori - whistleblowers») svolgono un ruolo decisivo nella denuncia e nella prevenzione di tali violazioni e nella salvaguardia del benessere della società.

Il rischio di ritorsioni e la protezione degli informatori

I potenziali informatori sono spesso poco inclini a segnalare inquietudini e sospetti nel timore di ritorsioni.

In tale contesto, l'importanza di garantire una protezione equilibrata ed efficace degli informatori è sempre più riconosciuta a livello sia unionale che internazionale, in quanto forniscono informazioni che portano all'indagine, all'accertamento e al perseguimento dei casi di violazione delle norme dell'Unione, rafforzando in tal modo i principi di trasparenza e responsabilità



La direttiva (UE) 2019/1937 del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione



Attualmente la protezione garantita agli informatori nell'Unione non è uniforme tra gli Stati membri e non è armonizzata tra i vari settori.

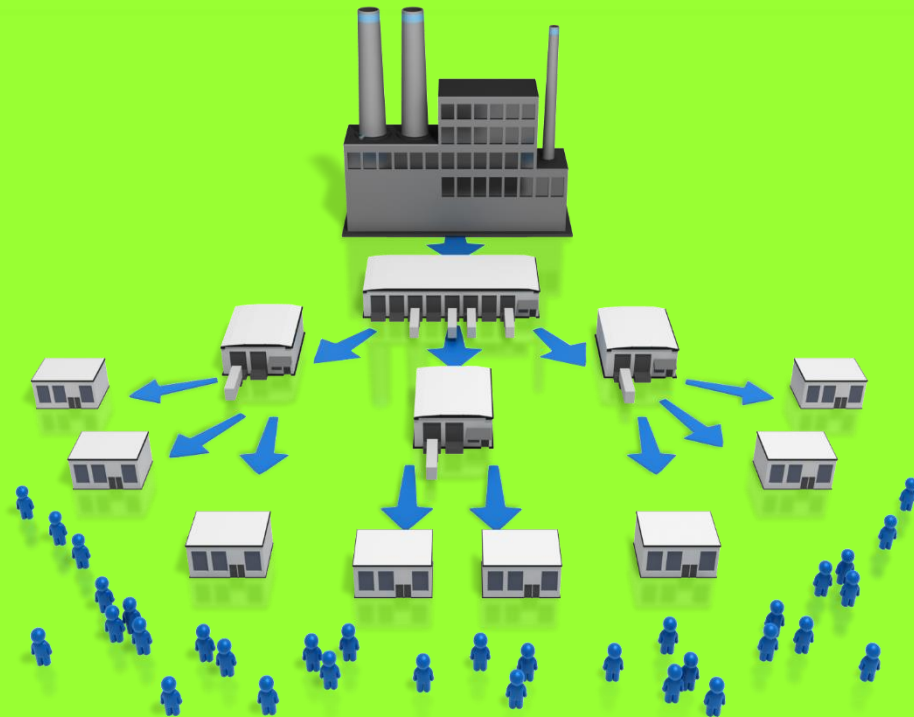
Le conseguenze delle violazioni del diritto dell'Unione aventi una dimensione transfrontaliera comunicate dagli informatori dimostrano come l'assenza di un livello di protezione sufficiente in un dato Stato membro può avere conseguenze negative sul funzionamento delle politiche dell'Unione non solo al suo interno ma anche in altri Stati membri e nell'Unione nel suo insieme.

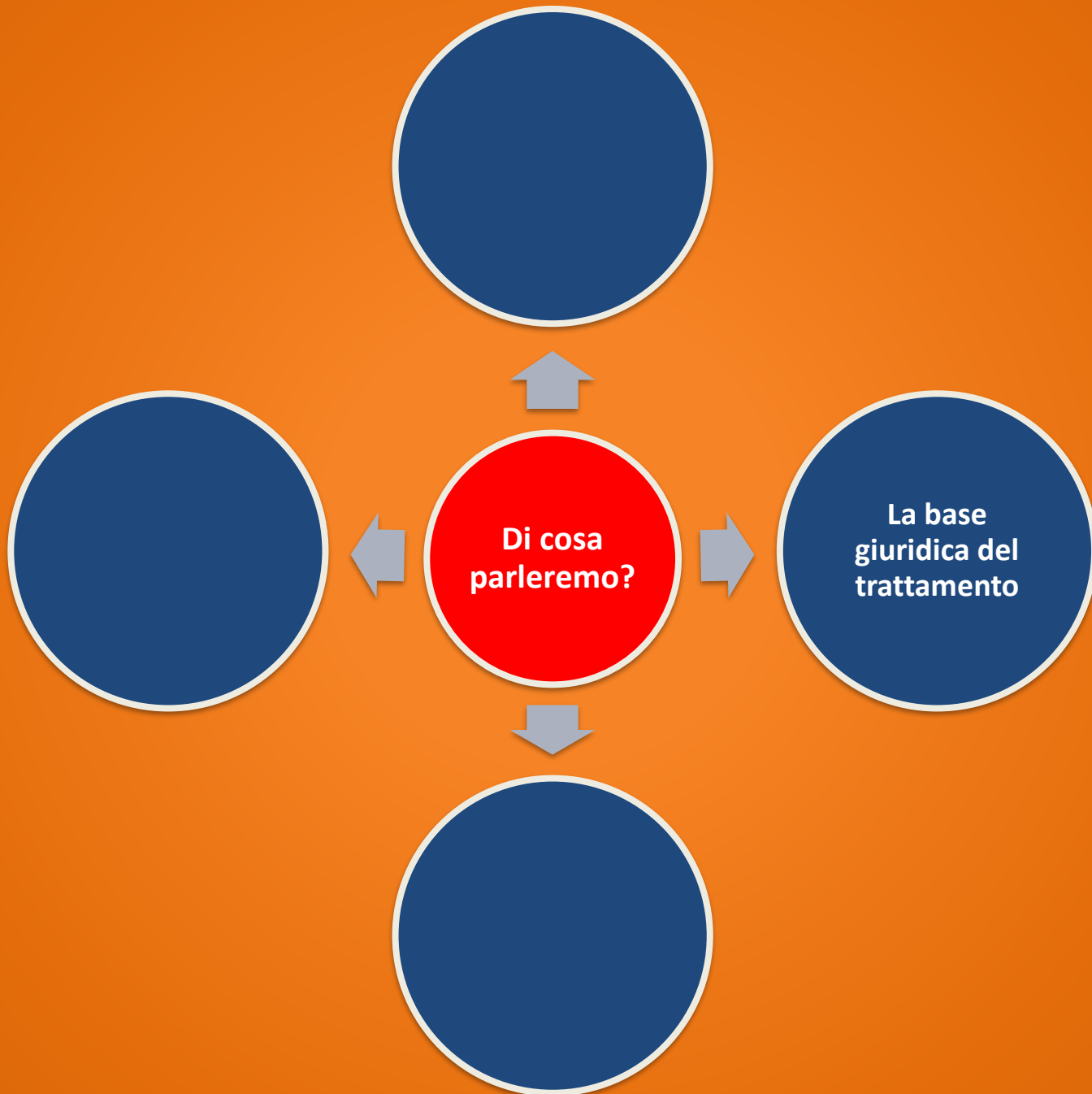
DECRETO LEGISLATIVO 10 marzo 2023, n. 24
attuazione della direttiva (UE) 2019/1937

Con il d.lgs. 24/2023 si raccoglie, in un unico testo normativo, l'intera disciplina dei canali di segnalazione e delle tutele riconosciute ai segnalanti sia del settore pubblico che privato.







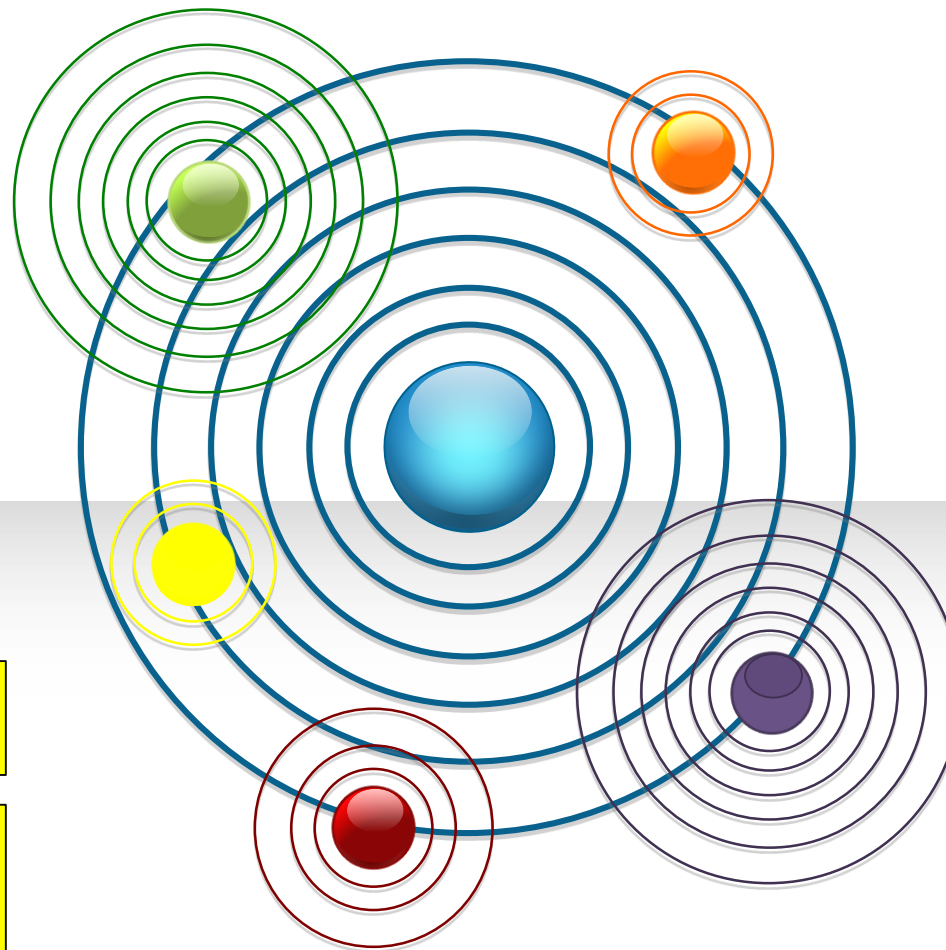
Settore privato



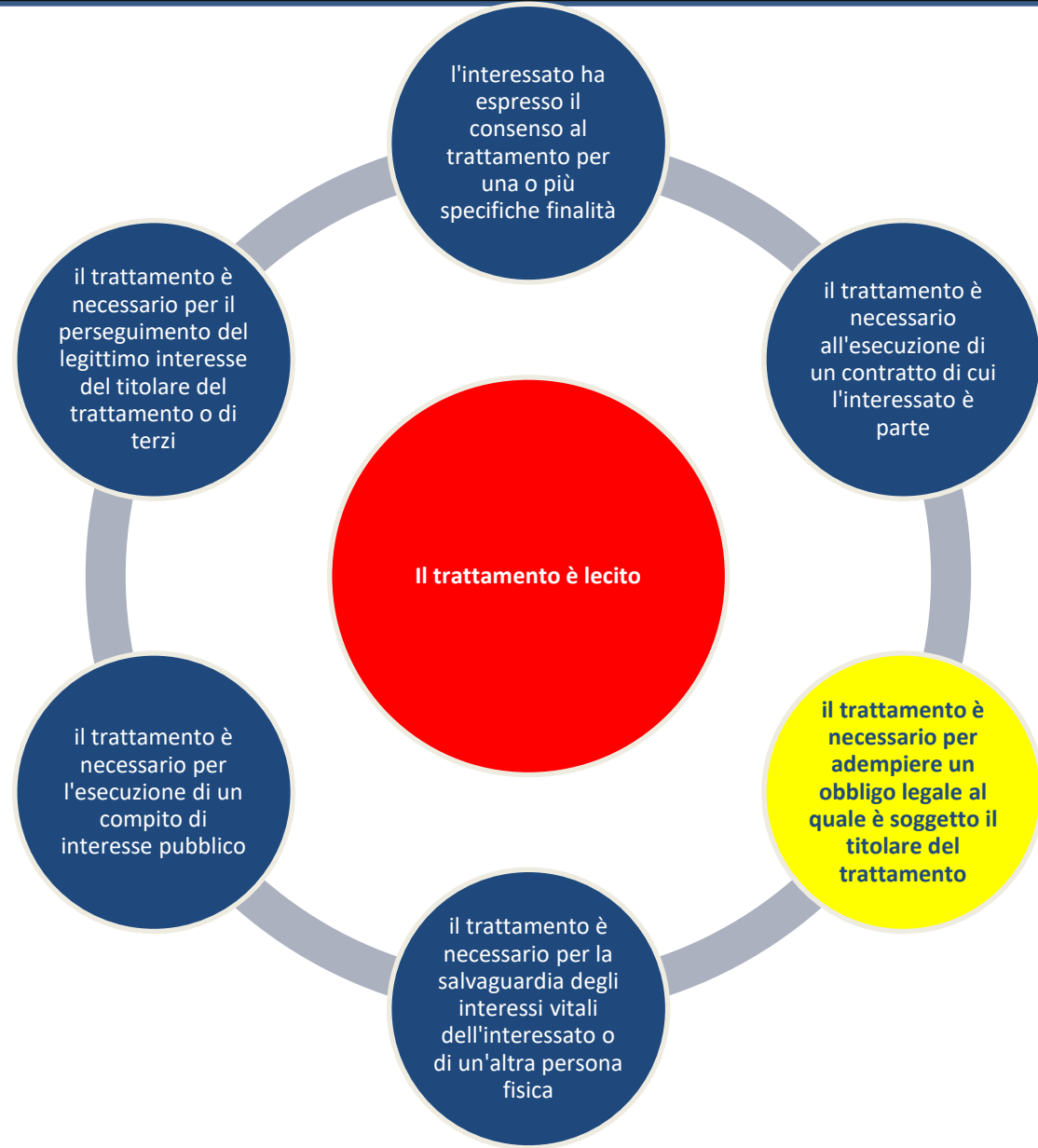


I principi del trattamento

-  Trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»).
-  Raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»)
-  Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione»)
-  Esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»)
-  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 («limitazione della conservazione»)
-  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 («integrità e riservatezza»)



La base giuridica



La norma come base giuridica del trattamento

La base su cui si fonda il trattamento dei dati di cui all'art. 6, par. 1, lettere c) ed e), dovrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui:

le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento

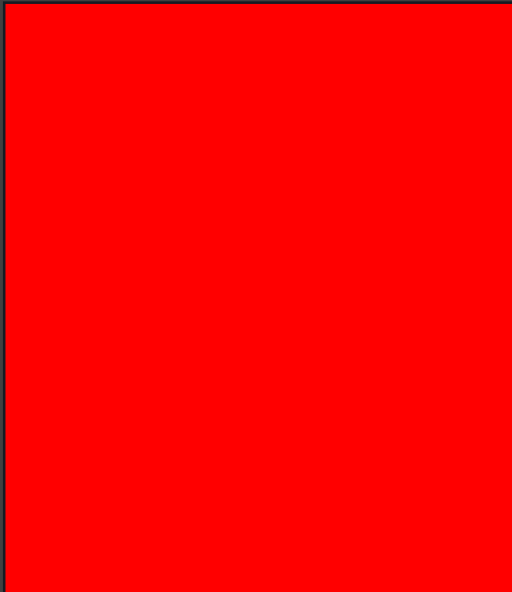
le tipologie di dati oggetto del trattamento

gli interessati

i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati

le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX.

Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.



**Elaborazione
atto legislativo**

L'autorità di controllo dovrebbe essere consultata durante l'elaborazione di una misura legislativa o regolamentare che prevede il trattamento di dati personali al fine di garantire che il trattamento previsto rispetti il presente regolamento e, in particolare, che si atteni il rischio per l'interessato (cons. 96).

**Fondamenti
dell'attività
consultiva**

L'autorità fornisce consulenza, a norma del diritto degli Stati membri, al parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento (art. 57, par 1, lett. C))

Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento (art. 36, par 4).

**La direttiva (UE) 2019/1937 del 23 ottobre 2019
riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione**



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Parere su uno schema di decreto legislativo recante attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione (cd. direttiva whistleblowing) - 11 gennaio 2023 [9844945]

VEDI ANCHE: [Newsletter del 24 gennaio 2023](#)

[doc. web n. 9844945]

Parere su uno schema di decreto legislativo recante attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione (cd. direttiva whistleblowing) e disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali - 11 gennaio 2023

RITENUTO

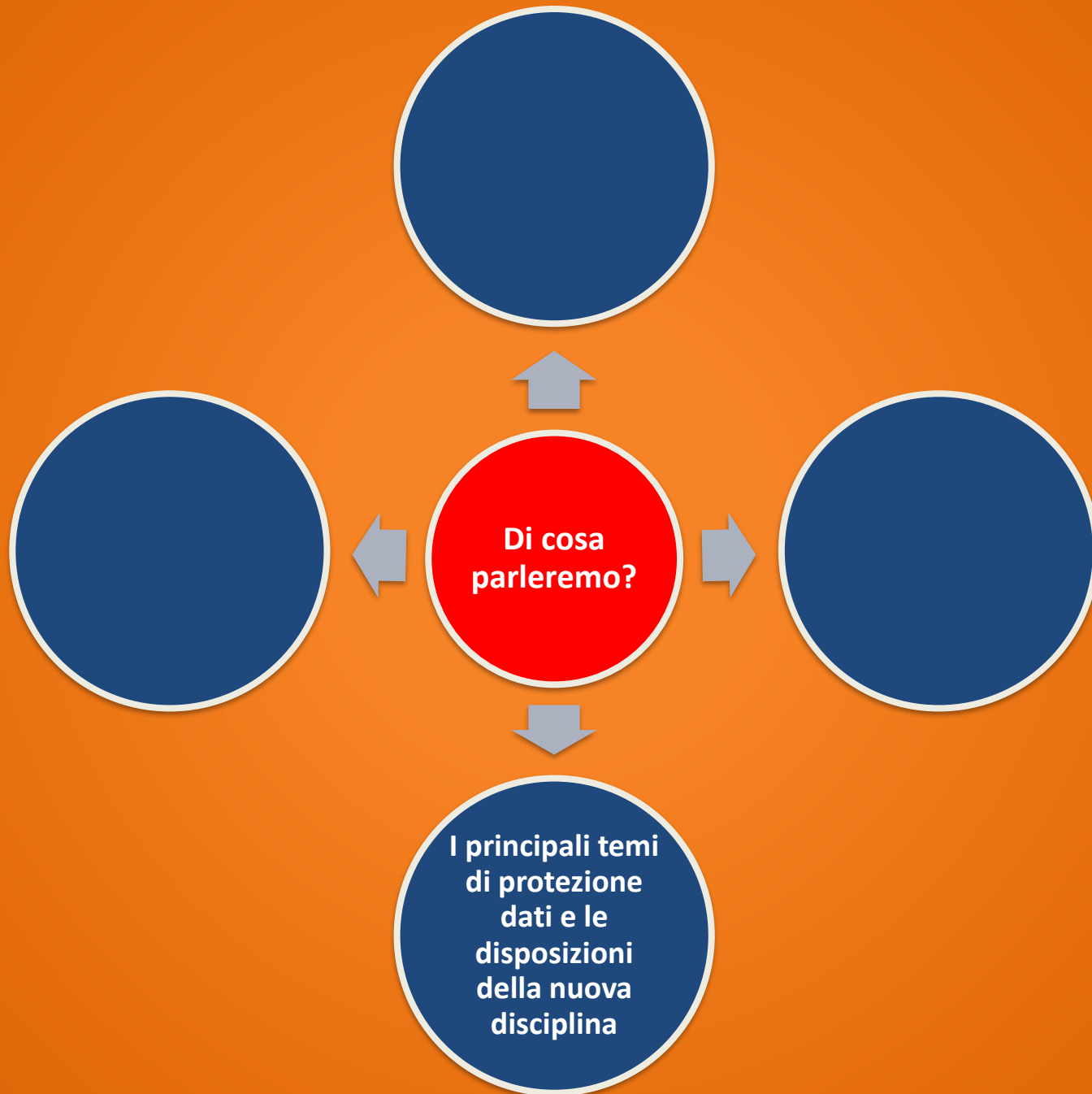
Lo schema di decreto recepisce pressoché tutte le indicazioni fornite dall'Autorità, al Governo, nell'ambito dei lavori preliminari alla stesura dell'odierno testo, con particolare riguardo:

- alla revisione, nel segno di una maggiore determinatezza, della nozione di violazione che, in quanto oggetto della segnalazione, condiziona l'ambito oggettivo di applicazione della disciplina;
- al perfezionamento della disciplina degli obblighi di riservatezza di cui all'articolo 12 e dell'oggetto delle linee guida da emanare (su parere del Garante) ai sensi dell'articolo 10;
- all'integrazione della disciplina, di cui all'articolo 13, del trattamento dei dati personali funzionali al ricevimento e alla gestione delle segnalazioni, con particolare riguardo alla corretta individuazione dei ruoli dei soggetti coinvolti nel trattamento e al divieto di raccolta (con obbligo di cancellazione in caso di acquisizione accidentale) dei dati eccedenti, ai sensi dell'articolo 17 della direttiva;
- alla revisione del termine massimo di conservazione della documentazione della segnalazione, secondo criteri di compatibilità anche con la durata media del termine

prescrizionale dei principali illeciti suscettibili di verificarsi e, comunque, con obbligo di adozione di adeguate misure volte a garantire la riservatezza dell'identità degli interessati;

- all'esigenza di novellare, in parte qua, la disposizione di cui all'art. 2-undecies, c. 1, lett. f), del Codice.

Il complessivo e più puntuale adeguamento, dell'odierno testo, alle rappresentate esigenze di garanzia del diritto alla protezione dei dati personali dei soggetti coinvolti dall'applicazione della disciplina e l'assenza di criticità residue motivano, pertanto, l'espressione di un parere favorevole.



Titolarità del trattamento



I soggetti pubblici e privati tenuti all'attivazione dei canali di segnalazione interna ed esterna (artt. 4 e 7) sono i **titolari del trattamento** (art. 13)

Utilizzo di un canale condiviso (contitolarità)

I comuni diversi dai capoluoghi di provincia possono condividere il canale di segnalazione interna e la relativa gestione e, nel settore privato imprese che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, non superiore a 249, possono condividere il canale di segnalazione interna e la relativa gestione.

In questo caso tali soggetti dovranno determinare in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi in materia di protezione dei dati personali, ai sensi dell'articolo 26 del Regolamento






Accountability misure preventive per assicurare la trasparenza e l'affidabilità del titolare in modo verificabile e misurabile

Accountability, voce del verbo dimostrare

Il principio di accountability ha una natura strumentale; serve a rafforzare l'applicazione delle regole generali che disciplinano il trattamento di dati personali.

La responsabilità del titolare del trattamento dipende non solo dal rispetto delle regole, ma anche dalla sua dimostrazione; ciò comporta quindi la **capacità di individuare il più opportuno livello di formalità che consenta di provare, in caso di necessità, che il trattamento è avvenuto nel rispetto delle norme del Regolamento.**

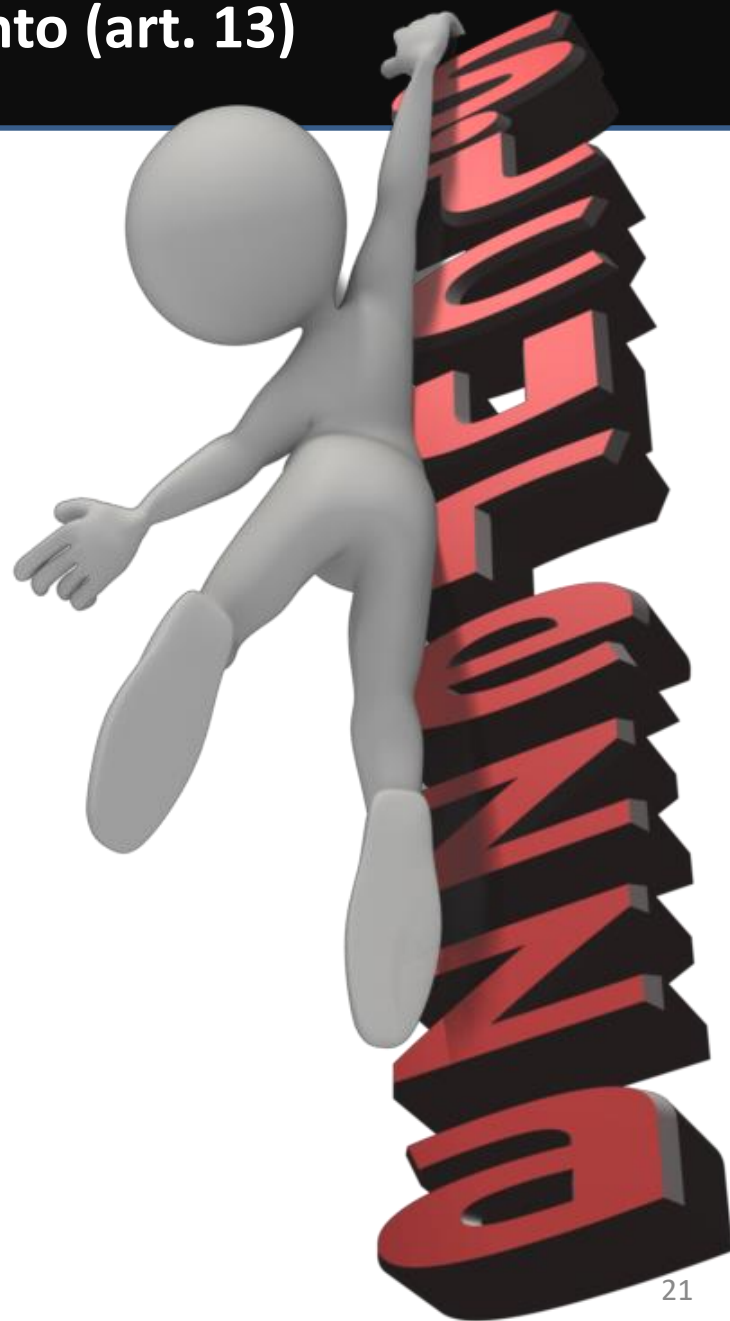
Maggiore libertà dunque, rispetto al passato, da specifici adempimenti e autorizzazioni preventive da parte dell'Autorità, ma anche più responsabilità.



**Dimostrare significa
provare una verità
con un
ragionamento
logico o con prove
di fatto**

La sicurezza del trattamento (art. 13)

I soggetti di cui all'articolo 4 definiscono il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, mediante una valutazione di impatto.





Il rischio in materia di protezione dei dati personali è la possibilità che a causa di un trattamento si possa produrre un effetto negativo sui diritti e sulle libertà delle persone coinvolte

Tale possibile ricaduta negativa, seppure non voluta o desiderata dal titolare, deve comunque essere considerata, valutata e gestita

La sicurezza del trattamento (art. 32 del Regolamento)

Tenendo conto di

stato
dell'arte

costi di
attuazione

natura

oggetto

contesto

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

il responsabile del trattamento

mettono in
atto misure

tecniche

organizzative

adeguate per garantire

un livello di sicurezza
adeguato al rischio

Data protection by default/by design (art. 25 del Regolamento)

Privacy by design

Il titolare del trattamento, sia **al momento di determinare i mezzi del trattamento sia all'atto del trattamento**, mette in atto misure tecniche e organizzative adeguate per attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati (es. pseudonimizzazione, minimizzazione).

Privacy by default

Il titolare del trattamento mette in atto 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. In particolare, dette misure garantiscono che, **per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.**

La sicurezza (in sintesi)



- **Non è più previsto, come in precedenza, un livello di misure minime di sicurezza:** spetta a ogni titolare/responsabile del trattamento individuare le misure adeguate per proteggere i dati in relazione agli elementi che abbiamo descritto in precedenza.
- La **sicurezza è vista più come percorso/metodo** che non come obiettivo tecnico assoluto
- L'adeguatezza delle misure di sicurezza deve essere **parametrata rispetto agli specifici rischi** incombenti sui dati, gestendo il rischio residuo
- La puntuale applicazione del principio di minimizzazione dei dati di cui all'art. 5 del Regolamento «*I dati personali sono... adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*» costituisce una generale misura di prevenzione rispetto ai rischi (gestibili ma mai eliminabili del tutto) del trattamento: **meno dati = meno rischi per sé e per gli interessati**

Indicazione di un criterio (tecnico) generale di riduzione del rischio (artt. 4 e 7)

Previsione dell'attivazione di canali di segnalazione, che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità



Interessati



Segnalante

Persona coinvolta (segnalato)

Persone (eventualmente) menzionate nella segnalazione

L'interessato e i suoi dati personali



«Interessato»: la **PERSONA FISICA** identificata o identificabile a cui si riferiscono (qualsiasi tipo) di informazioni trattate («dato personale»)

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

Obbligo di riservatezza (art. 12)



L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità **non possono essere rivelate**, senza il consenso espresso della stessa persona segnalante, **a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni**, espressamente autorizzate a trattare tali dati ai sensi degli articoli 29 e 32, paragrafo 4, del Regolamento (UE) 2016/679 e dell'articolo 2-*quaterdecies* del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.

La segnalazione è **sottratta all'accesso documentale** (l. 241/90) e **civico** (d. lgs 33/2013).

Trasparenza del trattamento

Fornire idonee informazioni alle persone segnalanti e alle persone coinvolte ai sensi degli articoli 13 e 14 del Regolamento.

Nell'ambito della gestione del canale di segnalazione interna, **devono essere messe a disposizione informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne, nonché sul canale, sulle procedure e sui presupposti per effettuare le segnalazione esterne.**

Le suddette informazioni sono **esposte e rese facilmente visibili nei luoghi di lavoro, nonché accessibili alle persone che pur non frequentando i luoghi di lavoro intrattengono un rapporto giuridico in una delle forme di cui all'articolo 3, commi 3 o 4.**

Se dotati di un proprio **sito internet**, i soggetti tenuti pubblicano le informazioni anche in una sezione dedicata del proprio sito.

Esercizio dei diritti



I diritti di cui agli articoli da 15 a 22 del Regolamento possono essere esercitati nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196 (ovvero **tramite il Garante**).

In tale ipotesi, il Garante informa l'interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale. **Il titolare del trattamento informa l'interessato delle facoltà di cui al presente comma.**

Minimizzazione

I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente (art. 12).



Indicazione di un criterio (organizzativo) generale di riduzione del rischio



La gestione del canale di segnalazione è affidata a una persona o a un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del canale di segnalazione (art. 4).

Le persone autorizzate

Le persone autorizzate al trattamento dei dati personali che operano sotto l'autorità diretta del titolare o del responsabile



L'art. 29 e Art. 32, par.4 le persone autorizzate al trattamento dei dati personali non possono trattare tali dati se non sono istruite in tal senso dal titolare o dal responsabile

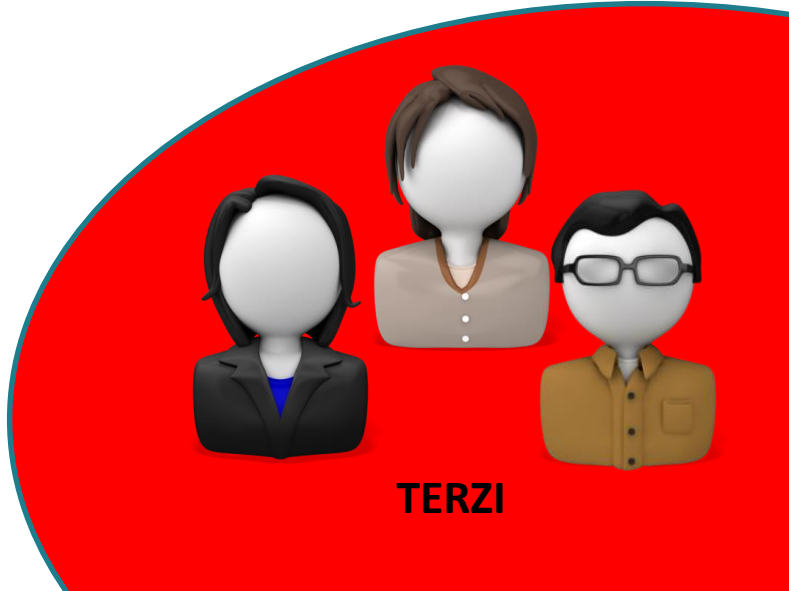
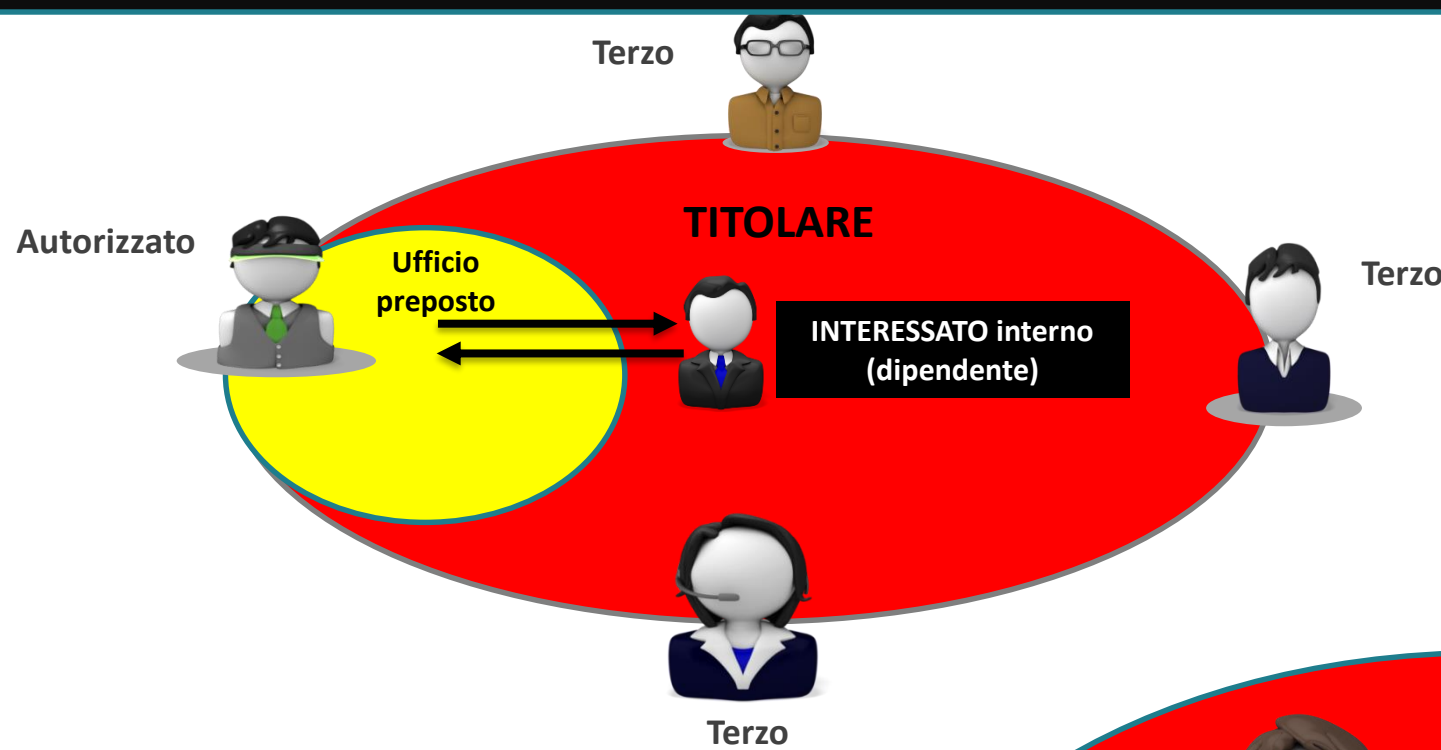


Individuano le modalità più opportune per autorizzare al trattamento le persone che operano sotto la loro autorità diretta

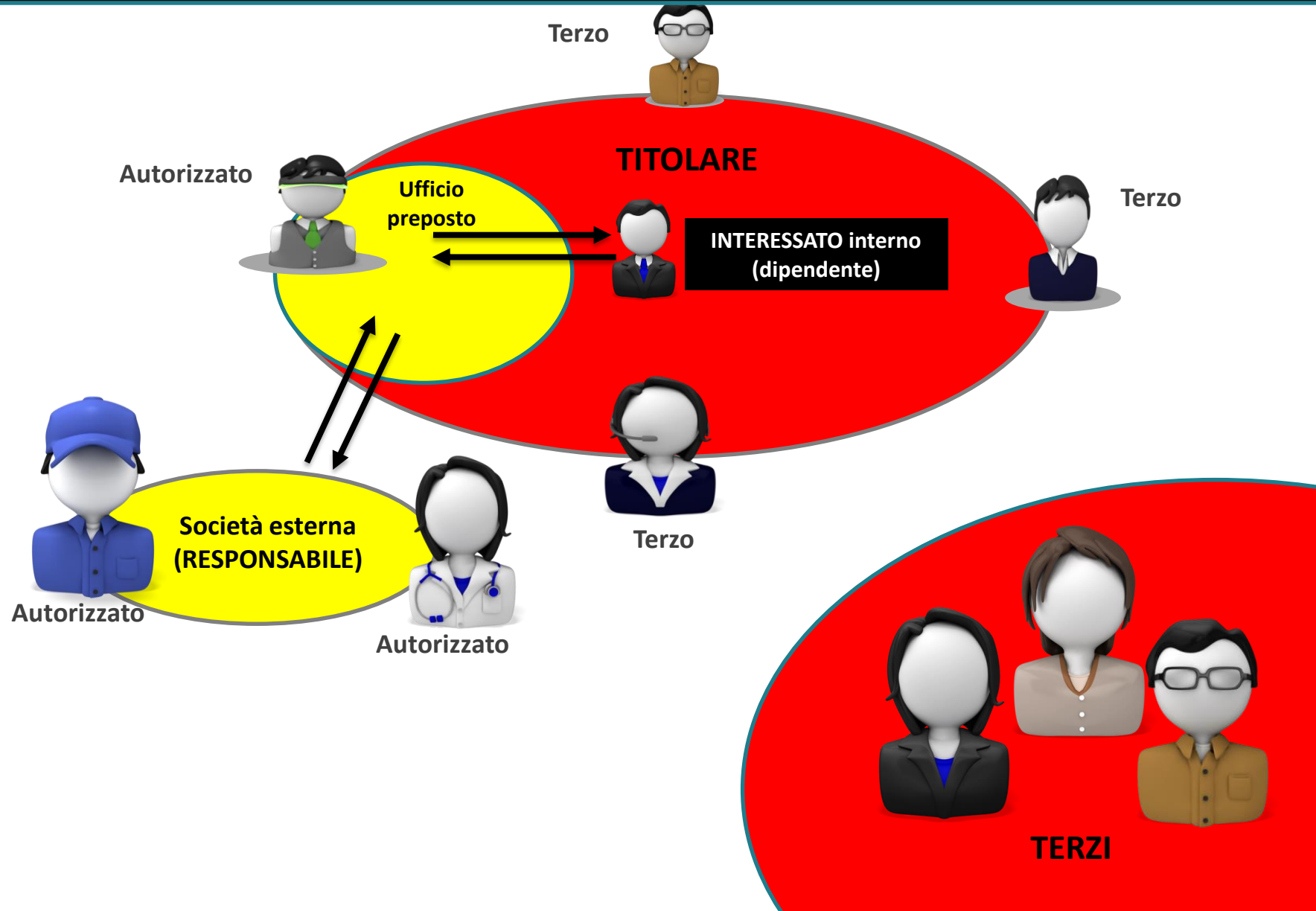


2-quaterdecies del Codice, titolare e responsabile possono prevedere sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo che specifiche funzioni siano attribuite a persone fisiche espressamente designate

Ambito del trattamento consentito e i terzi



Affidamento a un soggetto esterno = responsabile del trattamento (art. 13)





L'ANAC, sentito il Garante per la protezione dei dati personali, adotta, entro tre mesi dalla data di entrata in vigore del presente decreto, le linee guida relative alle procedure per la presentazione e la gestione delle segnalazioni esterne.

Le linee guida prevedono l'utilizzo di modalità anche informatiche e promuovono il ricorso a strumenti di crittografia per garantire la riservatezza dell'identità della persona segnalante, della persona coinvolta o menzionata nella segnalazione, nonché del contenuto delle segnalazioni e della relativa documentazione.

Principio della limitazione della conservazione (art. 10)

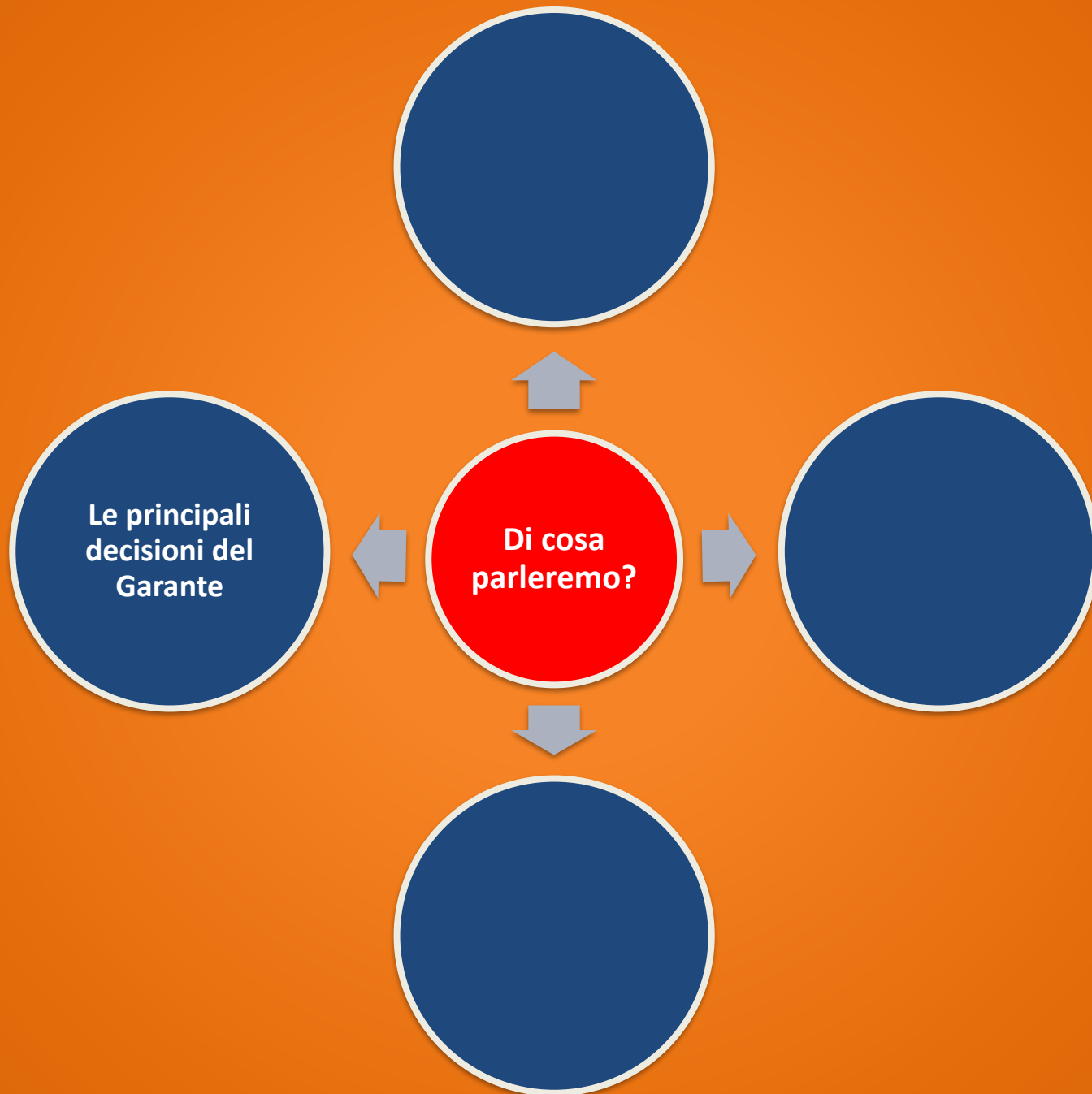
Le segnalazioni, interne ed esterne, e la relativa documentazione sono **conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione**, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del presente decreto e del principio di cui agli articoli 5, paragrafo 1, lettera e), del Regolamento



Coinvolgimento del RPD

Il titolare e il responsabile del trattamento si assicurano che il RPD sia **tempestivamente e adeguatamente coinvolto** in tutte le questioni riguardanti la protezione dei dati personali.







GPDP

**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Parere sullo schema di "Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis del d.lgs. 165/2001 (c.d. whistleblowing)" - 4 dicembre 2019 [9215763]

VEDI ANCHE [Newsletter del 20 dicembre 2019](#)

[doc. web n. 9215763]

Parere sullo schema di "Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis del d.lgs. 165/2001 (c.d. whistleblowing)" - 4 dicembre 2019

Registro dei provvedimenti
n. 215 del 4 dicembre 2019

I principali provvedimenti adottati e risvolti emersi

- **Provvedimento nei confronti di Aeroporto Guglielmo Marconi di Bologna S.p.a. - 10 giugno 2021 [9685922]**
- **Provvedimento nei confronti di aiComply S.r.l. - 10 giugno 2021 [9685947]**
- **Provvedimento nei confronti di Azienda ospedaliera di Perugia - 7 aprile 2022 [9768363]**
- **Provvedimento nei confronti di ISWEB S.p.A. - 7 aprile 2022 [9768387]**

- **Mancata regolazione del rapporto con il fornitore del servizio**
- **Mancato aggiornamento del registro del trattamento**
- **Assenza dell' informativa agli interessati**
- **Assenza di una valutazione di impatto**
- **Inadeguatezza delle misure di sicurezza:**
 - ✓ **Mancato utilizzo di tecniche crittografiche per il trasporto e la conservazione dei dati**
 - ✓ **Inidoneità delle modalità di gestione delle credenziali di autenticazione**
 - ✓ **Tracciamento degli accessi all'applicativo per l'acquisizione e la gestione delle segnalazioni di condotte illecite**

Domande?

