EDPB

Linee guida n. 07/2020

sui concetti di titolare e responsabile nel GDPR - versione 2.0

Adottate definitivamente il 07 luglio 2021

SINTESI

I **concetti** di titolare, contitolare e responsabile del trattamento **giocano un ruolo cruciale** nell'applicazione del Regolamento generale sulla protezione dei dati 2016/679 (GDPR), in quanto **determinano chi sarà responsabile per il rispetto delle diverse norme sulla protezione dei dati** e in che modo **gli interessati** possono **esercitare i propri diritti** in pratica.

Il significato preciso di questi concetti, nonché i criteri per la loro corretta interpretazione, devono essere sufficientemente chiari e coerenti in tutto lo Spazio economico europeo (SEE).

I concetti di **titolare**, **contitolare** e **responsabile** sono concetti **funzionali** in quanto mirano ad allocare le responsabilità **secondo i ruoli effettivi delle parti** e concetti **autonomi** nel senso che dovrebbero essere interpretati principalmente secondo il diritto dell'UE sulla protezione dei dati.

Titolare (“*controller*”)

In linea di principio, non vi è alcuna limitazione al tipo di soggetto che può assumere il ruolo di titolare del trattamento ma in pratica, **di solito**, **è l'organizzazione in quanto tale**, e non un individuo all'interno dell'organizzazione (come l'amministratore delegato, un dipendente o un membro del consiglio di amministrazione), che agisce in qualità di titolare.

Un **titolare** è un organismo che **decide** alcuni **elementi chiave** del trattamento.

La titolarità può essere **definita dalla legge** o può derivare da **un'analisi degli elementi di fatto** o delle circostanze del caso.

Alcune attività di trattamento possono essere considerate naturalmente legate al ruolo di un'entità (un datore di lavoro per i dipendenti, un editore rispetto agli abbonati o un'associazione relativamente ai suoi membri).

In molti casi, i termini di un contratto possono aiutare a identificare il titolare del trattamento, sebbene non siano determinanti in tutte le circostanze.

Il titolare del trattamento **determina le finalità e i mezzi del trattamento**, ovvero il motivo (il perché) e il modo (il come) del trattamento.

Il titolare del trattamento deve decidere (“***must decide***”) sia le finalità che i mezzi. Tuttavia, alcuni più pratici aspetti di attuazione del trattamento (di cui ai "***mezzi non essenziali***") possono essere lasciati decidere al responsabile del trattamento. Non è necessario che il titolare del trattamento abbia effettivamente accesso ai dati oggetto di trattamento per essere qualificato come titolare del trattamento.

Contitolari del trattamento (“*controllership*”)

La qualifica di contitolari del trattamento può sorgere qualora nel **trattamento sia coinvolto più di un soggetto**.

Il GDPR introduce **regole specifiche per i contitolari** del trattamento e definisce un quadro per disciplinare la loro relazione. Il **criterio generale** per l'esistenza del controllo congiunto è la **partecipazione congiunta di due o più soggetti nella determinazione delle finalità e dei mezzi** di un trattamento.

La partecipazione congiunta può assumere la forma di una **decisione comune** presa da due o più enti o risultare da **decisioni convergenti** di due o più entità, in cui le decisioni si completano a vicenda e sono necessarie affinché il trattamento avvenga in modo tale da avere un **impatto tangibile** sulla determinazione delle finalità e dei mezzi del trattamento.

Un **criterio** importante è che il il trattamento non sarebbe possibile senza la partecipazione di entrambe le parti, nel senso che il **trattamento** di ciascuna delle parti è **inseparabile**, cioè **indissolubilmente legato**.

La partecipazione congiunta necessita (“***needs***”) di includere la determinazione dei fini da un lato e la determinazione dei mezzi dall'altro.

Responsabile (“*processor*”)

Un responsabile del trattamento è una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che tratta dati personali **per conto del titolare** del trattamento. Esistono due condizioni fondamentali per qualificarsi come responsabile: (A) che sia **un'entità separata** rispetto al titolare del trattamento e che (B) **tratti i dati personali per suo conto**.

Il responsabile non deve trattare i dati se non secondo le **istruzioni** del titolare. Le istruzioni del titolare possono comunque lasciare un certo **grado di discrezionalità** su come attuare al meglio le finalità del titolare, consentendo al responsabile del trattamento di **scegliere il metodo tecnico** e **organizzativo** più idoneo per assicurarle.

Tuttavia, un responsabile del trattamento **viola il GDPR** se va oltre le istruzioni del responsabile del trattamento e inizia **a determinare le proprie finalità e i mezzi del trattamento**. Il responsabile sarà quindi considerato titolare del trattamento in relazione a tale trattamento e può essere soggetto a sanzioni per il mancato rispetto delle istruzioni del titolare.

Relazione tra titolare e responsabile del trattamento

Un titolare del trattamento deve utilizzare **solo** (“***must only use***”) **responsabili che forniscano garanzie sufficienti** per attuare adeguate misure tecniche e organizzative affinché il trattamento soddisfi i requisiti del GDPR. Gli elementi da prendere in considerazione potrebbero essere **l'esperienza** del responsabile (ad es. **competenza tecnica** in materia di misure di sicurezza e violazioni dei dati); **l'affidabilità** del responsabile; le risorse del responsabile e la sua **adesione a un**

codice di condotta approvato o a un meccanismo di certificazione.

Qualsiasi trattamento di dati personali da parte di un responsabile del trattamento **deve essere disciplinato da un contratto o altro atto giuridico** che deve la forma **scritta**, **anche** in formato **elettronico**, ed essere **vincolante**. Il titolare e il responsabile del trattamento possono scegliere di negoziare il proprio contratto comprensivo di tutti gli elementi obbligatori o di affidarsi, in toto o in parte, a clausole contrattuali standard.

Il GDPR elenca gli elementi che devono essere stabiliti nel contratto di trattamento. L'accordo non dovrebbe, tuttavia, limitarsi a riaffermare ("copiare") le disposizioni del GDPR; piuttosto, dovrebbe **includere informazioni specifiche e concrete su come saranno soddisfatti i requisiti** e quale livello di sicurezza si renda necessario per il trattamento dei dati personali oggetto del contratto di trattamento.

Rapporto tra contitolari del trattamento

I contitolari del trattamento **determinano e concordano** in modo **trasparente** le **rispettive responsabilità** per il rispetto degli obblighi previsti dal GDPR.

La determinazione delle loro rispettive responsabilità deve riguardare in particolare l'esercizio dei **diritti degli interessati** e i **doveri di fornire le informazione**. Oltre a ciò, la distribuzione delle responsabilità dovrebbe riguardare altri obblighi ed aspetti del trattamento quali (i) i principi generali di protezione dei dati, (ii) la base giuridica, (iii) le misure di sicurezza, (iv) l'obbligo di notifica della violazione dei dati, (v) la valutazioni d'impatto sulla protezione dei dati, (vi) l'utilizzo di responsabili del trattamento, (vii) i trasferimenti dei dati verso nazioni terze e (viii) i contatti con gli interessati e le autorità di controllo.

Ciascun contitolare ha il dovere di **assicurarsi di disporre di una base giuridica** per il trattamento e che i dati non siano ulteriormente trattati in modo incompatibile rispetto le finalità per le quali sono stati originariamente raccolti dal titolare che condivide i dati.

La **forma giuridica dell'accordo tra contitolari non è specificata** dal GDPR. Per la tutela della certezza del diritto e al fine di garantire trasparenza e responsabilità, il Comitato raccomanda che tale accordo sia **preso sotto forma di un documento vincolante come un contratto o altro atto legale vincolante** ai sensi del **diritto** dell'UE o dello Stato membro cui sono soggetti i titolari del trattamento.

L'accordo riflette debitamente **i rispettivi ruoli e rapporti dei contitolari** del trattamento nei confronti degli interessati e l'essenza dell'accordo che è da mettersi a disposizione dell'interessato. Indipendentemente dai termini dell'accordo, gli **interessati possono esercitare i propri diritti nei confronti di e contro ciascuno dei contitolari**. Le autorità di vigilanza non sono vincolate dai termini dell'accordo né sulla qualificazione data dalle parti contitolari del trattamento e neppure sul punto di contatto dalle stesse designato.

SOMMARIO

***

Il Comitato europeo per la protezione dei dati visto l'art. 70, co. 1, lettera e), del Reg. 2016/679/UE del Parlamento europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali dati e sulla libera circolazione di tali dati, e che abroga la Direttiva 95/46/CE, (di seguito "GDPR" o "il Regolamento"), visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37, come modificato dalla decisione del Comitato misto SEE n. 154/2018 del 6/07/2018,visti gli artt. 12 e 22 del suo regolamento interno, considerando che il lavoro preparatorio di queste linee guida ha comportato la raccolta di contributi dalle parti interessate, sia per iscritto che in occasione di un evento per gli stakeholder, al fine di identificare le sfide più urgenti,

HA ADOTTATO LE SEGUENTI LINEE GUIDA

INTRODUZIONE

1. Il presente documento intende fornire indicazioni sui concetti di titolare e responsabile del trattamento in base alle regole del GDPR e le definizioni nell'art. 4 e le disposizioni sugli obblighi nel capitolo IV. **L'obiettivo principale è chiarire il significato dei concetti** e chiarire i diversi ruoli e la **distribuzione di responsabilità** tra questi attori.

2. Il **concetto di titolare e la sua interazione con il concetto di responsabile** giocano un **ruolo cruciale** nella applicazione del GDPR, poiché **determinano chi sarà responsabile del rispetto delle diverse norme sulla protezione dei dati** e come gli interessati possono esercitare i propri diritti nella pratica. Il GDPR introduce in modo esplicito il principio di "***accountability***", vale a dire che il titolare del trattamento è responsabile e può dimostrare il rispetto dei principi relativi al trattamento dei dati personali di cui all'art. 5. Il GDPR introduce anche regole più specifiche sull'uso del/i responsabile/i e su alcune delle disposizioni in materia di trattamento dei dati personali che sono rivolte non solo ai titolari ma anche ai responsabili del trattamento.

3. È quindi di **fondamentale importanza che il significato preciso di questi concetti e dei criteri per il loro corretto utilizzo siano sufficientemente chiari** e **condivisi** in tutta l'Unione Europea e nel EEA.

4. Il Gruppo di lavoro art. 29 ha pubblicato orientamenti sui concetti di titolare e e responsabile del trattamento nel proprio parere n. 1/2010 (WP169) al fine di fornire chiarimenti ed esempi concreti con riguardo a tali concetti. Dall'entrata in vigore del GDPR, sono state **sollevate molte domande** sulla misura in cui il GDPR ha apportato modifiche ai concetti di titolare e responsabile del trattamento e ai rispettivi ruoli. Sono state **sollevate questioni in particolare sulla sostanza e sulle implicazioni del concetto di contitolarità** del trattamento (come ad es. previsto dall'art. 26 GDPR) e agli **obblighi specifici per i responsabili** del trattamento previsti al capo IV (ad es. previsti dall'art. 28 GDPR). Pertanto, siccome l'EDPB riconosce che l'applicazione concreta dei concetti necessita di ulteriori chiarimenti, si ritiene ora necessario fornire orientamenti più sviluppati e

specifici al fine di garantire un coerente e armonizzato approccio in tutta l'UE e nel SEE. **Le presenti linee guida sostituiscono il precedente parere del Gruppo di lavoro 29 su questi concetti** (WP169).

5. Nella **parte I**, queste linee guida discutono le definizioni dei diversi concetti di titolari, contitolari, responsabili e terzi/destinatari. Nella **parte II**, vengono fornite ulteriori indicazioni sulle conseguenze che sono legate ai diversi ruoli di titolare, contitolare e responsabile del trattamento.

PARTE I – CONCETTI

1) OSSERVAZIONI GENERALI

6. Il GDPR, all'**art. 5**, par. 2, introduce esplicitamente il principio di responsabilità (***accountability***), il che significa che **A)** il titolare del trattamento è **responsabile del rispetto** dei principi di cui all'art. 5, paragrafo 1 RGPD e **B)** il medesimo titolare del trattamento **deve essere in grado di dimostrare** il rispetto dei principi di cui all'art. 5, par. 1 RGPD. Questo principio è stato descritto in un parere dall'art. 29 WP e non sarà qui trattato in dettaglio.

7. L'obiettivo di incorporare il principio di ***accountability*** nel GDPR e renderlo un **principio centrale** era quello di sottolineare che **i titolari del trattamento devono attuare misure appropriate** ed efficaci ed **essere in grado di dimostrare** la conformità.

8. Il principio di ***accountability*** è stato ulteriormente elaborato nell'**art. 24**, il quale afferma che il titolare del trattamento adotta misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento viene eseguito in conformità con il GDPR. Tali misure devono essere riviste e aggiornato se necessario. Il principio di responsabilità si riflette anche nell'**art. 28**, che stabilisce gli obblighi del titolare in caso di nomina di un responsabile.

9. Il principio di ***accountability*** è rivolto direttamente al titolare del trattamento. Tuttavia, alcuni concetti più specifici sono rivolti sia ai titolari che ai responsabili del trattamento, avuto particolare riguardo ai poteri delle autorità di controllo di cui all'art. 58. Sia i titolari che i responsabili del trattamento possono essere sanzionati in caso di mancato rispetto del obblighi del GDPR che sono rilevanti per entrambi poiché direttamente responsabili nei confronti delle autorità di controllo in virtù degli obblighi di mantenere e fornire adeguata documentazione su richiesta, di collaborare in caso di indagine e rispettare le procedure amministrative e gli ordini. Allo stesso tempo va ricordato che i responsabili del trattamento devono sempre rispettare e agire solo su istruzioni del titolare.

10. Il **principio di *accountability***, unitamente alle altre più specifiche regole su come conformarsi al GDPR e sulla ripartizione delle responsabilità, **rende quindi necessaria la definizione dei diversi ruoli** dei diversi **attori** coinvolti in un'attività di trattamento dei dati personali.

11. Un'osservazione generale riguardo i concetti di titolare e responsabile nel GDPR è che gli stessi non sono cambiati rispetto alla Direttiva 95/46/CE e che nel

complesso, i criteri di attribuzione dei ruoli diversi, rimangono gli stessi.

12. I concetti di titolare e responsabile sono **concetti funzionali**: **mirano ad allocare le responsabilità secondo i ruoli effettivi** delle parti (cfr. opinion n. 1/2010 WP29, pag. 9). Ciò implica che lo **status giuridico** di un attore come "titolare" o come "responsabile del trattamento" **deve in linea di principio essere determinato dalle sue attività effettive in uno specifico situazione**, piuttosto che dalla designazione formale di un attore come "titolare" o "responsabile" (ad es. in un contratto). Ciò significa che **l'assegnazione dei ruoli di solito dovrebbe derivare da un'analisi degli elementi di fatto o delle circostanze del caso e come tale non è negoziabile**.

13. I concetti di titolare e responsabile sono **concetti autonomi** anche nel senso che, sebbene fonti legali esterne potrebbero aiutare a identificare chi è un titolare, gli stessi dovrebbero essere **interpretati principalmente secondo la normativa UE** sulla protezione dei dati. **Il concetto di titolare non dovrebbe essere pregiudicato da concetti** - a volte in collisione o sovrapposizione – di altri campi del diritto, come il concetto di creatore o di titolare del diritto di proprietà intellettuale o rispetto al diritto della concorrenza.

14. Poiché l'obiettivo di fondo dell'attribuzione del ruolo di titolare del trattamento è garantire la responsabilità e la protezione efficace e completa dei dati personali, il concetto di **"titolare del trattamento" dovrebbe essere interpretato in modo sufficientemente ampio**, privilegiando in modo quanto più possibile efficace e completo la **protezione degli interessati** al fine di garantire la piena efficacia del diritto dell'UE in materia di protezione dei dati, ed evitare lacune e prevenire possibili elusioni delle regole, pur non sminuendo il ruolo del responsabile.

2 DEFINIZIONE DI TITOLARE

2.1 Definizione di titolare

15. Un titolare del trattamento è definito dall'**art. 4**, par. 7, GDPR come "la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro organismo che, da solo o insieme a altri, determina le finalità e i mezzi del trattamento dei dati personali; ove finalità e mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento, o i criteri specifici per la sua designazione, possono essere previsti dall'Unione o dallo Stato membro legge".

16. La definizione di **titolare** contiene **cinque elementi costitutivi principali**, che verranno analizzati separatamente per le finalità delle presenti linee guida. Essi sono i seguenti:

1. "la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro organismo";
2. "determina";
3. "da solo o insieme ad altri";
4. "gli scopi e i mezzi";
5. "del trattamento dei dati personali".

2.1.1 "Persona fisica o giuridica, autorità pubblica, agenzia o altro ente"

17. Il primo elemento costitutivo riguarda il tipo di entità che può essere titolare del trattamento. In base al GDPR, il titolare del trattamento può essere "una persona fisica o giuridica, autorità pubblica, agenzia o altro organismo". Ciò significa che, in linea di principio, **non vi è alcuna limitazione al tipo di soggetto** che può assumere il ruolo di titolare del trattamento. Esso potrebbe essere un'organizzazione, ma potrebbe anche essere un individuo o un gruppo di individui. In pratica, tuttavia, di solito, è l'organizzazione in quanto tale e non un individuo all'interno dell'organizzazione (come l'amministratore delegato, un dipendente o un membro del cda), che agisce in qualità di titolare del trattamento ai sensi del GDPR.

Per quanto riguarda il trattamento dei dati all'interno di un **gruppo societario**, particolare attenzione deve essere prestata alla questione se uno stabilimento ("società") possa agire in qualità di titolare del trattamento o responsabile del trattamento, ad es. quando il trattamento dei dati avviene per conto della capogruppo.

18. **Talvolta**, le società e gli enti pubblici nominano **uno specifico responsabile** ("interno e convenzionale") dell'attuazione dell'attività di trattamento. Anche se una specifica persona fisica è nominata per garantire il rispetto della normativa sulla protezione dei dati, **questa persona non sarà il titolare del trattamento** ma agirà per conto dell'entità giuridica (società o ente pubblico) che sarà responsabile in ultima istanza in caso di violazione delle norme nella sua qualità come titolare. Allo stesso modo, anche se un particolare **dipartimento o unità di un'organizzazione** ha responsabilità operativa per garantire la conformità per determinate attività di trattamento, **ciò non significa che** questo dipartimento o unità (piuttosto che l'organizzazione nel suo insieme) **diventi titolare del trattamento**.

***

Esempio: Il **dipartimento marketing** della società ABC lancia una campagna pubblicitaria per promuovere dei prodotti della stessa società ABC. **Il reparto marketing decide la natura della campagna, i mezzi da utilizzare** (e-mail, *social media*...), a quali clienti rivolgersi e **quali dati utilizzare** per rendere la campagna di maggior successo possibile. **Anche se il reparto marketing ha agito con notevole indipendenza**, **La società ABC sarà in linea di principio considerata come il titolare** visto che la campagna pubblicitaria è lanciata dalla stessa società e si svolge nell'ambito delle sue attività imprenditoriali e per i suoi scopi.

***

19. In linea di principio, qualsiasi trattamento di dati personali da parte dei dipendenti che avviene nell'ambito di una organizzazione è da presumersi che avvenga sotto il controllo di tale organizzazione. In circostanze **eccezionali, tuttavia, può accadere che un dipendente decida di utilizzare i dati personali per propri scopi**, eccedendo in tal modo illegittimamente l'autorità che gli è stata

conferita. (ad es. costituire una propria società o per ipotesi simili). È quindi dovere dell'organizzazione in qualità di titolare assicurarsi che **esistano misure tecniche e organizzative adeguate**, tra cui ad es. formazione e informazione ai dipendenti, per garantire la conformità al GDPR.

2.1.2 "Determina"

20. Il secondo elemento costitutivo del concetto di **titolare** si riferisce **all'influenza dello stesso sul trattamento**, **in virtù** di un esercizio del **potere decisionale**. Un titolare è una entità che **decide in modo certo elementi chiave** del trattamento. Questa titolarità può essere definita **dalla legge** o può derivare da un **analisi degli elementi di fatto** o delle circostanze del caso.

Si dovrebbe guardare l'elaborazione specifica delle operazioni in questione e capire **chi le determina**, considerando/rispondendo innanzitutto le/alle seguenti domande: **A)** "***perché avviene questo trattamento?***" e **B)** "***chi ha deciso che il trattamento dovesse avere luogo per uno scopo particolare?***".

Circostanze che danno luogo alla titolarità

21. Premesso che la nozione di titolare del trattamento è una **nozione funzionale**, essa si **fonda quindi su un fatto** piuttosto che un'analisi formale, al fine di facilitare l'analisi, alcune regole pratiche e le presunzioni possono essere utilizzate per guidare e semplificare il processo.

Nella maggior parte delle situazioni, il "l'**organismo determinante**" può essere facilmente e chiaramente identificato facendo riferimento a determinate circostanze giuridiche e/o di fatto da cui normalmente si può desumere "l'**influenza**" determinante, a meno che altri elementi non indichino il contrario.

Si possono distinguere due categorie di situazioni:

- **(1) titolarità derivante da disposizioni di legge**; e
- **(2) titolarità derivante da un'influenza fattuale**.

(1) Titolarità derivante da disposizioni di legge

22. Vi sono casi in cui la titolarità può essere dedotta da una attribuzione giuridica esplicita, ad esempio quando il titolare del trattamento oppure i criteri specifici per la sua nomina sono **designati dal diritto nazionale** o **dell'Unione**. Infatti, l'art. 4, par. 7 afferma che "*laddove le finalità e i mezzi di tale trattamento siano determinati dall'Unione o dallo Stato membro, il titolare del trattamento o i criteri specifici per la sua nomina possono essere previsti dall'Unione o dal diritto degli Stati membri*". Sebbene l'art. 4, par. 7, si riferisca solo al "titolare del trattamento" al singolare, l'EDPB ritiene che il diritto dell'Unione o degli Stati membri possa anche designare più di uno titolare, eventualmente anche in qualità di contitolari.

23. Laddove il titolare del trattamento sia stato **specificamente individuato dalla legge**, ciò sarà **determinante per stabilire chi agisce in qualità di titolare**. Ciò

presuppone che il Legislatore abbia designato quale titolare del trattamento l'ente che ha una reale capacità di esercitare la titolarità. In alcuni paesi, la legge nazionale prevede che le autorità pubbliche rispondano ("ne abbiano la titolarità") del trattamento dei dati personali nell'ambito delle loro funzioni.

24. Tuttavia, **più comunemente**, piuttosto che nominare direttamente il titolare del trattamento o stabilire i criteri per la sua nomina, **la legge stabilirà un compito o imporrà a qualcuno l'obbligo di raccogliere e trattare determinati dati**.

In tali casi, la finalità del trattamento è spesso determinata dalla legge. **Il titolare sarà di norma il designato dalla legge per la realizzazione di tale finalità pubblica** o pubblico compito. Ad esempio, questo sarebbe il caso in cui un ente a cui sono affidati determinati compiti pubblici (es. previdenza sociale) che non possono essere adempiuti senza raccogliere almeno alcuni dati personali, crei una banca dati o un registro al fine di adempiere a tali compiti pubblici. In questo caso, **la legge, sia pure indirettamente, stabilisce chi è il titolare**. Più in generale, la legge può anche imporre un obbligo al soggetto pubblico o a soggetti privati di conservare o fornire determinati dati. Queste entità sarebbero quindi normalmente considerate come titolari del trattamento rispetto al trattamento necessario per adempiere a tale obbligo.

***

Esempio: disposizioni legali (contributi di sussistenza)
La **legge nazionale nel Paese A stabilisce l'obbligo** per le **autorità municipali di fornire servizi sociali e prestazioni assistenziali** (quali contributo assistenziale mensile) ai cittadini a seconda della loro situazione finanziaria. Per effettuare tali pagamenti, **l'amministrazione comunale deve raccogliere ed elaborare** i dati relativi alla situazione finanziaria dei richiedenti. Anche se la legge non prevede esplicitamente che il comune sia l'autorità **titolare di tale trattamento**, ciò **deriva implicitamente** dalle disposizioni di legge.

***

2) Titolarità derivante dall'influenza fattuale

25. In assenza di titolarità derivante da disposizioni di legge, la qualifica di un soggetto quale titolare del trattamento deve essere stabilito sulla base di una **valutazione delle circostanze di fatto** relative al trattamento. Tutte le circostanze di fatto pertinenti devono essere prese in considerazione al fine di giungere a una conclusione in merito a se **una determinata entità esercita un'influenza determinante** in relazione al **trattamento di dati** personali in questione.

26. La necessità di una valutazione fattuale significa anche che il ruolo di titolare del trattamento **non deriva dalla natura di un soggetto che tratta dati ma dalle sue attività concrete** in un contesto specifico. In altre parole, **lo stesso soggetto può agire contemporaneamente in qualità di titolare** per **talune operazioni** di trattamento **e in qualità di responsabile del trattamento per conto terzi** e la qualifica di titolare del trattamento o responsabile del trattamento deve essere valutata con riguardo **a ogni specifica attività di trattamento dei dati**.

27. In pratica, alcune attività di trattamento possono **essere considerate naturalmente legate al ruolo o alle attività di un soggetto** che in definitiva comporta responsabilità dal punto di vista della protezione dei dati. Questo può essere dovuto a disposizioni giuridiche più generali o a una prassi giuridica consolidata in diversi settori (diritto civile, commerciale diritto, diritto del lavoro, ecc.). In questo caso, **ruoli tradizionali esistenti e competenze professionali che normalmente implicano una certa responsabilità aiuteranno ad identificare il titolare del trattamento**, ad esempio: un **datore di lavoro** in relazione a trattamento di dati personali sui suoi dipendenti, un **editore che elabora dati personali sui suoi abbonati**, o **un'associazione che tratta dati personali sui suoi membri** o collaboratori. Quando una entità si impegna nel trattamento dei dati personali come parte delle sue interazioni con i propri dipendenti, clienti o membri, **sarà generalmente colei che determina lo scopo e i mezzi** intorno il trattamento e agisce quindi in qualità di titolare del trattamento ai sensi del GDPR.

***

Esempio: "studi legali"
La società ABC incarica uno studio legale di rappresentarla in una controversia. Per assolvere a questo compito lo Studio legale ha bisogno di trattare i dati personali relativi al caso. Le ragioni del trattamento dei dati personali risiedono nel **mandato ricevuto dallo Studio legale** per rappresentare il cliente in tribunale. Questo mandato, tuttavia, non è specificamente finalizzato al trattamento dei dati personali. **Lo studio legale agisce con un significativo grado di indipendenza, per esempio nel decidere quali informazioni utilizzare e come utilizzarle**, e **non ci sono istruzioni** da parte della società cliente in merito al trattamento dei dati personali. Il trattamento che lo studio legale effettua al fine di adempiere all'incarico di rappresentare la società in giudizio è quindi legato al funzionale ruolo dello Studio legale che, quindi, è da considerarsi **titolare** di tale trattamento.

Esempio: Operatori di telecomunicazioni
La fornitura di un servizio di comunicazione elettronica come un **servizio di posta elettronica** comporta l'elaborazione di dati personali. Il fornitore di tali servizi sarà normalmente considerato **un titolare del trattamento rispetto al trattamento dei dati personali necessari per il funzionamento del servizio in quanto tale** (es. traffico e dati di fatturazione).
Se, **"invece"**, **l'unico scopo e ruolo del provider è quello di consentire la trasmissione di e-mail messaggi**, il fornitore non sarà considerato titolare del trattamento dei dati personali contenuto nel messaggio stesso. **Il titolare del trattamento dei dati personali contenuti all'interno del messaggio sarà normalmente considerato la persona da cui proviene il messaggio**, piuttosto che il fornitore di servizi che offre il servizio di trasmissione.

***

28. In molti casi, una valutazione delle **condizioni contrattuali** tra le diverse parti

coinvolte **può facilitare** la determinazione di quale parte (o parti) agisce in qualità di titolare del trattamento. Anche se un contratto tace rispetto a chi sia il titolare del trattamento, può contenere elementi sufficienti per dedurre chi esercita un potere decisionale rispetto alle finalità e ai mezzi del trattamento. **Può anche darsi che il contratto contiene una dichiarazione esplicita sull'identità del titolare** del trattamento. Se non c'è motivo di dubitarne, e ciò **rispecchia fedelmente la realtà**, i termini del contratto non contrastano con il GDPR.

Tuttavia, i **termini di un contratto non sono decisivi** in tutte le circostanze, poiché ciò consentirebbe opportunisticamente alle parti di assegnare la responsabilità come meglio credono. **Non è possibile né diventare titolare del trattamento né sottrarsi agli obblighi del titolare semplicemente configurando il contratto in un certo modo** quando, per contro, le circostanze di fatto indicano qualcos'altro.

29. Se una parte **decide di fatto perché e come vengono trattati i dati** personali, quella parte **sarà titolare** del trattamento anche se un contratto dice che è un responsabile. Allo stesso modo, non è perché un contratto commerciale utilizza il termine "subappaltatore" che un'entità deve essere considerata un responsabile del trattamento dal punto di vista della legge sulla protezione dei dati.

30. In linea con l'approccio fattuale, la **parola "determina"** significa che l'entità che effettivamente esercita **un'azione d'influenza determinante sulle finalità e sui mezzi** del trattamento è il **titolare** del trattamento. Normalmente, un accordo stabilisce chi è la **parte determinante** (titolare) e la **parte istruita** (responsabile del trattamento).

Anche nel caso in cui il responsabile offra un servizio **preliminarmente definito** in modo specifico, **il titolare** è tenuto a valutare la descrizione dettagliata del servizio e **deve prendere la decisione finale** di attivamente approvare le modalità di svolgimento del trattamento e richiederne l'eventuale modifica. Inoltre, il responsabile non può in una fase successiva modificare gli elementi essenziali del trattamento senza il consenso del titolare.

***

Esempio: servizio di *cloud storage* standardizzato

Un grande provider di ***cloud storage*** offre ai propri clienti la possibilità di archiviare grandi volumi di dati personali. **Il servizio è completamente standardizzato, con i clienti che hanno poca o nessuna possibilità di personalizzare il servizio**. I termini del contratto sono determinati e **redatti unilateralmente dal fornitore di servizio cloud**, fornito al cliente su base **"prendere o lasciare"**.

La società X decide di avvalersi di tale provider cloud per memorizzare i dati personali relativi ai propri clienti. **La società X sarà ancora considerata un titolare del trattamento**, data **la sua decisione** di avvalersi di questo particolare fornitore di servizi cloud per elaborare dati personali per le sue finalità. Nella misura in cui il fornitore di servizi cloud non elabora i dati personali per i propri scopi e **conserva i dati esclusivamente per conto dei propri clienti** in conformità con le istruzioni ricevute, il fornitore di servizi sarà

considerato un responsabile del trattamento.

***

2.1.3 "Da solo o insieme ad altri"

31. L'art. 4, par. 7, riconosce che le "***finalità e mezzi***" del trattamento **potrebbero essere determinate da più di un attore**. Essa afferma che il titolare è l'attore che "***da solo o insieme ad altri***" determina le finalità e i mezzi del trattamento. Ciò significa che diverse entità possono agire come titolari del trattamento stesso, ciascuna delle quali sarà quindi soggetta alle applicabili disposizioni di protezione dei dati. Di conseguenza, **un'organizzazione può ancora essere titolare del trattamento anche se non assume tutte le decisioni in merito a scopi e mezzi**. I criteri per la contitolarità e la misura in cui due o più attori la esercitano congiuntamente possono assumere forme diverse, come chiarito in seguito.13

2.1.4 "Finalità e mezzi"

32. Il quarto elemento costitutivo della definizione del titolare si riferisce all'**oggetto dell'influenza del titolare**, ovvero le "**finalità e mezzi**" del trattamento. Rappresenta la **parte sostanziale del concetto di titolare**: è ciò che, in sostanza, una parte dovrebbe determinare per qualificarsi come titolare.

33. I dizionari definiscono lo "**scopo/finalità**" come "**un risultato previsto o che guida la pianificazione di "azioni" e "mezzi"** al fine di "ottenere un **risultato** o di raggiunge un **fine**".

34. Il GDPR stabilisce che i dati devono essere raccolti per **finalità determinate**, esplicite e legittime e non ulteriormente trattati in modo incompatibile con tali finalità. La **determinazione degli "scopi"** di trattamento **ed** i "**mezzi**" per realizzarli è quindi **particolarmente importante.**

35. Determinare le finalità e i mezzi equivale a decidere rispettivamente il **"perché" e** il **"come"** del trattamento: data una particolare operazione di trattamento, il titolare del trattamento è l'attore che **ha determinato il motivo** per cui ha luogo il trattamento (ad esempio, "a quale fine" o "per cosa") **e come questo obiettivo deve essere raggiunto** (ossia quali mezzi devono essere impiegati per raggiungere l'obiettivo). Un soggetto o una persona giuridica che esercita tale influenza sul trattamento dei dati personali, partecipa in tal modo alla determinazione delle finalità e dei mezzi di tale trattamento conformemente alla definizione di cui all'art. 4(7) GDPR.

36. Il titolare del trattamento **deve decidere sia le finalità che i mezzi del trattamento** come descritto di seguito ("***must decide on both purpose and means***"). Di conseguenza, **il titolare non può accontentarsi della sola determinazione dello scopo**. **Deve anche prendere decisioni sulle modalità del trattamento**.

Viceversa, la parte che agisce in qualità di **responsabile non può mai determinare le finalità** del trattamento.

37. In pratica, se un titolare del trattamento incarica un responsabile del

trattamento di eseguire il trattamento per suo conto, spesso significa che **il responsabile del trattamento sarà in grado di prendere determinate decisioni da solo** (solo) su **come** eseguire il trattamento.

L'EDPB riconosce che può esistere un certo margine di manovra affinché il responsabile sia anche in grado di prendere alcune decisioni in relazione al trattamento. In questa prospettiva, è necessario fornire indicazioni su quale livello di influenza **sul "perché" e sul "come"** dovrebbe comportare la qualificazione di un'entità in qualità di titolare del trattamento e in che **misura un responsabile del trattamento può prendere decisioni autonomamente**.

38. Quando **un'entità determina chiaramente finalità e mezzi**, affidando il trattamento ad un'altra entità in termini di attività che equivalgono all'esecuzione delle sue istruzioni dettagliate, la **situazione è semplice** e **non c'è dubbio** che la seconda entità debba essere considerata un responsabile, mentre la prima entità è il titolare.

Mezzi essenziali *vs* mezzi non essenziali

39. La questione si pone quando vi è da tracciare **il confine tra le decisioni** riservate al titolare e le decisioni che possono essere lasciate alla discrezionalità del responsabile del trattamento. Le **decisioni sulle finalità** del trattamento sono chiaramente **sempre** di competenza del **titolare**.

40[1]. **Per quanto riguarda la determinazione dei mezzi, si può distinguere tra mezzo essenziale e non essenziale**. I "mezzi essenziali" sono tradizionalmente e intrinsecamente riservati al titolare. I mezzi non essenziali possono essere determinati pure dal responsabile del trattamento. I mezzi essenziali, invece, devono essere determinati dal titolare.

"Mezzi essenziali"

sono mezzi **strettamente collegati allo scopo e all'ambito del trattamento,** come il **tipo di dati personali** oggetto di trattamento ("quali dati devono essere trattati?"), la **durata** del trattamento ("per quanto tempo devono essere trattati?"),

1 Si riporta il **punto n. 40 delle presenti linee guida nella formulazione originale** in **inglese per l'importanza che lo stesso può assumere**: *<<As regards the determination of means, a distinction can be made between essential and non-essential means. "Essential means" are traditionally and inherently reserved to the controller. While nonessential means can also be determined by the processor, essential means are to be determined by the controller. "Essential means" are means that are closely linked to the purpose and the scope of the processing, such as the type of personal data which are processed ("which data shall be processed?"), the duration of the processing ("for how long shall they be processed?"), the categories of recipients ("who shall have access to them?") and the categories of data subjects ("whose personal data are being processed?"). Together with the purpose of processing, the essential means are also closely linked to the question of whether the processing is lawful, necessary and proportionate. "Non-essential means" concern more practical aspects of implementation, such as the choice for a particular type of hard- or software or the detailed security measures which may be left to the processor to decide on>>*.

le **categorie di destinatari** ("chi avrà accesso ad essi?") e le **categorie di interessati** ("i cui dati personali sono trattati").

Insieme alle finalità del trattamento, le **modalità essenziali sono anche strettamente legate alla questione se il trattamento sia lecito, necessario e proporzionato**.

"Mezzi non essenziali"

riguardano **aspetti più pratici dell'attuazione**, come la **scelta di un particolare tipo di software o le misure di sicurezza dettagliate** che possono essere lasciate al responsabile del trattamento.

***

Esempio: gestione del pagamento degli stipendi
Il **datore di lavoro A** incarica una società di **gestire il pagamento degli stipendi ai propri dipendenti**. Il datore di lavoro A **dà istruzioni chiare** su chi pagare, quali **importi**, entro quale **data**, su quale **banca**, per quanto **tempo i dati devono essere conservati**, **quali dati devono essere comunicati** all'autorità fiscale ecc. In questo caso, il trattamento dei dati viene effettuato in base allo **scopo predeterminato dalla Società A** di pagare gli stipendi ai propri dipendenti e il gestore non può utilizzare i dati per scopi propri. **Il modo in cui effettuare il trattamento è in sostanza chiaramente e strettamente definito**.
Tuttavia, il gestore dei pagamenti può decidere **su alcune questioni di dettaglio** relative al trattamento, ad esempio sui software da utilizzare, o sul come distribuire l'accesso all'interno della propria organizzazione ecc. **Ciò non altera il suo ruolo come responsabile a condizione che il gestore non vada contro o oltre le istruzioni fornite** dalla Azienda A.

Esempio: pagamenti bancari
Nell'ambito delle istruzioni del datore di lavoro A, il gestore del libro paga **trasmette le informazioni alla Banca B** in modo che possa effettuare il pagamento effettivo ai dipendenti del Datore di lavoro A. Questa attività include trattamento dei dati personali da parte della Banca B che svolge per finalità di attività di *performing banking*. **All'interno di questa attività, la banca decide autonomamente rispetto al datore di lavoro A quali dati sono da trattare per fornire il servizio, per quanto tempo i dati devono essere conservati ecc**.
Il datore di lavoro A non può avere alcuna influenza sulle finalità e sui mezzi del trattamento dei dati da parte della Banca B. **La banca B deve quindi essere considerata titolare del trattamento** e la trasmissione dei dati personali dal gestore del libro paga deve essere considerata come **una comunicazione** di informazioni tra **due titolari del trattamento**, da Datore di lavoro A alla banca B.

Esempio: revisione contabile
Il datore di lavoro A incarica anche la **società di revisione C di svolgere revisioni della loro contabilità** e quindi **trasferisce i dati** sulle transazioni finanziarie (inclusi i dati personali) a C. società di contabilità C che tratta questi dati **senza istruzioni dettagliate** da parte di A.
La società di revisione C decide essa stessa, in conformità con le disposizioni di legge che regolano i compiti delle attività di revisione svolte da C, che i dati raccolti saranno trattati solo ai fini della revisione A e **determina quali dati** deve avere, **quali categorie di persone devono essere registrate**, per quanto **tempo i dati devono essere conservati** e quali mezzi tecnici sono da utilizzare. **In queste circostanze, la società di revisione contabile C è da considerarsi titolare del trattamento** quando svolge i propri servizi di revisione per A.
Tuttavia, questa **valutazione può essere diversa a seconda del livello delle istruzioni di A**. In una situazione in cui la legge non prevede specifiche obblighi per la società di revisione e la società cliente **fornisce istruzioni molto dettagliate** sull'elaborazione, la società di revisione agirebbe effettivamente in qualità di **responsabile del trattamento**. Si potrebbe fare una distinzione tra una situazione in cui il trattamento è - in conformità con le leggi che regolano questa professione - svolta nell'ambito dell'attività principale della società di revisione e laddove il trattamento sia più limitato, accessorio quale compito svolto nell'ambito dell'attività offerta all'azienda cliente.

Esempio: servizi di hosting
Il datore di lavoro A incarica del servizio di hosting H, ossia di **archiviare i dati crittografati sui propri server**. H svolge il mero servizio di hosting **senza determinare scopi né elaborare i dati in altro modo se non mediante archiviazione** sui propri server. Tale archiviazione è un esempio di attività di trattamento dei dati personali ove **H tratta i dati personali per conto del datore di lavoro A ed è quindi un mero responsabile del trattamento**. Il datore di lavoro A deve fornire le istruzioni necessarie a H e siglare un accordo sul trattamento dei dati secondo l'art. 28, richiedendo ad H di attuare la sicurezza tecnica e organizzativa delle misure necessarie. H deve assistere A nell'assicurare che siano prese le misure di sicurezza necessarie e notificare alla prima i casi di violazione dei dati personali.

***

41. Anche **se le decisioni su mezzi non essenziali possono essere lasciate al responsabile**, il **titolare del trattamento deve comunque inserire alcuni elementi nel contratto del responsabile**, come, ad esempio, in relazione al requisito della sicurezza dando indicazioni di adottare tutte le misure richieste ai sensi dell'art. 32 del GDPR.

Il contratto deve inoltre indicare che il responsabile del trattamento assiste il titolare del trattamento nel garantire il rispetto, ad esempio, dell'art. 32.

In ogni caso, **il titolare del trattamento rimane responsabile dell'attuazione di adeguate misure tecniche e organizzative** e deve garantire ed essere in grado di dimostrare che il trattamento è effettuato in conformità al Regolamento (art. 24).

In tal modo, il Titolare deve tener conto della natura, dell'ambito, del contesto e delle finalità del trattamento, nonché dei rischi per diritti e libertà delle persone fisiche. Per questo motivo, **il titolare del trattamento deve essere pienamente informato sui mezzi che vengono utilizzati** (dal responsabile) in modo che possa prendere una decisione informata al riguardo.

Affinché il titolare del trattamento possa dimostrare la liceità del trattamento, **si consiglia di documentare nel contratto**, o altro atto giuridicamente vincolante, **le misure tecniche e organizzative necessarie** quale strumento di regolazione dei rapporti tra titolare e responsabile.

***

Esempio: call center
L'azienda X decide di **esternalizzare** una parte delle sue relazioni con il servizio clienti a un **call center**. Il call center riceve dati identificabili sugli acquisti dei clienti, nonché informazioni di contatto. **Il call center utilizza il proprio software e la propria infrastruttura informatica per la gestione dei dati personali relativi alla Società X** clienti.
La società X firma un accordo di trattamento con il fornitore del call center in conformità con l'art. 28 GDPR, dopo aver accertato che le misure di sicurezza tecniche e organizzative proposte dal call center sono adeguate ai rischi in questione e che il call center sarà tenuto a trattare i dati personali solo per le finalità della Società X e secondo le sue istruzioni. **L'azienda X non fornisce ulteriori istruzioni al call center in merito al software specifico da essere utilizzati né alcuna istruzione dettagliata in merito alle misure di sicurezza specifiche da attuare**. In questo esempio, la **società X rimane titolare del trattamento**, **nonostante il call center abbia determinato i mezzi non essenziali del trattamento**.

***

2.1.5 “Del trattamento dei dati personali”

42. Le finalità e i mezzi determinati dal titolare del trattamento devono riguardare il "trattamento di dati personali". L'art. 4, par. 2, del GDPR definisce il trattamento dei dati personali come "**qualsiasi operazione** o **complesso di operazioni** che viene eseguito su dati personali o su insiemi di dati personali”. Di conseguenza, il **concetto di titolarità può essere collegato sia ad un singolo trattamento** che ad un **insieme di operazioni**.

In pratica, questo può significare che la titolarità esercitata da un determinato soggetto può estendersi **all'intero trattamento in questione ma può anche essere limitata a una fase particolare del trattamento stesso.**

43. In pratica, il trattamento dei dati personali che coinvolge più soggetti e può essere suddiviso in più piccole operazioni di trattamento per le quali ciascun attore potrebbe essere considerato titolare poiché determina le finalità e i mezzi individualmente rispetto al alcune operazioni.

D'altra parte, una sequenza o un insieme di operazioni di trattamento che coinvolgono più attori può avvenire anche per la(e) stessa(e) finalità(e), nel qual caso è possibile che il trattamento comporti uno o più **contitolari**. In altre parole, è possibile che a "**livello micro**" **le diverse elaborazioni e le operazioni della catena appaiono come sconnesse**, in quanto ciascuna di esse può avere uno scopo diverso. Tuttavia, è necessario **ricontrollare se anche** a "**livello macro**" queste operazioni di trattamento possono essere considerate come un "insieme di operazioni" che perseguono uno **scopo comune** utilizzando mezzi definiti congiuntamente.

44. Chiunque decida di trattare dati deve considerare se ciò includa dati personali e, in caso affermativo, quali sono gli obblighi secondo il GDPR. **Un attore** sarà **considerato un "titolare" anche se non mira deliberatamente a trattare dati personali** in quanto tali o ha erroneamente valutato che non elabora dati personali.

45. Non è necessario che il titolare del trattamento abbia effettivamente accesso ai dati oggetto di trattamento. **Chi esternalizza** un'attività di trattamento e, nel farlo, ha **un'influenza determinante sulla finalità e i mezzi** (**essenziali**) del trattamento (ad esempio, adeguando i parametri di un servizio in modo da esercitare influenze sui dati personali che devono essere trattati), è da considerarsi **titolare del trattamento** anche se non avrà mai accesso effettivo ai dati.

***

Esempio: ricerca di mercato 1
La **società ABC** desidera capire quali tipi di **consumatori hanno maggiori probabilità di essere interessati ai suoi prodotti** ed incarica un **fornitore di servizi, XYZ**, per ottenere le informazioni pertinenti. La società **ABC istruisce XYZ** sul tipo di informazioni a cui è interessata e **fornisce un elenco di domande** da porre ai partecipanti alla ricerca di mercato.
La **società ABC riceve solo informazioni statistiche** (ad es. identificazione delle tendenze dei consumatori per regione) da XYZ e non ha accesso ai dati personali stessi. Tuttavia, la società ABC ha deciso che il il trattamento deve aver luogo, e il trattamento è dunque effettuato **per la sua finalità e la sua attività** e ha fornito a XYZ istruzioni dettagliate su quali informazioni raccogliere. **La società ABC è quindi da considerarsi titolare del trattamento** rispetto al trattamento di dati personali che avviene al fine di ottenere le informazioni che ha richiesto. **XYZ** può trattare i dati solo per lo scopo indicato dalla Società ABC e secondo le sue dettagliate istruzioni ed è pertanto da considerarsi **responsabile** del trattamento.

Esempio: ricerca di mercato 2

La **società ABC** desidera capire quali tipi di consumatori hanno maggiori probabilità di essere interessati al suo prodotti. Il fornitore di servizi XYZ è **un'agenzia di ricerche di mercato che ha raccolto informazioni su interessi dei consumatori attraverso una serie di questionari che riguardano un'ampia varietà di prodotti e servizi**. Il fornitore di servizi XYZ ha raccolto e analizzato questi dati in modo indipendente, secondo la propria metodologia senza ricevere istruzioni dalla società ABC.

Per rispondere alla società ABC **il fornitore XYZ genererà informazioni statistiche, ma lo farà senza riceverne alcuna istruzione su quali dati personali dovrebbero essere trattati o come trattarli al fine di generare queste statistiche**. In questo esempio, XYZ agisce come **unico titolare del trattamento**, elaborazione dati personali per finalità di ricerche di mercato, determinando autonomamente le modalità per farlo.

La società ABC non ha alcun ruolo o responsabilità particolare ai sensi della legge sulla protezione dei dati in relazione a queste attività di trattamento, in quanto **la stessa Società ABC riceve statistiche anonime e non è coinvolta nella determinazione delle finalità e dei mezzi del trattamento**.

***

3 DEFINIZIONE DI CONTITOLARI

3.1 Definizione di contitolari del trattamento

46. La qualifica di contitolari del trattamento può sorgere qualora nel trattamento sia coinvolto più di un soggetto.

47. Sebbene il concetto non sia nuovo ed esistesse già ai sensi della direttiva 95/46/CE, il GDPR, nel suo art. 26, introduce regole specifiche per i contitolari del trattamento e definisce un quadro per disciplinare il loro rapporto. Inoltre, la Corte di Giustizia dell'Unione Europea (CGUE) in recenti sentenze ha portato chiarimenti su questo concetto e le sue implicazioni (cfr: *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie*, C-210/16, *Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta* C-25/17, ***Fashion ID** GmbH & Co. KG v Verbraucherzentrale NRW eV* C-40/17).

48. Come ulteriormente elaborato nella Parte II, sezione 2, la qualifica di contitolari del trattamento avrà principalmente conseguenze in termini di **attribuzione degli obblighi per il rispetto delle norme** sulla protezione dei dati e in particolare riguardo ai diritti degli individui.

49. In questa prospettiva, la sezione seguente mira a fornire indicazioni sulla nozione di contitolari del trattamento in conformità con il GDPR e la giurisprudenza della CGUE per assistere le entità nel determinare dove possono agire in qualità di contitolari del trattamento e applicare il concetto nella pratica.

3.2 Esistenza di contitolarità

3.2.1 Considerazioni generali

50. La definizione di titolare del trattamento di cui **all'art. 4, par. 7**, del GDPR costituisce il **punto di partenza** per la determinazione della titolarità congiunta. Le **considerazioni in questa sezione sono** quindi direttamente **collegate e integrano le considerazioni** nella sezione **sul concetto di titolare**. Di conseguenza, la valutazione della comune titolarità dovrebbe rispecchiare la valutazione della titolarità "unica" sviluppata sopra.

51. L'art. 26 del GDPR, che riflette la definizione di cui all'art. 4, par. 7, del GDPR, prevede che "[dove] ***due o più i titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, sono contitolari del trattamento***". In termini ampi la contitolarità esiste in relazione a una specifica attività di trattamento quando più parti determinano congiuntamente le finalità e i mezzi di tale trattamento. Pertanto, **valutare l'esistenza di contitolari richiede di esaminare se la determinazione delle finalità e dei mezzi che caratterizzano un titolare sono decise da più parti**. "**Congiuntamente**" deve essere interpretato con il significato di **"insieme con"** o **"non da solo"**, in diverse forme e combinazioni, come spiegato di seguito.

52. La valutazione della contitolarità dovrebbe essere **effettuata in base ad una analisi fattuale**, piuttosto che formale **dell'effettiva influenza sulle finalità e sui mezzi** del trattamento. Tutte le esistenti disposizioni dovrebbero essere verificate rispetto alle circostanze di fatto relative al rapporto tra parti.

Un criterio meramente formale non sarebbe sufficiente per almeno due ragioni: **A)** in alcuni casi, la nomina formale di un contitolare - prevista ad esempio dalla legge o da un contratto – potrebbe essere assente; **B)** in altri casi, potrebbe darsi che **la nomina formale non rifletta la realtà** degli accordi, affidando formalmente il ruolo di titolare del trattamento ad un soggetto che di fatto non è in posizione per "determinare" le finalità e i mezzi del trattamento.

53. Non tutti i trattamenti che coinvolgono più soggetti danno luogo alla contitolarità. Il criterio generale da seguire affinché possa sussistere la contitolarità è la **partecipazione congiunta di due o più soggetti alla determinazione delle finalità e dei mezzi del trattamento**. Più specificamente, la **partecipazione congiunta deve** includere **la determinazione dei fini da un lato e la determinazione dei mezzi dall'altro**. Se questi elementi sono determinati da tutti i soggetti interessati, essi devono essere considerati congiunti titolari del trattamento in questione.

3.2.2 Valutazione della partecipazione congiunta

54. La partecipazione congiunta alla determinazione delle **finalità e** dei **mezzi** implica che più soggetti abbiano **un'influenza decisiva sul se e sul come avviene il trattamento**.

In pratica, la partecipazione congiunta può assumere diverse forme. Ad esempio,

la partecipazione congiunta può assumere la forma di una **comune decisione** presa da due o più entità o derivare da **decisioni convergenti** di due o più entità riguardo alle **finalità** e ai **mezzi essenziali**.

55. La partecipazione congiunta attraverso una decisione comune significa decidere insieme e implica **un'azione** comune o **intenzione** secondo la più comune accezione del termine "congiuntamente" di cui al art. 26 del GDPR.

La situazione della partecipazione congiunta attraverso decisioni convergenti risulta più in particolare dalla giurisprudenza della CGUE sulla nozione di contitolari del trattamento. **Le decisioni possono essere considerate come convergenti su finalità e mezzi se si completano a vicenda e sono necessarie affinché il trattamento possa avere luogo ed in modo tale da avere un impatto tangibile sulla determinazione delle finalità e mezzi del trattamento**. Va sottolineato che la nozione di decisioni convergenti deve essere considerata in relazione alle finalità e ai mezzi del trattamento ma non ad altri aspetti del rapporto commerciale tra le parti.

In quanto tale, **un criterio** importante per identificare le convergenze di decisioni in questo contesto è **se il trattamento non fosse possibile** senza che entrambe **le parti partecipino alle finalità e ai mezzi, nel senso che il trattamento da parte di ciascuna parte è inseparabile**, cioè le partecipazioni siano **indissolubilmente legate**. La situazione dei contitolari che agiscono sulla base della convergenza di decisioni dovrebbero tuttavia essere distinte dal caso di un responsabile, poiché quest'ultimo – mentre partecipa all'esecuzione di un trattamento – non tratta i dati per finalità proprie ma effettua il trattamento per conto del titolare.

56. Il fatto che una delle parti non abbia accesso ai dati personali trattati non è sufficiente per escludere il controllo congiunto. **Ad esempio, nei casi dei Testimoni di Geova, la CGUE ha ritenuto che la comunità religiosa dovesse essere considerata un titolare insieme ai suoi membri** che si impegnavano nel trattamento di dati personali effettuato mediante **la predicazione porta a porta**. La CGUE ha ritenuto che non fosse necessario che la comunità avesse accesso ai dati in questione, o necessario stabilire che la comunità aveva dato ai suoi membri indicazioni scritte o istruzioni in relazione al trattamento dei dati. **La comunità ha partecipato alla determinazione delle finalità e dei mezzi, organizzando e coordinando le attività dei suoi membri, che hanno contribuito a raggiungere l'obiettivo della comunità dei Testimoni di Geova**. Inoltre, la comunità aveva la conoscenza, a livello generale, del fatto che tale trattamento è stato effettuato al fine di diffonderne la fede.

57. È inoltre importante sottolineare, come chiarito dalla CGUE, che un'entità sarà considerata contitolare del trattamento con un'altra entità solo in relazione alle operazioni per le quali determina, congiuntamente con altri, le modalità e le finalità del trattamento dei dati stessi in particolare in caso di convergenza di decisioni. Se uno di questi soggetti decide da solo le finalità e le modalità delle operazioni che precedono o sono successivi nella catena del trattamento, tale soggetto deve considerarsi unico titolare dell'operazione precedente o successiva.

58. L'esistenza della contitolarità **non implica** necessariamente la **pari**

responsabilità dei vari operatori coinvolti nel trattamento dei dati personali. Al contrario, **la CGUE ha chiarito che gli operatori possono essere coinvolti in diverse fasi di tale trattamento e in misura diversa** in modo che il il livello di responsabilità di ciascuno di essi deve essere valutato in relazione a tutte le circostanze rilevanti del caso particolare.

3.2.2.1 Scopo/i determinato/i congiuntamente

59. La contitolarità sussiste quando i soggetti coinvolti nel medesimo trattamento effettuano il trattamento per **finalità congiuntamente definite**. Ciò avverrà se i soggetti coinvolti trattano i dati per lo stesso scopo, oppure comune finalità.

60. Inoltre, quando i soggetti non hanno le stesse finalità del trattamento, la contitolarità può altresì, alla luce della giurisprudenza della CGUE, essere costituita quando i soggetti interessati perseguono **finalità strettamente collegate o complementari**.

Tale può essere il caso, ad esempio, di **quando sussiste un mutuo beneficio derivante dalla stessa operazione di trattamento, a condizione che ciascuno dei soggetti coinvolti partecipi alla determinazione delle finalità e dei mezzi** del relativo trattamento.

Tuttavia, la nozione di mutuo vantaggio non è decisiva e può essere **solo indicativa**.

In Fashion ID, per esempio, la CGUE ha chiarito che **un gestore di un sito** web partecipa alla determinazione delle finalità (e mezzi) del trattamento incorporando un social plug-in in un sito web al fine di ottimizzare la pubblicità dei propri prodotti rendendoli più visibili sui social network. **La CGUE ha ritenuto che il trattamento in questione sia stato effettuato nell'interesse economico sia del gestore del sito web e sia del fornitore del social plug-in**.

61. Parimenti, come rilevato dalla CGUE in Wirtschaftsakademie, il trattamento dei dati personali attraverso **le statistiche dei visitatori di una fan page** ha lo scopo di consentire a Facebook di migliorare i propri sistemi di pubblicità trasmessi tramite la sua rete e per consentire all'amministratore della pagina fan di ottenere statistiche per gestire la promozione della propria attività. Ciascun soggetto in questo caso persegue il proprio interesse ma entrambe **le parti partecipano alla determinazione delle finalità** (e dei mezzi) **del trattamento dei dati personali in quanto valutano i visitatori della fan page**.

62. Al riguardo, è importante evidenziare **che la mera esistenza di un vantaggio reciproco** (ad es. commerciale) **derivante da un'attività di trattamento non dà luogo a contitolarità**. Se le entità coinvolte nel trattamento non perseguono alcuna finalità propria in relazione al trattamento, ma sono semplicemente pagate per i servizi resi, agiscono come un responsabile piuttosto che come contitolari.

3.2.2.2 Mezzi determinati congiuntamente

63. La contitolarità richiede anche che due o più soggetti abbiano **esercitato**

un'influenza sui mezzi di trattamento. Ciò **non significa che, perché esista la contitolarità, ogni soggetto coinvolto abbia bisogno di determinare tutti i mezzi** in tutti i casi. Infatti, come chiarito dalla CGUE, diverse entità possono essere coinvolte in diverse fasi di tale trattamento e in gradi diversi. **Diversi titolari congiunti possono quindi definire le modalità del trattamento in misura diversa**, a seconda di chi è effettivamente in una posizione per farlo.

64. Può anche accadere che uno dei soggetti coinvolti fornisca i mezzi del trattamento rendendoli **disponibili per attività di trattamento di dati personali da parte di altri soggetti**. L'entità che decide di utilizzare tali mezzi affinché i dati personali possano essere trattati anche per uno scopo particolare partecipa alla determinazione delle modalità del trattamento.

65. Questo scenario può verificarsi in particolare **nel caso di piattaforme**, strumenti standardizzati o **altre infrastrutture** che consentono alle parti il trattamento dei dati personali o che siano stati in qualche modo predisposte da una delle parti ad essere utilizzate da altri che possono anche **decidere come costituirlo**. Quindi l'**uso di un sistema tecnico già esistente non esclude la contitolarità** quando gli utenti del sistema **possono decidere in merito al trattamento** dei dati personali da eseguire in questo contesto.

66. A titolo di esempio, la CGUE ha ritenuto in Wirtschaftsakademie che **l'amministratore di una fan page su Facebook, definendo parametri in base al suo pubblico di destinazione e agli obiettivi di gestione e promozione delle proprie attività**, deve considerarsi **partecipe alla determinazione delle modalità** del trattamento dei dati personali relativi **ai visitatori della sua fan page**.

67. Inoltre, la scelta operata da un **soggetto di utilizzare per i propri fini uno strumento o altro sistema sviluppato da un'altra entità**, consentendo il trattamento dei dati personali, **equivarrà probabilmente ad una comune decisione** sulle modalità di tale trattamento da parte di tali soggetti. Ciò deriva dal caso **Fashion ID** in cui la CGUE ha concluso che incorporando nel proprio sito web **il pulsante Mi piace di Facebook messo a disposizione da Facebook agli operatori del sito web, Fashion ID ha esercitato un'influenza decisiva** rispetto alle **operazioni che comportano la raccolta e la trasmissione dei dati personali** dei visitatori del suo sito Web a Facebook e aveva quindi **determinato congiuntamente con Facebook le modalità di tale trattamento**.

68. È importante sottolineare che l'uso di **un sistema o di un'infrastruttura comune** di elaborazione dei dati **non porterà in tutti i casi** a qualificare i soggetti coinvolti come **contitolari del trattamento**, in particolare laddove **il trattamento che effettuano è separabile** e potrebbe essere **eseguito da una parte senza l'intervento dell'altra** o se il fornitore **è un responsabile del trattamento in assenza di uno scopo** proprio (l'esistenza di un mero vantaggio commerciale per le parti coinvolte non è sufficiente per qualificarsi come uno scopo di in lavorazione).

***

Esempio: agenzia di viaggi
Un'**agenzia di viaggi** invia **i dati personali dei propri clienti** alla

compagnia aerea e a una catena di **hotel**, al fine di effettuare prenotazioni per un pacchetto di viaggio. La compagnia aerea e l'hotel confermano la disponibilità dei posti e camere richieste. L'agenzia di viaggi emette i documenti di viaggio e i voucher per i propri clienti.
(A) Ciascuno degli **attori tratta i dati per lo svolgimento delle proprie attività e utilizzando i propri mezzi**. In questo caso, l'agenzia di viaggi, la compagnia aerea e l'hotel sono **tre diversi titolari** del trattamento dati per finalità proprie e separate e **non vi è contitolarità**.
(B) L'agenzia di viaggi, la catena alberghiera e la compagnia aerea **decidono quindi di partecipare congiuntamente alla costituzione di un piattaforma comune basata su Internet allo scopo comune** di fornire pacchetti turistici. Essi **concordano i mezzi essenziali da utilizzare**, ad esempio **quali dati verranno archiviati**, come **saranno le prenotazioni assegnati e confermati**, e chi può avere accesso alle informazioni conservate. Inoltre, **decidono di condividere i dati** dei propri clienti al fine di svolgere azioni di **marketing congiunte**. In questo caso, l'agenzia di viaggi, la compagnia aerea e la catena alberghiera, determinano congiuntamente **perché e come** i dati personali dei loro i rispettivi clienti sono trattati e saranno pertanto **contitolari del trattamento** delle operazioni di trattamento relative alla piattaforma comune di prenotazione basata su Internet e alle comuni azioni di marketing. Tuttavia, ciascuno di essi manterrebbe comunque il controllo esclusivo sulle altre attività di trattamento al di fuori della piattaforma comune basata su Internet.

Esempio: progetto di ricerca di istituti
Diversi istituti di ricerca decidono di partecipare ad uno specifico **progetto di ricerca congiunto** e di **utilizzare a tale scopo la piattaforma esistente di uno degli istituti** coinvolti nel progetto. Ogni istituto **immette dati** personali che già detiene nella piattaforma ai fini della ricerca congiunta **e utilizza i dati forniti da altri** attraverso la piattaforma per lo svolgimento della ricerca.
(A) In questo caso, **tutti gli istituti si qualificano come congiunti titolari** del trattamento dei dati personali che avviene memorizzando e divulgando informazioni da questa piattaforma in quanto **hanno deciso insieme le finalità del trattamento e le modalità** per l'utilizzo della piattaforma esistente.
(B) Ciascuno degli istituti, **tuttavia, è un titolare separato per qualsiasi altro trattamento** che potrà essere effettuato al di fuori della piattaforma per le rispettive finalità.

Esempio: operazione di marketing
Le società A e B hanno **lanciato un prodotto C in co-branding** e desiderano organizzare un evento per promuovere tale prodotto. A tal fine, **decidono di condividere i dati dei rispettivi clienti** e dei potenziali clienti e decidono su questa base l'elenco degli invitati all'evento. **Concordano anche le modalità per inviare gli inviti** all'evento, come raccogliere feedback durante l'evento e follow-up azioni di marketing. Le società A e B possono essere considerate

contitolari del trattamento di dati personali relativi all'organizzazione dell'evento promozionale in quanto **decidono insieme finalità e mezzi essenziali** del trattamento dei dati definiti congiuntamente in questo contesto.

Esempio: studi clinici

Un operatore sanitario (lo **sperimentatore**) e **un'università** (lo sponsor) decidono di avviare insieme una **sperimentazione clinica** con lo stesso scopo.

(A) Collaborano insieme alla stesura del protocollo di studio (vale a dire scopo, **metodologia** e **progettazione** dello studio, **dati da raccogliere**, esclusione/inclusione del soggetto criteri, riutilizzo del database (se pertinente, ecc.). Possono **essere considerati contitolari del trattamento, per questo sperimentazione clinica in quanto determinano e concordano congiuntamente lo stesso scopo e i mezzi essenziali** della procedura.

(B) La raccolta di dati personali dalla cartella clinica del paziente al fine di ricerca **va distinta dalla conservazione e dall'utilizzo dei medesimi dati ai fini delle cure del paziente** per le quali il sanitario che offre assistenza sanitaria rimane il titolare del trattamento.

(C) Nel caso in cui lo sperimentatore non partecipi alla stesura del protocollo (si limita ad accettare il protocollo già elaborato dallo sponsor), e il protocollo è progettato solo dallo sponsor, lo **sperimentatore dovrebbe essere considerato un responsabile** e lo sponsor il titolare del trattamento di questa sperimentazione clinica.

Esempio: cacciatori di teste

La società X aiuta la società Y a **reclutare nuovo personale**, con il suo famoso servizio a valore aggiunto "***globale matchz***".

La società X ricerca candidati idonei **sia tra i CV ricevuti direttamente dall'Azienda Y sia tra quelli che ha già nel proprio database**. Tale database è creato e gestito dalla Società X da sola. Ciò garantisce che l'azienda X migliori l'incontro tra offerte di lavoro e persone in cerca di lavoro, al contempo ingrandendo le proprie entrate.

Anche se non hanno preso formalmente **una decisione insieme**, **X e Y partecipano congiuntamente al trattamento al fine di individuare candidati idonei in base a decisioni convergenti**: la decisione di creare e gestire il servizio “global matchz” per la società X e la decisione della società Y di arricchire il database con i CV ricevuti direttamente.

Tali decisioni si completano a vicenda, sono inseparabili e necessarie per il trattamento dell'idoneo reperimento di candidati.

Pertanto, in questo caso, dovrebbero essere considerati **congiunti titolari** di tale trattamento.

Tuttavia, la Società X è l'unica titolare del trattamento necessario per gestire il proprio database e la Società Y è l'unica titolare del successivo trattamento di assunzione per proprio scopo (organizzazione dei colloqui, conclusione del contratto e gestione dei dati).

Esempio: analisi dei dati sanitari

Società **ABC**, lo sviluppatore di **una app** per il monitoraggio della **pressione sanguigna** e Società **XYZ**, un fornitore di app per i professionisti medici, desiderano **entrambi esaminare come i cambiamenti della pressione sanguigna** possono aiutare a prevedere certe malattie. Le società decidono di avviare **un progetto congiunto** e si rivolgono **all'Ospedale DEF** per coinvolgere pure lui.

I dati personali che saranno trattati in questo progetto consistono in dati personali che ABC, L'ospedale DEF e XYZ trattano separatamente come titolari del trattamento individuali. **La decisione di elaborare questi dati per valutare le variazioni della pressione sanguigna è presa congiuntamente dai tre attori**. Società ABC, L'ospedale DEF e la società XYZ **hanno determinato congiuntamente le finalità** del trattamento.

La società XYZ prende l'iniziativa di proporre le modalità essenziali del trattamento. Sia la società **ABC che l'ospedale DEF accettano questi mezzi essenziali** dopo essere stati coinvolti nello sviluppo di alcune delle funzionalità dell'app in modo che i risultati possano essere sufficientemente utili per loro. **Le tre organizzazioni quindi concordano su uno scopo comune per il trattamento** che è la valutazione di come cambia la pressione sanguigna e sul come aiutare a prevedere alcune malattie. Una volta completata la ricerca, la società ABC, l'Ospedale DEF e la società XYZ possono beneficiare della valutazione utilizzando i risultati nelle proprie attività. **Per tutti questi motivi, si qualificano come contitolari per tale specifico trattamento congiunto**.

Se gli altri avessero semplicemente chiesto alla società XYZ di eseguire tale valutazione senza che questa avesse alcuno scopo proprio, semplicemente elaborando dati per conto di altri, la Società XYZ si qualificherebbe come responsabile del trattamento anche se gli è stata affidata la determinazione dei mezzi non essenziali.

***

3.2.3 Situazioni in cui NON esiste una contitolarità

69. Il fatto che più attori siano coinvolti nello stesso trattamento non significa che essi stiano agendo necessariamente in qualità di contitolari di tale trattamento. **Non tutti i tipi di partnership, cooperazione o collaborazioni implicano la qualificazione di contitolarità** in quanto tale qualificazione richiede **una valutazione caso per caso** e l'analisi di ogni trattamento in gioco e del ruolo preciso di ciascuna entità rispetto a ciascun trattamento.

I casi seguenti forniscono **esempi non esaustivi di situazioni in cui non esiste una contitolarità**.

70. Ad esempio, lo scambio degli stessi dati o insieme di dati tra due entità senza che le stesse determinino congiuntamente finalità o mezzi di trattamento dovrebbero essere considerati come **trasmissione di dati tra distinti titolari**.

***

Esempio: trasmissione dei dati dei dipendenti alle autorità fiscali

Una società raccoglie e tratta i dati personali dei propri dipendenti con lo scopo di gestire stipendi, assicurazioni sanitarie, ecc. **Una legge impone all'azienda l'obbligo di inviare tutti i dati sugli stipendi al fisco,** al fine di rafforzare il controllo fiscale.
In questo caso, anche se sia la società che l'amministrazione finanziaria trattano gli stessi dati riguardanti stipendi, **la mancanza di finalità e mezzi congiuntamente determinati** in relazione a tale trattamento dei dati comporterà la qualificazione dei due soggetti come **due distinti titolari del trattamento**.

***

71. La contitolarità può essere **esclusa** anche in una situazione in cui più soggetti utilizzano **una banca dati condivisa o un'infrastruttura comune**, **se ciascuna entità determina autonomamente i propri scopi**.

***

Esempio: operazioni di marketing in un gruppo di aziende che utilizzano un database condiviso:
Un **gruppo di società utilizza lo stesso database** per la gestione di clienti e prospect. Tale database è ospitato sui server della casa madre che è quindi un responsabile delle
altre società per quanto riguarda la conservazione dei dati.
Ogni entità del gruppo inserisce i dati dei propri clienti e potenziali clienti e tratta tali dati esclusivamente per i propri scopi. Inoltre, ogni entità decide indipendentemente l'accesso, i **periodi di conservazione**, la rettifica o cancellazione dei propri dati di clienti e dei potenziali clienti. **Non possono accedere o utilizzare i dati degli altri**. Il solo fatto che queste aziende utilizzino una banca dati di gruppo condivisa non comporta in quanto tale la contitolarità. In queste circostanze, **ciascuna società è quindi un titolare separato**.

Esempio: titolari indipendenti quando si utilizza un'infrastruttura condivisa
La società XYZ ospita un database e lo rende disponibile ad altre società per elaborare e ospitare dati personali sui propri dipendenti. **La società XYZ è un responsabile del trattamento** in relazione al trattamento e alla conservazione dei dati dei dipendenti di altre società in quanto tali operazioni sono svolte per conto e secondo le istruzioni di queste altre società. Inoltre, le altre società trattano i dati senza alcun coinvolgimento della società XYZ e per scopi che non sono in alcun modo condivisi dalla medesima società XYZ.

***

72. Inoltre, possono esserci **situazioni in cui vari attori elaborano, via via, gli stessi dati personali in una catena di operazioni**. Ciascuno di questi attori ha uno **scopo indipendente** e **mezzi indipendenti** rispetto agli altri attori e alla loro parte della catena. **In mancanza di partecipazione congiunta alla determinazione delle finalità e mezzi** dello stesso trattamento o insieme di operazioni, **la contitolarità deve essere esclusa** e i vari attori devono essere

considerati come successivi titolari indipendenti.

***

Esempio: analisi statistica per un compito di interesse pubblico
Un'autorità pubblica (Autorità A) ha il compito di **effettuare analisi e statistiche pertinenti su come il il tasso di occupazione** del paese si sviluppa. Per fare ciò, **molti altri enti pubblici sono legalmente tenuti a comunicare dati specifici all'Autorità A**. L'Autorità A decide di utilizzare un sistema specifico per elaborare i dati, compresa la raccolta. Ciò significa anche che le altre unità sono obbligate ad utilizzare il sistema per le proprie comunicazioni dei dati. In tal caso, ferma restando l'eventuale attribuzione di ruoli prevista dalla legge, l'Autorità **A sarà unico titolare del trattamento dei dati per finalità di analisi e statistica del tasso di occupazione per come trattati nel sistema**, perché l'Autorità A determina la finalità del trattamento e ha deciso come sarà organizzato il trattamento. Naturalmente, gli altri enti pubblici, in qualità di titolari per proprie attività di trattamento, devono garantire l'esattezza dei dati che sono stati precedentemente trattati e che poi comunicano all'Autorità A.

***

DEFINIZIONE DI RESPONSABILE

73. Un responsabile del trattamento è definito **all'art. 4, par. 8 del GDPR**, come una persona fisica o giuridica, autorità pubblica, agenzia o altro organismo, che **tratta i dati personali per conto del titolare** del trattamento. Similmente alla definizione di titolare, la definizione di responsabile del trattamento prevede un'ampia gamma di attori - può essere "***una persona fisica o giuridica, pubblica autorità, agenzia o altro organismo***". Ciò significa che in linea di principio non vi è alcuna limitazione su quale tipo di attore potrebbe assumere il ruolo di responsabile. Potrebbe essere un'organizzazione, ma potrebbe anche essere un individuo.

74. Il GDPR stabilisce obblighi direttamente e specificamente applicabili ai responsabili del trattamento come ulteriormente specificato nella Parte II, sezione 1 delle presenti linee guida. Un responsabile può essere ritenuto responsabile o multato in caso di mancato rispetto di tali obblighi o qualora agisca al di fuori o in contrasto con le legittime istruzioni del titolare.

75. Il trattamento dei dati personali può coinvolgere **più responsabili del trattamento**. Ad esempio, un titolare può scegliere di coinvolgere direttamente più responsabili, coinvolgendoli in diverse fasi separate del trattamento (più responsabili). Un titolare del trattamento potrebbe anche decidere di coinvolgere un responsabile, che a sua volta - previa autorizzazione del titolare - incarica uno o più altri responsabili del trattamento ("sub responsabili"). L'attività di trattamento affidata al responsabile può essere limitata a un compito molto specifico o contesto o può essere più generale ed estesa.

76. Due condizioni fondamentali per qualificarsi come responsabile sono:

- **A)** essere un **soggetto separato** rispetto al titolare del trattamento;

- **B)** e il trattamento di dati personali deve avvenire **per conto del titolare**.

77. Per **entità separata** si intende che il titolare del trattamento decide di delegare in tutto o in parte le attività di trattamento ad un **organismo esterno**. All'interno di un gruppo di società, una società può essere un responsabile per un'altra società che agisce in qualità di titolare, in quanto entrambe le società sono entità separate. D'altra parte, **un reparto all'interno di una società** (o azienda) **non può essere un responsabile del trattamento di un altro reparto all'interno della stessa entità**.

78. Se il titolare del trattamento decide di trattare personalmente i dati, utilizzando **risorse proprie all'interno della sua organizzazione**, per esempio attraverso il proprio personale, questa **non è una situazione per cui esiste un responsabile** del trattamento. I **dipendenti** e altre persone che agiscono sotto l'autorità diretta del titolare del trattamento, come il personale impiegato temporaneamente, **non devono essere visti come responsabili del trattamento** poiché tratteranno i dati personali come parte dell'entità del titolare. Ai sensi dell'art. 29 GDPR, sono altresì vincolati dalle istruzioni del titolare.

79. Il trattamento dei dati personali per conto del titolare del trattamento richiede in primo luogo che **l'entità separata tratti dati personali a beneficio del titolare**. All'art. 4, par. 2 GDPR, il trattamento è definito come un concetto che comprende una vasta gamma di operazioni che vanno dalla raccolta, conservazione e consultazione all'utilizzo, diffusione o comunque messa a disposizione e distruzione. Il concetto di "trattamento" è ulteriormente sopra descritto al punto 2.1.5.

80. In secondo luogo, il trattamento deve essere **effettuato per conto di un titolare** del trattamento, **ma non sotto il suo diretto controllo e autorità**. Agire **"per conto di" significa servire l'interesse di qualcun altro ciò che richiama il** concetto giuridico di "**delega**". Nel caso della normativa sulla protezione dei dati, un responsabile è chiamato ad **attuare le istruzioni impartite dal titolare** almeno in ordine alle finalità del trattamento e agli elementi essenziali del mezzo.

La liceità del trattamento ai sensi dell'art. 6 e dell'art. 9, se pertinente, del Regolamento deriva dall'attività del titolare e **il responsabile del trattamento non deve trattare i dati in modo non conforme alle istruzioni del titolare**. Anche qui, come sopra descritto, le istruzioni del titolare del trattamento **possono comunque lasciare un certo grado di discrezionalità su come servire al meglio gli interessi del titolare**, consentendo al **responsabile del trattamento di scegliere il mezzo tecnico e organizzativo più idoneo**.

81. Agire **"per conto di"** significa anche che il responsabile del trattamento **non può effettuare trattamenti per un proprio scopo**. Come previsto dall'art. 28, par. 10, un responsabile del trattamento viola il GDPR andando oltre le istruzioni del titolare ove inizi a determinare le proprie finalità e modalità ("essenziali") del trattamento. Il responsabile del trattamento sarà considerato titolare del trattamento e potrà essere soggetto a sanzioni se va oltre le istruzioni del titolare.

***

Esempio: fornitore di servizi denominato responsabile del trattamento ma che agisce in qualità di titolare

Il fornitore di servizi MarketinZ fornisce **pubblicità promozionale e servizi** di **marketing diretto** a varie aziende. La società GoodProductZ conclude un contratto con MarketinZ, in base al quale quest'ultima società fornisce pubblicità commerciale per i clienti GoodProductZ ed è indicata come responsabile dei dati. Tuttavia, **MarketinZ decide di utilizzare il database dei clienti di GoodProducts anche per altri scopi** diversi dalla pubblicità di GoodProducts, come lo sviluppo della propria attività commerciale. La decisione di aggiungere **una finalità ulteriore a quella per la quale i dati personali sono stati trasferiti trasforma MarketinZ in un titolare** del trattamento per questo insieme di operazioni di trattamento e il loro trattamento per questo scopo costituirebbe una violazione del GDPR.

***

82. L'EDPB ricorda che non tutti i fornitori di servizi che trattano dati personali nel corso di una fornitura di un servizio sono un "responsabile del trattamento" ai sensi del GDPR. **Il ruolo di un responsabile non deriva dalla natura di un soggetto che tratta dati ma dalle attività concrete dallo stesso espletate** in uno specifico contesto.
In altre parole, lo stesso soggetto può agire contemporaneamente come titolare per determinati trattamenti e come responsabile per altri, e la qualifica di titolare o responsabile devono essere valutate in relazione a specifici insiemi di dati o operazioni. La natura del servizio determinerà se l'attività di trattamento equivalga al trattamento di dati personali per conto del titolare del trattamento ai sensi del GDPR. In pratica, laddove il servizio erogato non sia specificamente rivolto a trattamento di dati personali o qualora tale trattamento non costituisca un elemento fondamentale del servizio, il prestatore di servizi può essere in grado di determinare autonomamente le finalità e i mezzi di tale operazione di trattamento necessario per fornire il servizio. In tale situazione, il fornitore di servizi deve essere considerato un titolare separato e non un responsabile del trattamento. Resta necessaria **un'analisi caso per caso** al fine di accertare **il grado di influenza** effettivamente **esercitata** da ciascun soggetto nella determinazione del **finalità** e **mezzi** del trattamento.

***

Esempio: servizio taxi

(A) Un **servizio taxi offre** una **piattaforma online** che consente alle aziende di **prenotare un taxi** per il trasporto dei dipendenti o ospiti da e per l'aeroporto. Al momento della prenotazione di un taxi, la società ABC specifica il **nome del dipendente che dovrebbe essere prelevato** dall'aeroporto in modo che l'autista possa confermare l'identità del dipendente al momento del ritiro. In questo caso, il servizio taxi tratta i dati personali del dipendente come parte del proprio servizio offerto alla società ABC, **ma il trattamento in quanto tale non è l'obiettivo del servizio**.

(B) **Il servizi taxi ha progettato la piattaforma** di prenotazione online come parte dello sviluppo **della propria attività commerciale** per fornire servizi di trasporto, **senza alcuna istruzione da parte della Società ABC**. Anche il servizio taxi **determina autonomamente le categorie di dati che raccoglie e per quanto tempo conservarli**. **Il servizio taxi agisce quindi in qualità di titolare a pieno titolo**, fermo restando che il trattamento ha luogo a seguito di una richiesta di servizio da parte della Società ABC.

***

83. L'EDPB osserva che un fornitore di servizi può ancora agire come **responsabile** del trattamento se il trattamento di dati personali non è l'oggetto principale o primario del servizio, a **condizione che il cliente del servizio determini ancora le finalità e i mezzi del trattamento nella pratica**. Quando si considera se affidare o non il trattamento dei dati personali a un particolare fornitore di servizi, **i titolari del trattamento dovrebbero valutare attentamente se il prestatore di servizi in questione consente loro di esercitare un grado sufficiente di titolarità**, tenuto conto della natura, dell'ambito, del contesto e delle finalità del trattamento, nonché dei potenziali rischi per gli interessati.

***

Esempio: call center
L'azienda X **esternalizza il proprio supporto clienti** all'azienda Y che fornisce un **call center** per aiutare I clienti dell'azienda X con le loro domande. Il servizio di assistenza clienti prevede che **l'azienda Y deve avere accesso alle banche dati dei clienti della Società X**. La società Y può accedere ai dati solo per fornire il supporto che la Società X ha richiesto e non può trattare i dati per scopi diversi da quelli stabiliti dalla società X. La **società di call center Y** deve essere vista come un **responsabile del trattamento** dei dati personali e un accordo deve essere concluso tra la società X e Y

Esempio: supporto IT generale
L'azienda Z incarica un fornitore di servizi IT per eseguire il supporto generale sui suoi sistemi IT che includono una grande quantità di dati personali. **L'accesso ai dati personali non è l'oggetto principale del servizio di supporto ma è inevitabile che il fornitore di servizi IT abbia sistematicamente accesso ai dati** personali durante l'esecuzione del servizio. L'azienda Z conclude quindi che il fornitore di servizi IT, essendo una separata società ed essendo inevitabilmente obbligato a trattare dati personali anche se questo non è il principale oggetto del servizio – **è da considerarsi un responsabile**. Un accordo da responsabile è quindi concluso con il fornitore di servizi IT.

Esempio: consulente IT che risolve un bug del software
La società ABC **incarica uno specialista IT di un'altra società per correggere un bug in un software** in uso alla società. Il consulente IT non è responsabile di elaborare i dati personali alla società ABC e **qualsiasi accesso ai dati personali sarà puramente accidentale** e quindi molto limitato nella pratica. ABC conclude quindi che lo

specialista informatico **non è un responsabile** del trattamento (né un titolare a pieno titolo) e che la società ABC adotterà misure appropriate ai sensi dell'art. 32 del GDPR al fine di prevenire che il consulente informatico compia trattamenti di dati personali in modo non autorizzato.

***

84. Come sopra esposto, nulla vieta al responsabile del trattamento di offrire un servizio **preliminarmente definito ma il il titolare deve prendere la decisione finale di approvare attivamente il modo in cui viene effettuato il trattamento**, almeno per quanto riguarda i **mezzi essenziali** del trattamento. Come detto sopra, un responsabile ha un **margine di manovra per quanto riguarda i mezzi non essenziali**, cfr. sopra al punto 2.1.4.

***

Esempio: fornitore di servizi cloud

Un comune ha deciso di utilizzare un fornitore di servizi cloud per la gestione delle informazioni nella sua scuola e servizi educativi. Il servizio cloud fornisce servizi di **messaggistica**, **videoconferenze**, **archiviazione** di documenti, **gestione del calendari**o, elaborazione testi ecc. e **comporterà il trattamento dei dati personali su scolari e insegnanti**. Il fornitore di servizi cloud ha proposto **un servizio standardizzato** che è offerto in tutto il mondo ed è da considerare responsabile del trattamento. **Il comune deve comunque assicurarsi che l'accordo in vigore sia conforme con l'art. 28**, paragrafo 3, del GDPR, e che i dati personali di cui è titolare sono trattati esclusivamente in attuazione dei fini stabiliti dal comune. Deve inoltre **assicurarsi che le sue istruzioni specifiche sui periodi di conservazione, cancellazione dei dati ecc. siano rispettate** dal fornitore di servizi cloud indipendentemente da ciò che viene generalmente offerto nel servizio standardizzato.

***

5 DEFINIZIONE DI TERZO/DESTINATARIO

85. Il regolamento definisce non solo i concetti di titolare e responsabile del trattamento, ma anche i concetti di **destinatario e terzo**. A differenza dei concetti di titolare e responsabile, il regolamento **non prevede obblighi** o responsabilità specifici **per i destinatari e per i terzi**. Questi possono essere concetti relativi nel senso che descrivono una relazione con un titolare del trattamento o un responsabile da un prospettiva specifica, ad es. un titolare del trattamento o un responsabile comunica i dati a un destinatario. Un destinatario di dati personali e una terza parte possono essere considerati contemporaneamente titolari o responsabili del trattamento da altre prospettive. Ad esempio, entità che devono essere viste come destinatari o terze parti da una prospettiva, sono titolari del trattamento di cui determinano le finalità e i mezzi.

Terzo

86. L'art. 4, paragrafo 10, definisce un "***terzo***" una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo **CHE NON SIA**

- l'interessato,
- il titolare,

- il responsabile e le persone che, sotto l'autorità diretta del titolare o del responsabile, sono autorizzate al trattamento dei dati personali.

87. La definizione corrisponde generalmente alla precedente definizione di "terzo" nella direttiva 95/46/CE.

88. Premesso che i termini "dati personali", "interessato", "titolare" e "responsabile" sono definiti nel Regolamento, la nozione di "persone che, sotto l'autorità diretta del titolare o del responsabile, sono autorizzate al trattamento dei dati personali" non lo è. È, tuttavia, generalmente inteso come riferito a persone che appartengono alla persona giuridica del titolare del trattamento o del responsabile (un dipendente o un ruolo altamente comparabile a quella dei dipendenti, ad es. personale interinale fornito tramite un'agenzia di lavoro interinale) ma solo nella misura in cui ed in quanto autorizzati al trattamento dei dati personali. **Un dipendente ecc. che accede ai dati senza autorizzazione o per scopi diversi da quello del datore di lavoro non rientra in tale categoria. Invece**, tale dipendente **dovrebbe essere considerato come una terza parte nei confronti del trattamento espletato** dal datore di lavoro.

Nella misura in cui **il dipendente tratta i dati personali per proprio conto e per fini distinti da quelli del suo datore di lavoro, sarà quindi considerato un titolare** del trattamento e dovrà assumersi tutte le conseguenze e le responsabilità che ne derivano in termini di trattamento dei dati personali.

89. Un terzo si riferisce quindi a qualcuno che, nella specifica situazione in esame, non è un interessato, un titolare, un responsabile del trattamento o un dipendente. Ad esempio, il titolare del trattamento può incaricare un responsabile di trasferire dati personali a terzi. Questa terza parte sarà quindi considerata di diritto un titolare del trattamento per il trattamento che effettua per le proprie finalità. Va evidenziato che, **all'interno di un gruppo di società, una società diversa dal titolare o dal responsabile del trattamento è una terza parte, anche se appartiene allo stesso gruppo** della società che agisce in qualità di titolare o responsabile.

Esempio: servizi di pulizia
L'impresa A stipula un contratto con un'impresa di servizi di pulizia per la **pulizia dei propri uffici**. Gli addetti alle pulizie non dovrebbero accedere o trattare in altro modo i dati personali. Anche se di tanto in tanto potrebbero venire "in potenziale contatto" con dei dati quando si spostano in ufficio, possono svolgere il loro compito senza accedere a tali dati ed è contrattualmente vietato accedere o trattare in altro modo i dati personali che la Società A mantiene come titolare. Gli addetti alle pulizie non sono dipendenti della società A né sono visti come sotto l'autorità diretta di tale società. **Non vi è alcuna intenzione di coinvolgere l'impresa di servizi di pulizia o i suoi dipendenti a trattare i dati personali per conto della Società A**. **L'impresa di pulizie e i suoi dipendenti sono quindi da considerare come una terza parte** e il titolare del trattamento deve assicurarsi che vi siano **adeguate misure di sicurezza per impedire l'accesso** ai dati e prescriverne la riservatezza dovere nel caso in cui dovessero imbattersi

accidentalmente in dati personali.

Esempio: gruppi di società – società madre e figlie
Le società X e Y fanno parte del Gruppo Z. Le società X e Y elaborano entrambe i dati sui loro rispettivi dipendenti ai fini della gestione dei dipendenti. Ad un certo punto, **la casa madre ZZ decide di richiedere i dati dei dipendenti a tutte le filiali al fine di produrre statistiche a livello di gruppo**. Quando vengono trasferiti dati dalle società X e Y a ZZ, quest'ultima è da considerarsi comunque **una terza parte** anche se tutte le società fanno parte dello stesso gruppo. La società **ZZ sarà considerata titolare del trattamento** per il suo trattamento dei dati a fini statistici.

***

Destinatario

90. L'art. 4, par. 9, definisce un "***destinatario***" come una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo, **a cui i dati personali sono comunicati,** siano essi soggetti terzi o meno.

Le autorità pubbliche non sono comunque considerate destinatari quando ricevono dati personali nell'ambito di una particolare **richiesta conformemente al diritto dell'Unione o degli Stati membri** (ad es. autorità fiscali e doganali, indagini finanziarie unità ecc.).

91. La definizione corrisponde generalmente alla precedente definizione di "destinatario" nella direttiva 95/46/CE.

92. La definizione riguarda chiunque riceva dati personali, siano essi terzi o meno. Ad esempio, quando un titolare del trattamento invia dati personali a un'altra entità (un responsabile del trattamento o ad una terza parte), questa entità è un destinatario. Un **destinatario terzo è considerato titolare del trattamento di qualsiasi trattamento che esegue per i propri scopi dopo aver ricevuto i dati**.

***

Esempio: Divulgazione di dati tra aziende
L'agenzia di viaggi **ExploreMore** organizza viaggi su richiesta dei propri clienti individuali. All'interno di questo servizio, **essa invia i dati personali dei clienti a compagnie aeree, hotel e organizzazioni di escursioni in modo da consentire loro di svolgere i rispettivi servizi**. ExploreMore, gli hotel, le compagnie aeree e i fornitori di escursioni **devono essere considerati ciascuno come titolare del trattamento** che effettua all'interno della propria offerta dei rispettivi servizi. Non esiste alcuna relazione titolare/responsabile. Tuttavia, le compagnie aeree, gli hotel e i fornitori di escursioni devono essere considerati destinatari quando ricevono i dati personali da ExploreMore.

***

PARTE II – CONSEGUENZE DELL'ATTRIBUZIONE DI RUOLI DIVERSI

1 RAPPORTO TRA TITOLARE E RESPONSABILE

93. Una nuova caratteristica distintiva del GDPR sono le disposizioni che impongono obblighi direttamente ai responsabili del trattamento.
Ad esempio, un responsabile del trattamento deve garantire che le persone autorizzate al trattamento dei dati personali abbiano o si siano impegnate alla riservatezza (art. 28, paragrafo 3); un responsabile deve mantenere un registro di tutte le categorie di attività di trattamento (art. 30, paragrafo 2) e deve attuare adeguate procedure tecniche e misure organizzative (art. 32). Un responsabile del trattamento deve inoltre designare un responsabile della protezione dei dati a determinate condizioni (art. 37) e ha il dovere di informare il titolare del trattamento senza indebito ritardo dopo essere venuto a conoscenza di una violazione dei dati personali (art. 33, paragrafo 2). Inoltre, le norme sui trasferimenti di dati verso i paesi terzi (Capitolo V) si applicano sia ai titolari del trattamento che ai responsabili del trattamento. A questo proposito, l'EDPB ritiene che l'art. 28, par. 3, del GDPR, pur imponendo un contenuto specifico per il contratto necessario tra titolare e responsabile del trattamento, impone obblighi diretti ai responsabili del trattamento, compreso l'obbligo di assistere il titolare del trattamento nell'assicurare la conformità.

1.1 Scelta del responsabile

94. Il **titolare del trattamento ha il dovere di utilizzare** "*solo* ***responsabili del trattamento che forniscano garanzie sufficienti*** *per attuare adeguate misure tecniche e organizzative*", in modo che il trattamento soddisfi i requisiti del GDPR - anche per la sicurezza del trattamento - e garantisca la tutela dei diritti degli interessati. **Spetta, pertanto, al titolare del trattamento valutare l'adeguatezza delle garanzie fornite dal responsabile** e dovrebbe essere in grado di dimostrare di aver preso in seria considerazione tutte le prescrizioni del GDPR.

95. Le garanzie "prestate" dal responsabile sono quelle che il responsabile è in grado di dimostrare che soddisfino il titolare del trattamento, in quanto sono gli unici che possono essere effettivamente presi in considerazione dal titolare del trattamento nel valutare il rispetto dei suoi obblighi. Spesso questo **richiederà uno scambio della documentazione pertinente** (es. *privacy policy,* termini di servizio, registro delle attività di trattamento, registri della politica di gestione e della politica di sicurezza delle informazioni, rapporti di *audit* esterni sulla protezione dei dati, riconosciute certificazioni internazionali, come la ISO 27000).

96. La valutazione da parte del titolare del trattamento se **le garanzie sono sufficienti** è **una forma di valutazione del rischio**, che dipenderà molto dal tipo di trattamento affidato al responsabile e che deve essere effettuato **caso per caso**, tenendo conto della natura, dell'ambito, del contesto e delle finalità del trattamento nonché dei rischi per i diritti e le libertà delle persone fisiche. Di conseguenza, l'EDPB non può fornire un elenco esaustivo dei documenti o delle azioni che il responsabile del trattamento deve mostrare e/o dimostrare in un dato scenario, poiché ciò dipende in gran parte dalle circostanze specifiche del trattamento.

97. I seguenti elementi dovrebbero essere presi in considerazione dal titolare del trattamento al fine di valutare la sufficienza delle garanzie: la conoscenza e **l'esperienza** del responsabile (es. **competenza tecnica** in materia di misure di sicurezza e violazioni dei dati); l'affidabilità del responsabile; le **risorse** del responsabile. Anche la **reputazione** del responsabile del trattamento sul mercato può essere un fattore rilevante da considerare per i titolari del trattamento.

98. Inoltre può essere utilizzata l'adesione a un **codice di condotta** approvato o a un **meccanismo di certificazione** come un elemento attraverso il quale possono essere dimostrate garanzie sufficienti. I responsabili del trattamento sono quindi spronati ad informare il titolare del trattamento di tale circostanza, nonché di ogni variazione di tale adesione.

99. L'obbligo di utilizzare solo responsabili del trattamento "che forniscano garanzie sufficienti" contenuto nell'art. 28, par. 1, GDPR è un obbligo continuativo. Non termina nel momento in cui concludono il titolare e il responsabile un contratto o altro atto giuridico. Piuttosto, il titolare del trattamento dovrebbe, **a intervalli appropriati, verificare** le garanzie del responsabile del trattamento, anche attraverso audit e ispezioni ove appropriato.

1.2 Forma del contratto o altro atto giuridico

100. Ogni trattamento di dati personali da parte di un responsabile del trattamento deve essere disciplinato da un contratto o altro atto giuridico ai sensi del diritto dell'UE o dello Stato membro che deve intercorrere tra il titolare e il responsabile del trattamento, come previsto dall'art. 28, par. 3, del GDPR.

101. Tale atto giuridico deve essere in **forma scritta**, **anche** in forma **elettronica**. Pertanto, accordi non scritti (indipendentemente da quanto approfonditi o efficaci siano) non possono essere considerati sufficienti per soddisfare i requisiti previsti dall'art. 28 GDPR. Per evitare qualsiasi difficoltà nel dimostrare che il contratto o altro atto giuridico sia effettivamente in vigore, l'EDPB raccomanda di garantire che l**e firme necessarie siano incluse** nell'atto giuridico, in linea con la legge applicabile (ad es. diritto contrattuale).

102. Inoltre, il contratto o altro atto giuridico ai sensi del diritto dell'Unione o degli Stati membri deve essere vincolante per il responsabile del trattamento rispetto al titolare del trattamento, ovvero **deve stabilire obblighi a carico del responsabile che sono vincolanti ai sensi del diritto dell'UE o degli Stati membri**. Inoltre deve stabilire gli obblighi del titolare.
Nella maggior parte dei casi, ci sarà un contratto, ma il Regolamento fa riferimento anche ad "***altro atto giuridico***", **come una legge nazionale** (primaria o secondaria) o **altro strumento giuridico**. Se l'atto giuridico non include tutto il contenuto minimo richiesto, deve essere integrato con un contratto o altro atto giuridico che include gli elementi mancanti.

103. Poiché il regolamento stabilisce un chiaro obbligo di stipulare un contratto scritto, laddove nessun altro atto giuridico pertinente sia in vigore, la sua assenza costituisce una violazione del GDPR. Sia il titolare del trattamento che il responsabile sono responsabili dell'esistenza di un contratto o di un altro atto

giuridico che regoli il trattamento. Fatto salvo quanto previsto dall'art. 83 del GDPR, l'autorità di controllo competente potrà irrogare una sanzione amministrativa sia al titolare che al responsabile, tenendo conto di conto delle circostanze di ogni singolo caso. Contratti che sono stati stipulati prima della data di applicazione del GDPR avrebbero dovuto essere aggiornati alla luce dell'art. 28, paragrafo 3. L'assenza di tale aggiornamento, al fine di allineare un contratto preesistente ai requisiti del GDPR, costituisce violazione dell'art. 28, par. 3.

Un contratto scritto ai sensi dell'art. 28, par, 3, del GDPR **può essere incorporato in un contratto più ampio**, come un accordo sul livello di servizio. Al fine di facilitare la dimostrazione della conformità al GDPR, l'EDPB raccomanda che gli elementi del contratto finalizzati a dare attuazione all'art. 28 GDPR siano chiaramente identificati come tali in una determinata parte del più ampio contratto (ad esempio in un allegato).

104. Al fine di adempiere **all'obbligo di stipulare un contratto, il titolare e il responsabile del trattamento possono scegliere di negoziare il proprio contratto comprensivo di tutti gli elementi obbligatori o affidarsi, in tutto o in parte, alle clausole contrattuali tipo in relazione agli obblighi di cui all'art. 28** ([2]).

105. Una serie di clausole contrattuali tipo (SCC) può essere, in alternativa, adottata dalla Commissione o adottata da un'autorità di controllo, conformemente al meccanismo di coerenza. Tali clausole potrebbero far parte di una certificazione rilasciata al titolare del trattamento o responsabile ai sensi degli articoli 42 o 43.

106. L'EDPB **desidera chiarire che non vi è alcun obbligo per i titolari e i responsabili del trattamento di stipulare un contratto basato su SCC**, né ciò è da preferire necessariamente alla negoziazione di un contratto individuale. Entrambe le opzioni sono praticabili ai fini del rispetto della normativa sulla

2 La **presenza (o l'assenza) di un accordo scritto, tuttavia, non è determinante per l'esistenza di un responsabile del trattamento**. Laddove vi sia motivo di ritenere che il contratto non corrisponda alla realtà in termini di controllo effettivo, sulla base di un'analisi fattuale delle circostanze del rapporto tra le parti e al trattamento dei dati personali in corso, il contratto può essere revocato. **Viceversa, un rapporto titolare-responsabile del trattamento potrebbe essere ritenuto sussistente anche in assenza di un accordo scritto**. Ciò, tuttavia, implicherebbe una violazione dell'art. 28, paragrafo 3, del GDPR. Inoltre, in determinate circostanze, l'assenza di una chiara definizione del rapporto tra titolare e responsabile del trattamento può sollevare il problema della mancanza di base giuridica su cui dovrebbe basarsi ogni trattamento, ad es. nei casi di comunicazione dei dati tra titolare e presunto responsabile.
L'art. 28, paragrafo 3, non è applicabile solo ai responsabili del trattamento. Nel caso in cui solo il responsabile del trattamento sia soggetto all'ambito territoriale del GDPR, l'obbligo sarà direttamente applicabile solo al responsabile del trattamento (cfr. anche EDPB Linee guida 3/2018 sull'ambito territoriale del GDPR, p. 12. 44 art. 28, paragrafo 6, GDPR). L'EDPB ricorda che le clausole contrattuali standard ai fini del rispetto dell'art. 28 del GDPR non coincidono con le clausole contrattuali standard di cui all'art. 46, paragrafo 2. Mentre il primo precisa e chiarisce ulteriormente come saranno soddisfatte le disposizioni dell'art. 28, paragrafi 3 e 4, quest'ultimo prevede garanzie adeguate in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale in l'assenza di una decisione di adeguatezza ai sensi dell'art. 45, paragrafo 3.

protezione dei dati, a seconda delle circostanze specifiche, purché soddisfino i requisiti dell'art. 28, par. 3.

107. Se le parti desiderano avvalersi di clausole contrattuali tipo, le clausole di protezione dei dati dei loro accordi devono essere le stesse di quelle delle SCC. Le SCC lasceranno spesso degli spazi vuoti da compilare o opzioni da selezionare dalle parti. Inoltre, come anche accennato in precedenza, le SCC saranno generalmente incorporate in un accordo più ampio che descriva l'oggetto del contratto, la sue condizioni finanziarie e le altre clausole pattuite: sarà possibile per le parti aggiungere clausole ulteriori (es. legge applicabile e giurisdizione) purché non contraddicano, direttamente o indirettamente, le SCC e non pregiudichino la protezione offerta dal GDPR e dalla protezione dei dati dell'UE o dalle leggi degli Stati membri.

108. I contratti tra titolari e responsabili del trattamento possono talvolta essere redatti unilateralmente da uno di essi. Il potere della parte o parti che redigono il contratto può dipendere da diversi fattori, tra cui: i) la posizione della parte nel mercato e il potere contrattuale, ii) la competenza tecnica, nonché iii) l'accesso a servizi legali. Ad esempio, alcuni fornitori di servizi tendono a stabilire termini e condizioni standard, che includono accordi per il trattamento dei dati.

109. **Un accordo** tra il titolare del trattamento e il responsabile del trattamento **deve soddisfare i requisiti dell'art. 28 GDPR al fine di garantire che il responsabile del trattamento tratti i dati personali in conformità con il GDPR**. Qualunque accordo dovrebbe tenere conto delle responsabilità specifiche dei titolari e dei responsabili del trattamento.
Sebbene l'art. 28 fornisca un elenco di punti che devono essere affrontati in qualsiasi contratto che disciplina il rapporto tra titolari e responsabili, esso lascia spazio a trattative tra le parti rispetto a tali contratti. In alcune situazioni un titolare o un responsabile può avere un potere di negoziazione più debole per personalizzare l'accordo sulla protezione dei dati. **L'affidarsi alle clausole contrattuali standard adottate ai sensi dell'art. 28 (commi 7 e 8) può contribuire al riequilibrio** delle posizioni negoziali e per garantire che i contratti rispettino il GDPR.

110. Il fatto che il contratto e le sue condizioni dettagliate siano predisposte dal prestatore di servizi piuttosto che dal titolare del trattamento non è di per sé problematico e non costituisce un fattore sufficiente per concludere che il fornitore di servizi debba essere considerato un titolare del trattamento. Inoltre, lo **squilibrio nel potere contrattuale di un piccolo titolare** del trattamento rispetto ai grandi fornitori di servizi non dovrebbe essere considerato come una **giustificazione dell'accettazione da parte del titolare di clausole e condizioni contrattuali non conformi** rispetto alla normativa sulla protezione dei dati, né può sollevare il responsabile del trattamento dai suoi obblighi in materia di protezione dei dati. Il titolare deve valutare i termini e nella misura in cui li accetta liberamente e si avvale del servizio, ha inoltre accettato la piena responsabilità del rispetto del GDPR.

Qualsiasi **modifica proposta**, da un responsabile, degli accordi sul trattamento dei dati inclusi nei termini e condizioni standard dovrebbe essere direttamente

notificato e **approvato dal titolare** del trattamento, tenuto conto del margine di manovra che il responsabile del trattamento gode rispetto a elementi non essenziali dei mezzi (paragrafi 40-41 supra). La semplice pubblicazione di tali modifiche sul sito web del responsabile non è conforme all'art. 28.

1.3 Contenuto del contratto o altro atto giuridico

111. Prima di soffermarsi su ciascuno dei requisiti dettagliati previsti dal GDPR in merito al contenuto del contratto o altro atto giuridico, sono necessarie alcune osservazioni generali.

112. Sebbene gli elementi previsti dall'art. 28 del Regolamento ne costituiscano il contenuto essenziale, il contratto dovrebbe essere un modo per il titolare e il responsabile del trattamento di chiarire ulteriormente come, mediante tali elementi fondamentali, sarà implementato il contratto con istruzioni dettagliate.

Pertanto, **il contratto di trattamento non dovrebbe limitarsi a ribadire le disposizioni del GDP**R: piuttosto, **dovrebbe includere più specifiche e concrete informazioni su come saranno soddisfatti i requisiti e quale livello di sicurezza è richiesto per il trattamento dei dati personali oggetto del contratto** di trattamento. Lungi dall'essere un esercizio teorico e pro-forma, la negoziazione e la stipulazione del contratto sono occasione per precisare i dettagli esecutivi in merito al trattamento. Infatti, la "tutela dei diritti e delle libertà degli interessati nonché la responsabilità dei titolari e dei responsabili [...] richiede **una chiara attribuzione della responsabilità**" ai sensi del GDPR.

113. Allo stesso tempo, il contratto dovrebbe tenere conto "**dei compiti e delle responsabilità specifici del responsabile del trattamento nell'ambito del trattamento da effettuarsi e del rischio per i diritti e le libertà dell'interessato**" (cfr. Considerandi 79 e 81 GDPR).

In linea generale, il contratto tra le parti deve essere redatto alla luce della specifica attività di trattamento dei dati. Ad esempio, non è necessario imporre condizioni particolarmente rigorose e procedure nei confronti di un responsabile incaricato di un'attività di trattamento dalla quale sorgono solo minimi rischi: mentre ciascun responsabile del trattamento deve rispettare i requisiti previsti dal Regolamento, le misure e le procedure dovrebbero essere adattate alla situazione specifica. In ogni caso, tutti gli elementi dell'art. 28, par. 3, devono essere disciplinati dal contratto. Allo stesso tempo, **il contratto dovrebbe includere alcuni elementi che possono aiutare il responsabile del trattamento a comprendere i rischi** per i diritti e le libertà dei soggetti i cui dati sono coinvolti dal trattamento: poiché l'attività è svolta per conto del titolare, spesso il titolare del trattamento ha una comprensione più profonda dei rischi che il trattamento comporta dal momento che il titolare è a conoscenza delle circostanze in cui è incorporato il trattamento.

114. Passando **al contenuto richiesto del contratto o di altro atto giuridico, EDPB interpreta l'art. 28, paragrafo 3, in un modo che deve definire**:

- **l'oggetto del trattamento** (che non deve essere generico come, ad esempio, registrazioni di persone in videosorveglianza che entrano ed

escono da una struttura di massima sicurezza). L'oggetto del trattamento è sì un concetto ampio ma deve essere **formulato con sufficienti specifiche** in modo che sia chiaro quale sia l'oggetto principale del trattamento;

- la **durata del trattamento**: l'esatto periodo di tempo, ovvero i criteri utilizzati per determinarlo, dovrebbero essere specificati: ad esempio, si potrebbe fare riferimento alla durata del trattamento di cui all'accordo;
- la **natura del trattamento**: il tipo di operazioni effettuate nell'ambito del trattamento (per esempio: "ripresa", "registrazione", "archiviazione di immagini", ...) e **finalità del trattamento** (per esempio: accertamento di ingresso illegale). Questa descrizione dovrebbe essere il più completa possibile, a seconda della specifica attività di trattamento, in modo da consentire a soggetti esterni (es. autorità) di comprendere il contenuto e i rischi del trattamento affidato al responsabile;
- il **tipo di dati personali**: questo dovrebbe essere specificato nel modo più dettagliato possibile (ad es esempio: immagini video di persone che entrano ed escono dalla struttura). Non sarebbe adeguato limitarsi a specificare che si tratta di "dati personali ai sensi dell'art. 4, paragrafo 1, GDPR" o "particolari" categorie di dati personali di cui all'art. 9". In caso di particolari categorie di dati, il contratto o atto giuridico dovrebbe almeno specificare quali tipi di dati sono coinvolti, ad esempio, "informazioni relative alle cartelle cliniche" o "informazioni sul fatto che l'interessato sia un membro di un sindacato";
- le **categorie di interessati**: anche questo dovrebbe essere indicato in modo specifico (per esempio: "visitatori", "dipendenti", servizi di consegna, ecc.);

52 **La durata del trattamento non è necessariamente equivalente alla durata del contratto** (potrebbero esserci **obblighi legali di una più lunga conservazione dei dati**).
- gli obblighi e i diritti del titolare del trattamento: i diritti del titolare del trattamento sono ulteriormente trattati nelle seguenti sezioni (ad esempio in relazione al **diritto del titolare del trattamento di eseguire ispezioni e audit**). Per quanto riguarda gli obblighi del titolare del trattamento, gli esempi includono **l'obbligo del titolare del trattamento di fornire al responsabile i dati** di cui al contratto, fornire e documentare eventuali **istruzioni** relative al trattamento dei dati da parte del responsabile, per garantire, prima e durante il trattamento, il rispetto degli obblighi previsti dal GDPR da parte di questo, a supervisionare il trattamento, anche conducendo audit e ispezioni con il responsabile del trattamento.

115. Mentre il GDPR elenca elementi che devono sempre essere inclusi nell'accordo, potrebbe essere necessario includerne di ulteriori , anche a seconda del contesto e dei rischi del trattamento in base ad ogni ulteriore requisito applicabile.

1.3.1 Il responsabile del trattamento deve trattare i dati solo su istruzioni documentate del titolare del trattamento (art. 28 (3) (a) GDPR)

116. **La necessità di specificare tale obbligo deriva dal fatto che il responsabile**

tratta dati per conto del titolare. I titolari del trattamento devono fornire ai propri responsabili le istruzioni relative a ciascun trattamento. Tali istruzioni possono includere il trattamento consentito e non consentito dei dati personali, oltre alle procedure dettagliate, alle modalità di protezione dei dati, ecc. **Il responsabile del trattamento non deve andare oltre quanto indicato dal titolare**. È comunque possibile per il responsabile del trattamento suggerisca elementi che, se accettati dal titolare, diventano parte integrante delle istruzioni impartite.

117. Quando un responsabile tratta dati al di fuori o oltre le istruzioni del titolare, e ciò equivale a una decisione che determina le finalità e i mezzi del trattamento, il responsabile violerà i suoi obblighi e sarà anche considerato titolare del trattamento in relazione a tale trattamento in conformità con l'art. 28, paragrafo 10 (cfr. sotto-sezione 1.5 infra 53).

118. Le **istruzioni impartite dal titolare del trattamento devono essere documentate**. Per questi scopi, si consiglia di includere in una procedura **un modello per fornire ulteriori istruzioni in allegato al contratto** o altro atto giuridico. In alternativa, le istruzioni possono essere fornite anche in qualsiasi forma scritta (ad es. **e-mail**) come in **qualsiasi altra forma documentata**, purché sia possibile conservare registrazioni di tali istruzioni. In qualunque caso, per evitare qualsiasi difficoltà nel dimostrare che le istruzioni del titolare sono state debitamente documentate, l'EDPB raccomanda di conservare tali istruzioni insieme al contratto o altro atto giuridico.

119. L'obbligo per il responsabile del trattamento di astenersi da qualsiasi attività di trattamento che non sia basata sulle istruzioni del titolare si applica anche ai trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale. Il **contratto dovrebbe specificare i requisiti per i trasferimenti verso paesi terzi o organizzazioni internazionali**, tenuto conto di quanto previsto dal Capo V del GDPR.

120. **L'EDPB raccomanda che il titolare presti la dovuta attenzione a questo punto specifico, specialmente quando il responsabile delegherà alcune attività di elaborazione ad altri responsabili e quando il responsabile ha divisioni o unità situate in paesi terzi**. Se le istruzioni del titolare non consentono trasferimenti o comunicazioni verso paesi terzi, il responsabile non sarà autorizzato a conferire il trattamento ad un sub-responsabile in un paese terzo, né potrà far trattare i dati in uno dei suoi divisioni extra-UE.

121. Un responsabile del **trattamento può trattare i dati in modo diverso** dalle istruzioni documentate ricevute dal titolare del trattamento **quando il medesimo responsabile del trattamento è tenuto a trattare e/o trasferire dati personali sulla base del diritto dell'UE o dello Stato membro cui è soggetto il responsabile del trattamento**. Questa disposizione rivela ulteriormente l'importanza di un'attenta negoziazione e redazione degli accordi per il trattamento dei dati, come, ad esempio, potrebbe essere necessaria una consulenza legale richiesta da una delle parti circa l'esistenza di tale requisito giuridico. Ciò deve essere fatto in modo tempestivo, in quanto **il responsabile ha l'obbligo di informare il titolare del trattamento di tale requisito prima di iniziare il**

trattamento. **Solo quando la stessa legge (dell'UE o dello Stato membro) vieta al responsabile del trattamento di informare il titolare del trattamento per "gravi motivi di interesse pubblico", non sussiste tale obbligo di informazione**. In in ogni caso, qualsiasi trasferimento o divulgazione può avvenire solo se autorizzata dal diritto dell'Unione, anche in ai sensi dell'art. 48 del GDPR.

1.3.2 Il responsabile del trattamento deve garantire che le persone autorizzate al trattamento dei dati personali abbiano e/o si siano impegnate alla riservatezza o siano soggette ad un'adeguata legge che obblighi alla riservatezza (Art. 28(3)(b) GDPR)

122. Il contratto deve prevedere che il responsabile del trattamento deve garantire che chiunque sia autorizzato al trattamento dei dati personali si **impegna alla riservatezza**. Ciò può avvenire sia (A) **tramite uno specifico contratto**, o (B) per **obblighi di legge** già in essere.

123. Il concetto ampio di "**persone autorizzate al trattamento dei dati personali**" include dipendenti e lavoratori temporanei. In generale, il responsabile dovrebbe rendere disponibili **solo i dati personali ai dipendenti che ne hanno effettivamente bisogno per svolgere compiti** per i quali il responsabile del trattamento è stato incaricato dal titolare.

124. L'impegno o **obbligo di riservatezza deve essere "appropriato"**, cioè deve effettivamente vietare alla persona autorizzata a divulgare informazioni riservate senza autorizzazione e deve essere sufficientemente ampio da comprendere tutti i dati personali trattati per conto del titolare del trattamento come nonché le condizioni alle quali i dati personali sono trattati.

1.3.3 Il responsabile del trattamento deve adottare tutte le misure richieste ai sensi dell'art. 32 (art. 28(3)(c) GDPR)

125. L'art. 32 richiede che il titolare del trattamento e il responsabile del trattamento **mettano in atto adeguate procedure tecniche e misure di sicurezza organizzative**. Sebbene tale obbligo sia già imposto direttamente al responsabile del trattamento le cui operazioni di trattamento rientrano nell'ambito di applicazione del GDPR, il **dovere di adottare tutte le misure necessarie ai sensi dell'art. 32 deve pure trovare riscontro nel contratto** relativo alle attività di trattamento affidato dal titolare del trattamento.

126. Come indicato in precedenza, il contratto di trattamento non dovrebbe limitarsi a ribadire le disposizioni del GDPR. Il **contratto deve includere o fare riferimento a informazioni sulle misure di sicurezza da adottare, e all'obbligo per il responsabile del trattamento di ottenere l'approvazione del titolare prima di apportare modifiche**, e una regolare revisione delle misure di sicurezza al fine di garantirne l'adeguatezza rispetto ai rischi, che possono evolvere nel tempo. **Il grado di dettaglio** delle informazioni relative alle misure di sicurezza da includere in un contratto deve essere **tale da consentire al titolare del trattamento di valutare l'adeguatezza delle misure** ai sensi dell'art. 32, paragrafo 1, del GDPR. Inoltre, la descrizione è necessaria anche per consentire al titolare del trattamento di adempiere al proprio obbligo di responsabilità ai sensi

dell'art. 5, paragrafo 2, e dell'art. 24 del GDPR per quanto riguarda le misure di sicurezza imposte al responsabile. Un **corrispondente obbligo del responsabile del trattamento di assistere titolare del trattamento e di mettere a disposizione tutte le informazioni necessarie per dimostrare la conformità** può essere dedotto dall'art. 28.3 (f) e (h) GDPR.

127. Il livello delle istruzioni fornite dal titolare al responsabile del trattamento in merito alle misure da implementare dipenderà dalle circostanze specifiche. In alcuni casi, **il titolare può (A) fornire una descrizione chiara e dettagliata delle misure** di sicurezza da attuare. **In altri casi (B), il titolare del trattamento può descrivere gli obiettivi minimi di sicurezza** da raggiungere, richiedendo al contempo responsabile di proporre l'attuazione di specifiche misure di sicurezza. In ogni caso, **il titolare del trattamento deve fornire al responsabile del trattamento una descrizione delle attività di trattamento e degli obiettivi di sicurezza** (in base alla valutazione dei rischi del titolare), nonché **approvare** le misure proposte dal responsabile. Questo potrebbe essere incluso in un allegato al contratto. **Il titolare esercita il proprio potere decisionale sulle caratteristiche principali delle misure di sicurezza, sia elencandole esplicitamente sia approvando quelle proposte** dal responsabile.

1.3.4 Il responsabile del trattamento deve rispettare le condizioni di cui all'art. 28, par. 2, e all'art. 28, par. 4, per l'indicazione di un ulteriore responsabile o sub-responsabile (art. 28, par. 3, lettera d) GDPR).

128. L'accordo deve specificare che il responsabile del trattamento non può incaricare un altro responsabile senza la **previa autorizzazione scritta del titolare** che sarà specifica o generale. In caso di autorizzazione **generale**, il responsabile del trattamento deve **informare il titolare** del trattamento di qualsiasi cambiamento di sub-responsabili previa autorizzazione scritta e dare al titolare la possibilità di opporsi. Si raccomanda che **il contratto ne preveda la procedura**. Va notato che il responsabile ha l'obbligo di informare il titolare di qualsiasi cambiamento di sub-responsabili indicando o segnalando attivamente tali cambiamenti nei confronti del titolare del trattamento. Inoltre, ove sia richiesta una **specifica autorizzazione**, il contratto dovrebbe definire la procedura per ottenere tale autorizzazione.

129. **Quando il responsabile incarica un altro responsabile, deve essere stipulato un contratto tra loro**, imponendo **gli stessi obblighi in materia di protezione dei dati di quelli imposti al responsabile del trattamento originario o a questi obblighi devono essere imposti da un altro atto giuridico** ai sensi del diritto dell'Unione o dello Stato membro (cfr. anche di seguito paragrafo 160). Ciò **include l'obbligo di cui all'art. 28, par. 3, lettera h), di consentire e contribuire agli audit dal titolare del trattamento o da un altro revisore incaricato dal titolare del trattamento**.

Il responsabile del trattamento è responsabile nei confronti del titolare del trattamento per l'adempimento degli obblighi di protezione dei dati da parte degli altri responsabili (per ulteriori dettagli su il contenuto raccomandato dell'accordo si veda la successiva sottosezione 1.6 56). Al riguardo non è ad es. sufficiente che il responsabile del trattamento fornisca al titolare del trattamento **un accesso**

generalizzato ad un elenco dei sub-responsabili che potrà essere aggiornato di volta in volta, senza indicare ogni nuovo sub-responsabile previsto. In altre parole, il responsabile del trattamento deve informare attivamente il titolare del trattamento di qualsiasi modifica dell'elenco (ossia, in particolare, di ogni nuovo sub-responsabile previsto). [Cfr. anche parere EDPB 14/2019 sulla bozza di clausole contrattuali standard presentata dalla DK SA (art. 28(8) GDPR), 9 luglio 2019, al paragrafo 44. Cfr. Parte II, sottosezione 1.6 ("Sub-responsabili")].

1.3.5 Il responsabile del trattamento deve assistere il titolare del trattamento per l'adempimento del suo obbligo di risposta alle richieste di esercizio dei diritti dell'interessato (art. 28, comma 3, lett. e) GDPR).

130. Pur garantendo che le richieste dei responsabili siano evase **spetta al titolare del trattamento, fare in modo che il contratto preveda che il responsabile del trattamento abbia l'obbligo di prestare assistenza "mediante mezzi tecnici adeguati e misure organizzative, per quanto possibile**". La natura di questa assistenza può variare notevolmente "tenendo conto della natura del trattamento" e in funzione del tipo di attività affidata al responsabile. I dettagli relativi all'assistenza che deve essere fornita dal responsabile del trattamento dovrebbero essere inclusi nel contratto o in un allegato allo stesso.

131. Mentre l'assistenza può consistere semplicemente nell'inoltro tempestivo di qualsiasi richiesta ricevuta e/o abilitante al titolare del trattamento per estrarre e gestire direttamente i dati personali rilevanti, **in alcune circostanze al responsabile saranno affidati compiti tecnici più specifici, soprattutto quando si trova nella posizione di estrarre e gestire dei dati personali**.

132. È fondamentale tenere presente che, sebbene la gestione pratica delle singole richieste possa essere affidata in *outsourcing* al responsabile, il titolare ha la responsabilità di ottemperare a tali richieste. Pertanto, la valutazione **dell'ammissibilità delle richieste degli interessati** e/o in base ai requisiti stabiliti dal GDPR e da soddisfarsi dovrebbero essere **eseguiti dal titolare** del trattamento, caso per caso base o mediante chiare istruzioni fornite al responsabile nel contratto prima dell'inizio del in lavorazione. Inoltre, i termini di cui al capo III non possono essere prorogati dal titolare del trattamento sulla base del fatto che le informazioni necessarie devono essere fornite dal responsabile del trattamento.

1.3.6 Il responsabile deve assistere il titolare nel garantire il rispetto degli obblighi ai sensi degli Articoli da 32 a 36 (Art. 28(3)(f) GDPR).

133. È necessario che il contratto eviti di limitarsi a ribadire questi doveri di assistenza: **l'accordo dovrebbe contenere dettagli su come viene chiesto al responsabile del trattamento di aiutare il titolare** del trattamento a soddisfare i requisiti e gli elencati obblighi. Ad esempio, procedure e modelli di moduli possono essere aggiunti negli allegati all'accordo, consentendo al responsabile del trattamento di fornire al titolare tutte le informazioni necessarie.

134. Il tipo e il grado di assistenza che deve essere fornito dal responsabile del

trattamento possono variare ampiamente "tenendo conto" conto della natura del trattamento e delle informazioni a disposizione del responsabile". Il titolare deve informare adeguatamente il responsabile del trattamento in merito al rischio connesso al trattamento e a qualsiasi altra circostanza che possa aiutare il responsabile del trattamento ad adempiere al proprio dovere.

135. Passando agli obblighi specifici, **il responsabile ha, in primo luogo, il dovere di assistere il titolare nell'adempimento dell'obbligo di adottare misure tecniche e organizzative adeguate** per garantire la sicurezza di elaborazione. Sebbene ciò possa sovrapporsi, in una certa misura, al requisito che il responsabile stesso adotta adeguate misure di sicurezza, laddove i trattamenti del responsabile rientrino nell'ambito di applicazione del GDPR, restano due obblighi distinti, poiché uno si riferisce al responsabile e l'altro si riferisce al titolare.

136. In secondo luogo, **il responsabile del trattamento deve assistere il titolare del trattamento nell'adempimento dell'obbligo di comunicazione delle violazioni** dei dati personali all'autorità di controllo e agli interessati. Il responsabile deve informare il titolare ogni volta che scopre una violazione dei dati personali che interessa le strutture del medesimo responsabile o di un sub-responsabile / sistemi informatici e aiutano il titolare del trattamento a ottenere le informazioni che devono essere indicate nella relazione all'autorità di controllo.

Il GDPR richiede che il titolare del trattamento notifichi una violazione senza indebito ritardo al fine di ridurre al minimo il danno per gli individui e massimizzare la possibilità di affrontare la violazione in maniera adeguata. Pertanto, dovrebbe avvenire anche la comunicazione del responsabile al titolare del trattamento senza indebito ritardo. A seconda delle caratteristiche specifiche del trattamento affidato al responsabile, può essere **opportuno che le parti includano nel contratto un periodo di tempo specifico** (ad es. numero di ore) entro il quale il responsabile deve informare il titolare del trattamento, nonché il punto di contatto per tali comunicazioni, la modalità e il contenuto minimo previsti dal titolare del trattamento. L'accordo tra il titolare e il responsabile del trattamento **può includere anche un'autorizzazione e l'obbligo per il responsabile del trattamento di notificare direttamente** una violazione dei dati ai sensi degli articoli 33 e 34, ma la responsabilità legale della notifica resta al titolare del trattamento. Se il responsabile del trattamento notifica direttamente una violazione dei dati all'autorità di controllo e informa gli interessati in conformità con Artt. 33 e 34, **deve altresì informare il titolare** del trattamento e fornirgli copia della comunicazione e dell'informativa agli interessati.

137. Inoltre, il responsabile deve anche assistere il titolare del trattamento nell'esecuzione della valutazione d'impatto sulla protezione dei dati quando richiesto, e rispetto alla consultazione con l'autorità di controllo quando l'esito rivela che esiste un rischio elevato che non può essere mitigato.

138. Il dovere di assistenza non consiste in uno spostamento di responsabilità, poiché tali obblighi sono imposti al titolare. Ad esempio, sebbene la valutazione d'impatto sulla protezione dei dati può in pratica essere effettuata da un responsabile, il titolare resta responsabile dell'obbligo di effettuarla e il responsabile è tenuto solo ad assistere il titolare "ove necessario e su richiesta".

Come conseguenza è il titolare del trattamento colui che deve prendere l'iniziativa per eseguire l'impatto sulla protezione dei dati valutazione, non il responsabile.

1.3.7 Al termine delle attività di trattamento, il responsabile deve, a scelta del titolare, cancellare o restituire tutti i dati personali al titolare e cancellare le copie esistenti (Art. 28(3)(g) GDPR)

139. I termini contrattuali hanno lo scopo di garantire che i dati personali siano soggetti a un'adeguata tutela dopo il termine della "prestazione dei servizi connessi al trattamento": spetta quindi al titolare del trattamento decidere cosa dovrebbe fare il responsabile del trattamento in relazione ai dati personali.

140. Il **titolare del trattamento può decidere in via preliminare se i dati personali devono essere cancellati o restituiti** specificandolo nel contratto, mediante comunicazione scritta da inviare tempestivamente al responsabile. Il contratto o altro atto giuridico dovrebbe riflettere la possibilità per il titolare del trattamento di modificare la scelta effettuate prima del termine della prestazione dei servizi connessi al trattamento. Il contratto dovrebbe specificare il processo per fornire tali istruzioni.

141. Se il titolare del trattamento sceglie che i dati personali siano cancellati, il responsabile dovrebbe garantire che la cancellazione avvenga in modo sicuro, anche al fine di ottemperare all'art. 32 GDPR. Il responsabile dovrebbe confermare al titolare del trattamento che la cancellazione è stata completata entro un lasso di tempo concordato e in maniera concordata.

142. Il **responsabile del trattamento deve cancellare tutte le copie esistenti dei dati, a meno che il diritto dell'UE o dello Stato membro non richieda ulteriore stoccaggio**. Se il titolare o il responsabile del trattamento è a conoscenza di tali requisiti legali, dovrebbe informare l'altra parte il prima possibile.

1.3.8 Il responsabile deve mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 e consentire e contribuire agli audit, comprese le ispezioni, condotte dal titolare o da altro revisore incaricato dal titolare del trattamento (art. 28(3)(h) GDPR).

143. Il contratto deve includere dettagli su quanto spesso e come il flusso di informazioni tra il responsabile del trattamento e il titolare del trattamento dovrebbe avvenire in modo che il titolare del trattamento sia pienamente informato sui dettagli del trattamenti rilevanti per dimostrare il rispetto degli obblighi di cui all'art. 28 RGPD. Ad esempio, le parti pertinenti dei registri delle attività di trattamento del responsabile del trattamento possono essere condivise con il titolare. Il **responsabile del trattamento dovrebbe fornire tutte le informazioni su come l'attività di elaborazione sarà effettuata per conto del titolare del trattamento**. Tali informazioni dovrebbero includere informazioni sul funzionamento dei **sistemi** utilizzati, sulle **misure di sicurezz**a, sulle modalità di adempimento degli obblighi di conservazione dei dati, sull'**ubicazione** dei dati, **trasferimenti d**i dati, **chi ha accesso** ai dati e **chi sono i destinatari** dei dati, i sub-responsabili del trattamento usato, ecc.

144. Nel contratto devono essere stabiliti anche ulteriori dettagli circa la capacità di eseguire e il dovere di contribuire **a ispezioni e verifiche da parte del titolare** del trattamento o di un altro revisore incaricato dal titolare del trattamento. Il GDPR specifica che le ispezioni e gli audit sono effettuati dal titolare del trattamento o da una terza parte mandata dal titolare. L'obiettivo di tale audit è di garantire che il titolare abbia tutte le informazioni in ordine all'attività di trattamento svolta per suo conto e alle garanzie prestate dal responsabile. Il **responsabile del trattamento può suggerire** la scelta di un revisore specifico, ma **la decisione finale deve essere lasciata al titolare** del trattamento ai sensi dell'art. 28, paragrafo 3, lettera h), del GDPR. Inoltre, anche se l'ispezione è eseguita da un revisore proposto dal responsabile del trattamento, il titolare del trattamento conserva il diritto di contestare la portata, la metodologia e i risultati dell'ispezione.65
Le parti dovrebbero **cooperare in buona fede** e valutare se e quando vi sia la necessità di eseguire audit presso la sede del responsabile, nonché quale tipo di audit o ispezione (remoto / in loco /altro modo per raccogliere le informazioni necessarie) sarebbe necessario e appropriato eseguire nel caso specifico tenendo conto anche dei problemi di sicurezza; la scelta finale su questo spetta al titolare.

A seguito dei risultati dell'ispezione, il titolare del trattamento dovrebbe essere in grado di chiedere al responsabile del trattamento di prendere misure successive, ad es. per porre rimedio alle carenze e alle lacune individuate. Allo stesso modo, dovrebbero essere stabilite specifiche procedure relative all'ispezione da parte del responsabile e del titolare del trattamento nei riguardi dei sub-responsabili (vedi sotto-sezione 1.6 di seguito67).

145. **La questione della ripartizione dei costi tra un titolare e un responsabile in materia di audit non è trattata dal GDPR** ed è soggetto a considerazioni commerciali. Tuttavia, l'art. 28, paragrafo 3, lettera h), richiede che il contratto includa l'obbligo per il responsabile del trattamento di mettere a disposizione tutte le informazioni necessarie al titolare del trattamento e l'obbligo di consentire e contribuire agli audit, comprese le ispezioni, condotta dal titolare del trattamento o da un altro revisore incaricato dal titolare del trattamento. **Ciò significa in pratica che le parti non devono inserire nel contratto clausole che prevedano il pagamento di costi o compensi che sarebbero manifestamente sproporzionati** o eccessivi, con conseguente effetto dissuasivo su una delle parti. Tali clausole implicherebbero infatti che i diritti e gli obblighi di cui all'art. 28, paragrafo 3, lettera h), non sarebbero mai esercitati in pratica e diventerebbero puramente teorici mentre formano parte integrante delle tutele di protezione dei dati previste dall'art. 28 GDPR.

1.4 Istruzioni che violano la legge sulla protezione dei dati

146. Ai sensi dell'art. 28, par. 3, **il responsabile del trattamento deve informare immediatamente il titolare del trattamento se, a suo avviso, l'istruzione viola il GDPR o altre disposizioni sulla protezione dei dati dell'Unione o degli Stati membri.**

147. Infatti, **il responsabile** ha il dovere di rispettare le istruzioni del titolare, ma

ha anche un generale obbligo di rispettare la legge. Un'istruzione che violi la legge sulla protezione dei dati causerebbe un conflitto tra i due suddetti obblighi.

148. Una volta informato che una delle sue istruzioni potrebbe violare la legge sulla protezione dei dati, il titolare del trattamento sarà tenuto a valutare la situazione e determinare se l'istruzione effettivamente viola la protezione dei dati legge.

149. L'EDPB raccomanda alle parti di negoziare e concordare nel contratto le conseguenze di una notifica effettuata dal responsabile al titolare circa una istruzione in violazione della legge imputabile al titolare e che cosa succede in caso di inerzia da parte del titolare del trattamento in tale contesto. **Un esempio potrebbe essere quello di inserire una clausola sulla risoluzione del contratto se il titolare del trattamento persiste con un'istruzione illecita**. Un altro esempio potrebbe essere una clausola sulla possibilità per il responsabile del trattamento di sospendere l'attuazione dell'istruzione interessata fino a quando il titolare conferma, modifica o revoca la sua istruzione (cfr Cfr. parere congiunto EDPB-GEPD 1/2021 sulle clausole contrattuali tipo tra titolari e responsabili del trattamento, paragrafo 39).

1.5 Responsabile che determina finalità e modalità del trattamento

150. Se il responsabile viola il Regolamento determinando le finalità e i mezzi del trattamento, deve essere considerato titolare del trattamento in relazione a tale trattamento (art. 28, paragrafo 10, GDPR).

1.6 Sub-responsabili

151. Le attività di trattamento dei dati sono spesso svolte da un gran numero di attori e le catene di sub-trattamento stanno diventando sempre più complesse. Il GDPR introduce obblighi specifici da rispettare quando un (sub)responsabile intende coinvolgere un altro attore, aggiungendo così un altro collegamento alla catena, affidandole attività che richiedono il trattamento di dati personali. L'analisi di se il prestatore di servizi agisce in qualità di sub-responsabile dovrebbe essere svolta in linea con quanto sopra descritto sulla nozione di responsabile del trattamento (cfr. supra, paragrafo 83).

152. **Sebbene la catena possa essere piuttosto lunga, il titolare mantiene il suo ruolo centrale nel determinare lo scopo e i mezzi di trattamento**. L'art. 28, par. 2, del GDPR stabilisce che il responsabile del trattamento non deve coinvolgere un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento (incluso in modulo elettronico). In caso di autorizzazione scritta generale, il responsabile deve **informare** il titolare del trattamento di qualsiasi modifica prevista riguardante l'aggiunta o la sostituzione di altri responsabili, dando così al titolare la possibilità di opporsi a tali modifiche. In entrambi i casi, il responsabile deve ottenere **l'autorizzazione scritta** del titolare del trattamento prima che qualsiasi trattamento di dati personali sia affidato al sub-responsabile.
Al fine di effettuare la valutazione e la decisione se autorizzare il sub-responsabile, o dei sub-responsabili previsti dovrà essere fornita al titolare del trattamento dal

responsabile l'elenco delle garanzie nel caso presenti ed attuate (incluso per ciascuno sub-responsabile: le posizioni e cosa faranno e le prove delle garanzie).

153. La preventiva autorizzazione scritta può essere specifica, ovvero riferita ad uno specifico sub-responsabile per una specifica attività di trattamento e in un momento specifico, ovvero generale. Questo dovrebbe essere specificato nel contratto o altro atto giuridico che ne disciplina il trattamento.

154. Nei casi in cui il titolare del trattamento decida di accettare determinati sub-responsabili al momento della firma del contratto, un elenco di sub-responsabili autorizzati dovrebbe essere incluso nel contratto o in un allegato allo stesso. L'elenco deve poi essere tenuto aggiornato, in accordo con l'autorizzazione generale o specifica rilasciata dal titolare.

155. Se il titolare del trattamento sceglie di concedere la propria autorizzazione specifica, dovrebbe specificare per iscritto quale sub-responsabile e a quale attività di trattamento esso si riferisce. **Qualsiasi modifica successiva dovrà essere ulteriormente autorizzata dal titolare** del trattamento prima che venga messa in atto. Se la richiesta del responsabile per uno specifico sub-responsabile non riceve risposta entro il termine stabilito, l'autorizzazione deve ritenersi negata. Il titolare dovrebbe prendere la sua decisione di concedere o negare l'autorizzazione tenendo conto del suo obbligo di utilizzare responsabile che forniscano "garanzie sufficienti" (cfr. la precedente sottosezione 1.170).

156. In alternativa, il titolare del trattamento può fornire la propria **autorizzazione generale** al ricorso a sub-responsabili (nel contratto, compreso un elenco con tali sub-responsabili in un allegato allo stesso), che dovrebbe essere integrata con **criteri per guidare la scelta del responsabile** (es. garanzie in termini di carattere tecnico e organizzativo misure, conoscenze specialistiche, affidabilità e risorse). In questo scenario, il responsabile deve informare a tempo debito il titolare del trattamento di qualsiasi prevista aggiunta o sostituzione del/i sub-responsabile/i in modo da dare al titolare la possibilità di opporsi.

157. Pertanto, la **principale differenza tra l'autorizzazione specifica e l'autorizzazione generale** sta nel significato dato al silenzio del titolare: **solo nella situazione di autorizzazione generale, la mancata opposizione del titolare entro il termine stabilito può essere interpretata come autorizzazione**.

158. In entrambi gli scenari, il contratto dovrebbe includere dettagli sui tempi per l'approvazione del titolare del trattamento o la sua opposizione e su come le parti intendono comunicare in merito a tale argomento (es. modelli). Tale **lasso di tempo deve essere ragionevole** alla luce del tipo di trattamento, della complessità delle attività affidate al responsabile (e ai sub-responsabili) e al loro rapporto. Inoltre, il contratto dovrebbe includere dettagli sulle fasi pratiche successive alla obiezione del titolare del trattamento (ad esempio specificando il termine entro il quale il titolare e il responsabile del trattamento dovrebbero decidere se interrompere il trattamento).

159. Indipendentemente dai criteri suggeriti dal titolare per la scelta dei fornitori, **il responsabile resta pienamente responsabile nei confronti del titolare per**

l'adempimento degli obblighi dei sub-responsabili (art. 28, par. 4, GDPR). Pertanto, il responsabile del trattamento dovrebbe assicurarsi di proporre sub-responsabili che forniscano garanzie sufficienti.

160. Inoltre, quando un responsabile del trattamento intende avvalersi di un **sub-responsabile** (autorizzato), deve **stipulare una contratto con esso che imponga gli stessi obblighi imposti al primo responsabile** dal titolare del trattamento o gli obblighi devono essere imposti da un altro atto giuridico ai sensi del diritto dell'UE o dello Stato membro.

L'intera **catena delle attività** di trattamento deve essere regolata da accordi scritti. Imponendo gli "stessi" obblighi che vanno interpretati in modo funzionale più che formale: **non è necessario che un contratto includa esattamente le stesse parole già utilizzate tra il titolare e il responsabile del trattamento, ma si dovrebbe garantire che gli obblighi nella sostanza siano gli stessi**. Questo significa anche che se il responsabile affida al sub-responsabile una parte specifica del trattamento, alla quale alcuni degli obblighi non possono applicarsi, tali obblighi non dovrebbero essere inclusi "per default" nel contratto con il sub-responsabile, in quanto ciò genererebbe solo incertezza. Ad esempio, per quanto riguarda l'assistenza con obblighi relativi alla violazione dei dati, notifica di una violazione dei dati da parte di un sub-responsabile direttamente al titolare potrebbe essere fatto se tutti e tre sono d'accordo. Tuttavia, in caso di tale notifica diretta il responsabile deve essere informato e ottenere una copia della notifica.

2 CONSEGUENZE DELLE AZIONI IN CONTITOLARITA'

2.1 Determinare in modo trasparente le rispettive responsabilità dei congiunti titolari del trattamento per il rispetto degli obblighi previsti dal GDPR

161. L'art. 26, par. 1, del GDPR prevede che i contitolari del trattamento **determinino in modo trasparente** e **concordano le rispettive responsabilità** per il rispetto degli obblighi previsti dal regolamento.

162. I contitolari del trattamento devono quindi **stabilire** "**chi fa cosa**" decidendo tra di loro chi dovrà svolgere i compiti al fine di garantire che il trattamento sia conforme alla normativa applicabile e agli obblighi previsti dal GDPR in relazione al trattamento congiunto in questione. In altre parole, una **distribuzione delle responsabilità** per la conformità deve essere resa come risultante dall'uso del termine "***rispettive***" di cui all'art. 26, par. 1. Ciò non esclude il fatto che **il diritto dell'UE o degli Stati membri possa già stabilire determinate responsabilità di ciascun contitolare**. In tal caso, l'accordo congiunto dovrebbe occuparsi anche di eventuali responsabilità aggiuntive necessarie per garantire la conformità al GDPR che non sono affrontate dalle disposizioni di legge.

163. L'obiettivo di queste regole è garantire che ove siano **coinvolti più attori**, specialmente in situazioni complesse, ambienti articolati di trattamento dei dati, **la responsabilità del rispetto delle norme sulla protezione dei dati sia chiaramente allocata** al fine di evitare che la protezione dei dati personali sia

ridotta, o che un conflitto negativo di competenza porti a scappatoie per cui alcuni obblighi non sono rispettati da nessuna delle parti coinvolti nel trattamento. Dovrebbe essere chiarito qui che **tutte le responsabilità devono essere assegnate secondo le circostanze di fatto** al fine di raggiungere un accordo operativo. L'EDPB osserva che si possono **verificare situazioni in cui l'influenza di un contitolare e la sua effettiva influenza complicano il raggiungimento** di un accordo. **Tuttavia, tali circostanze non negano la contitolarità e non può servire ad esentare nessuna delle parti dai propri obblighi ai sensi del GDPR**.

164. Più specificamente, l'art. 26, par. 1, specifica che la determinazione delle rispettive responsabilità (i.e. compiti) per il rispetto degli obblighi previsti dal GDPR deve essere svolto dai contitolari "in particolare" per quanto riguarda **l'esercizio dei diritti** dell'interessato e gli **obblighi di prestare le informazioni** di cui agli articoli 13 e 14, **a meno che e nella misura in cui le rispettive responsabilità dei titolari del trattamento siano determinate dal diritto dell'Unione o dello Stato membro cui sono soggetti i titolari del trattamento**.

165. Risulta chiaro da questa disposizione che i contitolari del trattamento devono definire chi rispettivamente sarà incaricato di rispondere alle richieste quando gli interessati esercitano i diritti riconosciuti dal GDPR e fornire informazioni agli stessi come previsto dagli artt. 13 e 14 del GDPR. Questo si riferisce solo alla definizione del loro rapporto interno onde stabilire quale delle parti è obbligata a rispondere alle richieste degli interessati.

Indipendentemente da tali accordi, l'interessato **può contattare** uno dei contitolari del trattamento ai sensi dell'art. 26, par. 3, GDPR. Tuttavia, l'uso dei termini "***in particolare***" indica che tali adempimenti non sono subordinati all'attribuzione di responsabilità da parte di ciascuna parte coinvolta in quanto le disposizioni di cui alla presente norma non sono esaustive. Ne consegue che **la distribuzione delle responsabilità** tra i contitolari per il rispetto degli obblighi **non si limita** alle materie di cui **all'art. 26**, para. 1, ma **si estende** agli altri obblighi del titolare ai sensi del GDPR. Infatti, **i contitolari del trattamento devono garantire che l'intero trattamento congiunto sia pienamente conforme al GDPR**.

166. In questa prospettiva, **le misure di conformità e i relativi obblighi** che dovrebbero considerare **i contitolari del trattamento** nella determinazione delle rispettive responsabilità, oltre a quelle specificamente previste dall'art 26(1), **includono tra l'altro e senza limitazione**:

- Attuazione dei principi generali di protezione dei dati (art. 5)
- Base giuridica del trattamento73 (art. 6)
- Misure di sicurezza (art. 32)
- Notifica di una violazione dei dati personali all'autorità di controllo e all'interessato74 (artt. 33 e 34)
- Valutazioni d'impatto sulla protezione dei dati (artt. 35 e 36)
- L'uso di un responsabile (art. 28)
- Trasferimenti di dati verso paesi terzi (Capitolo V)
- Organizzazione dei contatti con gli interessati e le autorità di controllo.

167. Altri argomenti che potrebbero essere considerati a seconda del trattamento in questione e dell'intenzione delle parti sono ad esempio le limitazioni all'uso dei

dati personali per un altro scopo da parte di uno dei contitolari del trattamento. A questo proposito, entrambi i titolari del trattamento hanno sempre il dovere di garantire che entrambi abbiano una base giuridica del trattamento. A volte, nell'ambito della titolarità congiunta, i dati personali sono trasferiti da un titolare ad un altro. **Per una questione di responsabilità, ogni titolare del trattamento ha il dovere di garantire che i dati non siano ulteriormente trattati in modo incompatibile con le finalità per che sono stati originariamente raccolti** dal titolare del trattamento che condivide i dati.

168. I contitolari del trattamento possono avere **un certo grado di flessibilità** nella distribuzione e ripartizione degli obblighi tra di loro purché garantiscano il pieno rispetto del GDPR riguardo al trattamento dei dati. **L'allocazione dovrebbe tenere conto di fattori quali chi è competente ed in grado di garantire i diritti** dell'interessato nonché il rispetto degli obblighi pertinenti ai sensi del GDPR. **L'EDPB raccomanda di documentare i fattori rilevanti e l'analisi interna effettuata al fine di attribuire i diversi obblighi**. Questa analisi fa parte della documentazione che dimostra il rispetto del principio di responsabilizzazione.

169. Gli obblighi non devono essere equamente distribuiti tra i contitolari. A questo proposito, la **CGUE** ha recentemente affermato che "***l'esistenza di una corresponsabilità non implica necessariamente uguale responsabilità dei diversi operatori coinvolti nel trattamento dei dati personali***". Tuttavia, possono verificarsi casi in cui non tutti gli obblighi possono essere distribuiti e non tutti i contitolari potrebbero dover rispettare gli stessi requisiti derivanti dal GDPR, tenendo conto della natura e del contesto del trattamento congiunto. Ad esempio, i contitolari del trattamento che utilizzano strumenti o sistemi di elaborazione dei dati condivisi devono garantire il rispetto, in particolare, del principio di limitazione delle finalità e attuare misure idonee a garantire la sicurezza dei dati personali trattati con gli strumenti condivisi.

170. Un altro esempio è l'obbligo per ciascun contitolare del trattamento di conservare un registro del trattamento attività o di designare un responsabile della protezione dei dati (**RPD**) se sono integrate le condizioni di cui all'art. 37, par. 1. Tali requisiti non sono relativi al trattamento congiunto ma sono applicabili agli stessi stessi titolari del trattamento.

2.2 L'attribuzione delle responsabilità deve essere effettuata mediante un accordo

2.2.1 Forma dell'accordo

171. L'art. 26, par. 1, del GDPR prevede un nuovo obbligo per i contitolari del trattamento che dovrebbero determinare le rispettive responsabilità "***per mezzo di un accordo tra di loro***". La forma giuridica di tale disposizione non è specificata dal GDPR. Pertanto, i contitolari sono liberi di concordarne la forma.

172. Inoltre, l'accordo sulla ripartizione delle responsabilità è vincolante per ciascun contitolare. Ciascuno è d'accordo e si impegna l'uno nei confronti dell'altro ad essere responsabili del rispetto e dei rispettivi obblighi indicati nell'accordo come da responsabilità dagli stessi assunta.

173. Pertanto, per motivi di certezza del diritto, anche se non vi è alcun requisito legale nel GDPR per redigere il contratto o altro atto giuridico, **l'EDPB raccomanda che tale accordo sia stipulato sotto forma di documento vincolante quale un contratto o altro atto giuridico vincolante ai sensi del diritto dell'UE o dello Stato membro** cui i titolari del trattamento sono soggetti. Ciò fornisce certezza e potrebbe essere utilizzato per dimostrare la trasparenza e la responsabilità. Infatti, in caso di mancato rispetto della pattuizione prevista nell' accordo, la sua natura vincolante consente a un titolare del trattamento di far valere la responsabilità dell'altro per ciò che è stato indicato nel contratto come di sua competenza. Inoltre, in linea con il principio di responsabilità, l'uso di un contratto o altro atto giuridico consentirà ai contitolari del trattamento di dimostrare che rispettano gli obblighi loro imposti dal GDPR.

174. Il modo in cui le responsabilità, ovvero i compiti, sono ripartiti tra ciascun contitolare deve essere indicato in **un linguaggio chiaro e semplice** nell'arrangiamento del contratto. Questo requisito è importante in quanto garantisce la legalità e la certezza, nonché evita possibili conflitti non solo nel rapporto tra i contitolari ma anche di fronte e nei confronti degli interessati e delle autorità di protezione dei dati.

175. Per inquadrare meglio la ripartizione delle responsabilità tra le parti, il **Comitato raccomanda che il l'accordo fornisca anche informazioni generali** sul trattamento congiunto specificando in particolare **l'oggetto**, la **materia** e le **finalità** del trattamento, la **tipologia di dati** personali e le **categorie di interessati**.

2.2.2 Obblighi nei confronti degli interessati

176. Il GDPR prevede diversi obblighi dei contitolari nei confronti degli interessati.

L'accordo riflette debitamente i rispettivi ruoli e i rapporti dei contitolari del trattamento nei confronti degli interessati

177. A complemento di quanto spiegato sopra nella sezione 2.1 delle presenti linee guida, è importante che **i contitolari chiariscano nell'accordo il loro rispettivo ruolo**, "in particolare" per quanto riguarda l'esercizio dei diritti dell'interessato e dei suoi doveri di fornire le informazioni di cui agli artt. 13 e 14. L'art. 26 del GDPR sottolinea l'importanza di questi specifici obblighi. I contitolari del trattamento devono quindi organizzarsi e concordare come e da chi saranno fornite **le informazioni** e come e da chi saranno fornite **le risposte** alle richieste dell'interessato. Indipendentemente dal contenuto dell'accordo su questo punto specifico, l'interessato può contattare uno dei contitolari di esercitare i propri diritti ai sensi dell'art. 26, par. 3, come ulteriormente spiegato di seguito.

178. Il modo in cui questi obblighi sono organizzati nell'accordo dovrebbe "debitamente", cioè accuratamente, **riflettere la realtà del sottostante trattamento** congiunto. Ad es., se solo uno dei contitolari comunica con gli interessati ai fini del trattamento esso potrebbe essere in una posizione migliore per informare gli interessati ed eventualmente rispondere alle loro richieste.

L'essenza dell'accordo è messa a disposizione dell'interessato

179. Tale disposizione mira a garantire che **l'interessato sia consapevole** dell'**"essenza dell'accordo"**. Ad esempio, deve essere completamente chiaro all'interessato quale titolare del trattamento funge da punto di contatto per l'esercizio dei diritti dell'interessato (fermo restando che può esercitare i suoi diritti verso e nei confronti di ciascun contitolare). L'obbligo di fornire l'essenza dell'accordo agli interessati è importante in caso di contitolarità per sapere quale dei titolari del trattamento è responsabile e di cosa.

180. Cosa dovrebbe riguardare la nozione di "**essenza dell'accordo**" non è specificato dal GDPR. **L'EDPB raccomanda che l'essenza copra almeno tutti gli elementi delle informazioni a cui si fa riferimento negli articoli 13 e 14** che dovrebbero essere già accessibili all'interessato, e per ciascuno di tali elementi, l'accordo dovrebbe specificare quale contitolare del trattamento è responsabile di garantire la conformità con gli stessi. L'essenza della disposizione deve indicare anche il punto di contatto, se designato.

181. **Non è specificato il modo** in cui tali informazioni devono essere messe a disposizione dell'interessato. Contrariamente ad altri disposizioni del GDPR (come l'art. 30, par. 4, per la registrazione del trattamento o l'art. 40, par. 11, per il registro dei codici di condotta approvati), **l'art. 26 non indica** che la disponibilità dovrebbe essere resa "su richiesta" né resa "disponibile al pubblico con mezzi appropriati". Pertanto, **spetta ai contitolari del trattamento decidere il modo più efficace per rendere disponibile l'essenza dell'accordo agli interessati** (ad esempio insieme alle informazioni di cui all'art. 13 o 14, nell'informativa sulla privacy o mediante una richiesta all'eventuale RPD o al referente eventualmente designato). I contitolari del trattamento dovrebbero rispettivamente garantire che le informazioni siano fornite in modo coerente.

L'accordo può designare un punto di contatto per gli interessati

182. L'art. 26, paragrafo 1, prevede la possibilità per i contitolari del trattamento di designare nell'accordo un **punto di contatto** per gli interessati. Tale designazione **non è obbligatoria**.

183. Essere informati in un unico modo per contattare eventuali più contitolari consente agli interessati di sapere a chi possono rivolgersi per tutte le questioni relative al trattamento dei propri dati personali. Inoltre, consente a più contitolari di coordinare in modo più efficiente le loro relazioni e comunicazioni nei confronti degli interessati.

184. Per questi motivi, al fine di agevolare l'esercizio dei diritti degli interessati ai sensi del GDPR, il **EDPB raccomanda ai contitolari del trattamento di individuare tale punto di contatto**.

185. Il punto di contatto può essere il DPO, se del caso, o il rappresentante nell'Unione (per i contitolari senza sede nell'Unione) o qualsiasi altro punto di contatto dove è possibile ottenere informazioni. Indipendentemente dai termini

dell'accordo, gli interessati possono esercitare i propri diritti verso e nei confronti di ciascuno dei contitolari.

186. Ai sensi dell'art. 26, par. 3, **l'interessato non è vincolato dai termini dell'accordo** e può esercitare i suoi diritti ai sensi del GDPR nei confronti e verso ciascuno dei contitolari del trattamento.

187. Ad esempio, in caso di contitolari stabiliti in Stati membri diversi, o se solo uno dei contitolari è stabilito nell'Unione, l'interessato può rivolgersi, a sua scelta, sia il titolare del trattamento stabilito nello Stato membro della sua residenza abituale o luogo di lavoro, o verso il titolare stabilito altrove nell'UE o nel SEE.

188. Anche se la disposizione e la sua essenza resa disponibile indicano un punto di contatto per ricevere e gestire tutte le richieste degli interessati, gli stessi interessati possono comunque scegliere diversamente.

189. Pertanto, è importante che i contitolari del trattamento organizzino in anticipo nel loro accordo come intendono gestire le risposte alle richieste che potrebbero ricevere dagli interessati. A questo proposito, si raccomanda che i contitolari comunichino agli altri titolari del trattamento o al referente designato, le richieste ricevute al fine di efficacemente gestirle. Richiedere agli interessati di contattare il punto di contatto designato o un titolare del trattamento imporrebbe un onere eccessivo al soggetto interessato, ciò che sarebbe contrario all'obiettivo di agevolare l'esercizio dei suoi diritti ai sensi del RGPD.

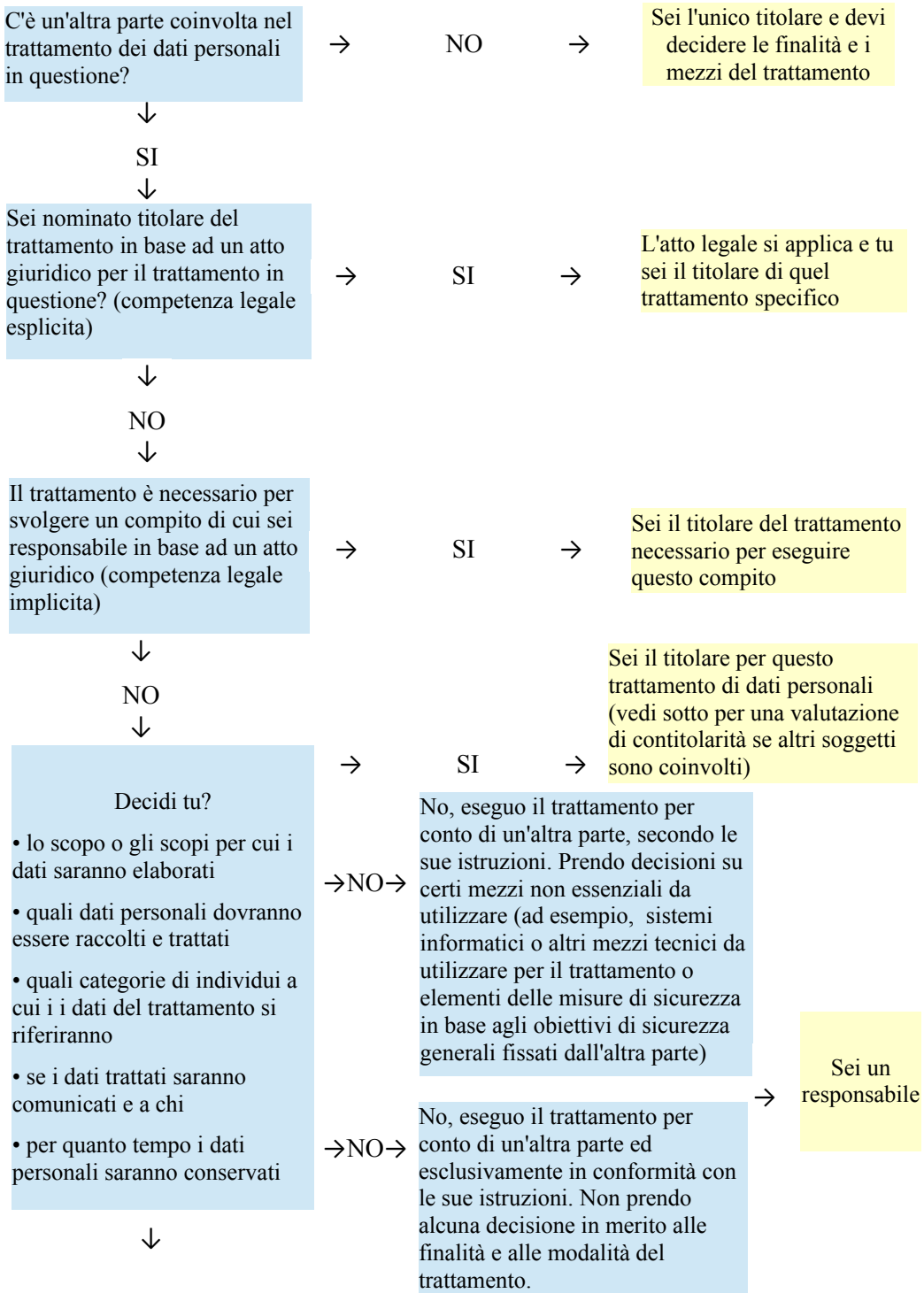
2.3 Obblighi nei confronti delle autorità di protezione dei dati

190. I contitolari del trattamento dovrebbero organizzare nell'accordo il modo in cui comunicheranno con l'autorità di controllo della protezione dei dati competenti. Tale comunicazione potrebbe coprire possibile consultazione ai sensi dell'art. 36 del GDPR, la notifica di una violazione dei dati personali, la designazione di un RPD.

191. Va ricordato che le autorità di protezione dei dati non sono vincolate dai termini dell'accordo sia in tema di qualificazione dei soggetti contitolari o del punto di contatto designato. Pertanto, le autorità possono contattare uno qualsiasi dei contitolari del trattamento per esercitare i loro poteri ai sensi dell'art. 58 in relazione al trattamento congiunto.

Allegato I – Diagramma di flusso per l'applicazione dei concetti di titolare del trattamento, responsabile e contitolari del trattamento nella pratica

Nota: per valutare correttamente il ruolo di ciascun soggetto coinvolto, è necessario prima individuare lo specifico trattamento dei dati personali in gioco e la sua esatta finalità. Se sono coinvolte più entità, è necessario valutare se le finalità e i mezzi siano decisi congiuntamente, determinando la contitolarità.



↓

NON LO SO

↓

Non so chi decida gli scopi e i mezzi del trattamento → I seguenti elementi possono aiutare a determinare la qualificazione appropriata dei ruoli

↓ ↓

• Ottieni un vantaggio da o hai un interesse nel trattamento (diverso dal mero pagamento per i servizi ricevuti da un altro titolare)

• Prendi decisioni sulle persone interessate come parte o risultato del trattamento (ad es. i soggetti sono i tuoi dipendenti)

• Le attività di trattamento possono essere considerate come naturalmente legate al tuo ruolo o alle tue attività (ad es. per ruoli tradizionali o competenze professionali) che comportano responsabilità dal punto di vista della protezione dei dati

• Il trattamento si riferisce al tuo rapporto con i soggetti come dipendenti, clienti, soci ecc.

• Hai completa autonomia nel decidere come i dati personali vengano trattati

• Hai affidato il trattamento dei dati personali ad un'organizzazione esterna per il trattamento dei dati personali per tuo conto

• Elabori i dati personali per gli scopi di un'altra parte e in conformità con le sue documentate istruzioni - non hai un tuo scopo.

• Un'altra parte controlla le tue attività di trattamento al fine di assicurare il rispetto delle istruzioni e dei termini di contratto.

• Non persegui un tuo scopo nel trattamento oltre a quello del tuo interesse economico di fornire servizi.

• Sei stato incaricato di svolgere specifiche attività di trattamento da parte di chi a sua volta è stato incaricato a trattare i dati per conto di un'altra parte esu istruzioni documentate di questa parte (sei un sub-responsabile del trattamento)

Contitolarità – se sei il titolare e un'altra parte è coinvolta nel trattamento dei dati personali

Tu e un'altra parte/i coinvolta/e determinate congiuntamente le finalità e i mezzi del trattamento?

Più di una parte ha un'influenza decisiva sul se e come avviene il trattamento – sia attraverso una decisione comune o mediante decisioni convergenti che si completano a vicenda e che sono necessarie per il trattamento perché hanno un impatto tangibile sullla determinazione delle finalità e dei mezzi?

Ciò significa che il trattamento non sarebbe possibile senza la partecipazione di entrambe le parti - il trattamento da parte di ogni parte è inseparabile, cioè indissolubilmente legato.

→ NO → Tu sei l'unico titolare – le altre parti coinvolte possono essere titolari indipendenti separati per un proprio scopo o responsabili in accordo con il diagramma di flusso sopra

SI

↓

Le decisioni comuni o convergenti sugli scopi e mezzi si riferiscono all'intero trattamento in questione?

→ SI → Siete contitolari per l'intero trattamento

↓

NO

↓

No, le decisioni comuni o convergenti riguardano solo fasi specifiche del trattamento

→ Siete contitolari per le fasi del trattamento per le quali determinate scopi e mezzi insieme e titolari separati per quelle operazioni di trattamento in cui determinate scopi e mezzi separatamente