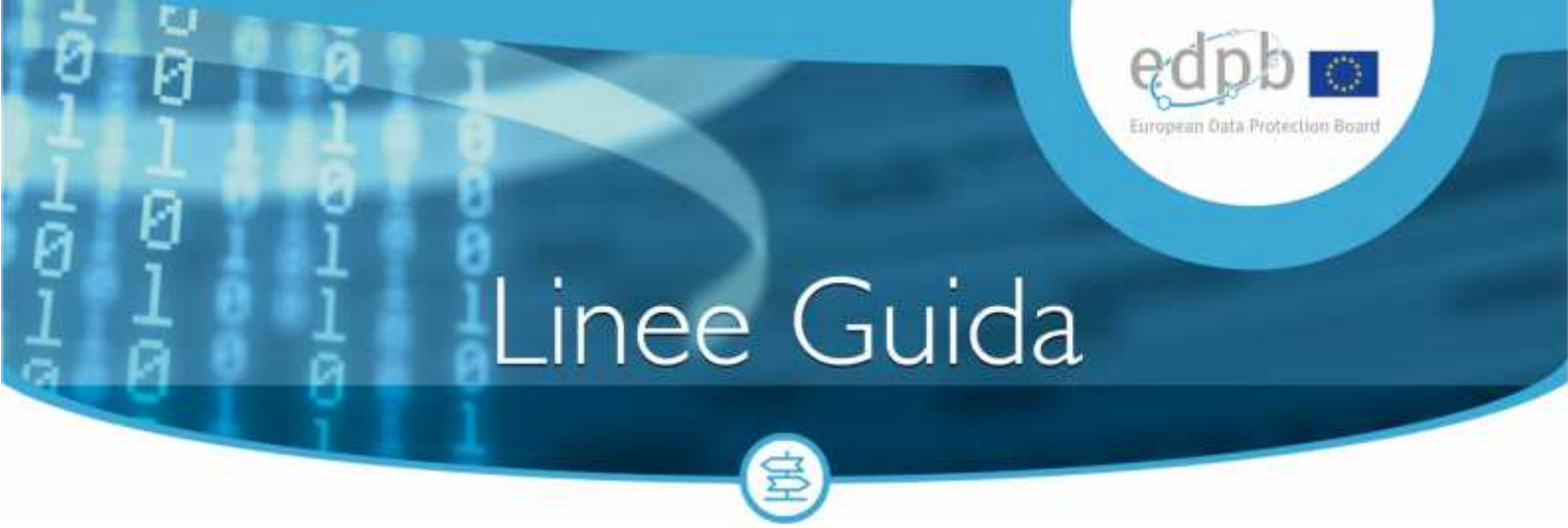



# Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR

## Versione 2.0

## Adottate il 7 luglio 2021

# Cronologia delle versioni

| | | |
|---|---|---|
| Versione 2.0 | 7 luglio 2021 | Adozione delle linee guida in seguito a consultazione pubblica |
| Versione 1.0 | 2 settembre 2020 | Adozione delle linee guida per consultazione pubblica |

# SINTESI

I concetti di titolare del trattamento, di contitolare del trattamento e di responsabile del trattamento svolgono un ruolo fondamentale nell'applicazione del regolamento generale sulla protezione dei dati [GDPR, regolamento (UE) 2016/679)], in quanto stabiliscono chi è il responsabile del rispetto delle diverse norme in materia di protezione dei dati e in che modo gli interessati possono esercitare i propri diritti in concreto. Il significato preciso di tali concetti e i criteri per una corretta interpretazione degli stessi devono essere sufficientemente chiari e coerenti in tutto lo Spazio economico europeo (SEE).

I concetti di titolare del trattamento, di contitolare del trattamento e di responsabile del trattamento sono *funzionali*, in quanto mirano a ripartire le responsabilità in funzione dei ruoli effettivi delle parti, e *autonomi*, nel senso che dovrebbero essere interpretati principalmente ai sensi del diritto dell'UE in materia di protezione dei dati.

Titolare del trattamento

In linea di principio non vi sono limitazioni per quanto concerne la natura dei soggetti che possono assumere il ruolo di titolare del trattamento, tuttavia in pratica è solitamente l'organizzazione in quanto tale e non una persona fisica all'interno dell'organizzazione (come l'amministratore delegato, un dipendente o un membro del consiglio di amministrazione) ad agire in qualità di titolare del trattamento.

Il titolare del trattamento è il soggetto che *decide* in merito a determinati elementi chiave del trattamento stesso. La titolarità può essere definita a norma di legge o può derivare da un'analisi degli elementi di fatto o delle circostanze del caso. Talune attività di trattamento possono essere considerate come naturalmente connesse al ruolo ricoperto da un determinato soggetto (il datore di lavoro rispetto ai dipendenti, l' editore rispetto agli abbonati o un'associazione rispetto ai membri). In molti casi, le condizioni previste da un contratto possono agevolare l'individuazione del titolare del trattamento, sebbene non siano sempre determinanti.

Il titolare stabilisce le finalità e i mezzi del trattamento, ossia il *motivo* e le *modalità* del trattamento. Il titolare del trattamento è chiamato a decidere tanto sulle finalità quanto sui mezzi. Tuttavia, taluni aspetti più prettamente pratici legati all'implementazione del trattamento («mezzi non essenziali») possono essere delegati al responsabile del trattamento. Per essere qualificato come titolare del trattamento non è necessario che tale soggetto abbia accesso effettivo ai dati trattati.

Contitolari del trattamento

La contitolarità di trattamento può configurarsi laddove più di un soggetto sia coinvolto nel trattamento. Il GDPR introduce norme specifiche per i contitolari del trattamento e definisce un quadro per disciplinare i loro rapporti. Il criterio generale per la sussistenza della contitolarità di trattamento è la partecipazione congiunta di due o più soggetti nella definizione delle finalità e dei mezzi di un'operazione di trattamento. La partecipazione congiunta può assumere la forma di una *decisione comune*, presa da due o più soggetti, o può derivare dalle *decisioni convergenti* di due o più soggetti, qualora tali decisioni si integrino vicendevolmente e siano necessarie affinché il trattamento abbia luogo così da esplicare un effetto tangibile sulla definizione delle finalità e dei mezzi del trattamento. Un criterio importante è che il trattamento non sarebbe possibile senza la partecipazione di entrambi i soggetti, nel senso che i trattamenti svolti da ciascun soggetto sono tra loro indissociabili, ovverosia indissolubilmente legati. La partecipazione congiunta comprende, da un lato, la determinazione delle finalità e, dall'altro, la determinazione dei mezzi.

Responsabile del trattamento

Il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organo che tratta dati personali per conto del titolare del trattamento. Due condizioni sono indispensabili per configurare il ruolo di responsabile del trattamento: essere un soggetto distinto rispetto al titolare del trattamento e trattare dati personali per conto del titolare del trattamento.

Al responsabile del trattamento non è consentito trattare i dati in modo diverso rispetto a quanto indicato nelle istruzioni del titolare. Tuttavia, le istruzioni del titolare del trattamento possono lasciare un certo margine di discrezionalità su come servirne al meglio gli interessi, consentendo al responsabile del trattamento di avvalersi dei mezzi tecnici e organizzativi più idonei. Ciononostante, un responsabile del trattamento viola il GDPR qualora non si limiti a trattare i dati in base alle istruzioni del titolare del trattamento e inizi a definire mezzi e finalità propri. Il responsabile del trattamento sarà pertanto considerato titolare rispetto a tale ultimo trattamento e può essere soggetto a sanzioni qualora non si limiti a trattare i dati in base alle istruzioni impartite dal titolare del trattamento.

Rapporto tra titolare e responsabile del trattamento

Il titolare del trattamento deve avvalersi unicamente di responsabili del trattamento che presentino garanzie sufficienti per l'attuazione di misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del GDPR. Gli elementi di cui tenere conto potrebbero essere le conoscenze specialistiche del responsabile del trattamento (ad esempio, le competenze tecniche in materia di misure di sicurezza e di violazione dei dati), il grado di affidabilità, le risorse di cui dispone il responsabile e l'adesione di quest'ultimo a un codice di condotta o a un meccanismo di certificazione riconosciuti.

Qualsivoglia trattamento di dati personali da parte di un responsabile del trattamento deve essere disciplinato da un contratto o da un atto giuridico di altra natura, redatto per iscritto, anche in formato elettronico, con carattere di vincolatività. Il titolare e il responsabile del trattamento possono negoziare un contratto specifico, comprensivo di tutti gli elementi obbligatori, oppure basarsi, in tutto o in parte, su clausole contrattuali tipo.

Il GDPR elenca gli elementi che devono figurare nell'accordo di trattamento, il quale tuttavia non dovrebbe limitarsi a ribadire le disposizioni del GDPR; piuttosto, tale accordo dovrebbe disciplinare in modo più specifico e concreto come saranno soddisfatti i requisiti applicabili e quale sia il livello di sicurezza richiesto per il trattamento dei dati personali oggetto dell'accordo stesso.

Rapporto tra contitolari del trattamento

I contitolari del trattamento stabiliscono e concordano in modo trasparente le rispettive responsabilità per quanto concerne l'adempimento degli obblighi di cui al GDPR. La determinazione delle rispettive responsabilità deve riguardare in particolare l'esercizio dei diritti degli interessati e gli obblighi di informazione. Inoltre, la ripartizione delle responsabilità dovrebbe riguardare altri obblighi in capo al titolare del trattamento, quali il rispetto dei principi generali in materia di protezione dei dati, la base giuridica, le misure di sicurezza, l'obbligo di notifica di violazione dei dati, le valutazioni d'impatto sulla protezione dei dati, il ricorso a responsabili del trattamento, i trasferimenti verso paesi terzi e i contatti con gli interessati e le autorità di controllo.

Ciascun contitolare è tenuto a disporre di una base giuridica per il trattamento e a garantire che i dati non siano oggetto di ulteriore trattamento secondo modalità incompatibili con le finalità per le quali sono stati inizialmente raccolti dal titolare che li comunica.

Il GDPR non specifica la forma giuridica dell'accordo tra contitolari del trattamento. Ai fini della certezza del diritto e per garantire il rispetto dei principi di trasparenza e responsabilizzazione, l'EDPB raccomanda che l'accordo sia stipulato sotto forma di documento vincolante, ossia di contratto o di atto giuridico vincolante di altra natura, ai sensi del diritto dell'UE o dello Stato membro cui sono soggetti i titolari del trattamento.

L'accordo riflette debitamente i ruoli e i rapporti rispettivi dei contitolari di trattamento nei confronti degli interessati e i suoi elementi essenziali sono messi a disposizione dell'interessato.

Indipendentemente dai termini dell'accordo, gli interessati hanno facoltà di esercitare i propri diritti nei confronti di e contro ciascuno dei contitolari del trattamento. Le autorità di controllo non sono vincolate dalle condizioni dell'accordo né per quanto concerne la qualifica di contitolari né per quanto concerne i punti di contatto designati.

# SOMMARIO

## Il comitato europeo per la protezione dei dati

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito il «GDPR» o «il regolamento»),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo n. 37 dello stesso, modificati dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018[1],

visti gli articoli 12 e 22 del proprio regolamento interno,

considerando che il lavoro preparatorio delle presenti linee guida ha comportato la raccolta di contributi da parte delle parti interessate, sia per iscritto che in occasione di un evento dedicato alle stesse, al fine di individuare le sfide più urgenti,

**HA ADOTTATO LE SEGUENTI LINEE GUIDA**

# INTRODUZIONE

1. Il presente documento è inteso a fornire orientamenti sui concetti di titolare del trattamento e di responsabile del trattamento, ai sensi delle norme del GDPR relative alle definizioni di cui all'articolo 4 e delle disposizioni relative agli obblighi di cui al capo IV. L'obiettivo principale è chiarire il significato dei concetti nonché i diversi ruoli e la ripartizione delle responsabilità tra i soggetti in questione.

2. Il concetto di titolare del trattamento e la sua interazione con quello di responsabile del trattamento svolgono un ruolo fondamentale nell'applicazione del GDPR, in quanto determinano chi è responsabile del rispetto delle diverse norme in materia di protezione dei dati e in che modo gli interessati possono esercitare i propri diritti in concreto. Il GDPR introduce esplicitamente il principio di responsabilizzazione, nel senso che il titolare del trattamento è competente per il rispetto dei principi relativi al trattamento dei dati personali di cui all'articolo 5 ed è in grado di comprovarlo. Inoltre, il GDPR introduce norme più specifiche sul ricorso a uno o più responsabili del trattamento, e talune disposizioni in materia di trattamento dei dati personali riguardano non solo i titolari ma anche i responsabili del trattamento.

3. È pertanto di fondamentale importanza che il significato preciso di tali concetti e i criteri per il loro corretto utilizzo siano sufficientemente chiari e condivisi in tutta l'Unione europea e nel SEE.

4. Il gruppo di lavoro Articolo 29 ha pubblicato orientamenti sui concetti di titolare del trattamento e responsabile del trattamento [rispettivamente «responsabile» e «incaricato» nel parere 1/2010 (WP 169)][2], allo scopo di fornire chiarimenti ed esempi concreti in merito. Dall'entrata in vigore del GDPR ci si è interrogati più volte sulla misura in cui quest'ultimo avesse modificato i concetti di titolare del trattamento e di responsabile del trattamento e i rispettivi ruoli. In particolare, sono stati sollevati interrogativi sul merito e sulle implicazioni del concetto di contitolarità di trattamento (ad esempio, ai

[1] Nel presente documento, con «Stati membri» ci si riferisce agli «Stati membri del SEE».
[2] Gruppo di lavoro Articolo 29, Parere 1/2010 sui concetti di «responsabile del trattamento» e di «incaricato del trattamento», adottato il 16 febbraio 2010, 264/10/IT, WP 169.

sensi dell'articolo 26 del GDPR) e sugli obblighi specifici per i responsabili del trattamento di cui al capo IV (ad esempio, ai sensi dell'articolo 28 del GDPR). Pertanto, e poiché riconosce che l'applicazione concreta dei concetti richiede ulteriori chiarimenti, l'EDPB ritiene necessario fornire orientamenti più articolati e specifici, al fine di garantire un approccio coerente e armonizzato in tutta l'UE e nel SEE. Le presenti linee guida sostituiscono il precedente parere del gruppo di lavoro Articolo 29 su tali concetti (WP 169).

5. Nella parte I, le presenti linee guida esaminano le definizioni dei diversi concetti di titolare del trattamento, contitolari di trattamento, responsabile del trattamento e terzo/destinatario. Nella parte II sono forniti ulteriori orientamenti sulle conseguenze legate ai diversi ruoli svolti dal titolare del trattamento, dai contitolari di trattamento e dal responsabile del trattamento.

# PARTE I – CONCETTI

## 1 OSSERVAZIONI GENERALI

6. L'articolo 5, paragrafo 2, del GDPR introduce esplicitamente il principio di responsabilizzazione. Ciò significa che:

   - il titolare del trattamento è *responsabile del rispetto* dei principi di cui all'articolo 5, paragrafo 1, del GDPR;
   - il titolare del trattamento è in grado di *dimostrare il rispetto* dei principi di cui all'articolo 5, paragrafo 1, del GDPR.

   Questo principio è stato descritto in un parere del gruppo di lavoro Articolo 29[3] e non sarà trattato in dettaglio nelle presenti linee guida.

7. L'obiettivo di integrare il principio di responsabilizzazione nel GDPR e di renderlo un principio centrale era volto a sottolineare che i titolari del trattamento devono attuare misure adeguate ed efficaci ed essere in grado di dimostrare la conformità al regolamento.[4]

8. L'articolo 24 specifica ulteriormente il principio di responsabilizzazione, prevedendo l'obbligo in capo al titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di **dimostrare** che il trattamento è effettuato in conformità del GDPR. Tali misure sono riesaminate e aggiornate, se del caso. Anche l'articolo 28, che stabilisce gli obblighi del titolare del trattamento laddove si avvalga di un responsabile del trattamento, richiama il principio di responsabilizzazione.

9. Il principio di responsabilizzazione si rivolge direttamente al titolare del trattamento. Tuttavia, talune norme più specifiche, come quelle sui poteri delle autorità di controllo di cui all'articolo 58, sono rivolte sia ai titolari sia ai responsabili del trattamento. Entrambi possono essere oggetto di sanzioni in caso di inadempimento degli obblighi cui sono soggetti ai sensi del GDPR ed entrambi sono direttamente responsabili nei confronti delle autorità di controllo, in virtù dell'obbligo di conservare e fornire la documentazione adeguata su richiesta, di cooperare in caso di indagini e di ottemperare ai

[3] Gruppo di lavoro Articolo 29, Parere 3/2010 sul principio di responsabilizzazione, adottato il 13 luglio 2010, 00062/10/EN WP 173.
[4] Cfr. il considerando 74 del GDPR.

provvedimenti amministrativi. Al contempo, occorre rammentare che i responsabili del trattamento devono attenersi sempre alle istruzioni del titolare del trattamento e agire unicamente in base a esse.

10. Il principio di responsabilizzazione, insieme alle altre norme che disciplinano in modo più specifico le modalità di adempimento del GDPR e la ripartizione delle responsabilità, rende pertanto necessario definire i diversi ruoli dei vari soggetti coinvolti in un'attività di trattamento di dati personali.

11. Un'osservazione di natura generale riguardante i concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR è che tali concetti non hanno subito cambiamenti rispetto alla direttiva 95/46/CE e che, nel complesso, i criteri per l'attribuzione dei vari ruoli restano immutati.

12. Quelli di titolare del trattamento e di responsabile del trattamento sono concetti *funzionali*: mirano a ripartire le responsabilità in funzione dei ruoli effettivamente svolti.[5] Ciò implica che lo status giuridico di un soggetto in quanto «titolare del trattamento» o «responsabile del trattamento» deve, in linea di principio, essere determinato dalle attività effettivamente svolte in una situazione specifica, piuttosto che dalla sua designazione formale in quanto «titolare del trattamento» o «responsabile del trattamento» (ad esempio in un contratto).[6] Ciò significa che la ripartizione dei ruoli dovrebbe, di norma, derivare da un'analisi degli elementi di fatto o delle circostanze del caso e, in quanto tale, non è negoziabile.

13. I concetti di titolare del trattamento e di responsabile del trattamento sono altresì concetti *autonomi*, nel senso che, sebbene fonti giuridiche esterne possano contribuire all'individuazione del titolare del trattamento, la loro interpretazione dovrebbe basarsi principalmente sul diritto dell'UE in materia di protezione dei dati. Il concetto di titolare del trattamento non dovrebbe essere confuso con altri concetti, talvolta contrastanti o coincidenti, propri di altri campi del diritto, come quello di autore o di titolare dei diritti in materia di proprietà intellettuale o di diritto della concorrenza.

14. Poiché l'obiettivo di fondo nell'attribuzione del ruolo di titolare del trattamento è garantire il rispetto del principio di responsabilizzazione e una protezione efficace e completa dei dati personali, il concetto di «titolare del trattamento» dovrebbe essere interpretato in modo sufficientemente estensivo, favorendo il più possibile una tutela efficace e completa degli interessati[7], in modo da garantire la piena efficacia del diritto dell'UE in materia di protezione dei dati, evitare lacune e prevenire elusioni potenziali delle norme, senza sminuire, al contempo, il ruolo del responsabile del trattamento.

# 2 DEFINIZIONE DI TITOLARE DEL TRATTAMENTO

## 2.1 Definizione di titolare del trattamento

15. L'articolo 4, paragrafo 7, del GDPR definisce come titolare del trattamento

[5] Gruppo di lavoro Articolo 29, Parere 1/2010, WP 169, pag. 9.
[6] Cfr. anche le conclusioni dell'avvocato generale Mengozzi in *Testimoni di Geova*, C-25/17, ECLI:EU:C:2018:57, punto 68 («*ai fini della determinazione del "titolare del trattamento" ai sensi della direttiva 95/46, sono incline a ritenere [...] che un formalismo eccessivo renderebbe facile eludere le disposizioni della direttiva 95/46 e che, di conseguenza, occorre basarsi su un'analisi più fattuale che formale [...]*»).
[7] CGUE, causa C-131/12, Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, sentenza del 13 maggio 2014, punto 34; CGUE, causa C-210/16, Wirtschaftsakademie Schleswig-Holstein, sentenza del 5 giugno 2018, punto 28; CGUE, causa C-40/17, Fashion ID GmbH & Co.KG contro Verbraucherzentrale NRW eV, sentenza del 29 luglio 2019, punto 66.

*«**la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo** che, **singolarmente o insieme ad altri, determina** le **finalità e i mezzi** del **trattamento di dati personali**; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere **stabiliti dal diritto dell'Unione o degli Stati membri**»*.

16. La definizione di titolare del trattamento prevede cinque elementi principali, che saranno analizzati separatamente ai fini delle presenti linee guida. Questi elementi sono:

- «la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo»
- «determina»
- «singolarmente o insieme ad altri»
- «le finalità e i mezzi»
- «del trattamento dei dati personali».

### 2.1.1 «Persona fisica o giuridica, autorità pubblica, servizio o altro organismo»

17. Il primo elemento costitutivo si riferisce alla natura soggettiva del titolare del trattamento. Ai sensi del GDPR, il titolare del trattamento può essere «*una persona fisica o giuridica, un'autorità pubblica, un servizio o un altro organismo*». Ciò significa che, in linea di principio, non vi sono limitazioni riguardo alle caratteristiche soggettive del titolare del trattamento. Potrebbe trattarsi di un'organizzazione, ma anche di un singolo o di un gruppo di persone[8]. In pratica, tuttavia, è solitamente l'organizzazione in quanto tale e non una persona fisica all'interno dell'organizzazione (come l'amministratore delegato, un dipendente o un membro del consiglio di amministrazione) ad agire in qualità di titolare del trattamento ai sensi del GDPR. Per quanto riguarda il trattamento all'interno di un gruppo di società, occorre prestare particolare attenzione alla questione se uno stabilimento possa agire in qualità di titolare o di responsabile del trattamento, ad esempio quando tratta dati per conto della società controllante.

18. Talvolta le società e gli organismi pubblici designano una persona specifica quale responsabile dell'esecuzione dell'attività di trattamento. Anche se viene designata una persona fisica specifica per garantire il rispetto delle norme in materia di protezione dei dati, tale persona non sarà il titolare del trattamento, ma agirà per conto del soggetto giuridico (società o organismo pubblico) che risponderà in ultima istanza, in caso di violazione delle norme, in qualità di titolare del trattamento. Nella stessa ottica, anche se un determinato dipartimento o unità all'interno di un'organizzazione ha la responsabilità operativa di garantire la conformità di determinate attività di trattamento, ciò non significa che tale dipartimento o unità (anziché l'organizzazione nel suo insieme) assuma il ruolo di titolare del trattamento.

**Esempio**

Il dipartimento marketing della società ABC lancia una campagna pubblicitaria per promuovere i suoi prodotti. Il dipartimento decide in merito alla natura della campagna, ai mezzi da utilizzare (e-mail, social media...), ai clienti ai quali rivolgersi e ai dati da utilizzare per ottenere il miglior risultato possibile. Anche se il dipartimento marketing ha agito con notevole indipendenza, in linea di principio

[8] Ad esempio, nella sentenza relativa alla causa *Testimoni di Geova*, C-25/17, ECLI:EU:C:2018:551, punto 75, la CGUE ha ritenuto che una comunità religiosa di testimoni di Geova agisse come titolare del trattamento, insieme ai singoli membri. Sentenza nella causa *Testimoni di Geova*, C-25/17, ECLI:EU:C:2018:551, punto 75.

la società ABC sarà considerata titolare del trattamento, visto che la campagna pubblicitaria è avviata da tale società e si svolge nell'ambito delle sue attività commerciali e per le sue finalità.

19. In linea di principio, si può presumere che qualsivoglia trattamento di dati personali da parte dei dipendenti nell'ambito delle attività di un'organizzazione abbia luogo sotto il controllo di quest'ultima.[9] In circostanze eccezionali, tuttavia, può avvenire che un dipendente decida di utilizzare i dati personali per finalità proprie, andando così illegittimamente oltre l'autorità conferitagli (ad esempio per costituire una propria società o per fini analoghi). Spetta pertanto all'organizzazione, in quanto titolare del trattamento, assicurarsi che siano poste in essere misure tecniche e organizzative adeguate, ivi comprese, ad esempio, la formazione e l'informazione dei dipendenti, per garantire la conformità al GDPR.[10]

### 2.1.2 «Determina»

20. Il secondo elemento costitutivo del concetto di titolare del trattamento si riferisce all'*influenza* di tale soggetto sul trattamento stesso, in virtù di un *esercizio del potere decisionale*. Il titolare del trattamento è un soggetto che *decide* taluni elementi chiave del trattamento. Tale titolarità può essere definita a norma di legge o può derivare da un'analisi degli elementi di fatto o delle circostanze del caso. Occorre studiare le specifiche operazioni di trattamento in questione e capire chi le determina, esaminando in primo luogo le seguenti questioni: «*Perché il trattamento ha luogo?*» e «*Chi ha deciso che il trattamento debba avvenire per una determinata finalità?*».

*Circostanze che danno luogo alla funzione di controllo*

21. Appurato che quello di titolare del trattamento è un concetto funzionale, esso si basa pertanto su un'**analisi fattuale piuttosto che formale**. Per agevolare l'analisi possono essere utilizzati alcuni criteri guida e ipotesi pratiche per guidare e semplificare il processo. Nella maggior parte dei casi, il «soggetto decisore» può essere individuato facilmente e chiaramente sulla base di determinate circostanze giuridiche e/o fattuali dalle quali si può normalmente dedurre l'«influenza», a meno che altri elementi depongano in senso contrario. Si possono distinguere due categorie di situazioni: 1) titolarità derivante da *disposizioni giuridiche*; 2) titolarità derivante da un'*influenza concreta*.

1) *Titolarità derivante da disposizioni giuridiche*

22. Vi sono casi in cui la titolarità può essere ricavata dalla competenza espressamente conferita per legge, ad esempio quando il titolare del trattamento o i criteri specifici per la sua designazione sono determinati dal diritto nazionale o dell'Unione. Infatti, l'articolo 4, paragrafo 7, stabilisce che «*quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*». Mentre l'articolo 4, paragrafo 7, fa riferimento unicamente al «titolare del trattamento» al singolare, l'EDPB ritiene che il diritto dell'Unione o degli Stati membri possa anche designare più titolari del trattamento, eventualmente anche in qualità di contitolari.

23. Il fatto che la titolarità del trattamento sia stata definita specificamente per legge sarà determinante per stabilire chi agisce in quanto titolare. Ciò presuppone che il legislatore abbia designato come titolare del trattamento un soggetto che è effettivamente in grado di esercitare un controllo. La

[9] In linea generale, ai sensi dell'articolo 29 del GDPR, i dipendenti aventi accesso ai dati personali all'interno di un'organizzazione non sono considerati «titolari del trattamento» o «responsabili del trattamento», bensì persone che «agiscono sotto l'autorità del titolare del trattamento o del responsabile del trattamento».
[10] Articolo 24, paragrafo 1, del GDPR.

legislazione nazionale di taluni paesi prevede che le autorità pubbliche siano responsabili del trattamento dei dati personali nell'ambito delle rispettive competenze.

24. Tuttavia, più comunemente, anziché designare direttamente il titolare del trattamento o stabilire i criteri per la sua designazione, la legge definisce un compito o impone l'obbligo di raccogliere e trattare determinati dati. In tali casi, la finalità del trattamento è spesso determinata per legge. Il titolare del trattamento è di norma il soggetto cui la legge demanda la realizzazione di tale finalità, di tale funzione pubblica. Ciò sarebbe il caso, ad esempio, laddove un soggetto cui sono affidati determinati compiti pubblici (ad es., prestazioni previdenziali), che non possono essere assolti senza raccogliere almeno un certo numero di dati personali, istituisca una banca dati o un registro per svolgere detta funzione pubblica. In tal caso, la legge stabilisce, pur se indirettamente, chi è il titolare del trattamento. Più in generale, la legge può altresì imporre, a soggetti pubblici o privati, l'obbligo di conservare o fornire determinati dati. Di norma, tali soggetti sarebbero pertanto considerati titolari del trattamento necessario per l'adempimento dell'obbligo in questione.

**Esempio: disposizioni giuridiche**

La legislazione nazionale del paese A prevede l'obbligo per le autorità comunali di erogare prestazioni sociali quali versamenti mensili ai cittadini in base alla loro situazione finanziaria. Per effettuare tali pagamenti, l'amministrazione comunale deve acquisire ed elaborare dati sulla situazione finanziaria dei richiedenti. Anche se non è previsto esplicitamente dalla legge, le autorità comunali sono i titolari di tale trattamento in virtù, implicitamente, delle disposizioni giuridiche.

2) *Titolarità derivante da un'influenza concreta*

25. In assenza di titolarità derivante da disposizioni giuridiche, la qualifica di titolare del trattamento deve essere stabilita sulla base di una valutazione delle circostanze concrete del trattamento. Occorre prendere in considerazione tutte le circostanze di fatto pertinenti al fine di stabilire se uno specifico soggetto eserciti un'influenza determinante sul trattamento dei dati personali in questione.

26. La necessità di una valutazione fattuale significa anche che la titolarità di un trattamento non deriva dalle caratteristiche soggettive di chi tratta i dati, ma dalle attività concretamente svolte da tale soggetto in un contesto specifico. In altre parole, uno stesso soggetto può agire contemporaneamente in qualità di titolare del trattamento per determinate operazioni di trattamento, e in qualità di responsabile del trattamento per altre operazioni; inoltre, la qualifica di titolare o di responsabile del trattamento va valutata in relazione a ciascuna specifica attività di trattamento dei dati.

27. In pratica, talune operazioni di trattamento possono essere considerate come intrinseche al ruolo o alle attività di un determinato soggetto e, in ultima analisi, tali da comportare responsabilità dal punto di vista della protezione dei dati. Ciò può essere dovuto a disposizioni giuridiche di natura più generale o a una prassi giuridica consolidata in singoli settori (diritto civile, commerciale, del lavoro, ecc.). In tal caso, l'esistenza di determinati ruoli tradizionali e di determinate competenze professionali che, di norma, comportano specifiche responsabilità contribuirà a individuare il titolare del trattamento. Si pensi agli esempi seguenti: un datore di lavoro in relazione al trattamento dei dati personali relativi ai propri dipendenti; un editore che tratta i dati personali degli abbonati; un'associazione che tratta i dati personali riguardanti i soci o collaboratori. Quando un soggetto tratta dati personali nell'ambito delle sue interazioni con i propri dipendenti, clienti o soci, tale soggetto, di norma, determina la finalità e i mezzi relativi al trattamento e agisce pertanto in qualità di titolare del trattamento stesso ai sensi del GDPR.

**Esempio: studi legali**

La società ABC si rivolge a uno studio legale per rappresentarla in una controversia. Per svolgere tale compito, lo studio legale è tenuto a trattare i dati personali relativi alla causa. Il trattamento dei dati personali è motivato dal mandato dello studio legale di rappresentare il cliente in tribunale. Detto mandato, tuttavia, non riguarda specificamente il trattamento dei dati personali. Lo studio legale agisce con un grado significativo di indipendenza, ad esempio nel decidere quali informazioni utilizzare e come utilizzarle e non vi sono istruzioni della società cliente in merito al trattamento dei dati personali. Il trattamento effettuato dallo studio per svolgere il compito di rappresentante legale della società è pertanto legato al ruolo funzionale dello studio stesso, che deve essere considerato titolare del trattamento.

**Esempio: operatori di telecomunicazioni**[11]

La fornitura di un servizio di comunicazione elettronica, come la posta elettronica, comporta il trattamento di dati personali. Il fornitore di tali servizi sarà di norma considerato titolare del trattamento dei dati personali necessari per il funzionamento del servizio in quanto tale (ad esempio, dati relativi al traffico e alla fatturazione). Se l'unica finalità e ruolo del fornitore è quello di consentire la trasmissione di messaggi di posta elettronica, il fornitore non sarà considerato titolare del trattamento per quanto riguarda i dati personali contenuti nel messaggio stesso. Il titolare del trattamento dei dati personali contenuti nel messaggio è di norma la persona da cui proviene il messaggio, piuttosto che il prestatore di servizi che offre il servizio di trasmissione.

28. In molti casi, l'analisi delle clausole contrattuali che disciplinano i rapporti tra le diverse parti coinvolte può facilitare l'individuazione del soggetto (o dei soggetti) che opera(no) in qualità di titolare del trattamento. Anche se il contratto non stabilisce chi è il titolare del trattamento, esso può contenere elementi sufficienti per desumere chi decide in merito alle finalità e ai mezzi del trattamento. Può anche accadere che il contratto preveda un'indicazione esplicita sull'identità del titolare del trattamento. Se non sussiste motivo di dubitare che ciò rispecchi fedelmente la realtà, niente vieta di attenersi alle previsioni del contratto. Tuttavia, queste ultime non sono determinanti in modo assoluto, poiché altrimenti le parti potrebbero attribuire le responsabilità a proprio piacimento. Non è possibile assumere il ruolo di titolare del trattamento né esimersi dagli obblighi in capo al titolare del trattamento semplicemente redigendo il contratto in un determinato modo, laddove ciò non corrisponda alle circostanze di fatto.

29. Se una parte decide di fatto le finalità e le modalità del trattamento di dati personali, essa sarà il titolare del trattamento anche laddove un contratto la indichi come responsabile di tale trattamento. Analogamente, non è sufficiente che un contratto designi una parte come «subappaltatore» affinché tale parte contrattuale sia considerata responsabile del trattamento ai sensi della normativa in materia di protezione dei dati.[12]

30. In linea con l'approccio fattuale, il termine «determina» significa che il titolare del trattamento è il soggetto che esercita effettivamente un'influenza determinante sulle finalità e sui mezzi del trattamento stesso. Di norma, un contratto che disciplini il trattamento di dati definisce la parte che

[11] L'EDPB ritiene che questo esempio, precedentemente contemplato al considerando 47 della direttiva 95/46/CE, continui a essere pertinente anche ai sensi del GDPR.

[12] Cfr., ad esempio, gruppo di lavoro Articolo 29 per la protezione dei dati, Parere 10/2006 sul trattamento dei dati personali da parte della Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 novembre 2006, WP 128, pag. 11.

decide sul trattamento (titolare del trattamento) e la parte che opera secondo specifiche istruzioni (responsabile del trattamento). Anche se il responsabile del trattamento offre un servizio definito in via preliminare in modo specifico, al titolare del trattamento deve essere messa a disposizione una descrizione dettagliata di tale servizio e spetta al titolare adottare la decisione finale con cui si approvano le modalità di esecuzione del trattamento nonché chiedere eventuali modifiche. Inoltre, il responsabile del trattamento non può modificare successivamente gli elementi essenziali dello stesso senza l'approvazione del titolare del trattamento.

**Esempio: servizio standardizzato di archiviazione su cloud**

Un grande fornitore di servizi di archiviazione su cloud offre ai propri clienti la possibilità di archiviare volumi ingenti di dati personali. Il servizio è completamente standardizzato e i clienti hanno scarsa o nessuna capacità di personalizzarlo. I termini contrattuali sono stabiliti e redatti unilateralmente dal fornitore di servizi cloud e forniti al cliente in un'ottica di «prendere o lasciare». La società X decide di avvalersi del fornitore di servizi cloud per archiviare dati personali relativi ai propri clienti. La società X continuerà a essere considerata titolare del trattamento, alla luce della sua decisione di avvalersi di questo fornitore specifico di servizi cloud per trattare dati personali per le proprie finalità. Nella misura in cui il fornitore di servizi cloud non tratti i dati personali per le proprie finalità e li archivi esclusivamente per conto dei propri clienti e conformemente alle istruzioni, il fornitore di servizi sarà considerato responsabile del trattamento.

### 2.1.3 «Singolarmente o insieme ad altri»

31. L'articolo 4, paragrafo 7, riconosce che le «finalità e i mezzi» del trattamento possono essere determinati da più di un soggetto. Inoltre, prevede che il titolare del trattamento sia il soggetto che «singolarmente o insieme ad altri» determina le finalità e i mezzi del trattamento. Ciò significa che più soggetti possono agire in qualità di titolare per un medesimo trattamento e che a ciascuno di essi si applicano pertanto le pertinenti disposizioni in materia di protezione dei dati. Analogamente, un soggetto può essere titolare del trattamento anche laddove non adotti tutte le decisioni in merito alle finalità e ai mezzi. I criteri della contitolarità del trattamento e la misura in cui due o più soggetti esercitano congiuntamente il controllo possono assumere forme diverse, come chiarito di seguito.[13]

### 2.1.4 «Finalità e mezzi»

32. Il quarto elemento costitutivo della definizione di titolare del trattamento fa riferimento all'oggetto dell'influenza esercitata dal titolare stesso,, vale a dire «finalità e mezzi» del trattamento. Ciò rappresenta la parte sostanziale del concetto di titolare del trattamento: quali elementi dovrebbero essere definiti da un soggetto affinché questi possa essere considerato titolare del trattamento.

33. I dizionari definiscono la «finalità» come «un risultato atteso o al quale tendono le azioni pianificate» e «mezzi» come «la modalità con la quale si ottiene un risultato o si raggiunge un fine».

34. Il GDPR stabilisce che i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in un modo che non sia incompatibile con tali finalità. La determinazione delle «finalità» del trattamento e dei «mezzi» per conseguirle riveste pertanto particolare importanza.

[13] Cfr. parte I, sezione 3 («Definizione di contitolari del trattamento»).

35. Determinare le finalità e i mezzi equivale a decidere, rispettivamente, il «perché» e il «come» del trattamento:[14] data un'operazione di trattamento specifica, il titolare del trattamento è il soggetto che ha determinato il *perché* del trattamento (ovverosia «a quale fine» o «per che cosa» viene svolto) e *come* tale obiettivo è raggiunto (ovverosia quali mezzi sono impiegati per conseguirlo). Una persona fisica o giuridica che esercita tale influenza sul trattamento dei dati personali partecipa alla determinazione delle finalità e dei mezzi dello stesso trattamento, conformemente alla definizione di cui all'articolo 4, paragrafo 7, del GDPR.[15]

36. Il titolare del trattamento deve decidere in merito alla finalità e ai mezzi del trattamento come descritto di seguito. Di conseguenza, il titolare del trattamento non può limitarsi alla sola determinazione della finalità: deve anche prendere decisioni in merito ai mezzi del trattamento. Per contro, la parte che agisce in qualità di responsabile del trattamento non può in alcun caso determinarne la finalità.

37. In pratica, se un titolare incarica un responsabile del trattamento di effettuare il trattamento per suo conto, ciò significa spesso che il responsabile del trattamento è in grado di adottare autonomamente determinate decisioni sulle modalità di effettuazione del trattamento in oggetto. L'EDPB riconosce la sussistenza di un certo margine di manovra affinché anche il responsabile del trattamento possa prendere decisioni in relazione al trattamento. In quest'ottica, è necessario fornire orientamenti rispetto al grado **di influenza esercitata** sulla definizione del «perché» e del «come» che comporta l'attribuzione a un soggetto della qualifica di titolare del trattamento nonché rispetto alla misura in cui un responsabile del trattamento possa adottare decisioni in autonomia.

38. Quando un soggetto determina chiaramente le finalità e i mezzi, affidando a un diverso soggetto attività di trattamento che consistono nell'esecuzione delle sue istruzioni dettagliate, la situazione è chiara e non vi sono dubbi che tale diverso soggetto debba essere considerato responsabile del trattamento, mentre il primo è il titolare del trattamento.

*Mezzi essenziali rispetto a mezzi non essenziali*

39. La questione è dove tracciare la linea di demarcazione tra le decisioni riservate al titolare del trattamento e quelle che possono essere lasciate a discrezione del responsabile del trattamento. Le decisioni sulla finalità del trattamento sono chiaramente sempre di competenza del titolare del trattamento.

40. Per quanto concerne la definizione dei mezzi, si può operare una distinzione tra mezzi essenziali e non essenziali. I «mezzi essenziali» sono tradizionalmente e intrinsecamente riservati al titolare del trattamento. Mentre i mezzi non essenziali possono essere determinati anche dal responsabile del trattamento, i mezzi essenziali sono determinati necessariamente dal titolare del trattamento. Per «mezzi essenziali» si intendono i mezzi strettamente legati alla finalità e alla portata del trattamento, tra cui il tipo di dati personali trattati («*quali dati sono trattati*?»), la durata del trattamento («*per quanto tempo sono trattati*?»), le categorie di destinatari («*chi vi ha accesso*?») e le categorie di interessati («*i dati personali di quali individui sono oggetto di trattamento*?»). Insieme alla finalità del trattamento, i mezzi essenziali sono inoltre strettamente connessi alla liceità, necessità e proporzionalità del trattamento stesso. I «mezzi non essenziali» riguardano aspetti più pratici legati all'esecuzione del trattamento, quali la scelta di un particolare tipo di hardware o di software o le misure di sicurezza specifiche in merito alle quali può decidere il responsabile del trattamento.

[14] Cfr. anche le conclusioni dell'avvocato generale Bot nella causa *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2017:796, punto 46.

[15] Sentenza nella causa *testimoni di Geova*, C-25/17, ECLI:EU:C:2018:551, punto 68.

**Esempio: gestione delle buste paga**

Il datore di lavoro A assume un'altra società per gestire il pagamento degli stipendi ai propri dipendenti, impartendo istruzioni chiare su chi pagare, sugli importi, entro quale data, a quale banca, per quanto tempo i dati sono archiviati, quali dati comunicare all'amministrazione fiscale, ecc. In tal caso, il trattamento dei dati è effettuato affinché la società A eroghi gli stipendi ai dipendenti e il responsabile delle buste paga non può utilizzare i dati per finalità proprie. Il modo in cui quest'ultimo dovrebbe effettuare il trattamento è sostanzialmente definito in modo chiaro e rigoroso. Tuttavia, il responsabile delle buste paga può decidere su talune questioni specifiche relative al trattamento, tra cui il software da utilizzare, le modalità di distribuzione dell'accesso all'interno dell'organizzazione ecc. Ciò non altera il suo ruolo di responsabile del trattamento, a condizione che si limiti a trattare i dati in base alle istruzioni impartite dalla società A.

**Esempio: pagamenti bancari**

Nell'ambito delle istruzioni del datore di lavoro A, l'ufficio stipendi trasmette informazioni alla banca B affinché possa effettuare i pagamenti ai dipendenti del datore di lavoro A. Tale attività prevede il trattamento di dati personali da parte della banca B, che essa svolge ai fini dell'esercizio dell'attività bancaria. Nell'ambito di detta attività, la banca decide indipendentemente dal datore di lavoro A quali dati trattare per erogare il servizio, per quanto tempo i dati devono essere archiviati ecc. Il datore di lavoro A non può influire sulla finalità e sui mezzi del trattamento dei dati da parte della banca B. La banca B va pertanto considerata come titolare ai fini del trattamento e la trasmissione dei dati personali da parte dell'ufficio stipendi va considerata come una comunicazione di informazioni tra due titolari del trattamento, dal datore di lavoro A alla banca B.

**Esempio: commercialisti**

Il datore di lavoro A si rivolge inoltre alla società contabile C per la revisione della propria contabilità e pertanto trasferisce i dati relativi alle operazioni finanziarie (compresi i dati personali) a detta società contabile C. Quest'ultima tratta tali dati senza istruzioni dettagliate da parte di A: decide autonomamente, conformemente alle disposizioni di legge disciplinanti i compiti delle attività di revisione che svolge in quanto studio contabile, che i dati raccolti saranno trattati unicamente ai fini della revisione contabile di A e determina i dati di cui ha bisogno, quali categorie di persone registrare, per quanto tempo i dati sono archiviati e i mezzi tecnici da impiegare. In siffatte circostanze, la società contabile C va considerata come titolare del trattamento nell'esecuzione dei servizi di revisione contabile per A. Tuttavia, tale valutazione può differire in base al livello di istruzioni impartite da A. Ove la legge non preveda obblighi specifici per la società contabile e la società cliente fornisca istruzioni molto dettagliate sul trattamento, la società contabile agirebbe di fatto come responsabile del trattamento. Si potrebbe anche distinguere tra una situazione in cui il trattamento è, conformemente alle norme disciplinanti tale professione, effettuato nell'ambito dell'attività principale della società contabile e una diversa situazione in cui il trattamento è un compito accessorio più limitato svolto nell'ambito dell'attività della società cliente.

**Esempio: servizi di hosting**

Il datore di lavoro A ricorre al servizio di hosting H per archiviare dati criptati sui server di H. Il servizio di hosting H non stabilisce se i dati che ospita sono dati personali né tratta i dati in modo diverso dall'archiviazione nei propri server. Poiché l'archiviazione è un esempio di attività di trattamento di

dati personali, il servizio di hosting H tratta dati personali per conto del datore di lavoro A ed è pertanto responsabile del trattamento. Il datore di lavoro A deve impartire le istruzioni necessarie a H e, a norma dell'articolo 28, deve essere concluso un accordo per il trattamento dei dati, con l'obbligo per H di attuare misure tecniche e organizzative di sicurezza. H deve assistere A nel garantire che siano adottate le misure di sicurezza necessarie e notificare ad A i casi di violazione dei dati personali.

41. Anche se le decisioni sui mezzi non essenziali possono essere lasciate al responsabile del trattamento, il titolare del trattamento deve comunque stabilire determinati elementi nell'accordo sul trattamento dei dati quali, ad esempio, in relazione al requisito della sicurezza, l'istruzione di adottare tutte le misure richieste a norma dell'articolo 32 del GDPR. L'accordo deve inoltre prevedere che il responsabile del trattamento assista il titolare nel garantire, ad esempio, l'adempimento degli obblighi di cui all'articolo 32. In ogni caso, il titolare del trattamento rimane responsabile dell'attuazione di misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento (articolo 24). Nel far ciò, il titolare del trattamento deve tenere conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e per le libertà delle persone fisiche. Per tale motivo, il titolare del trattamento deve essere pienamente informato dei mezzi utilizzati, in modo da poter adottare una decisione in merito con cognizione di causa. Affinché il titolare del trattamento possa dimostrare la liceità dello stesso è consigliabile documentare quanto meno le misure tecniche e organizzative necessarie nel contratto o in un altro strumento giuridicamente vincolante tra il titolare e il responsabile del trattamento.

**Esempio: call center**

La società X decide di esternalizzare una parte del servizio clienti a un call center, che quindi riceve dati identificabili sugli acquisti dei clienti nonché informazioni di contatto. Il call center utilizza il proprio software e la propria infrastruttura informatica per gestire i dati personali relativi ai clienti della società X. La società X firma un accordo di trattamento con il fornitore dei servizi di call center, a norma dell'articolo 28 del GDPR, dopo aver stabilito che le misure di sicurezza tecniche e organizzative proposte dal call center stesso sono adeguate ai rischi in questione e che i dati personali saranno trattati unicamente per le finalità della società X e conformemente alle istruzioni della stessa. La società X non impartisce ulteriori istruzioni al call center in merito al software specifico da utilizzare né istruzioni dettagliate sulle misure di sicurezza specifiche da mettere in atto. In questo esempio, la società X rimane titolare del trattamento, nonostante il call center abbia definito determinati mezzi non essenziali del trattamento in questione.

### 2.1.5 «Del trattamento dei dati personali»

42. Le finalità e i mezzi determinati dal titolare devono riguardare il «trattamento dei dati personali». L'articolo 4, paragrafo 2, del GDPR definisce il trattamento dei dati personali come «*qualsiasi operazione o insieme di operazioni [...] applicate a dati personali o insiemi di dati personali*». Di conseguenza, il concetto di titolare del trattamento può essere collegato a una singola operazione di trattamento o a una serie di operazioni. In pratica, ciò può significare che il controllo esercitato da un determinato soggetto può estendersi alla totalità del trattamento in questione, ma può anche essere limitato a una fase specifica dello stesso.[16]

[16] Sentenza *Fashion ID* (C-40/17, ECLI:EU:C:2019:629, punto 74): «*Ne consegue, come rilevato, in sostanza, dall'avvocato generale [...] che una persona fisica o giuridica risulta poter essere responsabile, ai sensi dell'articolo 2, lettera d), della direttiva 95/46, insieme ad altri, soltanto delle operazioni di trattamento di dati personali di cui essa determina congiuntamente le finalità e gli strumenti. Per contro, [...] tale persona fisica o*

43. In pratica, un trattamento di dati personali che coinvolge più soggetti può essere suddiviso in più operazioni di trattamento per ciascuna delle quali ognuno di tali soggetti potrebbe essere considerato titolare, ossia colui che determina la finalità e i mezzi nel singolo caso. D'altro canto, una sequenza o un insieme di trattamenti che coinvolgono più soggetti possono avere luogo anche per la/le medesima/e finalità; in tal caso è possibile che il trattamento coinvolga uno o più contitolari . In altre parole, è possibile che a «livello micro» le diverse operazioni di trattamento della catena appaiano scollegate, in quanto ciascuna di esse può avere una finalità diversa. Tuttavia, è necessario un doppio controllo atto a verificare se, a «livello macro», queste operazioni di trattamento non debbano essere considerate come un «insieme di operazioni» che perseguono una finalità comune mediante mezzi definiti congiuntamente.

44. Chiunque decida di trattare dati deve valutare se questi comprendano dati personali e, in caso affermativo, quali siano gli obblighi previsti dal GDPR. Un soggetto sarà considerato «titolare del trattamento» anche se non tratta deliberatamente dati personali in quanto tali o se ha ritenuto, erroneamente, di non trattare dati personali.

45. Non è necessario che il titolare abbia effettivamente accesso ai dati oggetto del trattamento.[17] Un soggetto che esternalizzi un'attività di trattamento e in tal modo eserciti un'influenza determinante sulla finalità e sui mezzi (essenziali) del trattamento stesso (ad esempio configurando i parametri di un servizio in modo tale da definire quali dati personali debbano essere trattati) è da ritenersi il titolare del trattamento anche se non avrà mai accesso effettivo ai dati.

**Esempio: ricerche di mercato 1**

La società ABC desidera sapere quali tipi di consumatori sono maggiormente interessati ai suoi prodotti e stipula un contratto con il fornitore di servizi XYZ per ottenere informazioni pertinenti.

ABC informa XYZ in merito alle tipologie di informazioni che la interessano e fornisce un elenco di domande da porre ai partecipanti alla ricerca di mercato.

ABC riceve da XYZ solo informazioni statistiche (ad esempio, l'identificazione delle tendenze dei consumatori per regione) e non ha accesso ai dati personali. Tuttavia, la società ABC ha deciso che il trattamento doveva aver luogo, il trattamento è effettuato per le sue finalità e attività e la società ABC ha fornito a XYZ istruzioni dettagliate sulle informazioni da raccogliere. ABC va pertanto ancora considerata titolare del trattamento dei dati personali che ha luogo al fine di fornire le informazioni richieste. XYZ può trattare i dati solo per la finalità indicata dalla società ABC e secondo le sue istruzioni dettagliate e va pertanto considerata come responsabile del trattamento.

**Esempio: ricerche di mercato 2**

La società ABC desidera sapere quali tipi di consumatori sono maggiormente interessati ai suoi prodotti. Il fornitore di servizi XYZ è un'agenzia di ricerche di mercato che ha raccolto informazioni sugli interessi dei consumatori attraverso una serie di questionari relativi a un'ampia gamma di prodotti e servizi. XYZ ha raccolto e analizzato tali dati in modo indipendente, secondo la propria metodologia, senza ricevere istruzioni dalla società ABC. Per rispondere alla richiesta della società ABC, il fornitore di servizi XYZ genera informazioni statistiche, senza tuttavia ricevere ulteriori istruzioni su quali dati

*giuridica non può essere considerata responsabile, ai sensi di detta disposizione, delle operazioni anteriori o successive della catena di trattamento di cui essa non determina né le finalità né gli strumenti».*

[17] Sentenza nella causa *Wirtschaftsakademie*, C-201/16, ECLI:EU:c:2018:388, punto 38.

personali vadano trattati o su come trattarli al fine di generare tali statistiche. In questo esempio, il fornitore di servizi XYZ agisce in qualità di titolare unico del trattamento, trattando i dati personali ai fini della ricerca di mercato e determinando autonomamente i mezzi per attuarla. Ai sensi della normativa in materia di protezione dei dati la società ABC non ha alcun ruolo o responsabilità particolari in relazione a tali attività di trattamento, in quanto riceve statistiche anonimizzate e non è coinvolta nella determinazione delle finalità e dei mezzi del trattamento.

# 3 DEFINIZIONE DI CONTITOLARI DEL TRATTAMENTO

## 3.1 Definizione di contitolari del trattamento

46. La contitolarità di trattamento può configurarsi laddove più di un soggetto sia coinvolto nel trattamento.

47. Sebbene il concetto non sia nuovo e già esistesse ai sensi della direttiva 95/46/CE, il GDPR introduce all'articolo 26 norme specifiche per i contitolari del trattamento e stabilisce un quadro per disciplinarne le relazioni. Inoltre, in sentenze recenti la Corte di giustizia dell'Unione europea (CGUE) ha apportato chiarimenti su questo concetto e sulle sue implicazioni.[18]

48. Come ulteriormente precisato nella parte II, sezione 2, la qualifica di contitolari del trattamento avrà principalmente conseguenze in termini di ripartizione degli obblighi di rispetto delle norme in materia di protezione dei dati e, in particolare, per quanto concerne i diritti delle persone fisiche.

49. In tale prospettiva, la sezione seguente mira a fornire orientamenti sul concetto di contitolari del trattamento, ai sensi del GDPR e della giurisprudenza della Corte di giustizia dell'Unione europea, al fine di contribuire alla definizione dei casi ove si sia in presenza di contitolarità nonché all'applicazione concreta di tale nozione.

## 3.2 Esistenza di una contitolarità del trattamento

### 3.2.1 Considerazioni generali

50. La definizione di titolare del trattamento di cui all'articolo 4, paragrafo 7, del GDPR costituisce il punto di partenza per determinare la contitolarità del trattamento. Le considerazioni di cui alla presente sezione sono pertanto direttamente collegate a quelle di cui alla sezione sul concetto di titolare del trattamento e le integrano. Di conseguenza, la valutazione della contitolarità del trattamento dovrebbe essere speculare a quella concernente la titolarità «unica» di cui sopra.

51. L'articolo 26 del GDPR, che rispecchia la definizione di cui all'articolo 4, paragrafo 7, dello stesso regolamento, stabilisce che *«allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento.»* In termini generali, sussiste una contitolarità del trattamento in relazione a una specifica attività di trattamento quando soggetti diversi determinano *congiuntamente* la finalità e i mezzi di tale attività di trattamento. Pertanto, per valutare l'esistenza di contitolari del trattamento è necessario esaminare se la determinazione delle

[18] Cfr., in particolare, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein contro Wirtschaftsakademie*, (C-210/16), *Tietosuojavaltuutettu contro Jehovan todistajat – uskonnollinen yhdyskunta* (C-25/17), *Fashion ID GmbH & Co. KG contro Verbraucherzentrale NRW eV* (C-40/17). Va osservato che, sebbene tali sentenze siano state rese dalla CGUE sull'interpretazione del concetto di contitolari del trattamento ai sensi della direttiva 95/46/CE esse restano valide nell'ambito del GDPR, dato che gli elementi che determinano tale concetto, ai sensi del GDPR, rimangono invariati rispetto a quelli previsti dalla direttiva.

finalità e dei mezzi che è prerogativa del titolare del trattamento sia appannaggio di più di un solo soggetto. Il termine «congiuntamente» deve essere interpretato nel senso di «insieme con» o «non isolatamente», in diverse forme e combinazioni, come spiegato nel prosieguo.

52. La valutazione della contitolarità del trattamento dovrebbe essere fondarsi su di un'analisi fattuale, piuttosto che formale, dell'influenza effettivamente esercitata sulle finalità e sui mezzi del trattamento. Qualsivoglia configurazione esistente o prevista dovrebbe essere verificata alla luce delle circostanze concretamente relative al rapporto tra le parti. Un criterio meramente formale non sarebbe sufficiente per almeno due motivi: in taluni casi, la designazione formale di un contitolare del trattamento, prevista ad esempio ai sensi di legge o da un contratto, potrebbe mancare; in altri casi, può risultare che la designazione formale non rispecchi la realtà dei meccanismi in atto, poiché si attribuisce formalmente il ruolo di titolare del trattamento a un soggetto che di fatto non è in grado di «determinare» le finalità e i mezzi del trattamento.

53. Non tutti i trattamenti che coinvolgono più soggetti danno luogo a una contitolarità del trattamento. Il criterio generale per la sussistenza della contitolarità del trattamento è la **partecipazione congiunta di due o più soggetti alla determinazione delle finalità e dei mezzi** dello stesso. Più specificamente, la partecipazione congiunta deve comprendere, da un lato, la determinazione delle finalità e, dall'altro, la determinazione dei mezzi. Se ciascuno di questi elementi è determinato da tutti i soggetti coinvolti, questi ultimi dovrebbero essere considerati contitolari del trattamento in questione.

### 3.2.2 Valutazione della partecipazione congiunta

54. La partecipazione congiunta nella determinazione delle finalità e dei mezzi implica che più soggetti esercitino un'influenza determinante sull'effettuazione del trattamento e sulle relative modalità. In pratica, la partecipazione congiunta può assumere diverse forme, come, ad esempio, quella di una **decisione comune** presa da due o più soggetti, oppure derivare da **decisioni convergenti** di due o più soggetti per quanto concerne le finalità e i mezzi essenziali.

55. La partecipazione congiunta mediante una *decisione comune* implica l'assunzione di una decisione e un'intenzione condivisa di adottare tale decisione, in base all'interpretazione più corrente del termine «congiuntamente» di cui all'articolo 26 del GDPR.

La situazione della partecipazione congiunta attraverso *decisioni convergenti* deriva in particolare dalla giurisprudenza della CGUE sul concetto di contitolari del trattamento. Le decisioni possono essere considerate convergenti sulle finalità e sui mezzi **se si integrano a vicenda e se sono necessarie affinché il trattamento abbia luogo, in modo tale da avere un impatto tangibile sulla determinazione delle finalità e dei mezzi del trattamento**. Occorre sottolineare che il concetto di decisioni convergenti va considerato in relazione alle finalità e ai mezzi del trattamento, ma non con riguardo ad altri aspetti del rapporto commerciale tra le parti.[19] In tal senso, un criterio importante per individuare decisioni convergenti in questo ambito **consiste nel verificare se il trattamento non sarebbe possibile senza la partecipazione di entrambe le parti alle finalità e ai mezzi, nel senso che i trattamenti di ciascuna parte sono tra loro indissociabili, ovverosia indissolubilmente legati**. La situazione in cui contitolari del trattamento agiscono sulla base di decisioni convergenti dovrebbe tuttavia essere distinta da quella del responsabile del trattamento, poiché quest'ultimo, pur partecipando all'esecuzione dello stesso, non tratta i dati per le proprie finalità ma per conto del relativo titolare.

[19] In effetti, tutti gli accordi commerciali comportano la convergenza delle decisioni nell'ambito del processo mediante il quale viene raggiunto un accordo.

56. Il fatto che una delle parti non abbia accesso ai dati personali trattati non è sufficiente per escludere la contitolarità del trattamento.[20] Ad esempio, nella causa *Testimoni di Geova* la CGUE ha ritenuto che una comunità religiosa dovesse essere considerata titolare, insieme ai suoi membri praticanti la predicazione, del trattamento dei dati personali effettuato da questi ultimi nell'ambito della predicazione porta a porta.[21] La CGUE ha ritenuto che non fosse necessario che la comunità avesse accesso ai dati in questione né stabilire che avesse fornito ai suoi membri linee guida o istruzioni scritte in relazione al trattamento di dati.[22] La comunità ha partecipato alla determinazione delle finalità e dei mezzi organizzando e coordinando le attività dei propri membri, il che ha contribuito al perseguimento dell'obiettivo della stessa comunità dei Testimoni di Geova.[23] Inoltre, la comunità era a conoscenza, a livello generale, del fatto che tale trattamento veniva effettuato al fine di diffondere il proprio credo.[24]

57. È altresì importante sottolineare, come chiarito dalla CGUE, che un soggetto sarà considerato contitolare del trattamento insieme ad altri solo per quelle operazioni rispetto alle quali determina, insieme ad altri, i mezzi e le finalità di quello stesso trattamento dei dati, in particolare in caso di decisioni convergenti. Se uno dei soggetti in questione decide isolatamente le finalità e i mezzi delle operazioni precedenti o successive nelle varie fasi del trattamento, tale soggetto deve essere considerato l'unico titolare di tale operazione di trattamento precedente o successiva.[25]

58. L'esistenza di una responsabilità congiunta non implica necessariamente pari responsabilità dei vari operatori coinvolti nel trattamento dei dati personali. Al contrario, la CGUE ha chiarito che tali operatori possono essere coinvolti in fasi diverse di tale trattamento e in misura diversa, cosicché il livello di responsabilità di ciascuno di essi deve essere valutato alla luce di tutte le circostanze pertinenti del caso di specie.

#### *3.2.2.1 Determinazione congiunta delle finalità*

59. Una contitolarità del trattamento sussiste allorquando soggetti coinvolti nel medesimo trattamento lo effettuano per finalità definite congiuntamente. Ciò avviene se i soggetti in questione trattano i dati per le medesime finalità o per finalità comuni.

60. Inoltre, laddove tali soggetti non perseguano la medesima finalità in relazione al trattamento, alla luce della giurisprudenza della Corte di giustizia dell'Unione europea la contitolarità del trattamento può configurarsi anche qualora i soggetti perseguano finalità strettamente collegate o complementari. Ciò può verificarsi, ad esempio, quando esiste un vantaggio reciproco derivante dalla medesima operazione di trattamento, a condizione che ciascuno dei soggetti coinvolti partecipi alla determinazione delle finalità e dei mezzi del trattamento in questione. Tuttavia, il concetto di vantaggio reciproco non è decisivo e ha valore puramente indicativo. In *Fashion ID*, ad esempio, la CGUE ha chiarito che un gestore di siti web partecipa alla determinazione delle finalità (e dei mezzi) del trattamento inserendo un «plug-in social» su un sito web, al fine di ottimizzare la pubblicità dei propri prodotti rendendoli più visibili sul social network. La CGUE ha ritenuto che le operazioni di

[20] Sentenza nella causa *Wirtschaftsakademie*, C-210/16, ECLI:EU:c:2018:388, punto 38.
[21] Sentenza nella causa *testimoni di Geova*, C-25/17, ECLI:EU:C:2018:551, punto 75.
[22] Ibidem.
[23] Ibidem, punto 71.
[24] Ibidem.
[25] Sentenza nella causa *Fashion ID*, C-40/17, ECLI:EU:2018:1039, punto 74: «*Per contro, e fatta salva un'eventuale responsabilità civile prevista dal diritto nazionale a tal riguardo, tale persona fisica o giuridica non può essere considerata responsabile, ai sensi di detta disposizione, delle operazioni anteriori o successive della catena di trattamento di cui essa non determina né le finalità né gli strumenti*».

trattamento in questione fossero effettuate nell'interesse economico sia dell'operatore del sito internet che del fornitore del plug-in social.[26]

61. Analogamente, come rilevato dalla CGUE nella causa *Wirtschaftsakademie*, il trattamento di dati personali mediante statistiche dei visitatori di una «fanpage» mira a consentire a Facebook di migliorare il sistema di pubblicità trasmessa attraverso la propria rete e consente al gestore della fanpage di ottenere statistiche per gestire la promozione della propria attività.[27] In tal caso ogni soggetto persegue il proprio interesse, ma per quanto concerne i visitatori della fanpage entrambi partecipano alla determinazione delle finalità (e dei mezzi) del trattamento dei dati personali.[28]

62. A tale riguardo, è importante sottolineare che la semplice esistenza di un vantaggio reciproco (ad esempio di natura commerciale), derivante da un'attività di trattamento, non comporta una contitolarità del trattamento. Se il soggetto coinvolto nel trattamento non persegue alcuna finalità propria in relazione allo stesso, ma viene semplicemente remunerato per i servizi prestati, esso agisce in qualità di responsabile del trattamento anziché di contitolare.

#### *3.2.2.2 Determinazione congiunta dei mezzi*

63. La contitolarità del trattamento prevede, inoltre, che due o più soggetti abbiano esercitato un'influenza sui mezzi del trattamento. Ciò non significa che, affinché sussista una contitolarità del trattamento, ciascun soggetto coinvolto debba in ogni caso determinarne tutti i mezzi. Di fatto, come chiarito dalla CGUE, soggetti diversi possono essere coinvolti in fasi diverse del trattamento e a livelli diversi. I diversi contitolari del trattamento possono pertanto determinare i mezzi del trattamento in misura diversa, a seconda di chi sia effettivamente in grado di effettuare tale determinazione.

64. Può anche accadere che uno dei soggetti coinvolti fornisca i mezzi del trattamento e li metta a disposizione per le attività di trattamento dei dati personali da parte di altri soggetti. Anche il soggetto che decide di avvalersi di tali mezzi affinché i dati personali possano essere trattati per una determinata finalità partecipa alla determinazione dei mezzi del trattamento.

65. Tale situazione può verificarsi, in particolare, nel caso di piattaforme, strumenti standardizzati o di altre infrastrutture che consentono alle parti di trattare gli stessi dati personali e che sono stati predisposti in un certo modo da una delle parti per essere utilizzati da altre che possono anche decidere come impostarli.[29] L'uso di un sistema tecnico già esistente non esclude la contitolarità del trattamento laddove gli utenti del sistema possano decidere in merito al trattamento dei dati personali da effettuare in tale contesto.

66. A titolo di esempio, nella sentenza *Wirtschaftsakademie* la CGUE ha statuito che, nel definire i parametri basati sul pubblico destinatario e sugli obiettivi di gestione e promozione delle proprie attività, l'amministratore di una «fanpage» su Facebook dovesse essere considerato come un soggetto che partecipa alla determinazione dei mezzi di trattamento dei dati personali dei relativi visitatori.

67. Inoltre, la scelta da parte di un soggetto di utilizzare per le proprie finalità uno strumento o un altro sistema sviluppato da altri per il trattamento di dati personali costituirà probabilmente una decisione congiunta sui mezzi di tale trattamento da parte dei soggetti in questione. Ciò risulta dalla causa Fashion ID, in cui la CGUE ha concluso che, inserendo nel proprio sito internet il pulsante Facebook

[26] Sentenza nella causa *Fashion ID*, C-40/17, ECLI:EU: 2018:1039, punto 80.
[27] Sentenza nella causa *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, punto 34.
[28] Sentenza nella causa *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, punto 39.
[29] Il fornitore del sistema può essere contitolare del trattamento se sono soddisfatti i criteri di cui sopra, ossia se partecipa alla determinazione delle finalità e dei mezzi. In caso contrario, il fornitore dovrebbe essere considerato responsabile del trattamento.

Like, messo da Facebook a disposizione degli operatori di siti web, Fashion ID ha esercitato un'influenza determinante sulle operazioni che comportano la raccolta e la trasmissione dei dati personali dei visitatori del suo sito internet a Facebook e ha pertanto determinato, congiuntamente con Facebook, i mezzi di tale trattamento.[30]

68. È importante sottolineare che **l'uso di un sistema o di un'infrastruttura comuni per il trattamento dei dati non comporterà in tutti i casi la contitolarità del trattamento da parte dei soggetti coinvolti,** in particolare allorquando il trattamento da essi effettuato è scindibile e potrebbe essere eseguito da un soggetto senza l'intervento dell'altro, o se il fornitore è un responsabile del trattamento che non persegue una finalità propria (l'esistenza di un mero vantaggio commerciale per le parti coinvolte non è sufficiente a configurare una finalità di trattamento).

**Esempio: agenzia di viaggi**

Un'agenzia di viaggi invia alla compagnia aerea e a una catena di alberghi i dati personali dei propri clienti, al fine di effettuare prenotazioni per un pacchetto turistico. La compagnia aerea e l'albergo confermano la disponibilità dei posti e delle camere richiesti. L'agenzia di viaggi rilascia ai clienti i documenti di viaggio e i buoni. Ciascuno dei soggetti tratta i dati per svolgere le proprie attività e utilizzando i propri mezzi. In questo caso, l'agenzia di viaggi, la compagnia aerea e l'albergo sono tre distinti titolari del trattamento che perseguono finalità autonome e separate e non sussiste una contitolarità del trattamento.

L'agenzia di viaggi, la catena alberghiera e la compagnia aerea decidono poi di partecipare congiuntamente alla creazione di una piattaforma comune su internet per la finalità comune di offrire pacchetti turistici. Concordano i mezzi essenziali da utilizzare, quali i dati da archiviare, le modalità di assegnazione e conferma delle prenotazioni e chi può avere accesso alle informazioni memorizzate. Inoltre, decidono di condividere i dati dei clienti al fine di effettuare operazioni di marketing congiunte. In questo caso, l'agenzia di viaggi, la compagnia aerea e la catena alberghiera determinano congiuntamente le finalità e le modalità di trattamento dei dati personali dei rispettivi clienti e saranno pertanto contitolari del trattamento per quanto riguarda le operazioni di trattamento relative alla piattaforma comune di prenotazione via internet e le operazioni congiunte di marketing. Tuttavia, ciascuna di esse manterrebbe la titolarità esclusiva di altre attività di trattamento svolte al di fuori della piattaforma comune su internet.

**Esempio: progetto di ricerca da parte di più istituti**

Diversi istituti di ricerca decidono di partecipare a un progetto comune specifico e di utilizzare a tal fine la piattaforma esistente di uno di essi. Ai fini della ricerca congiunta ciascun istituto alimenta la piattaforma con i dati personali che detiene e utilizza i dati forniti da altri attraverso la piattaforma per svolgere l'attività di ricerca. In questo caso, tutti gli istituti si qualificano come contitolari del trattamento dei dati personali svolto mediante l'archiviazione e la divulgazione di informazioni provenienti dalla piattaforma, in quanto hanno deciso congiuntamente la finalità del trattamento e i mezzi da utilizzare (la piattaforma esistente). Tuttavia, ciascuno degli istituti è un titolare autonomo rispetto a qualsivoglia trattamento effettuato al di fuori della piattaforma per proprie finalità.

**Esempio: operazione di marketing**

[30] Sentenza nella causa Fashion ID, C-40/17, ECLI:EU:2018:1039, punti 77-79.

Le società A e B hanno lanciato un prodotto con il marchio comune C e desiderano organizzare un evento per promuovere tale prodotto. A tal fine decidono di condividere dati tratti dai rispettivi database della clientela esistente e potenziale e su tale base decidono in merito all'elenco degli invitati all'evento. Concordano inoltre le modalità di invio degli inviti all'evento, le modalità di raccolta dei riscontri durante lo stesso e il follow-up delle operazioni di marketing. Le società A e B possono essere considerate contitolari del trattamento dei dati personali relativo all'organizzazione dell'evento promozionale in quanto decidono congiuntamente, in tale contesto, in merito alla determinazione congiunta della finalità e dei mezzi essenziali del trattamento.

**Esempio: sperimentazioni cliniche**[31]

Un prestatore di assistenza sanitaria (lo sperimentatore) e un'università (lo sponsor) decidono di avviare congiuntamente una sperimentazione clinica avente la medesima finalità. Collaborano all'elaborazione del protocollo di studio (ossia finalità, metodologia/progettazione dello studio, dati da raccogliere, criteri di esclusione/inclusione dei soggetti, riutilizzo delle banche dati, se del caso, ecc.). Possono essere considerati contitolari del trattamento per detta sperimentazione clinica in quanto stabiliscono e concordano congiuntamente una stessa finalità e i mezzi essenziali del trattamento. La raccolta di dati personali dalla cartella clinica del paziente ai fini di ricerca va distinta dalla conservazione e dall'uso degli stessi dati ai fini dell'assistenza del paziente, per i quali il fornitore di assistenza sanitaria rimane titolare del trattamento.

Nel caso in cui lo sperimentatore non partecipi alla stesura del protocollo (in quanto accetta semplicemente il protocollo già elaborato dallo sponsor) e il protocollo sia elaborato solo dallo sponsor, ai fini della sperimentazione clinica il ricercatore dovrebbe essere considerato responsabile del trattamento e lo sponsor il titolare del trattamento.

**Esempio: agenzie di selezione di personale («*headhunters*»)**

La società X aiuta la società Y ad assumere nuovo personale mediante il suo famoso servizio a valore aggiunto «global matchz». La società X cerca candidati idonei sia tra i CV ricevuti direttamente dalla società Y che tra quelli già presenti nella propria banca dati. Tale banca dati è creata e gestita dalla sola società X. Così facendo la società X può migliorare la corrispondenza tra offerte e richieste di lavoro, incrementando le entrate. Sebbene non abbiano formalmente assunto una decisione congiunta, le società X e Y partecipano congiuntamente al trattamento, al fine di individuare candidati idonei sulla base di decisioni convergenti: la decisione di creare e di gestire il servizio «global matchz» per la società X, e la decisione della società Y di arricchire la banca dati con i CV che riceve direttamente. Tali decisioni si integrano reciprocamente, sono indissociabili e necessarie per il trattamento connesso alla ricerca di candidati idonei. Pertanto, in questo caso particolare, X e Y dovrebbero essere considerate contitolari di tale trattamento. Tuttavia, la società X è l'unico titolare del trattamento necessario per la gestione della propria banca dati e la società Y è l'unico titolare del successivo trattamento di assunzione per le proprie finalità (organizzazione dei colloqui, conclusione del contratto e gestione dei dati delle risorse umane).

**Esempio: analisi dei dati sanitari**

[31] L'EDPB prevede di fornire ulteriori orientamenti in relazione alle sperimentazioni cliniche nel contesto delle prossime linee guida sul trattamento dei dati personali a fini medici e di ricerca scientifica.

La società ABC, che ha sviluppato un'applicazione per il monitoraggio della pressione sanguigna, e la società XYZ, fornitore di applicazioni per professionisti del settore medico, desiderano esaminare in che modo le variazioni della pressione sanguigna possano contribuire a prevedere determinate malattie. Le società decidono di avviare un progetto comune e di coinvolgere anche l'ospedale DEF.

I dati personali che saranno trattati nell'ambito del progetto sono quelli che la società ABC, l'ospedale DEF e la società XYZ trattano separatamente in quanto titolari autonomi di trattamento. La decisione di trattare i dati per valutare le variazioni di pressione sanguigna è presa congiuntamente dai tre soggetti. La società ABC, l'ospedale DEF e la società XYZ hanno stabilito congiuntamente le finalità del trattamento. La società XYZ prende l'iniziativa di proporre i mezzi essenziali del trattamento. Sia la società ABC che l'ospedale DEF approvano detti mezzi essenziali dopo essere stati anch'essi coinvolti nello sviluppo di alcune caratteristiche dell'applicazione, in modo tale da poterne utilizzare i risultati in misura sufficiente. I tre soggetti convengono quindi di perseguire una finalità comune per il trattamento, ossia valutare in che modo le variazioni della pressione sanguigna possano contribuire alla previsione di determinate malattie. Una volta completata la ricerca, la società ABC, l'ospedale DEF e la società XYZ potranno beneficiare della valutazione utilizzando i risultati nell'ambito delle rispettive attività. Per tutti questi motivi, essi si qualificano come contitolari di tale specifico trattamento congiunto.

Se la società XYZ fosse stata semplicemente invitata dalle altre a effettuare tale valutazione senza avere alcuna finalità propria e trattando i dati per conto delle altre, essa si qualificherebbe come responsabile del trattamento anche qualora fosse stata incaricata della determinazione dei mezzi non essenziali di tale trattamento.

### 3.2.3 Situazioni in cui non sussiste contitolarità del trattamento

69. Il fatto che più soggetti siano coinvolti nello stesso trattamento non significa che essi agiscano necessariamente in qualità di contitolari del trattamento. Non tutti i tipi di partenariato, cooperazione o collaborazione implicano la qualifica di contitolari del trattamento, in quanto è necessaria un'analisi caso per caso di ciascun trattamento in questione e del ruolo preciso svolto da ciascun soggetto in relazione a tale trattamento. I casi che seguono forniscono esempi non esaustivi di situazioni in cui non sussiste contitolarità del trattamento.

70. Ad esempio, lo scambio degli stessi dati o insiemi di dati tra due soggetti in assenza di finalità o mezzi di trattamento determinati congiuntamente dovrebbe essere considerato una trasmissione di dati tra titolari del trattamento distinti.

**Esempio: trasmissione dei dati dei dipendenti alle autorità fiscali**

Una società raccoglie e tratta i dati personali dei propri dipendenti allo scopo di gestire le retribuzioni, le assicurazioni malattia ecc. La legge impone alla società l'obbligo di inviare alle autorità fiscali tutti i dati relativi alle retribuzioni, al fine di un controllo fiscale più accurato.

In questo caso, anche se tanto la società quanto le autorità fiscali trattano gli stessi dati relativi alle retribuzioni, la mancanza di una determinazione congiunta della finalità e dei mezzi riferiti a tale trattamento dei dati porterà a qualificare i due soggetti come titolari distinti del trattamento dei dati.

71. La contitolarità del trattamento può essere esclusa anche nel caso in cui più soggetti utilizzino una banca dati condivisa o un'infrastruttura comune, qualora ciascuna di esse determini autonomamente le proprie finalità.

**Esempio: operazioni commerciali all'interno di un gruppo societario che utilizza una banca dati condivisa**

Un gruppo di società utilizza la stessa banca dati per la gestione dei clienti (esistenti e potenziali). La banca dati è ospitata sui server della società controllante, che agisce pertanto da responsabile del trattamento delle controllate per quanto riguarda l'archiviazione dei dati. Ciascun soggetto appartenente al gruppo inserisce i dati dei propri clienti (esistenti e potenziali) e li elabora esclusivamente per le proprie finalità. Inoltre, ciascun soggetto decide autonomamente in merito all'accesso, ai periodi di archiviazione, alla rettifica o alla cancellazione dei dati dei propri clienti e potenziali tali, senza potere accedere ai dati degli altri partecipanti o utilizzarli. Il semplice fatto che tali società utilizzino una banca dati condivisa non comporta, di per sé, una contitolarità del trattamento. In siffatte circostanze, ciascuna società è pertanto un titolare del trattamento distinto.

**Esempio: titolari indipendenti che utilizzano un'infrastruttura condivisa**

La società XYZ ospita una banca dati e la mette a disposizione di altre società per il trattamento e l'archiviazione dei dati personali relativi ai dipendenti di tali altre società. La società XYZ è un responsabile del trattamento in quanto tratta e archivia i dati dei dipendenti di altre società per conto e secondo le istruzioni di queste ultime. Inoltre, le altre società trattano i dati senza alcuna partecipazione da parte della società XYZ e per finalità che non sono in alcun modo condivise da quest'ultima.

72. Vi possono essere altresì situazioni in cui vari soggetti trattano successivamente gli stessi dati personali in una catena di operazioni: ciascuno di essi ha una finalità indipendente e impiega mezzi indipendenti relativamente al segmento della catena di rispettiva competenza. In mancanza di una partecipazione congiunta nella determinazione delle finalità e dei mezzi di una stessa operazione di trattamento o dello stesso insieme di operazioni di trattamento, la contitolarità deve essere esclusa e i vari soggetti devono essere considerati come titolari del trattamento indipendenti che agiscono in momenti successivi.

**Esempio: analisi statistica per un compito di interesse pubblico**

Un'autorità pubblica (autorità A) ha il compito stabilito per legge di elaborare analisi e statistiche sull'evoluzione del tasso di occupazione nel paese. A tal fine, numerosi altri soggetti pubblici sono tenuti per legge a comunicare dati specifici all'autorità A, che decide di utilizzare un sistema specifico per trattare i dati, ivi compresa la raccolta. Ciò significa fra l'altro che le altre autorità pubbliche sono obbligate a utilizzare tale sistema per la comunicazione dei dati. In questo caso, fatta salva l'eventuale attribuzione dei ruoli per legge, l'autorità A sarà l'unico titolare del trattamento ai fini dell'analisi e delle statistiche del tasso di occupazione attraverso il sistema, in quanto determina la finalità del trattamento e ha deciso in merito alla modalità di organizzazione dello stesso. Naturalmente, gli altri soggetti pubblici, in quanto titolari delle rispettive attività di trattamento, hanno la responsabilità di garantire l'esattezza dei dati da essi precedentemente trattati e successivamente comunicati all'autorità A.

# 4 DEFINIZIONE DI RESPONSABILE DEL TRATTAMENTO

73. L'articolo 4, paragrafo 8, definisce il responsabile del trattamento come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. Analogamente alla definizione di titolare del trattamento, la definizione di responsabile

del trattamento prevede un'ampia gamma di soggetti: può trattarsi di *una persona fisica o giuridica, un'autorità pubblica, un servizio o un altro organismo*. Ciò significa che, in linea di principio, non vi sono limitazioni riguardo alle caratteristiche soggettive del responsabile del trattamento. Potrebbe trattarsi di un'organizzazione, ma anche di un singolo.

74. Il GDPR stabilisce obblighi direttamente e specificamente applicabili ai responsabili del trattamento, come meglio illustrato nella parte II, sezione 1, delle presenti linee guida. Il responsabile del trattamento può essere ritenuto responsabile o sanzionato in caso di inadempimento di detti obblighi o qualora agisca al di fuori o in contrasto con le istruzioni legittime del titolare del trattamento.

75. Il trattamento dei dati personali può coinvolgere più responsabili. Ad esempio, un titolare del trattamento può decidere di utilizzare direttamente più responsabili del trattamento, coinvolgendone diversi in fasi separate dello stesso (molteplici responsabili del trattamento). Un titolare del trattamento potrebbe anche decidere di rivolgersi a un solo responsabile del trattamento che, a sua volta, previa autorizzazione dello stesso titolare, utilizza uno o più responsabili del trattamento («sub-responsabili»). L'attività affidata al responsabile del trattamento può essere limitata a un compito o a un contesto molto specifico o può essere di natura più generale e ampia.

76. Le due condizioni fondamentali per la qualifica di responsabile del trattamento sono:

    a) essere un *soggetto distinto* rispetto al titolare del trattamento;

    b) trattare i dati personali *per conto del titolare del trattamento*.

77. *Un soggetto distinto* significa che il titolare del trattamento decide di delegare tutte o parte delle attività di trattamento a un soggetto esterno. All'interno di un gruppo di società, una di esse può essere responsabile del trattamento di un'altra che agisce in qualità di titolare del trattamento, in quanto le due società sono entità distinte. Di converso, un dipartimento all'interno di una società non può essere responsabile del trattamento per conto di un altro dipartimento all'interno della stessa società.

78. Se il titolare del trattamento decide di trattare direttamente i dati utilizzando le proprie risorse interne, ad esempio attraverso il proprio personale, non vi sono responsabili del trattamento. I dipendenti e le altre persone che agiscono sotto l'autorità diretta del titolare del trattamento, come il personale assunto temporaneamente, non vanno considerati responsabili del trattamento poiché trattano dati personali in quanto parte della struttura del titolare del trattamento. Conformemente all'articolo 29, essi sono altresì vincolati dalle istruzioni del suddetto titolare.

79. *Il trattamento di dati personali per conto del titolare* comporta innanzitutto che il soggetto distinto tratti i dati personali a beneficio del titolare del trattamento. All'articolo 4, paragrafo 2, per trattamento si intende un'ampia gamma di operazioni, dalla raccolta alla conservazione, dalla consultazione all'uso, dalla diffusione o qualsiasi altra forma di messa a disposizione fino alla distruzione. Il concetto di «trattamento» è ulteriormente trattato al punto 2.1.5 che precede.

80. In secondo luogo, il trattamento deve essere effettuato per conto di un titolare, ma non agendo sotto la sua autorità o controllo diretti. Agire «per conto di» significa servire gli interessi di terzi e richiama la nozione giuridica di «delega». Nel caso della normativa in materia di protezione dei dati, il responsabile del trattamento è chiamato a seguire le istruzioni impartite dal titolare almeno per quanto concerne la finalità del trattamento e gli elementi essenziali che ne costituiscono i mezzi. La liceità del trattamento, ai sensi dell'articolo 6 e, se pertinente, dell'articolo 9 del regolamento, deriva dall'attività del titolare del trattamento: il responsabile del trattamento non deve trattare i dati in modo diverso da quanto indicato nelle istruzioni del suddetto titolare. Tuttavia, come detto in precedenza, le istruzioni del titolare del trattamento possono lasciare un certo margine di

discrezionalità su come servire al meglio i suoi interessi; ciò consente al responsabile del trattamento di scegliere i mezzi tecnici e organizzativi più idonei.[32]

81. Agire «per conto di» significa inoltre che il responsabile del trattamento non può effettuare trattamenti per finalità proprie. Ai sensi dell'articolo 28, paragrafo 10, il responsabile del trattamento è in violazione del GDPR qualora non si limiti a trattare i dati in base alle istruzioni del titolare del trattamento e inizi a definire proprie finalità e propri mezzi di trattamento. Il responsabile del trattamento si configura come titolare in un caso del genere e può essere soggetto a sanzioni qualora non si limiti a trattare i dati in base alle istruzioni del titolare.

**Esempio: prestatore di servizi indicato come responsabile del trattamento ma che agisce in qualità di titolare del trattamento**

Il fornitore di servizi MarketinZ fornisce servizi di pubblicità promozionale e di marketing diretto a varie società. La società GoodProductZ conclude un contratto con MarketinZ, in base al quale quest'ultima fornisce servizi di pubblicità commerciale ai clienti di GoodProductZ ed è designata responsabile del trattamento dei dati. Tuttavia, MarketinZ decide di utilizzare la banca dati dei clienti di GoodProductZ anche per finalità diverse dalla pubblicità per GoodProductZ, ad esempio per sviluppare la propria attività commerciale. La decisione di aggiungere un'ulteriore finalità a quella per la quale i dati personali sono stati trasferiti converte MarketinZ in titolare del trattamento dei dati per questa serie di operazioni di trattamento e il trattamento a tal fine costituirebbe una violazione del GDPR.

82. L'EDPB rammenta che, ai sensi del GDPR, non tutti i fornitori di servizi che trattano dati personali nel corso della prestazione di detti servizi sono «responsabili del trattamento». Il ruolo di responsabile del trattamento non scaturisce dalle caratteristiche del soggetto che tratta dati, ma dalle sue attività concrete in un contesto specifico. In altre parole, uno stesso soggetto può agire contemporaneamente come titolare del trattamento per determinate operazioni di trattamento e come responsabile del trattamento per altre; inoltre la qualifica di titolare o di responsabile del trattamento deve essere valutata in relazione a un insieme specifico di dati o di operazioni. La natura del servizio determinerà se l'attività di trattamento abbia per oggetto il trattamento di dati personali per conto del titolare ai sensi del GDPR. In pratica, se il servizio prestato non è destinato specificamente al trattamento di dati personali o se non prevede tale trattamento come un elemento essenziale, il prestatore del servizio può essere in grado di determinare in modo indipendente le finalità e i mezzi di tale trattamento necessario ai fini della prestazione. In siffatta situazione, il prestatore di servizi va considerato come un autonomo titolare del trattamento e non come responsabile dello stesso.[33] Resta tuttavia necessaria un'analisi caso per caso per stabilire il grado di influenza esercitata da ciascun soggetto nella determinazione delle finalità e dei mezzi del trattamento.

**Esempio: servizio di taxi**

Un servizio di taxi offre una piattaforma online che consente alle società di prenotare un taxi per trasportare dipendenti o ospiti da e verso 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 il conducente possa verificarne l'identità all'arrivo. In questo caso, il servizio taxi tratta i dati personali del dipendente nell'ambito del servizio prestato alla società ABC, ma il trattamento in quanto

[32] Cfr. parte I, sottosezione 2.1.4, sulla distinzione tra mezzi essenziali e non essenziali.

[33] Cfr. anche il considerando 81 del GDPR, che fa riferimento all'«affida[mento] delle attività di trattamento a un responsabile del trattamento», secondo cui le suddette attività, in quanto tali, sono una parte importante della decisione del titolare del trattamento di chiedere a un responsabile del trattamento di trattare dati personali per suo conto.

tale non è l'obiettivo del servizio. Il servizio taxi ha concepito 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. Il servizio taxi determina inoltre in modo indipendente le categorie dei dati raccolti e la durata dell'archiviazione. Il servizio agisce quindi in quanto titolare del trattamento pienamente autonomo, malgrado il fatto che il trattamento dei dati abbia luogo a seguito di una richiesta di prestazione del servizio da parte della società ABC.

83. L'EDPB osserva che un fornitore di servizi può comunque agire come responsabile del trattamento anche laddove il trattamento dei dati personali non sia l'oggetto principale o primario del servizio, a condizione che, nella pratica, il cliente del servizio continui a determinarne le finalità e i mezzi. Nel decidere se affidare o meno il trattamento dei dati personali a un determinato prestatore di servizi, i titolari del trattamento dovrebbero valutare attentamente se il prestatore dei servizi in questione consenta loro di esercitare un livello di controllo sufficiente, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi potenziali per gli interessati.

**Esempio: call center**

La società X esternalizza l'assistenza al cliente alla società Y, che mette a disposizione un call center per agevolare le risposte ai clienti della società X. La fornitura del servizio di assistenza clienti implica che la società Y abbia accesso alle banche dati relative ai clienti della società X. La società Y può accedere ai dati solo per fornire l'assistenza che la società X ha acquistato e non può trattare i dati per finalità diverse da quelle dichiarate dalla società X. La società Y deve essere considerata responsabile del trattamento dei dati personali e tra la società X e la Y deve essere concluso un accordo di trattamento.

**Esempio: servizi informatici generali**

La società Z si rivolge a un fornitore di servizi informatici per la manutenzione generale dei propri sistemi informatici che contengono una grande quantità di dati personali. L'accesso ai dati personali non è l'oggetto principale del servizio di assistenza, ma è inevitabile che il fornitore di servizi informatici vi abbia sistematicamente accesso durante la fornitura del servizio. La società Z desume pertanto che il fornitore di servizi informatici, essendo una società distinta che inevitabilmente è tenuta a trattare dati personali, anche se questo non è l'obiettivo principale del servizio, debba essere considerata responsabile del trattamento. Un accordo di trattamento è pertanto concluso con il fornitore di servizi informatici.

**Esempio: consulente informatico che risolve un problema di software**

La società ABC si rivolge a uno specialista informatico di un'altra società per risolvere un «bug» in un proprio software. Il consulente informatico non è ingaggiato per trattare dati personali e la società ABC stabilisce che l'accesso a tali dati sarà puramente accessorio e, pertanto, estremamente limitato nella pratica. La società ABC conclude pertanto che lo specialista informatico non sia responsabile del trattamento (né un autonomo titolare del trattamento) e decide di adottare misure adeguate, a norma dell'articolo 32 del GDPR, al fine di impedirgli di trattare i dati personali in modo non autorizzato.

84. Come indicato in precedenza, nulla osta a che un responsabile del trattamento offra un servizio secondo caratteristiche predeterminate, ma il titolare deve prendere la decisione finale di approvare attivamente le modalità di esecuzione del trattamento, almeno per quanto concerne i mezzi essenziali

dello stesso. Come detto, un responsabile del trattamento dispone di un margine di manovra per quanto riguarda i mezzi non essenziali (cfr. la sottosezione 2.1.4).

**Esempio: fornitore di servizi cloud**

Un comune ha deciso di utilizzare un fornitore di servizi cloud per la gestione delle informazioni nei propri servizi scolastici e di istruzione. Il servizio cloud fornisce servizi di messaggistica, videoconferenze, archiviazione di documenti, gestione del calendario, trattamento testi, ecc. e ciò comporterà il trattamento di dati personali relativi agli alunni e agli insegnanti. Il fornitore di servizi cloud ha proposto un servizio standardizzato, offerto a livello mondiale. Il comune deve comunque assicurarsi che l'accordo in vigore sia conforme all'articolo 28, paragrafo 3, del GDPR, e che i dati personali di cui è titolare siano trattati esclusivamente per le proprie finalità. Deve inoltre assicurarsi che le sue istruzioni specifiche, concernenti per esempio i periodi di archiviazione, la cancellazione dei dati ecc. siano rispettate dal fornitore di servizi cloud, indipendentemente da quanto previsto in via generale dal servizio standardizzato.

# 5 DEFINIZIONE DI TERZO/DESTINATARIO

85. Il regolamento definisce non solo i concetti di titolare del trattamento e di responsabile del trattamento, ma anche quelli di destinatario e di terzo. A differenza di quanto avviene per il titolare e il responsabile del trattamento, il regolamento non stabilisce obblighi o responsabilità specifici per i destinatari e i terzi. Si tratta di concetti relazionali, nel senso che rimandano a una relazione con un titolare o con un responsabile del trattamento da una prospettiva specifica; ad esempio, il titolare del trattamento o il responsabile del trattamento comunica i dati a un destinatario. Un destinatario di dati personali e un terzo possono essere considerati al contempo titolari o responsabili del trattamento da altri punti di vista. Ad esempio, soggetti da considerarsi destinatari o terzi sotto un determinato punto di vista, sono per altri versi titolari di un trattamento del quale determinano la finalità e i mezzi.

**Terzi**

86. L'articolo 4, paragrafo 10, definisce «*terzo*» la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia:

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

87. La definizione corrisponde in linea generale alla precedente definizione di «*terzi*» di cui alla direttiva 95/46/CE.

88. Mentre i termini «*dati personali*», «*interessato*», «*titolare del trattamento*» e «*responsabile del trattamento*» sono definiti dal regolamento, non lo è il concetto di «*persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile [del trattamento]*». Tuttavia, generalmente si intende che con tale formulazione ci si riferisca a persone appartenenti alla struttura giuridica del titolare o del responsabile del trattamento (un dipendente o una persona che occupi una posizione molto simile a quella di dipendente, ad esempio il personale fornito da un'agenzia di lavoro interinale), ma solo nella misura in cui siano autorizzate a trattare dati personali. Non rientra in

suddetta categoria un lavoratore dipendente o un'altra figura professionale che acceda a dati ai quali non è autorizzato ad accedere e per finalità diverse da quelle del datore di lavoro. Un tale dipendente dovrebbe invece essere considerato terzo rispetto al trattamento effettuato dal datore di lavoro. Nella misura in cui il dipendente tratti dati personali per le proprie finalità, diverse da quelle del datore di lavoro, sarà considerato titolare del trattamento, risponderà di tutte le conseguenze e si assumerà tutte le responsabilità che ne derivano in termini di trattamento dei dati personali.[34]

89. Per "terzo" si intende pertanto un soggetto che, nella specifica situazione in esame, non è né un interessato né un titolare del trattamento, un responsabile del trattamento o un dipendente. Ad esempio, il titolare del trattamento può assumere un responsabile del trattamento e incaricarlo di trasferire dati personali a terzi. Tale terzo sarà quindi considerato titolare a tutti gli effetti del trattamento che effettua per le proprie finalità. Va notato che, all'interno di un gruppo di società, una società diversa da quella del titolare del trattamento o del responsabile del trattamento è un terzo, anche se appartiene al medesimo gruppo al quale appartiene la società che agisce in qualità di titolare o di responsabile del trattamento.

**Esempio: servizi di pulizia**

La società A stipula un contratto con un'impresa di servizi di pulizia per i propri uffici. Gli addetti alle pulizie non sono tenuti ad accedere ai dati personali o a trattarli. Anche se occasionalmente possono venire in contatto con i dati quando operano all'interno dell'ufficio, essi possono svolgere i compiti loro assegnati senza accedervi e per contratto è fatto loro divieto di accedere ai dati personali che la società A detiene in quanto titolare del trattamento o di trattarli in qualsivoglia modalità. Gli addetti alle pulizie non sono dipendenti dalla società A né sotto la diretta autorità di quest'ultima. Non vi è alcuna intenzione di ricorrere all'impresa di servizi di pulizia o ai suoi dipendenti per trattare dati personali per conto della società A. L'impresa di servizi di pulizia e i relativi dipendenti devono pertanto essere considerati terzi e il titolare del trattamento deve assicurare l'esistenza di misure di sicurezza adeguate atte a impedire l'accesso ai dati e stabilire un obbligo di riservatezza in caso di accesso accidentale a tali dati.

**Esempio: gruppi di società – società capogruppo e controllate**

Le società X e Y, che fanno parte del gruppo Z, trattano i dati relativi ai rispettivi dipendenti ai fini della gestione delle risorse umane. A un certo punto, la società capogruppo ZZ decide di richiedere i dati dei dipendenti a tutte le controllate, al fine di elaborare statistiche a livello di gruppo. Nel trasferire dati dalle società X e Y a ZZ, quest'ultima deve essere considerata come terzo, indipendentemente dal fatto che tutte le società facciano parte del medesimo gruppo. La società ZZ sarà considerata titolare del trattamento dei dati a fini statistici.

**Destinatario**

90. L'articolo 4, paragrafo 9, definisce *destinatario* la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Le autorità pubbliche non vanno tuttavia considerate destinatari quando ricevono dati personali

[34] Il datore di lavoro (in qualità di titolare del trattamento originario) potrebbe tuttavia continuare ad avere una certa responsabilità nel caso in cui il nuovo trattamento abbia luogo a causa della mancanza di misure di sicurezza adeguate.

nell'ambito di un'indagine specifica, conformemente al diritto dell'Unione o degli Stati membri (ad esempio autorità fiscali e doganali, squadre di indagine finanziaria ecc.).[35]

91. La definizione corrisponde in linea generale a quella precedente di «*destinatario*» di cui alla direttiva 95/46/CE.

92. La definizione si applica a chiunque riceva dati personali, che si tratti o meno di terzi. Ad esempio, quando un titolare del trattamento invia dati personali a un altro soggetto, a un responsabile del trattamento o a terzi, tale soggetto è un destinatario. Un terzo destinatario è considerato titolare di qualsivoglia trattamento che effettua per le proprie finalità dopo aver ricevuto i dati.

**Esempio: comunicazione di dati tra società**

L'agenzia di viaggi ExploreMore organizza viaggi su richiesta di singoli clienti. Nell'ambito di tale servizio, invia i dati personali dei clienti a compagnie aeree, ad alberghi e alle agenzie che organizzano escursioni affinché possano erogare i rispettivi servizi. ExploreMore, gli alberghi, le compagnie aeree e i fornitori di servizi di escursione sono considerati titolari del trattamento da essi effettuato nell'ambito dei rispettivi servizi. Non esiste alcun rapporto titolare-responsabile. Tuttavia, le compagnie aeree, gli alberghi e i fornitori di servizi di escursione vanno considerati destinatari quando ricevono dati personali da ExploreMore.

# PARTE II – CONSEGUENZE DERIVANTI DAI DIVERSI RUOLI ATTRIBUITI

# 1 RAPPORTO TRA TITOLARE DEL TRATTAMENTO E RESPONSABILE DEL TRATTAMENTO

93. Un'innovazione distintiva introdotta dal GDPR è costituita dalle disposizioni che impongono obblighi direttamente ai responsabili del trattamento. Ad esempio, un responsabile del trattamento deve garantire che le persone autorizzate a trattare i dati personali si siano impegnate alla riservatezza (articolo 28, paragrafo 3), deve tenere un registro di tutte le categorie di attività relative al trattamento (articolo 30, paragrafo 2) e attuare misure tecniche e organizzative adeguate (articolo 32). A determinate condizioni (articolo 37) il responsabile del trattamento deve inoltre designare un responsabile della protezione dei dati e ha il dovere di informare il titolare del trattamento, senza ingiustificato ritardo, dopo essere venuto a conoscenza di una violazione dei dati personali (articolo 33, paragrafo 2). Inoltre, le norme sui trasferimenti di dati verso paesi terzi (capo V) si applicano sia ai responsabili sia ai titolari del trattamento. A tale riguardo, l'EDPB ritiene che l'articolo 28, paragrafo 3, del GDPR, pur conferendo un contenuto specifico al contratto che deve essere stipulato tra il titolare e il responsabile del trattamento, imponga a quest'ultimo obblighi diretti, ivi compreso il dovere di assistere il titolare del trattamento nel garantire la conformità alle disposizioni del regolamento.[36]

## 1.1 Scelta del responsabile del trattamento

[35] Cfr. anche il considerando 31 del GDPR.

[36] Ad esempio, il responsabile del trattamento dovrebbe assistere il titolare del trattamento, ove necessario e su richiesta, nel garantire l'adempimento degli obblighi relativi alle valutazioni d'impatto sulla protezione dei dati (considerando 95 del GDPR). Tale obbligo deve figurare nel contratto tra il titolare del trattamento e il responsabile del trattamento, ai sensi dell'articolo 28, paragrafo 3, lettera f), del GDPR.

94. Il titolare del trattamento ha il **dovere di impiegare «unicamente responsabili del trattamento che presentino garanzie sufficienti** per mettere in atto misure tecniche e organizzative adeguate», in modo tale che il trattamento soddisfi i requisiti del GDPR, anche in merito alla sicurezza dello stesso, e garantisca la tutela dei diritti degli interessati.[37] Il titolare del trattamento è pertanto responsabile della valutazione dell'adeguatezza delle garanzie presentate dal responsabile del trattamento e dovrebbe essere in grado di dimostrare di aver preso in seria considerazione tutti gli elementi di cui al GDPR.

95. Le garanzie «presentate» dal responsabile del trattamento sono quelle che il responsabile del trattamento è in grado di **dimostrare in modo soddisfacente al titolare del trattamento**, essendo queste le uniche che possono essere effettivamente prese in considerazione da detto titolare nel valutare l'adempimento dei suoi obblighi. Spesso ciò richiederà uno scambio di documentazione pertinente (ad esempio, politica in materia di privacy, condizioni di erogazione del servizio, registro delle attività di trattamento, meccanismi di gestione dei log, politica in materia di sicurezza delle informazioni, relazioni di audit esterni sulla protezione dei dati e certificazioni internazionali riconosciute, come la serie ISO 27000).

96. La valutazione della sufficienza delle garanzie da parte del titolare del trattamento è una forma di valutazione del rischio che dipenderà in larga misura dal tipo di trattamento affidato al responsabile e va effettuata caso per caso, tenendo conto della natura, dell'ambito di applicazione, 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 attività che il responsabile del trattamento è tenuto a presentare o a dimostrare in un dato caso, in quanto ciò dipende in larga misura dalle circostanze specifiche del trattamento.

97. Il titolare del trattamento dovrebbe tenere conto dei seguenti elementi[38], al fine di valutare l'adeguatezza delle garanzie: le **conoscenze specialistiche** (ad esempio, le competenze tecniche in materia di misure di sicurezza e di violazione dei dati), l'**affidabilità** e le **risorse** del responsabile del trattamento. Anche la reputazione del responsabile del trattamento sul mercato può essere un fattore pertinente di cui i titolari del trattamento possono tenere conto.

98. Inoltre, l'adesione a un codice di condotta o a un meccanismo di certificazione approvato può essere utilizzata come elemento in grado di dimostrare garanzie sufficienti.[39] Si consiglia pertanto ai responsabili del trattamento di informare il titolare del trattamento in merito a detta circostanza e a qualsiasi modifica intervenuta in rapporto alla suddetta adesione.

99. L'obbligo di impiegare solo responsabili del trattamento «che presentano garanzie sufficienti», ai sensi dell'articolo 28, paragrafo 1, del GDPR è un obbligo permanente. Esso non viene meno laddove il titolare e il responsabile del trattamento concludano un contratto o un atto giuridico di altra natura. A intervalli adeguati, il titolare del trattamento dovrebbe verificare le garanzie offerte dal responsabile del trattamento, anche mediante attività di revisione e ispezioni, se del caso.[40]

### 1.2 Forma del contratto o dell'atto giuridico di altra natura

100. Qualsivoglia trattamento di dati personali da parte di un responsabile del trattamento deve essere disciplinato da un contratto o altro atto giuridico, a norma del diritto dell'Unione o degli Stati membri,

[37] Articolo 28, paragrafo 1, e considerando 81 del GDPR.
[38] Cfr. il considerando 81 del GDPR.
[39] Articolo 28, paragrafo 5, e considerando 81 del GDPR.
[40] Cfr. anche l'articolo 28, paragrafo 3, lettera h), del GDPR.

concluso tra il titolare e il responsabile del trattamento, conformemente all'articolo 28, paragrafo 3, del GDPR.

101. Tale atto giuridico deve essere **per iscritto, anche in formato elettronico**.[41] Pertanto, gli accordi non scritti (indipendentemente dalla completezza o dall'efficacia) non possono essere considerati sufficienti per soddisfare i requisiti di cui all'articolo 28 del GDPR. Per evitare difficoltà nel dimostrare che il contratto o altro atto giuridico è effettivamente in vigore, l'EDPB raccomanda di accertarsi che le firme necessarie vi siano incluse, in linea con il diritto applicabile (ad esempio, il diritto contrattuale).

102. Inoltre, ai sensi del diritto dell'Unione o degli Stati membri il contratto o l'altro atto giuridico deve **vincolare il responsabile del trattamento** nei confronti del titolare del trattamento, ovverosia deve definire obblighi vincolanti in capo al responsabile del trattamento, conformemente al diritto dell'UE o degli Stati membri. Deve altresì definire gli obblighi del titolare del trattamento. Nella maggior parte dei casi vi sarà un contratto, tuttavia il regolamento fa riferimento altresì ad un «altro atto giuridico», come il diritto nazionale (primario o derivato) o un altro strumento giuridico. Se l'atto giuridico non prevede tutti i contenuti minimi richiesti, deve essere integrato da un contratto o da un altro atto giuridico che contenga gli elementi mancanti.

103. Poiché il regolamento stabilisce con chiarezza l'obbligo di stipulare un contratto scritto, qualora non sia in vigore nessun altro atto giuridico pertinente si ha una violazione del GDPR.[42] Sia il titolare sia il responsabile del trattamento hanno la responsabilità di garantire l'esistenza di un contratto o di un altro atto giuridico che disciplini il trattamento.[43] Fatte salve le disposizioni di cui all'articolo 83 del GDPR, l'autorità di controllo competente potrà infliggere una sanzione amministrativa pecuniaria sia al titolare sia al responsabile del trattamento, tenendo conto delle circostanze di ogni singolo caso. I contratti stipulati prima della data di applicazione del GDPR dovrebbero essere stati aggiornati ai sensi dell'articolo 28, paragrafo 3. L'assenza di tale aggiornamento, inteso ad allineare un contratto precedentemente esistente ai requisiti del GDPR, costituisce una violazione dell'articolo 28, paragrafo 3.

Un contratto scritto a norma dell'articolo 28, paragrafo 3, del GDPR può essere integrato in un contratto più ampio, come un accordo sul livello dei servizi. Al fine di agevolare la dimostrazione della conformità al GDPR, l'EDPB raccomanda che gli elementi del contratto volti a dare attuazione all'articolo 28 del GDPR siano chiaramente identificati come tali in un unico punto (ad esempio in un allegato).

[41] Articolo 28, paragrafo 9, del GDPR.

[42] La presenza (o l'assenza) di un accordo scritto, tuttavia, non è determinante ai fini della sussistenza di un rapporto titolare-responsabile del trattamento. Qualora, sulla base di un'analisi delle circostanze concrete relative al rapporto tra le parti e al trattamento dei dati personali in corso, vi sia motivo di ritenere che il contratto non corrisponda alla realtà in termini di controllo effettivo, si può non tenere conto di tale contratto. Di converso, un rapporto titolare-responsabile del trattamento potrebbe sussistere anche in assenza di un accordo di trattamento per iscritto. Ciò implicherebbe, tuttavia, una violazione dell'articolo 28, paragrafo 3, del GDPR. Inoltre, in determinate circostanze, l'assenza di una definizione chiara del rapporto tra il titolare e il responsabile del trattamento può comportare il problema della mancanza di una base giuridica su cui qualsivoglia trattamento dovrebbe basarsi, ad esempio in merito alla comunicazione dei dati tra il titolare e il presunto responsabile del trattamento.

[43] L'articolo 28, paragrafo 3, non si applica unicamente ai titolari del trattamento. Nel caso in cui solo il responsabile del trattamento sia soggetto all'ambito di applicazione territoriale di cui al GDPR, l'obbligo è direttamente applicabile unicamente a detto responsabile (cfr. anche le linee guida dell'EDPB 3/2018 sull'ambito di applicazione territoriale del RGPD, pag. 12).

104. Per adempiere all'obbligo di stipula di un contratto, **il titolare e il responsabile del trattamento possono scegliere di negoziarne uno proprio**, ivi compresi tutti gli elementi obbligatori, **o di basarsi, in tutto o in parte, su clausole contrattuali tipo in relazione agli obblighi di cui all'articolo 28**.[44]

105. Una serie di clausole contrattuali tipo (SCC) può essere adottata in alternativa dalla Commissione[45] o da un'autorità di controllo, conformemente al meccanismo di coerenza.[46] Tali clausole potrebbero far parte di una certificazione rilasciata al titolare o al responsabile del trattamento, ai sensi degli articoli 42 o 43.[47]

106. L'EDPB desidera chiarire che non vi è alcun obbligo in capo ai titolari e ai responsabili del trattamento di stipulare un contratto basato su SCC né ciò deve necessariamente avere la precedenza rispetto alla stipula di un contratto ad hoc. Entrambe le opzioni sono ammissibili ai fini dell'adempimento alla normativa in materia di protezione dei dati, a seconda delle circostanze specifiche, purché siano soddisfatti i requisiti di cui all'articolo 28, paragrafo 3.

107. Se le parti desiderano avvalersi delle clausole contrattuali tipo, le clausole di protezione dei dati previste dall'accordo devono essere le stesse delle SCC. Le SCC presenteranno spesso spazi vuoti da compilare od opzioni che le parti devono selezionare. Inoltre, come indicato in precedenza, le SCC saranno generalmente integrate in un accordo più ampio che descriva l'oggetto del contratto, le condizioni finanziarie e le altre clausole concordate: le parti potranno aggiungere ulteriori clausole (ad esempio il diritto applicabile e la giurisdizione), purché non siano in contrasto, direttamente o indirettamente, con le SCC[48] e non pregiudichino la tutela conferita dal GDPR e dalle normative dell'UE o degli Stati membri in materia di protezione dei dati.

108. I contratti tra titolari del trattamento e responsabili del trattamento possono talvolta essere redatti unilateralmente da una delle parti. Diversi fattori possono determinare la parte o le parti che redige/redigono il contratto, tra cui: posizionamento sul mercato e potere contrattuale, le competenze

[44] Articolo 28, paragrafo 6, del GDPR. L'EDPB rammenta che le clausole contrattuali tipo ai fini della conformità all'articolo 28 del GDPR non sono le stesse delle clausole contrattuali tipo di cui all'articolo 46, paragrafo 2. Mentre le prime precisano e chiariscono in che modo saranno soddisfatte le disposizioni di cui all'articolo 28, paragrafi 3 e 4, le seconde forniscono garanzie adeguate in caso di trasferimento di dati personali verso un paese terzo o verso un'organizzazione internazionale, in assenza di una decisione di adeguatezza, ai sensi dell'articolo 45, paragrafo 3.

[45] Articolo 28, paragrafo 7, del GDPR; cfr. il parere congiunto 1/2021 dell'EDPB e del GEPD sulle clausole contrattuali tipo tra titolari e responsabili del trattamento https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_it.

[46] Articolo 28, paragrafo 8, del GDPR. Il registro delle decisioni adottate dalle autorità di controllo e dalle autorità giudiziariesu questioni trattate nell'ambito del meccanismo di coerenza, ivi comprese le clausole contrattuali tipo ai fini della conformità all'articolo 28 del GDPR, è disponibile al seguente indirizzo: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_it.

[47] Articolo 28, paragrafo 6, del GDPR.

[48] L'EDPB rammenta che, a norma dell'articolo 46, paragrafo 2, lettera c), o dell'articolo 46, paragrafo 2, lettera d) del GDPR, il medesimo grado di flessibilità è consentito quando le parti scelgono di avvalersi delle clausole contrattuali tipo come tutela adeguata per i trasferimenti verso paesi terzi. Il considerando 109 del GDPR chiarisce che «*la possibilità che il titolare del trattamento o il responsabile del trattamento utilizzi clausole tipo di protezione dei dati adottate dalla Commissione o da un'autorità di controllo non dovrebbe precludere ai titolari del trattamento o ai responsabili del trattamento la possibilità di includere tali clausole tipo in un contratto più ampio, anche in un contratto tra il responsabile del trattamento e un altro responsabile del trattamento, né di aggiungere altre clausole o garanzie supplementari, purché non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo [...] o ledano i diritti o le libertà fondamentali degli interessati. I titolari del trattamento e i responsabili del trattamento dovrebbero essere incoraggiati a fornire garanzie supplementari attraverso impegni contrattuali che integrino le clausole tipo di protezione*».

tecniche e l'accesso a servizi giuridici. Ad esempio, alcuni fornitori di servizi tendono a stabilire termini e condizioni standard, tra cui accordi di trattamento dei dati.

109. Un accordo tra il titolare e il responsabile del trattamento deve rispettare i requisiti di cui all'articolo 28 del GDPR, al fine di garantire che il responsabile tratti i dati personali in conformità con lo stesso GDPR. Qualsivoglia accordo di questo tipo dovrebbe tenere conto delle responsabilità specifiche dei titolari e dei responsabili del trattamento. Sebbene l'articolo 28 preveda un elenco di elementi che devono essere contemplati in ogni contratto che disciplini il rapporto tra titolari e responsabili del trattamento, esso lascia margini di negoziato tra le parti di tali contratti. In talune situazioni il titolare o il responsabile del trattamento godono di un minore potere negoziale ai fini di una personalizzazione dell'accordo sulla protezione dei dati. Il ricorso alle clausole contrattuali tipo adottate a norma dell'articolo 28 (paragrafi 7 e 8) può contribuire a riequilibrare le posizioni negoziali e a garantire che i contratti rispettino il GDPR.

110. Il fatto che il contratto e le condizioni commerciali in esso dettagliate siano redatti dal prestatore di servizi piuttosto che dal titolare del trattamento non è di per sé problematico e non costituisce di per sé una ragione sufficiente per concludere che il prestatore di servizi debba essere considerato titolare del trattamento. Inoltre, lo squilibrio di potere contrattuale tra un piccolo titolare del trattamento e grandi fornitori di servizi non dovrebbe essere considerato una giustificazione per l'accettazione, da parte del suddetto titolare, di clausole e di condizioni contrattuali non conformi alla normativa in materia di protezione dei dati né può esonerarlo dai relativi obblighi. Il titolare del trattamento deve valutare i termini contrattuali e, nella misura in cui li accetta liberamente e si avvale del servizio, assumersi altresì la piena responsabilità del rispetto del GDPR. Qualsivoglia proposta di modifica, da parte di un responsabile del trattamento, degli accordi di trattamento dei dati di cui alle condizioni generali di contratto dovrebbe essere notificata e approvata direttamente dal titolare del trattamento, tenendo conto del margine di discrezionalità di cui il responsabile del trattamento dispone in merito agli elementi non essenziali dei mezzi (cfr. paragrafi 40-41 che precedono). La mera pubblicazione di tali modifiche sul sito web del responsabile del trattamento non è conforme all'articolo 28.

### 1.3 Contenuto del contratto o altro atto giuridico

111. Prima di esaminare nel dettaglio i singoli requisiti specifici definiti dal GDPR rispetto al contenuto del contratto o di un altro atto giuridico, occorre svolgere alcune osservazioni di natura generale.

112. Se è vero che gli elementi di cui all'articolo 28 del regolamento ne costituiscono il contenuto essenziale, il contratto dovrebbe essere uno strumento con cui il titolare e il responsabile del trattamento possono chiarire ulteriormente in che modo detti elementi essenziali saranno attuati mediante istruzioni dettagliate. Pertanto, **l'accordo relativo al trattamento dovrebbe non già meramente ribadire le disposizioni del GDPR,** bensì prevedere informazioni più specifiche e concrete sul modo in cui saranno soddisfatti i requisiti e sul livello di sicurezza previsto per il trattamento dei dati personali oggetto dell'accordo. Lungi dall'essere un esercizio formalistico, la negoziazione e la stipula del contratto sono un'opportunità per specificare i dettagli relativi al trattamento.[49] In effetti, ai sensi del GDPR, la «protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento [...] esigono una chiara ripartizione delle responsabilità».[50]

[49] Cfr. anche il parere 14/2019 dell'EDPB sul progetto di clausole contrattuali tipo presentato dall'autorità di controllo danese (articolo 28, paragrafo 8, del GDPR), pag. 5.
[50] Cfr. il considerando 79 del GDPR.

113. Nel contempo, il contratto dovrebbe **tener conto *«dei compiti e responsabilità specifici del responsabile del trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'interessato»***.[51] In linea generale, il contratto tra le parti dovrebbe essere redatto tenendo conto della specifica attività di trattamento dei dati. Ad esempio, non è necessario imporre tutele e procedure particolarmente rigorose a un responsabile del trattamento preposto a un'attività di trattamento che presenta solo rischi minori: sebbene ciascun responsabile del trattamento sia tenuto a rispettare i requisiti di cui al regolamento, le misure e le procedure dovrebbero essere calibrate in base alla situazione specifica. In ogni caso, il contratto deve contemplare tutti gli elementi di cui all'articolo 28, paragrafo 3. Nel contempo, dovrebbe prevedere taluni elementi che possano aiutare il responsabile del trattamento a comprendere i rischi per i diritti e le libertà degli interessati insiti nel trattamento: poiché l'attività è svolta per conto del titolare, spesso quest'ultimo ha una comprensione più approfondita dei rischi che il trattamento comporta dal momento che è a conoscenza delle circostanze in cui avviene.

114. Quanto al **contenuto obbligatorio** del contratto o di altro atto giuridico, l'EDPB interpreta l'articolo 28, paragrafo 3, in modo tale per cui deve esservi stabilito:

- l'**oggetto** del trattamento (ad esempio, registrazioni di videosorveglianza di persone che entrano o escono da una struttura ad alta sicurezza). Sebbene sia un concetto ampio, esso deve essere formulato con specifiche sufficienti affinché l'oggetto principale del trattamento sia chiaro;
- la **durata**[52] del trattamento: occorre specificare il periodo di tempo esatto o i criteri utilizzati per determinarlo; ad esempio, si potrebbe fare riferimento alla durata dell'accordo relativo al trattamento;
- la **natura** del trattamento: il tipo di operazioni eseguite nell'ambito del trattamento (ad esempio: «ripresa», «registrazione», «archiviazione di immagini» ecc.) **e la finalità** del trattamento (ad esempio: la rilevazione degli ingressi illegittimi). Tale descrizione dovrebbe essere la più completa possibile, a seconda dell'attività di trattamento specifica, in modo da consentire a soggetti esterni (ad esempio le autorità di controllo) di comprendere il contenuto e i rischi del trattamento affidato al relativo responsabile;
- la **tipologia di dati personali**: questo elemento dovrebbe essere specificato nel modo più dettagliato possibile (ad esempio: le immagini video delle persone che entrano ed escono dalla struttura). Non sarebbe sufficiente limitarsi a specificare che si tratta di «dati personali, ai sensi dell'articolo 4, paragrafo 1, del GDPR» o «di categorie particolari di dati personali, ai sensi dell'articolo 9». Nel caso di categorie particolari di dati, il contratto o l'atto giuridico dovrebbero specificare almeno i tipi di dati in questione, ad esempio «informazioni relative alle cartelle cliniche» o «informazioni sull'appartenenza dell'interessato a un sindacato»;
- le **categorie di interessati**: anche questo aspetto dovrebbe essere indicato in modo piuttosto specifico (ad esempio: «visitatori», «dipendenti», servizi di consegna ecc.);
- gli **obblighi e i diritti del titolare del trattamento**: tali diritti sono esaminati ulteriormente nelle sezioni successive (ad esempio, per quanto riguarda il diritto del titolare del trattamento di effettuare ispezioni e attività di revisione). Quanto agli obblighi del titolare del trattamento, tra gli esempi figurano quello di fornire al responsabile del trattamento i dati di cui al contratto, di fornire e documentare qualsivoglia istruzione relativa al trattamento dei dati da parte del

[51] Cfr. il considerando 81 del GDPR.

[52] La durata del trattamento non è necessariamente equivalente alla durata dell'accordo (possono sussistere obblighi giuridici di conservare i dati più a lungo o per un tempo inferiore).

responsabile del trattamento, di garantire, prima e durante l'intero corso del trattamento, l'adempimento degli obblighi di cui al GDPR posti in capo al responsabile, di controllare detto trattamento anche mediante attività di revisione e ispezioni unitamente al suddetto responsabile.

115. Sebbene il GDPR elenchi gli elementi che vanno sempre inclusi nell'accordo, può essere necessario prevedere altre informazioni pertinenti, in funzione del contesto e dei rischi posti dal trattamento nonché di eventuali ulteriori requisiti applicabili.

### *1.3.1 Obbligo del responsabile del trattamento di trattare i dati solo su istruzione documentata del titolare del trattamento (articolo 28, paragrafo 3, lettera a) del GDPR)*

116. La necessità di specificare tale obbligo deriva dal fatto che il responsabile del trattamento tratta i dati per conto del titolare. I titolari del trattamento devono fornire ai responsabili istruzioni relative a ciascuna attività di trattamento. Tali istruzioni possono riguardare trattamenti ammessi e quelli vietati, procedure più dettagliate, la modalità di messa in sicurezza dei dati, ecc. Il responsabile si limita a quanto disposto dal titolare del trattamento, ma ha la possibilità di suggerire elementi che, se accettati dal titolare del trattamento, diventano parte delle istruzioni impartite.

117. Quando un responsabile tratta i dati non limitandosi alle istruzioni del titolare del trattamento, e ciò equivale a una decisione che determina le finalità e i mezzi dello stesso, il suddetto responsabile è in violazione dei propri obblighi e può anche essere considerato titolare di tale trattamento, ai sensi dell'articolo 28, paragrafo 10 (cfr. infra, sottosezione 1.5).[53]

118. Le istruzioni impartite dal titolare del trattamento devono essere **documentate**. A tal fine, si raccomanda di prevedere una procedura e un modello per fornire ulteriori istruzioni attraverso un allegato al contratto o altro atto giuridico. In alternativa, le istruzioni possono essere impartite in qualsiasi forma scritta (ad esempio per posta elettronica) e in qualsivoglia altra forma documentata, purché sia possibile documentarle. In ogni caso, per evitare difficoltà nel dimostrare che le istruzioni del titolare del trattamento sono state debitamente documentate, l'EDPB raccomanda di accorpare tali istruzioni al contratto o al diverso atto giuridico.

119. L'obbligo in capo al responsabile del trattamento di astenersi da qualsivoglia attività di trattamento non 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 tenendo conto delle disposizioni di cui al capo V del GDPR.

120. L'EDPB raccomanda al titolare del trattamento di prestare la dovuta attenzione a questo punto specifico, in particolare laddove il responsabile deleghi talune attività di trattamento ad altri responsabili e laddove abbia divisioni o unità ubicate in paesi terzi. Se le istruzioni del titolare del trattamento non consentono trasferimenti o comunicazioni verso paesi terzi, il responsabile non sarà autorizzato ad assegnare il trattamento a un sub-responsabile in un paese terzo né potrà far trattare i dati in una sua divisione non ubicata nell'UE.

121. Un responsabile del trattamento può trattare dati in modo difforme dalle istruzioni documentate del titolare **laddove sia tenuto a trattare e/o a trasferire dati personali ai sensi del diritto dell'UE o del**

[53] Cfr. parte II, sottosezione 1.5 («Responsabile del trattamento che determina le finalità e i mezzi del trattamento»).

**diritto dello Stato membro cui il responsabile del trattamento è soggetto**. Tale disposizione rivela inoltre l'importanza di negoziare e di redigere con attenzione gli accordi di trattamento dei dati, in quanto, ad esempio, può avvenire che una delle parti necessiti di una consulenza legale in merito alla sussistenza di un siffatto obbligo giuridico. Ciò deve avvenire tempestivamente, in quanto il responsabile del trattamento ha l'obbligo di informare il titolare in merito all'esistenza di un obbligo del genere prima di iniziare il trattamento stesso. Tale obbligo di informazione non sussiste solo laddove il diritto stesso (dell'UE o dello Stato membro) vieti al responsabile del trattamento di informare il titolare in merito a «rilevanti motivi di interesse pubblico». In ogni caso, qualsivoglia trasferimento o comunicazione può aver luogo solo se autorizzato dal diritto dell'Unione, anche in conformità all'articolo 48 del GDPR.

### *1.3.2 Obbligo del responsabile del trattamento di garantire che le persone autorizzate a trattare i dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza (articolo 28, paragrafo 3, lettera b) del GDPR)*

122. Il contratto deve prevedere l'obbligo in capo al responsabile del trattamento di garantire che chiunque quest'ultimo autorizzi a trattare dati personali sia tenuto alla riservatezza. Ciò può avvenire mediante un accordo contrattuale specifico o in forza degli obblighi di legge già in vigore.

123. Il concetto ampio di «persone autorizzate a trattare i dati personali» contempla i lavoratori dipendenti e temporanei. In linea generale, il responsabile del trattamento dovrebbe mettere i dati personali a disposizione solo dei dipendenti che ne hanno effettivamente bisogno per svolgere i compiti per i quali il responsabile è stato incaricato dal titolare del trattamento.

124. L'impegno o l'obbligo di riservatezza deve essere «adeguato», ovverosia esso deve vietare effettivamente alla persona autorizzata di divulgare informazioni riservate senza autorizzazione e deve essere sufficientemente ampio da comprendere tutti i dati personali trattati per conto del titolare del trattamento nonché le condizioni alle quali tali dati sono trattati.

### *1.3.3 Obbligo del responsabile del trattamento di adottare tutte le misure richieste a norma dell'articolo 32 (articolo 28, paragrafo 3, lettera c) del GDPR)*

125. L'articolo 32 impone al titolare e al responsabile del trattamento di mettere in atto misure tecniche e organizzative di sicurezza adeguate. Sebbene tale obbligo sia già direttamente imposto al responsabile del trattamento i cui trattamenti rientrano nell'ambito di applicazione del GDPR, l'obbligo a norma dell'articolo 32 di adottare tutte le misure richieste deve comunque figurare nel contratto relativo alle attività di trattamento affidate dal titolare .

126. Come già rilevato, il contratto relativo al trattamento non dovrebbe limitarsi a ribadire le disposizioni del GDPR. È necessario che il contratto preveda o faccia riferimento alle misure di sicurezza da adottare, **all'obbligo in capo al responsabile del trattamento di ottenere l'approvazione del titolare del trattamento prima di apportare modifiche** e a un riesame periodico delle misure di sicurezza, al fine di garantirne l'adeguatezza rispetto ai rischi, che può cambiare nel tempo. Ai sensi dell'articolo 32, paragrafo 1, del GDPR le informazioni relative alle misure di sicurezza da includere nel contratto devono essere sufficientemente dettagliate da consentire al titolare del trattamento di valutare l'adeguatezza delle misure stesse. Inoltre, la descrizione è necessaria anche per consentire al titolare del trattamento di adempiere al proprio obbligo in materia di responsabilizzazione, a norma dell'articolo 5, paragrafo 2, e dell'articolo 24 del GDPR, per quanto concerne le misure di sicurezza imposte al responsabile del trattamento. Un obbligo corrispondente cui è soggetto il responsabile del trattamento, quello di assistere il titolare del trattamento e di mettere a disposizione tutte le

informazioni necessarie per dimostrare la conformità al regolamento, può essere desunto dall'articolo 28, paragrafo 3, lettere f) e h), del GDPR.

127. Il livello di istruzioni fornite dal titolare al responsabile del trattamento in merito alle misure da attuare dipende dalle circostanze specifiche. In taluni casi, il titolare del trattamento può fornire una descrizione chiara e dettagliata delle misure di sicurezza da attuare. In altri casi, può definire gli obiettivi minimi di sicurezza da conseguire, chiedendo al responsabile del trattamento di proporre l'attuazione di misure di sicurezza specifiche. In ogni caso, il titolare deve fornire al responsabile del trattamento una descrizione delle attività di trattamento e degli obiettivi di sicurezza (sulla base della valutazione del rischio eseguita dallo stesso titolare) nonché approvare le misure proposte dal responsabile del trattamento. Quanto sopra potrebbe essere incluso in un allegato al contratto. Il titolare del trattamento esercita il proprio potere decisionale sulle caratteristiche principali delle misure di sicurezza, sia elencandole esplicitamente sia approvando quelle proposte dal responsabile del trattamento.

### *1.3.4 Obbligo del responsabile del trattamento di rispettare le condizioni di cui all'articolo 28, paragrafo 2, e all'articolo 28, paragrafo 4, per ricorrere a un altro responsabile del trattamento (articolo 28, paragrafo 3, lettera d) del GDPR)*

128. L'accordo deve specificare che il responsabile del trattamento non può ricorrere a un altro responsabile del trattamento senza previa autorizzazione scritta del titolare e indicare se detta autorizzazione abbia natura specifica o generica. In caso di autorizzazione generica, il responsabile del trattamento è tenuto a informare il titolare in merito a qualsivoglia modifica riguardante il sub-responsabile del trattamento ai sensi di un'autorizzazione scritta e a dare al titolare del trattamento la possibilità di opporsi. Si raccomanda che il contratto definisca la procedura a tal fine. Va osservato che il dovere del responsabile di informare il titolare di qualsivoglia modifica relativa a sub-responsabili del trattamento implica che il responsabile del trattamento comunichi o segnali attivamente tali modifiche al titolare.[54] Inoltre, qualora sia richiesta un'autorizzazione specifica, il contratto dovrebbe definire la procedura per ottenere detta autorizzazione.

129. Quando il responsabile del trattamento ricorre a un altro responsabile del trattamento, tra di essi deve essere concluso un contratto che imponga i medesimi obblighi in materia di protezione dei dati che figurano in capo al responsabile del trattamento originario; in alternativa, tali obblighi devono essere imposti da un altro atto giuridico, ai sensi del diritto dell'Unione o dello Stato membro (cfr. anche il paragrafo160). Ciò include l'obbligo ai sensi dell'articolo 28, paragrafo 3, lettera h), di consentire e contribuire alle attività di revisione da parte del titolare del trattamento o di un altro soggetto da questi incaricato.[55] Sul responsabile del trattamento incombe la responsabilità, nei confronti del titolare del trattamento, di assicurare il rispetto degli obblighi in materia di protezione dei dati da parte degli altri sub-responsabili del trattamento (per ulteriori dettagli sul contenuto raccomandato per l'accordo, cfr. la sottosezione 1.6 in appresso).[56]

[54] A tale riguardo, di converso, non è sufficiente, ad esempio, che il responsabile del trattamento si limiti a fornire al titolare del trattamento un accesso generalizzato a un elenco dei sub-responsabili del trattamento che potrebbe essere aggiornato, a cadenza periodica, senza comunicare i nominativi ogni nuovo sub-responsabile del trattamento previsto. In altre parole, il responsabile del trattamento deve informare attivamente il titolare del trattamento di qualsivoglia modifica dell'elenco (ovverosia, in particolare, di ogni nuovo sub-responsabile del trattamento previsto).

[55] Cfr. anche il parere 14/2019 dell'EDPB sul progetto di clausole contrattuali tipo presentato dall'autorità di controllo danese (articolo 28, paragrafo 8, del GDPR), del 9 luglio 2019, punto 44.

[56] Cfr. parte II, sottosezione 1.6 («Sub-responsabili»).

### *1.3.5 Obbligo del responsabile del trattamento di assistere il titolare del trattamento nell'adempimento dell'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato (articolo 28, paragrafo 3, lettera e), del GDPR)*

130. Pur stipulando che dare seguito alle richieste degli interessati sia di competenza del titolare del trattamento, il contratto deve prevedere che il responsabile del trattamento abbia l'obbligo di fornire assistenza «con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile». La natura di tale assistenza può variare notevolmente «tenendo conto della natura del trattamento» e a seconda del tipo di attività affidata al responsabile. I dettagli relativi all'assistenza che il responsabile del trattamento è tenuto a fornire dovrebbero essere previsti nel contratto o in un suo allegato.

131. Mentre l'assistenza in questione può consistere semplicemente nel trasmettere tempestivamente qualsiasi richiesta ricevuta e/o nel consentire al titolare del trattamento di estrarre e gestire direttamente i dati personali pertinenti, in talune circostanze al responsabile saranno affidati compiti tecnici più specifici, in particolare laddove sia in grado di estrarre e gestire i dati personali.

132. È fondamentale tenere presente che, sebbene la gestione pratica delle singole richieste possa essere esternalizzata al responsabile del trattamento, è al titolare che spetta soddisfarle. Pertanto, la valutazione dell'ammissibilità delle richieste degli interessati e/o del rispetto dei requisiti di cui al GDPR dovrebbe essere effettuata dal titolare del trattamento, caso per caso o mediante istruzioni chiare fornite al responsabile per mezzo del contratto prima dell'inizio del trattamento. Inoltre, i termini di cui al capo III non possono essere prorogati dal titolare sulla base del fatto che le informazioni necessarie devono essere fornite dal responsabile del trattamento.

### *1.3.6 Obbligo del responsabile del trattamento di assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 (articolo 28, paragrafo 3, lettera f), del GDPR)*

133. È necessario che il contratto eviti semplicemente di ribadire tali funzioni di assistenza: **l'accordo dovrebbe contenere informazioni dettagliate sulle modalità con le quali al responsabile del trattamento è richiesto di assistere il titolare nell'adempiere agli obblighi elencati**. Ad esempio, negli allegati all'accordo possono essere aggiunti moduli e procedure che consentano al responsabile del trattamento di fornire al titolare tutte le informazioni necessarie.

134. Il tipo e il grado di assistenza che il responsabile del trattamento è tenuto a fornire possono variare notevolmente «*tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento*». Il titolare deve informare adeguatamente il responsabile del trattamento in merito ai rischi di quest'ultimo e a qualsiasi altra circostanza che possa aiutare il responsabile del trattamento a svolgere i propri compiti.

135. Passando agli obblighi specifici, il responsabile del trattamento ha innanzitutto il dovere di assistere il titolare nell'adempimento dell'obbligo di adottare misure tecniche e organizzative adeguate per garantire la sicurezza del trattamento.[57] Sebbene in una certa misura ciò possa coincidere con il requisito che il responsabile del trattamento stesso adotti misure di sicurezza adeguate qualora le operazioni di trattamento da questi svolte rientrino nell'ambito di applicazione del GDPR, si tratta ciononostante di due obblighi distinti, in quanto uno si riferisce alle misure del responsabile e l'altro riguarda quelle del titolare del trattamento.

[57] Articolo 32 del GDPR.

136. In secondo luogo, il responsabile del trattamento deve assistere il titolare nell'adempimento dell'obbligo di notificare le violazioni dei dati personali all'autorità di controllo e agli interessati. Il responsabile del trattamento deve informare il titolare ogniqualvolta rilevi una violazione dei dati personali che interessa le strutture o i sistemi informatici del responsabile o di un sub-responsabile del trattamento e deve aiutare il titolare del trattamento a ottenere le informazioni da comunicare nella notifica all'autorità di controllo.[58] Il GDPR prevede che il titolare del trattamento notifichi una violazione senza indebito ritardo, al fine di ridurre al minimo il danno per le persone fisiche e di massimizzare la possibilità di porre rimedio alla violazione in modo adeguato. Pertanto, la notifica da parte del responsabile al titolare del trattamento dovrebbe avvenire senza indebiti ritardi.[59] In base alle caratteristiche specifiche del trattamento affidato al responsabile, può essere opportuno che le parti includano nel contratto un lasso di tempo specifico (ad esempio, il numero di ore) entro il quale il responsabile del trattamento informa il titolare nonché il punto di contatto per tali notifiche, le relative modalità e il contenuto minimo previsto dal titolare del trattamento.[60] L'accordo contrattuale tra il titolare e il responsabile del trattamento può altresì autorizzare il responsabile a segnalare direttamente una violazione dei dati, ai sensi degli articoli 33 e 34; tuttavia, l'obbligo legale della notifica resta in capo al titolare del trattamento.[61] Se il responsabile del trattamento notifica una violazione direttamente all'autorità di controllo e ne informa gli interessati, conformemente agli articoli 33 e 34, tale responsabile deve informarne anche il titolare del trattamento e fornirgli copia della notifica e delle informazioni.

137. Inoltre, il responsabile del trattamento deve assistere il titolare anche nello svolgimento di valutazioni d'impatto sulla protezione dei dati, se necessario, e nella consultazione dell'autorità di controllo qualora il risultato di tali valutazioni indichi la sussistenza di un rischio elevato che non può essere attenuato.

138. L'obbligo di assistenza non può consistere in un trasferimento della responsabilità, in quanto gli obblighi in questione sono imposti al titolare del trattamento. Ad esempio, sebbene la valutazione d'impatto sulla protezione dei dati possa essere effettuata in concreto da un responsabile del trattamento, in capo al titolare permane il dovere di effettuare la valutazione[62] e il responsabile del trattamento è tenuto solo ad assistere il titolare «se necessario e su richiesta».[63] Di conseguenza, è il titolare del trattamento (e non il responsabile) che deve prendere l'iniziativa di effettuare la valutazione d'impatto sulla protezione dei dati.

[58] Articolo 33, paragrafo 3, del GDPR.

[59] Per maggiori informazioni, cfr. le Linee guida sulla notifica di violazioni dei dati personali ai sensi del regolamento (UE) 2016/679, WP 250 rev.01, 6 febbraio 2018, pagg. 13-14.

[60] Cfr. anche il parere 14/2019 dell'EDPB sul progetto di clausole contrattuali tipo presentato dall'autorità di controllo danese (articolo 28, paragrafo 8, del GDPR), del 9 luglio 2019, punto 40.

[61] Linee guida sulla notifica di violazioni dei dati personali ai sensi del regolamento (UE) 2016/679, WP 250 rev.01, 6 febbraio 2018, pag. 14.

[62] Gruppo di lavoro Articolo 29, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento «possa presentare un rischio elevato», ai fini del regolamento (UE) 2016/679, WP 248 rev.01, pag. 14.

[63] Cfr. il considerando 95 del GDPR.

### *1.3.7 Obbligo del responsabile del trattamento, al termine della relativa attività, di cancellare o restituire, su scelta del titolare del trattamento, tutti i dati personali al titolare del trattamento e cancellare le copie esistenti (articolo 28, paragrafo 3, lettera g), del GDPR)*

139. I termini contrattuali sono intesi a garantire che i dati personali siano oggetto di una protezione adeguata dopo la fine della «prestazione di servizi relativi al trattamento»: spetta pertanto al titolare decidere cosa il responsabile del trattamento debba fare in relazione ai dati personali.

140. Il titolare del trattamento può inizialmente decidere in merito alla cancellazione o alla restituzione dei dati personali, specificandolo nel contratto, mediante una comunicazione scritta da inviare tempestivamente al responsabile del trattamento. Il contratto o altro atto giuridico dovrebbe prevedere la possibilità per il titolare del trattamento di modificare la scelta operata prima della fine della prestazione dei servizi relativi al trattamento. Il contratto dovrebbe inoltre specificare la procedura per fornire tali istruzioni.

141. Se il titolare del trattamento sceglie di cancellare i dati personali, il responsabile del trattamento dovrebbe garantire che la cancellazione sia effettuata in modo sicuro, anche ai fini dell'adempimento dell'articolo 32 del GDPR. Il responsabile dovrebbe confermare al titolare del trattamento che la cancellazione è stata completata entro un termine concordato e secondo modalità convenute.

142. Il responsabile del trattamento deve cancellare tutte le copie esistenti dei dati, salvo che il diritto dell'UE o degli Stati membri non preveda un'ulteriore conservazione. Se il responsabile o il titolare del trattamento sono a conoscenza di tali obblighi di legge, ne informano l'altra parte al più presto.

### *1.3.8 Obbligo del responsabile del trattamento di mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato (articolo 28, paragrafo 3, lettera h), del GDPR)*

143. Il contratto deve prevedere disposizioni dettagliate sulla frequenza e sulle modalità del flusso di informazioni tra il responsabile e il titolare del trattamento, in modo tale che il titolare del trattamento sia pienamente informato in merito a quegli elementi del trattamento atti a dimostrare il rispetto degli obblighi di cui all'articolo 28 del GDPR. Ad esempio, le sezioni pertinenti dei registri delle attività di trattamento del responsabile possono essere condivise con il titolare del trattamento. Il responsabile del trattamento dovrebbe fornire tutte le informazioni sulle modalità di effettuazione dei trattamenti svolti per conto del titolare. Tali informazioni dovrebbero includere dettagli sul funzionamento dei sistemi utilizzati, sulle misure di sicurezza, sul modo in cui sono soddisfatti i requisiti di conservazione dei dati, sull'ubicazione e sui trasferimenti dei dati, su chi vi ha accesso e su chi sono i relativi destinatari, sui sub-responsabili ecc.

144. Il contratto deve prevedere ulteriori disposizioni per quanto concerne la facoltà del titolare o di un altro revisore da questi incaricato di svolgere ispezioni e attività di revisione e gli obblighi di contribuire a tali attività.

Il GDPR specifica che le ispezioni e le attività di revisione sono svolte dal titolare del trattamento o da un terzo da questi incaricato. L'obiettivo di dette attività di revisione è garantire che il titolare disponga di tutte le informazioni relative all'attività di trattamento svolta per suo conto e alle garanzie fornite dal responsabile del trattamento. Quest'ultimo può suggerire la scelta di un revisore specifico, tuttavia, ai sensi dell'articolo 28, paragrafo 3, lettera h), del GDPR, la decisione finale è lasciata al titolare del

trattamento.[64] Inoltre, anche se l'ispezione è effettuata da un revisore proposto dal responsabile del trattamento, il titolare si riserva 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 sia necessario effettuare attività di revisione presso il responsabile del trattamento nonché quale tipo di revisione o ispezione (a distanza/in loco/secondo altre modalità utili per raccogliere le informazioni necessarie) sia necessario e appropriato nel caso di specie, tenendo conto altresì delle questioni in materia di sicurezza; la scelta finale in merito spetta al titolare del trattamento. In seguito ai risultati dell'ispezione, il titolare del trattamento dovrebbe avere la facoltà di chiedere al responsabile di adottare misure successive, ad esempio per rimediare alle carenze e alle lacune individuate.[66] Analogamente, dovrebbero essere stabilite procedure specifiche per quanto riguarda l'ispezione dei sub-responsabili del trattamento da parte del responsabile e del titolare del trattamento (cfr. la sottosezione 1.6 in appresso).[67]

145. La questione della ripartizione dei costi tra un titolare e un responsabile del trattamento per quanto riguarda le attività di revisione non è contemplata dal GDPR ed è soggetta a considerazioni di ordine commerciale. Tuttavia, l'articolo 28, paragrafo 3, lettera h), stabilisce che il contratto preveda l'obbligo, in capo al responsabile del trattamento, di mettere a disposizione del titolare tutte le informazioni necessarie nonché l'obbligo di consentire e contribuire alle attività di revisione, ivi comprese le ispezioni, effettuate dal titolare del trattamento o da un altro revisore da esso incaricato. Ciò significa, in pratica, che le parti non dovrebbero inserire nel contratto clausole che prevedano il pagamento di costi o oneri manifestamente sproporzionati o eccessivi, aventi un conseguente effetto dissuasivo su una di esse. Tali clausole implicherebbero infatti che i diritti e gli obblighi di cui all'articolo 28, paragrafo 3, lettera h), non sarebbero mai esercitati nella pratica e diventerebbero puramente teorici, sebbene costituiscano parte integrante delle garanzie in materia di protezione dei dati di cui all'articolo 28 del GDPR.

### 1.4 Istruzioni che violano la normativa in materia di protezione dei dati

146. Ai sensi dell'articolo 28, paragrafo 3, il responsabile del trattamento deve informare tempestivamente il titolare del trattamento qualora, a suo avviso, un'istruzione violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

147. Di fatto, il responsabile del trattamento ha il dovere di rispettare le istruzioni del titolare del trattamento, ma ha anche l'obbligo generale di rispettare la legge. Un'istruzione che violi la normativa in materia di protezione dei dati causerebbe un conflitto tra i due obblighi di cui sopra.

148. Una volta informato che una delle sue istruzioni potrebbe essere in violazione del diritto in materia di protezione dei dati, il titolare del trattamento è tenuto a valutare la situazione e a verificare se detta violazione effettivamente sussista.

149. L'EDPB raccomanda alle parti di concordare nel contratto le conseguenze della notifica inviata dal responsabile del trattamento secondo cui una determinata istruzione comporta una violazione della normativa nonché le conseguenze dell'eventuale inerzia da parte del titolare del trattamento in tale

[64] Cfr. parere congiunto 1/2021 dell'EDPB e del GEPD sulle clausole contrattuali tipo tra titolari e responsabili del trattamento, punto 43.
[65] Cfr. il parere 14/2019 sul progetto di clausole contrattuali tipo presentato dall'autorità di controllo danese (articolo 28, paragrafo 8, del GDPR), punto 43.
[66] Cfr. il parere 14/2019 sul progetto di clausole contrattuali tipo presentato dall'autorità di controllo danese (articolo 28, paragrafo 8, del GDPR), punto 43.
[67] Cfr. parte II, sottosezione 1.6 («Sub-responsabili»).

contesto. Un esempio potrebbe essere l'inserimento di una clausola sulla risoluzione del contratto se il titolare del trattamento insiste nell'impartire un'istruzione illecita. Un altro esempio potrebbe essere una clausola sulla possibilità per il responsabile del trattamento di sospendere l'attuazione dell'istruzione in questione fino a quando il titolare del trattamento non la confermi, modifichi o ritiri.[68]

### 1.5 Responsabile del trattamento che determina le finalità e i mezzi del trattamento

150. Se viola il regolamento nel determinare le finalità e i mezzi del trattamento, il responsabile è considerato titolare del trattamento in questione (articolo 28, paragrafo 10, del GDPR).

### 1.6 Sub-responsabili

151. Le attività di trattamento dei dati sono spesso svolte da un gran numero di soggetti e le catene di esternalizzazione diventano sempre più complesse. Il GDPR introduce obblighi specifici che scaturiscono laddove un (sub-)responsabile del trattamento intenda coinvolgere un altro soggetto, aggiungendo in tal modo un altro anello alla catena, affidandogli attività che richiedono il trattamento di dati personali. L'analisi volta a stabilire se il prestatore di servizi agisca in qualità di sub-responsabile dovrebbe essere effettuata in linea con quanto sopra detto sul concetto di responsabile del trattamento (cfr. paragrafo 83).

152. Sebbene la catena possa essere alquanto lunga, il titolare del trattamento mantiene un ruolo centrale nella determinazione della finalità e dei mezzi dello stesso. L'articolo 28, paragrafo 2, del GDPR stabilisce che il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento (anche in formato elettronico). In caso di autorizzazione scritta generale, il responsabile deve informare il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare di cui sopra la possibilità di opporsi a dette modifiche. In entrambi i casi, prima che qualsivoglia trattamento di dati personali sia affidato al sub-responsabile del trattamento, il responsabile deve ottenere l'autorizzazione scritta del titolare dello stesso. Per effettuare la valutazione e decidere se autorizzare o meno tale ulteriore esternalizzazione, il responsabile del trattamento dovrà fornire al titolare un elenco dei sub-responsabili previsti (contenente, per ciascuno di essi: l'ubicazione, le modalità di esecuzione e la prova delle garanzie messe in atto).[69]

153. La previa autorizzazione scritta di cui sopra può essere specifica, vale a dire riferita a un determinato sub-responsabile per una determinata attività di trattamento e in un momento specifico, o generale. Ciò dovrebbe essere specificato nel contratto o nel diverso atto giuridico disciplinante il trattamento.

154. Qualora il titolare del trattamento decida di accettare determinati sub-responsabili, al momento della firma del contratto è opportuno inserire nello stesso o in un suo allegato un elenco dei sub-responsabili del trattamento approvati. L'elenco dovrebbe quindi essere tenuto aggiornato, conformemente all'autorizzazione generale o specifica concessa dal titolare del trattamento.

155. Se il titolare del trattamento sceglie di concedere un'**autorizzazione specifica** dovrebbe specificare per iscritto a quale sub-responsabile e a quale attività di trattamento fa riferimento. Qualsivoglia modifica

[68] Cfr. parere congiunto 1/2021 dell'EDPB e del GEPD sulle clausole contrattuali tipo tra titolari e responsabili del trattamento, punto 39.

[69] Tali informazioni sono necessarie affinché il titolare del trattamento possa soddisfare il principio di responsabilità di cui all'articolo 24 e le disposizioni di cui all'articolo 28, paragrafo 1, all'articolo 32 e al capo V del GDPR.

successiva richiederà un'ulteriore autorizzazione del titolare del trattamento prima di essere posta in essere. Qualora la richiesta di un'autorizzazione specifica da parte del responsabile del trattamento non riceva risposta entro il termine stabilito, la si considera respinta. Il titolare del trattamento dovrebbe decidere se concedere o meno l'autorizzazione tenendo conto dell'obbligo di ricorrere unicamente a responsabili del trattamento in grado di offrire «garanzie sufficienti» (cfr. la sottosezione 1.1 che precede).[70]

156. In alternativa, il titolare del trattamento può fornire la propria **autorizzazione generale** all'uso di sub-responsabili del trattamento (nel contratto, compreso un elenco di tali sub-responsabili in allegato), che dovrebbe essere integrata da criteri che guidino la scelta del responsabile del trattamento (ad esempio garanzie in termini di misure tecniche e organizzative, conoscenze specialistiche, affidabilità e risorse).[71] In un contesto del genere, il responsabile del trattamento è tenuto a informare a tempo debito il titolare del trattamento in merito a eventuali aggiunte o sostituzioni previste di uno o più sub-responsabili del trattamento, in modo da garantire al titolare di cui sopra la possibilità di opporsi.

157. Pertanto, la differenza principale tra l'autorizzazione specifica e l'autorizzazione generale risiede nel significato attribuito al silenzio del titolare del trattamento: nel caso di un'autorizzazione generale, la mancata obiezione da parte del titolare del trattamento, entro il termine stabilito, può essere interpretata come assenso e quindi autorizzazione.

158. In entrambi i casi, il contratto dovrebbe prevedere informazioni dettagliate sulle tempistiche relative all'approvazione o meno da parte del titolare del trattamento e sulle modalità di comunicazione tra le parti a tal riguardo (ad esempio mediante modulistica specifica). Dette tempistiche devono essere ragionevoli in base al tipo di trattamento, alla complessità delle attività affidate al responsabile (e ai sub-responsabili) del trattamento e al rapporto tra le parti. Inoltre, il contratto dovrebbe prevedere informazioni dettagliate sugli adempimenti concreti successivi a un'eventuale obiezione del titolare del trattamento (ad esempio specificando il termine entro cui il titolare e il responsabile dovrebbero pronunciarsi per porre fine al trattamento).

159. Indipendentemente dai criteri proposti dal titolare del trattamento nella scelta dei fornitori, il responsabile del trattamento conserva nei confronti del titolare l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile (articolo 28, paragrafo 4, del GDPR). Pertanto, il responsabile del trattamento si assicura di proporre sub-responsabili in grado di offrire garanzie sufficienti.

160. Inoltre, quando un responsabile del trattamento intende avvalersi di un sub-responsabile (autorizzato) deve concludere con quest'ultimo un contratto che preveda i medesimi obblighi imposti dal titolare al primo responsabile del trattamento; in alternativa, gli obblighi devono essere previsti da un altro atto giuridico, ai sensi del diritto dell'UE o dello Stato membro. L'intera catena delle attività di trattamento deve essere disciplinata da accordi scritti. L'imposizione dei «medesimi» obblighi dovrebbe essere interpretata in senso funzionale piuttosto che formale: non è necessario che il contratto contenga esattamente la stessa formulazione impiegata nel contratto tra il titolare e il responsabile del trattamento; tuttavia dovrebbe garantire che, nella sostanza, gli obblighi siano identici. Ciò significa anche che se il responsabile del trattamento affida a un sub-responsabile una parte specifica del trattamento, alla quale taluni obblighi non possono applicarsi, detti obblighi non dovrebbero essere inclusi «automaticamente» nel contratto con il sub-responsabile del trattamento in questione, in quanto ciò genererebbe solo incertezza. Ad esempio, per quanto concerne l'assistenza in materia di

[70] Cfr. parte II, sottosezione 1.1 («Scelta del responsabile del trattamento»).

[71] Tale dovere del titolare del trattamento deriva dal principio di responsabilità di cui all'articolo 24 e dall'obbligo di adempiere alle disposizioni di cui all'articolo 28, paragrafo 1, all'articolo 32 e al capo V del GDPR.

obblighi connessi a una violazione dei dati, la notifica di una tale violazione, da parte di un sub-responsabile del trattamento, direttamente al titolare potrebbe essere effettuata previo consenso di tutte e tre le parti. Tuttavia, nel caso di una notifica diretta, il responsabile del trattamento dovrebbe essere informato e ottenerne una copia.

# 2 CONSEGUENZE DELLA CONTITOLARITÀ DEL TRATTAMENTO

## 2.1 Determinazione in modo trasparente delle responsabilità rispettive dei contitolari del trattamento per quanto riguarda il rispetto degli obblighi previsti dal GDPR

161. L'articolo 26, paragrafo 1, del GDPR stabilisce che i contitolari del trattamento determinano e concordano in modo trasparente le rispettive responsabilità in merito all'osservanza degli obblighi previsti dal regolamento.

162. I contitolari del trattamento stabiliscono pertanto «chi fa cosa» decidendo tra loro chi dovrà svolgere un determinato compito, al fine di garantire la conformità agli obblighi applicabili, ai sensi del GDPR, in relazione al trattamento congiunto in questione. In altre parole, la ripartizione delle responsabilità in materia di conformità va effettuata in base all'uso del termine «*rispettive*» di cui all'articolo 26, paragrafo 1. Ciò non preclude il fatto che il diritto dell'UE o degli Stati membri possa già stabilire determinate responsabilità di ciascun contitolare del trattamento. In tal caso, l'accordo relativo al contitolare del trattamento dovrebbe contemplare altresì eventuali responsabilità aggiuntive, atte a garantire il rispetto del GDPR, non contemplate dalle disposizioni giuridiche.[72]

163. L'obiettivo di tali norme è garantire che, laddove siano coinvolti più soggetti, in particolare in contesti di trattamento complessi, la responsabilità del rispetto delle norme in materia di protezione dei dati personali sia attribuita chiaramente, al fine di evitare che ne risulti sminuita o che un conflitto negativo di competenze dia luogo a lacune tali da consentire a una delle parti coinvolte nel trattamento di non rispettare taluni obblighi. Occorre chiarire che qualsivoglia responsabilità va attribuita in funzione delle circostanze di fatto, al fine di addivenire a un accordo operativo. L'EDPB osserva il verificarsi di situazioni ove l'influenza di un contitolare del trattamento e le relative conseguenze pratiche complicano il raggiungimento di un accordo. Tuttavia, tali circostanze non ostano alla contitolarità del trattamento e non possono esonerare le parti dai loro obblighi ai sensi del GDPR.

164. Più specificamente, l'articolo 26, paragrafo 1, prevede che la determinazione delle responsabilità rispettive (ossia dei compiti) ai fini dell'osservanza degli obblighi derivanti dal GDPR spetti ai contitolari del trattamento, «*con particolare riguardo*» all'esercizio dei diritti dell'interessato e alle rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le responsabilità rispettive dei titolari del trattamento siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti.

165. Da tale disposizione emerge chiaramente che spetta ai contitolari del trattamento definire chi, rispettivamente, sarà incaricato di rispondere alle richieste laddove gli interessati esercitino i diritti loro conferiti dal GDPR e di fornire a questi ultimi le informazioni, a norma degli articoli 13 e 14 del

[72] «In ogni caso, l'accordo relativo al contitolare del trattamento dovrebbe contemplare in modo esaustivo tutte le responsabilità dei contitolari del trattamento, ivi comprese quelle che potrebbero già essere state definite nel diritto pertinente dell'UE o dello Stato membro e fatto salvo l'obbligo dei contitolari del trattamento di mettere a disposizione il contenuto essenziale dell'accordo che li riguarda, a norma dell'articolo 26, paragrafo 2, del GDPR».

GDPR. Si tratta soltanto di definire, nel loro rapporto interno, quali parti sono tenute a rispondere alle richieste degli interessati. Indipendentemente da tali accordi, l'interessato può contattare qualsivoglia contitolare del trattamento, a norma dell'articolo 26, paragrafo 3, del GPDR. Tuttavia, l'uso del termine «*con particolare riguardo*» significa che gli obblighi soggetti alla ripartizione delle responsabilità per la conformità di ciascuna delle parti interessate, di cui alla presente disposizione, non sono esaustivi. Ne consegue che, ai sensi del GDPR, la ripartizione delle responsabilità in materia di conformità tra i contitolari del trattamento non si limita agli aspetti di cui all'articolo 26, paragrafo 1, ma si estende ad altri obblighi di ciascun titolare. Di fatto, i contitolari del trattamento sono tenuti a garantire che l'intero trattamento congiunto sia pienamente conforme al GDPR.

166. In quest'ottica, le misure di conformità e i relativi obblighi che i contitolari del trattamento dovrebbero prendere in considerazione, al momento di determinare le rispettive responsabilità, oltre a quelle specificamente menzionate all'articolo 26, paragrafo 1, riguardano tra l'altro, a titolo esemplificativo e in via non esaustiva,:

- l'attuazione dei principi generali di protezione dei dati (articolo 5);
- la base giuridica del trattamento[73] (articolo 6);
- le misure di sicurezza (articolo 32);
- la notifica di una violazione dei dati personali all'autorità di controllo e all'interessato[74] (articoli 33 e 34);
- le valutazioni d'impatto sulla protezione dei dati (articoli 35 e 36);[75]
- il ricorso a un responsabile del trattamento (articolo 28);
- i trasferimenti di dati verso paesi terzi (capo V);
- l'organizzazione del contatto con gli interessati e le autorità di controllo.

167. Altri temi che potrebbero essere presi in considerazione a seconda del trattamento in questione e dell'intenzione delle parti sono, ad esempio, le limitazioni all'uso dei dati personali per un'altra finalità da parte di uno dei contitolari del trattamento. A tale riguardo, i contitolari del trattamento sono sempre tenuti a garantire di disporre ciascuno di una base giuridica per il trattamento. Talvolta, nell'ambito della contitolarità del trattamento, i dati personali sono condivisi tra un titolare del trattamento e un altro. In termini di responsabilizzazione, ciascun titolare del trattamento ha il dovere

[73] Sebbene il GDPR non impedisca ai contitolari del trattamento di avvalersi di una base giuridica diversa per i vari trattamenti da essi effettuati, si raccomanda di utilizzare, ove possibile, la stessa base giuridica per una finalità specifica.

[74] Cfr. altresì Gruppo di lavoro Articolo 29, Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 (WP 250.rev.01), a norma delle quali il controllo congiunto comprende la «*determinazione di chi sarà responsabile di adempiere agli obblighi di cui agli articoli 33 e 34*. *Il gruppo di lavoro Articolo 29 raccomanda che gli accordi contrattuali tra contitolari del trattamento prevedano disposizioni che stabiliscano quale titolare del trattamento assumerà il comando o sarà responsabile del rispetto degli obblighi di notifica delle violazioni previsti dal regolamento*» (pag. 14).

[75] Cfr. altresì le linee guida dell'EDPB sulle valutazioni d'impatto sulla protezione dei dati, WP 248.rev01, che stabiliscono quanto segue: «*Qualora il trattamento coinvolga contitolari del trattamento, questi ultimi devono definire con precisione le rispettive competenze. La loro valutazione d'impatto sulla protezione dei dati deve stabilire quale parte sia competente per le varie misure volte a trattare i rischi e a proteggere i diritti e le libertà degli interessati. Ciascun titolare del trattamento deve esprimere le proprie esigenze e condividere informazioni utili senza compromettere eventuali segreti (ad esempio protezione di segreti aziendali, proprietà intellettuale, informazioni aziendali riservate) o divulgare vulnerabilità.*» (pag. 8).

di garantire che i dati non siano ulteriormente trattati in modo incompatibile con le finalità per le quali sono stati inizialmente raccolti dal titolare del trattamento che li condivide.[76]

168. I contitolari del trattamento possono disporre di un certo grado di flessibilità nella distribuzione e nella ripartizione degli obblighi rispettivi, a condizione che garantiscano la piena conformità al GDPR per quanto concerne il trattamento in questione. Tale ripartizione dovrebbe tenere conto di fattori quali, ad esempio, chi è competente per e in grado di garantire efficacemente i diritti dell'interessato ovvero di rispettare gli obblighi pertinenti di cui al GDPR. L'EDPB raccomanda di documentare i fattori pertinenti e l'analisi interna effettuata al fine di ripartire i diversi obblighi. L'analisi fa parte della documentazione, in base al principio di responsabilizzazione.

169. Non è necessario che gli obblighi siano equamente distribuiti tra i contitolari del trattamento. A tale riguardo, la CGUE ha recentemente affermato che «*l'esistenza di una corresponsabilità non si traduce necessariamente in una responsabilità equivalente dei diversi operatori nell'ambito di un trattamento di dati personali*».[77] Tuttavia, vi possono essere casi in cui non tutti gli obblighi possono essere ripartiti cosicché tutti i contitolari del trattamento possono essere tenuti ad adempiere agli stessi obblighi derivanti dal GDPR, tenendo conto della natura e del contesto del trattamento congiunto. Ad esempio, i contitolari del trattamento che si avvalgono di strumenti o di sistemi condivisi di trattamento dei dati sono tenuti a garantire il rispetto, in particolare, del principio di limitazione delle finalità e ad attuare misure adeguate a garantire la sicurezza dei dati personali trattati nell'ambito di tali strumenti condivisi.

170. Un altro esempio è l'obbligo per ciascun contitolare del trattamento di tenere un registro delle attività di trattamento o di designare un responsabile della protezione dei dati (RPD) qualora siano soddisfatte le condizioni di cui all'articolo 37, paragrafo 1. Tali obblighi non sono legati al trattamento congiunto ma si applicano ai contitolari in quanto titolari del trattamento.

## 2.2 Obbligo di effettuare la ripartizione delle responsabilità mediante un accordo

### 2.2.1 Forma dell'accordo

171. L'articolo 26, paragrafo 1, del GDPR prevede come nuovo obbligo per i contitolari del trattamento di determinare le responsabilità rispettive «*mediante un accordo interno*». Il GDPR non specifica la forma giuridica di tale accordo. Pertanto, i contitolari del trattamento sono liberi di concordarne la forma.

172. Inoltre, l'accordo sulla ripartizione delle responsabilità è vincolante per ciascuno dei contitolari del trattamento. Ciascuno di essi concorda e si assume l'impegno *nei confronti degli altri* di essere responsabile dell'adempimento dei propri obblighi di cui all'accordo in quanto responsabilità propria.

173. Pertanto, ai fini della certezza del diritto, sebbene il GDPR non preveda requisiti giuridici relativi a un contratto o a un altro atto giuridico, l'EDPB raccomanda che tale accordo sia concluso sotto forma di documento vincolante, quale un contratto o un altro atto giuridico vincolante, ai sensi del diritto dell'UE o degli Stati membri cui i titolari del trattamento sono soggetti. Ciò garantirebbe certezza e potrebbe essere utilizzato per dimostrare il rispetto degli obblighi di trasparenza e responsabilizzazione. Di fatto, in caso di mancato rispetto della ripartizione concordata prevista

[76] Ogni comunicazione da parte di un titolare del trattamento richiede una base giuridica e una valutazione di compatibilità, indipendentemente dal fatto che il destinatario sia un diverso titolare del trattamento o un contitolare del trattamento. In altre parole, l'esistenza di un rapporto di contitolarità del trattamento non significa automaticamente che il contitolare che riceve i dati possa legittimamente trattarli anche per finalità aggiuntive che esulano dall'ambito della titolarità congiunta.
[77] Sentenza nella causa *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, punto 43.

dall'accordo, la natura vincolante di quest'ultimo consente a un titolare del trattamento di invocare la responsabilità dell'altro per quanto indicato nell'accordo come rientrante nella responsabilità di tale altro contitolare. Inoltre, in linea con il principio di responsabilizzazione, il ricorso a un contratto o altro atto giuridico consente ai contitolari del trattamento di dimostrare il rispetto degli obblighi imposti loro dal GDPR.

174. L'accordo dovrà esplicitare, in un linguaggio chiaro e semplice, il modo in cui le responsabilità, vale a dire i compiti, sono ripartiti tra ciascun contitolare del trattamento.[78] Tale requisito è importante in quanto garantisce la certezza del diritto ed evita possibili conflitti non solo nei rapporti tra i contitolari del trattamento, ma anche nei confronti degli interessati e delle autorità di protezione dei dati.

175. Per inquadrare meglio la ripartizione delle responsabilità tra le parti, l'EDPB raccomanda che l'accordo contenga anche informazioni generali sul trattamento congiunto, specificando in particolare l'oggetto e la finalità di tale trattamento, le tipologie di dati personali e le categorie di interessati.

### 2.2.2 Obblighi nei confronti degli interessati

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

#### L'accordo deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari *nei confronti* degli interessati.

177. A integrazione di quanto illustrato nella sezione 2.1 delle presenti linee guida, è importante che i contitolari del trattamento chiariscano nell'accordo il ruolo rispettivo, «*con particolare riguardo*» all'esercizio dei diritti dell'interessato e alle funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14. L'articolo 26 del GDPR sottolinea l'importanza di tali obblighi specifici. I contitolari del trattamento devono pertanto prevedere e concordare come e da chi saranno fornite le informazioni nonché chi risponderà e in quale modo alle richieste dell'interessato. Indipendentemente dal contenuto dell'accordo su questo punto specifico, l'interessato può contattare uno dei contitolari del trattamento per esercitare i propri diritti, conformemente all'articolo 26, paragrafo 3, come spiegato di seguito.

178. La modalità di adempimento di tali obblighi come definita nell'accordo dovrebbe riflettere «*adeguatamente*», ossia accuratamente, la realtà del trattamento congiunto. Ad esempio, se soltanto uno dei contitolari comunica con gli interessati ai fini del trattamento congiunto, tale contitolare potrebbe essere in una posizione migliore per informare gli interessati ed eventualmente rispondere alle loro richieste.

#### Obbligo di mettere a disposizione degli interessati gli elementi essenziali dell'accordo («Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato»)

179. Questa disposizione mira a garantire che l'interessato sia a conoscenza del «*contenuto essenziale dell'accordo*». Ad esempio, deve essere del tutto chiaro all'interessato quale titolare del trattamento funga da punto di contatto per l'esercizio dei propri diritti (sebbene possa esercitare tali diritti nei confronti di e rispetto a qualsivoglia contitolare del trattamento). L'obbligo di mettere a disposizione degli interessati il contenuto essenziale dell'accordo è importante in caso di contitolarità del

[78] Come indicato al considerando 79 del GDPR, «*(...) la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esigono una chiara ripartizione delle responsabilità ai sensi del presente regolamento, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento*».

trattamento affinché l'interessato sappia chi tra i titolari del trattamento risponde di un determinato ambito.

180. Il GDPR non specifica quale sia il «*contenuto essenziale dell'accordo*». L'EDPB raccomanda che tale contenuto essenziale riguardi almeno tutte le informazioni di cui agli articoli 13 e 14 che dovrebbero già essere accessibili all'interessato e, per ciascuno di tali elementi, l'accordo dovrebbe specificare il contitolare del trattamento responsabile di garantirne il rispetto. Il contenuto essenziale dell'accordo deve comprendere anche il punto di contatto, se designato.

181. Non viene specificato in che modo tali informazioni siano messe a disposizione dell'interessato. Contrariamente ad altre disposizioni del GDPR (quali l'articolo 30, paragrafo 4, in materia di registro dei trattamenti, o l'articolo 40, paragrafo 11, per il registro dei codici di condotta approvati), l'articolo 26 non prevede che la messa a disposizione debba essere «*su richiesta*» o «*resa pubblica mediante mezzi appropriati*». Spetta pertanto ai contitolari del trattamento decidere il modo più efficace per mettere il contenuto essenziale dell'accordo a disposizione degli interessati (ad esempio allegandolo alle informazioni di cui all'articolo 13 o 14, inserendolo nella politica in materia di privacy o, su richiesta, comunicandolo al responsabile della protezione dei dati, se del caso, o al punto di contatto eventualmente designato). I contitolari del trattamento dovrebbero garantire, per quanto di rispettiva competenza, che le informazioni siano fornite in modo coerente.

### Possibilità di designare nell'accordo un punto di contatto per gli interessati («Tale accordo può designare un punto di contatto per gli interessati»)

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

183. Il fatto di essere informati dell'esistenza di un singolo canale per contattare molteplici contitolari del trattamento consente agli interessati di sapere chi possono contattare in merito a tutte le questioni relative al trattamento dei loro dati personali. Inoltre, ciò consente ai contitolari del trattamento di coordinare in modo più efficiente i rapporti e le comunicazioni *nei confronti* degli interessati.

184. Per tali motivi, al fine di agevolare l'esercizio dei diritti degli interessati a norma del GDPR, l'EDPB raccomanda ai contitolari del trattamento di designare detto punto di contatto.

185. Il punto di contatto può essere l'eventuale responsabile della protezione dei dati, il rappresentante nell'Unione (per i contitolari del trattamento non stabiliti nell'Unione) o qualsivoglia altro punto di contatto presso il quale sia possibile ottenere informazioni.

### Facoltà degli interessati di esercitare i propri diritti nei confronti di e contro ciascuno dei contitolari del trattamento, indipendentemente dai termini dell'accordo

186. Ai sensi dell'articolo 26, paragrafo 3, l'interessato non è vincolato dai termini dell'accordo e può esercitare i propri diritti ai sensi del GDPR nei confronti di e contro ciascuno dei contitolari del trattamento.

187. Ad esempio, nel caso di contitolari del trattamento stabiliti in Stati membri diversi, o qualora solo uno dei contitolari sia stabilito nell'Unione, l'interessato può contattare, a sua scelta, il titolare del trattamento stabilito nello Stato membro in cui ha la residenza abituale o il luogo di lavoro oppure il titolare stabilito altrove nell'UE o nel SEE.

188. Anche se l'accordo e il relativo contenuto essenziale messo a disposizione degli interessati prevedono un punto di contatto per ricevere e trattare tutte le richieste degli interessati, questi ultimi possono comunque operare scelte diverse.

189. È pertanto importante che i contitolari del trattamento organizzino in anticipo la gestione delle risposte alle richieste che potrebbero ricevere dagli interessati. A tale riguardo, si raccomanda che i contitolari del trattamento comunichino agli altri titolari del trattamento responsabili o al punto di contatto designato le richieste da essi ricevute affinché siano trattate in modo efficace. Imporre agli interessati di contattare il punto di contatto designato o il titolare del trattamento competente costituirebbe un onere eccessivo, in contrasto con l'obiettivo di agevolare l'esercizio dei diritti degli interessati a norma del GDPR.

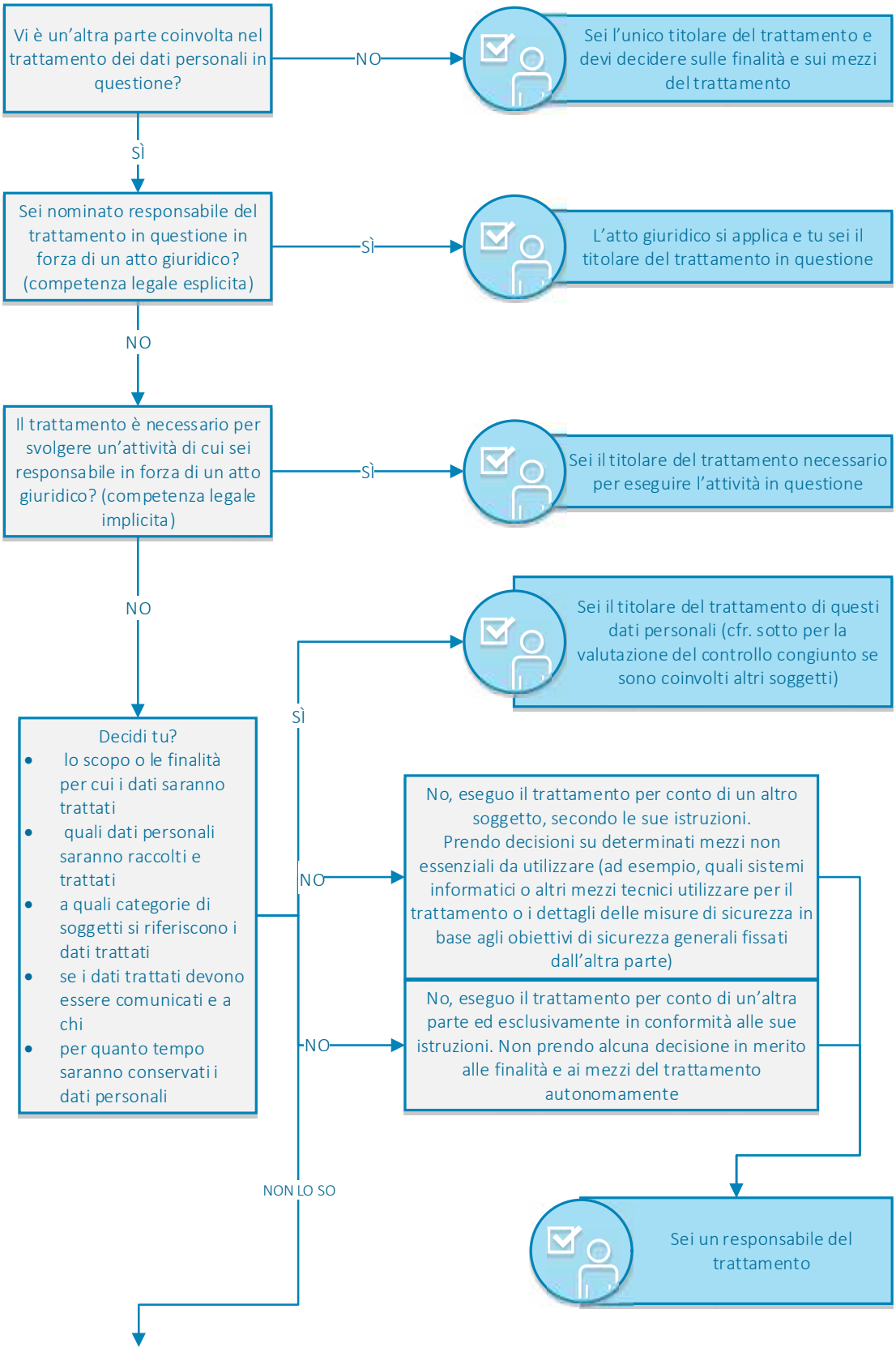
## 2.3 Obblighi nei confronti delle autorità di protezione dei dati

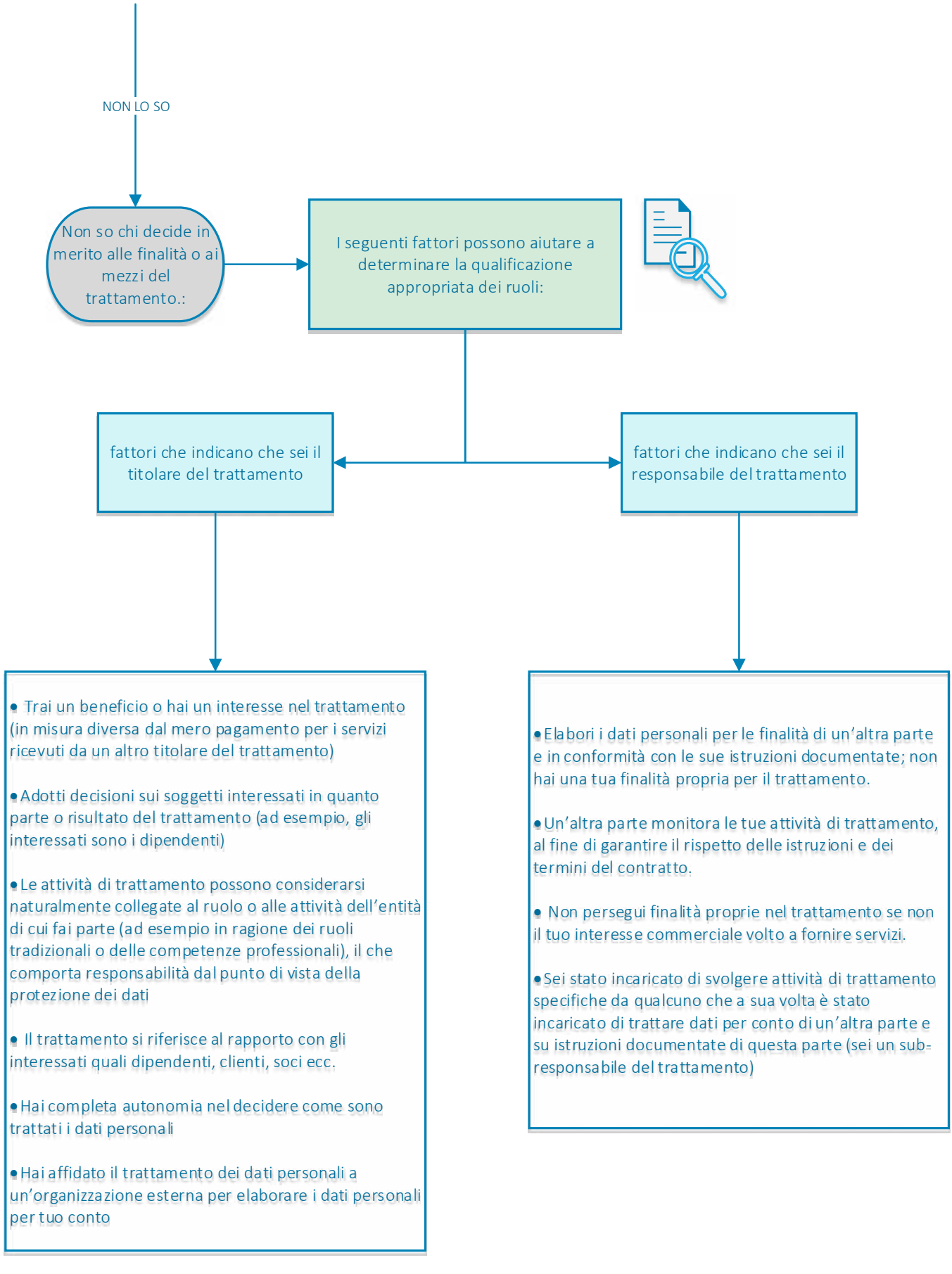
190. I contitolari del trattamento dovrebbero prevedere nell'accordo le modalità di comunicazione con le autorità di controllo competenti. Le comunicazioni in questione potrebbero riguardare l'eventuale consultazione ai sensi dell'articolo 36 del GDPR, la notifica di una violazione dei dati personali e la designazione di un responsabile della protezione dei dati.

191. È opportuno rammentare che le autorità preposte alla protezione dei dati non sono vincolate dai termini dell'accordo per quanto concerne l'individuazione dei contitolari o del punto di contatto designato. Pertanto, in relazione al trattamento congiunto, le autorità possono contattare qualunque contitolare del trattamento per esercitare i loro poteri, a norma dell'articolo 58.

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

**Nota: per valutare correttamente il ruolo di ciascuna entità coinvolta, è necessario innanzitutto identificare il trattamento specifico dei dati personali in questione e l'esatta finalità. Se sono coinvolti più soggetti è necessario valutare se finalità e mezzi siano determinati congiuntamente, determinando una contitolarità del trattamento.**




NON LO SO
Non so chi decide in merito alle finalità o ai mezzi del trattamento.:
I seguenti fattori possono aiutare a determinare la qualificazione appropriata dei ruoli:
fattori che indicano che sei il titolare del trattamento
fattori che indicano che sei il responsabile del trattamento
• Trai un beneficio o hai un interesse nel trattamento (in misura diversa dal mero pagamento per i servizi ricevuti da un altro titolare del trattamento)
• Adotti decisioni sui soggetti interessati in quanto parte o risultato del trattamento (ad esempio, gli interessati sono i dipendenti)
• Le attività di trattamento possono considerarsi naturalmente collegate al ruolo o alle attività dell'entità di cui fai parte (ad esempio in ragione dei ruoli tradizionali o delle competenze professionali), il che comporta responsabilità dal punto di vista della protezione dei dati
• Il trattamento si riferisce al rapporto con gli interessati quali dipendenti, clienti, soci ecc.
• Hai completa autonomia nel decidere come sono trattati i dati personali
• Hai affidato il trattamento dei dati personali a un'organizzazione esterna per elaborare i dati personali per tuo conto
• Elabori i dati personali per le finalità di un'altra parte e in conformità con le sue istruzioni documentate; non hai una tua finalità propria per il trattamento.
• Un'altra parte monitora le tue attività di trattamento, al fine di garantire il rispetto delle istruzioni e dei termini del contratto.
• Non persegui finalità proprie nel trattamento se non il tuo interesse commerciale volto a fornire servizi.
• Sei stato incaricato di svolgere attività di trattamento specifiche da qualcuno che a sua volta è stato incaricato di trattare dati per conto di un'altra parte e su istruzioni documentate di questa parte (sei un sub-responsabile del trattamento)

**Contitolarità - Se sei titolare del trattamento e altre parti sono coinvolte nel trattamento dei dati personali:**