

Le definizioni fondamentali

Chiara Angiolini

Abstract: The chapter analyses the main data protection definitions provided for by Reg. UE 2016/679, such as that of personal data, data subjects, data controllers and data processors. Furthermore, the intersections between EU Reg. 2016/679, Reg. 2022/868 and EU Reg. 2023/2854 are analysed with regard to basic definitions of Data Law.

Keywords: Data protection definitions, data subject, data processor, data controller, data protection officer, personal data

Sommario: 1. I dati personali 35; 2. La persona interessata 37; 3. Il trattamento 37; 4. Le categorie particolari di dati personali 38; 5. Il titolare del trattamento e la contitolarità 41; 6. Il responsabile del trattamento 43; 7. Il responsabile della protezione dei dati 43; 8. Le definizioni nel Regolamento 2022/868 sulla governance dei dati e nel Regolamento 2023/2854 sui dati e il coordinamento con il GDPR 45; 8.1. La definizione dei soggetti 46; Riferimenti bibliografici 48

1. I dati personali

I dati personali sono definiti dall'art. 4, par. 1, n. 1 del Reg. UE 2016/679 (d'ora in avanti: GDPR) come «informazione[i] riguardant[i] una persona fisica identificata o identificabile “interessato”».

L'analisi della definizione si può scomporre in due parti, la prima, oggettiva, relativa alla nozione di 'informazione' e la seconda relativa al versante soggettivo e dunque al legame fra i dati e la persona che è descritta da tali dati.

Con riguardo alla nozione di informazione, in linea generale questa può indicare un processo, così come il suo risultato. Nel linguaggio normativo del GDPR la nozione di dati personali si basa prevalentemente sulla seconda accezione. Infatti, gli artt. 15 e 20 GDPR fanno riferimento al formato dei dati e il GDPR ne regola la conservazione, la cancellazione (art. 17), la richiesta di copia (art 15).

Questa impostazione, che guarda ai dati come risultati, rende possibile scinderli dall'interessato e da chi li ha raccolti e dunque dare loro un connotato di oggettività.

Considerare i dati come oggetti permette anche di dar conto di quelle ipotesi, sempre più frequenti, in cui i dati personali descrivono dei comportamenti che non riguardano un solo soggetto e delle relazioni, ma una collettività. Si pensi ad esempio alle informazioni circa l'età e il nome delle persone che hanno visualizzato un post di un utente di *Instagram*, ai dati relativi all'esistenza di un contratto fra due parti, o alle annotazioni di un esaminatore relative a una pro-

Chiara Angiolini, University of Siena, Italy, chiara.angiolini@unisi.it

Referee List (DOI 10.36253/fup_referee_list)

FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Chiara Angiolini, *Le definizioni fondamentali*, © Author(s), CC BY-SA 4.0, DOI 10.36253/979-12-215-0796-6.05, in Chiara Angiolini, Antonello Iuliani (edited by), *Manuale sulla protezione e circolazione dei dati personali*, pp. 35-48, 2025, published by Firenze University Press and USiena PRESS, ISBN 979-12-215-0796-6, DOI 10.36253/979-12-215-0796-6

va d'esame, personali sia rispetto al valutatore che al candidato (quest'ultima ipotesi è tratta da: CGUE, 20 dicembre 2017, C-434/16).

Sul piano normativo la definizione di dati personali crea un legame persistente fra tali dati e l'interessato. I profili più rilevanti sono due.

In primo luogo, la posizione dell'interessato non è tutelata soltanto perché i dati lo riguardano, per così dire, originariamente, ma anche in quanto sono utilizzati riferendoli a questi. A tal proposito il Gruppo di Lavoro Art. 29 ha affermato che se un impiego dei dati può avere un impatto sui diritti e gli interessi dell'interessato, questi sono da ritenere personali (Gruppo di Lavoro Art. 29, *Parere 4/2007 sul concetto di dati personali*).

A contrario, i dati c.d. «fittizi», utilizzati ad esempio come strumento per test informatici o a fini di ricerca, non sono dati personali, in quanto non descrivono una persona fisica identificata o identificabile ma una persona che non esiste (così CGUE, 5 dicembre 2023, C-683/21, § 55).

In secondo luogo, la connessione fra persona interessata e dati personali creata a livello normativo è resa particolarmente forte grazie al riferimento nella definizione giuridica di dati personali, non soltanto a una persona identificata, ma anche identificabile. La nozione di identificabilità assume sicura importanza nei contesti di trattamento massivo dei dati. Sul punto, il considerando 26 GDPR recita:

Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici.

È di particolare interesse qui il caso *Breyer*, nel quale la Corte di Giustizia dell'Unione Europea ha affermato che ai fini della qualificazione di un dato come personale non è necessario che tutte le informazioni che consentono di identificare la persona interessata «debbano essere in possesso di una sola persona» (CGUE, 19 ottobre 2016, C-582/14, §§ 43 ss.; si veda anche: CGUE, 9 novembre 2023, C-319/2022). Di recente la Corte di Giustizia dell'UE è ritornata sulla questione, affermando che la circostanza per cui un soggetto non acceda alle informazioni Y che, associate a quelle X, che tratta, permettono di identificare una persona fisica non esclude la qualificazione delle informazioni X trattate come dati personali (CGUE, 7 marzo 2024, C-604/22, §§ 38 ss.).

A fronte di tale orientamento, la sentenza della Corte di Giustizia dell'UE del 4 settembre 2025, C-413/23 P è di particolare rilevanza. In questa pronuncia la Corte assume una prospettiva soggettiva con riguardo alla definizione di dati personali, applicata in ragione delle informazioni disponibili per il titolare del trattamento. In particolare, con riguardo ai dati pseudonimizzati la Corte distingue, non sempre con un'argomentazione chiara, fra i soggetti che hanno accesso o possono aver accesso ai codici di identificazione o altre informazioni aggiuntive che permettano l'identificazione o l'identificabilità degli interessati, per cui i dati sono

personali, e i soggetti che hanno accesso ai soli dati pseudonimizzati, senza avere la possibilità di accesso ai codici di identificazione o ad altre informazioni aggiuntive che permettano l'identificazione o l'identificabilità degli interessati. Rispetto a tali ultimi soggetti, la Corte afferma che i dati non sono da considerare personali. L'impatto e l'interpretazione di tale pronuncia sono in discussione in dottrina.

La nozione di identificabilità è molto ampia e non definibile una volta per tutte, in quanto assume importanza il contesto di riferimento e lo sviluppo tecnologico, come emerge anche dalla lettura del considerando 26 GDPR già richiamato. È ben possibile quindi che un dato inizialmente anonimo divenga personale, in ragione del tipo di trattamento o dell'evoluzione della tecnologia (Purtova 2018).

Il procedimento inverso, l'anonimizzazione, è ritenuto sempre più difficile da ottenere in pratica: l'attuale tecnologia ha portato la comunità scientifica e poi anche il Gruppo di Lavoro Art. 29, a sottolineare la difficoltà di un'anonimizzazione sicura e dunque di avere certezza circa una definitiva trasformazione dei dati da personali ad anonimi, con il conseguente venir meno del legame, giuridicamente sancito, fra dati personali e interessato (Gruppo di Lavoro Art. 29, *Parere 5/2014 sulle tecniche di anonimizzazione*, 10 aprile 2014).

2. La persona interessata

La nozione di persona interessata è strettamente legata a quella di dato personale come risulta evidente dalla lettura dell'art. 4, par. 1, n. 1 GDPR, già citato in apertura del precedente paragrafo.

Infatti, i dati sono «personali» in quanto descrivono una persona fisica ed è proprio il legame, anche giuridico, fra dati e persona la ragione principale per la definizione di un regime *ad hoc*. In proposito, è stato da tempo mostrato che il trattamento dei dati personali permette di acquisire una conoscenza anche molto approfondita dell'interessato, modulata in base al punto di vista di chi raccoglie e tratta i dati. Tale conoscenza risulta utile a vari fini e la letteratura ha a più riprese sottolineato come questa fondi un potere capace di incidere sulle relazioni di cui l'interessato è parte (Rodotà 1995; Zuboff 2019). In una prospettiva giuridica, i trattamenti possono incidere sulla sfera della personalità e delle relazioni dell'interessato, ed è questa una delle ragioni per cui i dati personali sono utili a vari fini, anche profittevoli.

Una questione giuridica si pone rispetto ai diritti delle persone decedute su cui si rinvia al relativo box nel capitolo *I diritti dell'interessato*.

3. Il trattamento

Il trattamento dei dati personali, secondo quanto previsto dall'art. 4, par. 1, n. 2 GDPR, è:

qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'a-

dattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

L'ampiezza di questa definizione, che include un elenco non tassativo di operazioni (così CGUE, 7 marzo 2024, C-740/20) contribuisce a garantire un'applicazione estesa della disciplina in materia di trattamento dei dati personali, funzionale alla tutela del diritto fondamentale alla protezione dei dati personali di cui all'art. 8 CDFUE (così CGUE, 5 ottobre 2023, C-659/22, §§ 27-28; v. anche CGUE, 5 ottobre 2023, C-659/22; sull'art. 8 CDFUE v. cap. *Le fonti della disciplina in materia di dati personali*).

A titolo di esempio, far comparire su una pagina Internet dati personali è da considerare come un'operazione di trattamento (CGUE, 6 novembre 2003, C-101/01, § 25), anche quando riguardano informazioni già pubblicate nei media tali e quali (CGUE, 13 maggio 2014, C-131/12, § 30). Ancora, la CGUE qualifica come trattamento la comunicazione orale di dati personali (CGUE, 7 marzo 2024, C-740/20).

Alcune operazioni di trattamento, come la raccolta e la conservazione, hanno regole peculiari, dovute alla loro specificità rispetto all'uso dei dati personali. Infatti, la raccolta è l'operazione che permette di creare i dati personali come un oggetto, anche giuridico, distinto dall'interessato, e la conservazione rende possibili ulteriori usi dei dati personali (Angiolini 2020).

Altri tipi di trattamenti si distinguono in ragione delle modalità, anche tecniche. Un esempio è quello della profilazione, che è definita dall'art. 4, par. 1, n. 4 GDPR come:

qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

La profilazione porta con sé alcuni rischi, legati alla mancata trasparenza delle tecniche usate per attuarla e alle conseguenze per gli interessati e può avere effetti discriminatori (Gruppo di Lavoro Art. 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Reg. UE 2016/679*, 6 febbraio 2018). E per questo ad essa si applicano anche particolari norme, come l'art. 22 GDPR, rubricato «processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione» (v. cap. *I diritti dell'interessato*).

4. Le categorie particolari di dati personali

L'art. 9 GDPR detta un regime specifico per le «categorie particolari di dati personali» (v. cap. *La disciplina dell'attività di trattamento*). Questi dati sono denominati anche 'sensibili' in quanto il loro trattamento può avere conseguenze significative rispetto alle libertà e ai diritti fondamentali dell'interessato (si vedano in proposito: il considerando 51 GDPR e le seguenti pronunce della Corte

di Giustizia dell'UE CGUE, 4 luglio 2023, C-252/21, spec. §§ 66 ss.; CGUE, 21 dicembre 2023, C-667/21, spec. §§ 37 ss.).

Le categorie particolari di dati personali sono descritte dal par. 1 dell'art. 9 GDPR, come quelle relative a quei dati che:

rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché [...] dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Tale elenco va letto congiuntamente all'art. 4, par. 1 nn. 13, 14 e 15 GDPR, che definisce i dati relativi alla salute, i dati genetici e i dati biometrici.

I dati relativi alla salute sono definiti come «i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute».

Rispetto alla definizione di tale categoria di dati, la Corte di Giustizia dell'UE ha affermato che l'espressione «dati relativi alla salute» deve essere interpretata in modo ampio, «in modo da includere informazioni relative a tutti gli aspetti, sia fisici che mentali, della salute di un individuo» (CGUE 6 novembre 2003, C-101/01; cfr., altresì, CGUE, 4 ottobre 2024, C-21/23, secondo la quale nel caso in cui il gestore di una farmacia commercializzi, tramite una piattaforma online, medicinali la cui vendita è riservata alle farmacie, le informazioni che i clienti di tale gestore inseriscono al momento dell'ordine online dei medicinali, quali il loro nome, l'indirizzo di consegna e gli elementi necessari all'individualizzazione dei medicinali, costituiscono dati relativi alla salute anche qualora la vendita di tali medicinali non sia soggetta a prescrizione medica).

Nella stessa ottica, il Comitato Europeo per la Protezione dei Dati (d'ora in avanti: EDPB) ha ritenuto che i dati relativi alla salute possono essere ricavati da fonti diverse; ad esempio, possono essere raccolti da un operatore sanitario nel corso di una visita di controllo o in una cartella clinica o ancora vi possono essere dati che, mediante riferimenti incrociati con altri dati, divengono «relativi alla salute» in quanto rivelano lo stato di salute o i rischi per la salute (EDPB, *Linee guida 03/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al COVID-19*, 21 aprile 2020).

Poi, sono considerati dati genetici ex art. 4, par. 1, n. 13:

i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione [si veda anche il considerando 34 del Reg. Ue 2016/679].

La peculiarità di tali dati è che possono riguardare più persone, come riconosciuto dalla Corte Europea dei Diritti dell'Uomo nella causa *Marper c. Regno Unito*, del 4 dicembre 2008, ric. n. 30562/04 e 30566/04.

A questo proposito, il Gruppo di lavoro art. 29 (ora sostituito dall'EDPB v. cap. *La regolamentazione e la tutela amministrativa*) nel suo documento di lavoro sui dati genetici, adottato il 17 marzo 2004, ha affermato che:

se da un lato le informazioni genetiche sono uniche e distinguono un individuo da altri individui, dall'altro possono anche rivelare informazioni e avere implicazioni per i parenti di sangue di quell'individuo (famiglia biologica), compresi quelli delle generazioni successive e precedenti. Inoltre, i dati genetici possono caratterizzare un gruppo di persone (ad esempio, comunità etniche).

I dati genetici sono una categoria di dati che mostra la complessità della dimensione individuale e collettiva dei dati e della protezione della salute: questi dati possono riguardare più persone e il loro trattamento può essere necessario per proteggere la salute di una o di molte di esse.

I dati biometrici sono definiti dall'art. 4, par. 1, n. 14 GDPR come

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

Dunque, ai sensi dell'art. 4, par. 1, n. 14 GDPR i dati biometrici sono generati attraverso l'uso di tecnologie specifiche che elaborano le caratteristiche degli individui per identificare (identificazione biometrica) o confermare (verifica biometrica) l'identità della persona interessata.

Nel leggere congiuntamente l'art. 4, par. 1, n. 14 e l'art. 9 GDPR emerge una questione interpretativa, discussa in dottrina; il regime, più rigoroso, definito dall'art. 9 GDPR relativo alle categorie particolari di dati personali (su cui v. cap. *Le definizioni fondamentali*) si applica anche a quei dati biometrici che non sono utilizzati per identificare in modo univoco una persona?

Dal punto di vista degli indici normativi, il nodo interpretativo sorge in quanto l'art. 9 GDPR fa riferimento ai «dati biometrici intesi a identificare in modo univoco una persona fisica», mentre l'art. 4 GDPR si riferisce ai dati che «ne consentono o confermano l'identificazione univoca».

L'interrogativo a cui rispondere è dunque se vi siano dati biometrici ai sensi dell'art. 4 GDPR che non siano però sottoposti al regime di cui all'art. 9 GDPR in quanto non sono, in concreto, trattati al fine di identificare in modo univoco una persona fisica.

La soluzione di tale questione interpretativa è in discussione. Infatti, se gli indici normativi non escludono *a priori* la possibilità di individuare dati biometrici ex art. 4 GDPR che non rientrino nelle categorie particolari di dati personali, d'altro canto da più parti si è notato che a prescindere dallo scopo per cui un dato biometrico viene utilizzato, le caratteristiche che possono essere estratte da esso mantengono un notevole potenziale per consentire l'identificazione delle persone o per influenzarle negativamente (European Union Agency for Fundamental Rights 2020, 8). Tali ultime considerazioni mostrano i rischi di una lettura restrittiva dell'art. 9 GDPR, e la necessità di interpretare le norme in materia di protezione dei dati personali alla luce della Carta dei Diritti Fondamentali dell'UE.

A fronte di una pluralità di interpretazioni dottrinali, nel contesto italiano è esemplificativa la pronuncia della Corte di Cassazione del 13 maggio 2024, n.

12967, dove la Corte, naturalmente anche in ragione del caso concreto che le era sottoposto, ha enunciato il seguente principio di diritto:

In tema di trattamento dei dati personali, ai sensi dell'art. 9 del Reg (UE) 2016/679, ricorre un trattamento di dati biometrici, come definiti dall'art. 4, n. 14 del Regolamento 2016/679, quando i dati personali sono ottenuti mediante un trattamento tecnico automatizzato specifico, realizzato con un software che, sulla base di riprese e analisi delle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, le elabora, evidenziando comportamenti o elementi anomali, e che perviene a un esito conclusivo, costituito da una elaborato video/foto che consente (o che conferma) l'identificazione univoca della persona fisica, restando irrilevante la circostanza che l'esito finale del trattamento sia successivamente sottoposto alla verifica finale di una persona fisica.

5. Il titolare del trattamento e la contitolarità

Il titolare del trattamento, secondo quanto prevede l'art. 4, par. 1, n. 7 GDPR è:

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

Dunque, sono principalmente due gli elementi che definiscono la figura del titolare: la determinazione dei mezzi e delle finalità del trattamento.

Occorre sottolineare che la qualifica di titolare del trattamento non dipende dalla volontà di chi tratta i dati ma dal ruolo che questi assume rispetto alla pianificazione del trattamento; con un esempio, sarà possibile scegliere se determinare finalità e mezzi del trattamento, ma una volta che si sia scelto questo assetto, non ci si potrà sottrarre alla qualificazione di titolare del trattamento.

La *ratio* di tale scelta legislativa è chiara: al soggetto che ha un ruolo molto significativo nell'organizzazione del trattamento sono anche attribuiti specifici obblighi (v. anche il considerando 74 GDPR), come quello relativo all'informativa di cui agli artt. 13 e 14 GDPR, e responsabilità, regolate anche dall'art. 82 GDPR (su cui v. il cap. *Il risarcimento del danno da illecito trattamento dei dati personali*).

Guardando alla giurisprudenza, la nozione di titolare del trattamento è stata interpretata in senso estensivo dalla Corte di Giustizia dell'UE, secondo cui

qualsiasi persona fisica o giuridica che influisca, per fini che le sono propri, sul trattamento di tali dati e partecipi pertanto alla determinazione delle finalità e dei mezzi di tale trattamento può essere considerata titolare di detto trattamento. A tal riguardo, non è necessario che le finalità e i mezzi del trattamento siano determinati mediante orientamenti scritti o istruzioni da parte del titolare del trattamento [...], né che quest'ultimo sia stato formalmente designato come tale. (CGUE, C-683/21, 5 dicembre 2023, *Nacionalinis Visuomenės Sveikatos Centras*, § 30)

Con riguardo alle ipotesi in cui la determinazione delle finalità e dei mezzi del trattamento sia fatta dal diritto nazionale, la Corte di Giustizia dell'UE ha affermato che la designazione del titolare da parte del diritto nazionale può essere anche implicita, purché «derivi in maniera sufficientemente certa dal ruolo, dalla funzione e dalle attribuzioni devoluti alla persona o all'entità» (CGUE, 11 gennaio 2024, C-231/22, § 30).

Quando più soggetti determinano congiuntamente i mezzi e le finalità del trattamento, questi sono contitolari. Una questione interpretativa significativa riguarda la definizione dei confini entro cui i mezzi o le finalità del trattamento sono determinati congiuntamente.

In proposito, la Corte di Giustizia dell'UE ha affermato che vi può essere una contitolarità anche se i ruoli dei contitolari sono diversi, tanto che non è necessario che tutti i contitolari abbiano accesso ai dati (CGUE, 10 luglio 2018, C-25/17, § 69; così anche CGUE, 7 marzo 2024, C-604/22). Si legge nella pronuncia CGUE, 5 dicembre 2023, C-683/21, che

la partecipazione alla determinazione delle finalità e dei mezzi del trattamento può assumere forme diverse, potendo tale partecipazione risultare sia da una decisione comune adottata da due o più soggetti sia da decisioni convergenti di tali soggetti. Orbene, in quest'ultimo caso, dette decisioni devono integrarsi, di modo che ciascuna di esse abbia un effetto concreto sulla determinazione delle finalità e dei mezzi del trattamento. (CGUE, 5 dicembre 2023, C-683/21, *Nacionalinis Visuomenės Sveikatos Centras*, § 43; si vedano anche: 5 giugno 2018, C-210/16, *Wirtschaftsakademie Schleswig-Holstein*; 29 luglio 2019, *Fashion ID*, C-40/17, 10 luglio 2018, *Jehovan todistajat*, C-25/17; CEPD, *Linee guida 7/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR*).

Ancora, a più riprese la Corte di Giustizia ha affermato che i contitolari possono non avere una responsabilità equivalente quando sono coinvolti in fasi diverse del trattamento e con differenti modalità (CGUE, 5 dicembre 2023, C-683/21, § 43; CGUE 5 giugno 2018, C-210/16).

L'art. 26 GDPR prevede alcuni obblighi in capo ai contitolari del trattamento. In particolare, i contitolari devono stabilire

in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, [...].

2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

L'art. 26, par. 3 GDPR prevede inoltre che l'interessato possa comunque esercitare i diritti previsti dall'GDPR verso ciascun titolare del trattamento.

Qualora i contitolari violino l'accordo di contitolarità secondo la più recente giurisprudenza della Corte di Giustizia dell'UE, vi sarà una violazione del GDPR che non comporta un trattamento illecito di dati personali, in quanto l'art. 26

GDPR non è parte del gruppo di norme, riunite attorno all'art. 6 GDPR rubricato «liceità del trattamento» che concorrono a determinare la liceità di un trattamento (CGUE, 4 maggio 2023, C-60/22).

Dunque, i rimedi per reagire a tale violazione andranno individuati nei poteri correttivi delle autorità di controllo (*ex art. 58 par. 2, GDPR*), nella proposizione di un reclamo all'autorità di controllo (*art. 77, par. 1, GDPR*) e nel risarcimento del danno eventualmente cagionato dal titolare del trattamento *ex art. 82 GDPR* (così CGUE, 4 maggio 2023, C-60/22).

6. Il responsabile del trattamento

Il responsabile del trattamento è definito dall'art. 4, par. 1, n. 8 GDPR come: «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

Dal punto di vista soggettivo, il responsabile è soggetto distinto dal titolare e non sono posti limiti particolari alla natura del soggetto che può essere nominato come responsabile, e può dunque essere una persona fisica, una persona giuridica, un'autorità pubblica, o un ente.

L'elemento che connota la figura del responsabile è che questi tratta i dati *per conto* del titolare da parte del responsabile, come risulta evidente anche dalla lettura dell'art. 28 GDPR, rubricato 'Responsabile del trattamento', su cui si tornerà (v. cap. 7 *La regolamentazione di diversi rapporti che riguardano i dati personali*), e il cui par. 2, lett. a) prevede che il responsabile tratti i dati personali «soltanto su istruzione documentata del titolare del trattamento», salve alcune eccezioni.

Proprio perché il responsabile del trattamento tratta i dati personali per conto del titolare, fra i suoi obblighi vi sono l'adozione delle misure che garantiscano la sicurezza del trattamento *ex art. 32 GDPR* e quello di assistere il titolare nel garantire la sicurezza del trattamento e nel dare seguito alle richieste per l'esercizio dei diritti dell'interessato (su cui v. cap. *I diritti dell'interessato*).

7. Il responsabile della protezione dei dati

Il responsabile per la protezione dei dati è una figura disciplinata dagli articoli da 37 a 39 del GDPR, che deve avere, *ex art. 37, par. 5 GDPR*, una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati.

Secondo quanto previsto dall'art. 39 RGDP, il responsabile della protezione dei dati deve:

- a) informare e fornire consulenza al titolare o al responsabile del trattamento rispetto agli obblighi derivanti dalla legislazione in materia di protezione dei dati;
- b) sorvegliare l'osservanza della legislazione sulla protezione dei dati;
- c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 GDPR;
- d) cooperare con l'autorità di controllo e fungere da punto di contatto per tale autorità per questioni connesse al trattamento.

L'art. 38 GDPR prevede alcune regole specifiche che concernono il rapporto fra il responsabile per la protezione dei dati e il titolare o il responsabile che lo designa.

In primo luogo, il responsabile per la protezione dei dati deve essere «tempestivamente e adeguatamente» coinvolto in tutte le questioni riguardanti la protezione dei dati personali e deve essere messo in condizioni di assolvere i propri compiti e dunque anche di accedere ai dati personali e ai trattamenti.

In secondo luogo, il titolare e il responsabile del trattamento si devono assicurare che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione dei suoi compiti, e non possono rimuoverlo o penalizzarlo per l'esecuzione dei suoi compiti.

Inoltre, il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento, ed è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

Infine, gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

Non sempre il titolare e il responsabile del trattamento sono obbligati a nominare un responsabile per la protezione dei dati.

Secondo quanto dispone l'art. 37 GDPR il titolare del trattamento e il responsabile del trattamento devono designare il responsabile per la protezione dei dati nei seguenti casi:

- a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
- c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Nelle altre ipotesi – e ove non sia previsto l'obbligo di nomina da altri atti normativi – i titolari del trattamento e i responsabili del trattamento *possono* designare tale figura.

Rispetto alla figura del Responsabile della Protezione dei Dati si possono menzionare il *Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico*, adottato dal Garante per la Protezione dei Dati nel 2021 e *le Linee guida sui responsabili della protezione dei dati, nella versione adottata in data 5 aprile 2017 dal Gruppo di Lavoro Art. 29*, oggetto dell'*Endorsement 1/2018* del Comitato Europeo per la Protezione dei Dati (EDPB), documenti utili anche rispetto all'attività che in concreto svolgono i Responsabili della Protezione dei Dati.

8. Le definizioni nel Regolamento 2022/868 sulla governance dei dati e nel Regolamento 2023/2854 sui dati e il coordinamento con il GDPR

Oltre alle definizioni previste dal GDPR di cui ci si è occupati nei paragrafi precedenti, occorre considerare anche le nozioni introdotte con il Regolamento sulla governance dei dati n. 2022/868 del 30 maggio 2022 (d'ora in avanti: *Data Governance Act*) e il Regolamento sui dati n. 2023/2854, del 13 dicembre 2023 (d'ora in avanti *Data Act*).

Entrambi i regolamenti prevedono delle definizioni e una norma relativa al rapporto con il GDPR.

In particolare, l'art. 1 del *Data Governance Act* prevede che:

3. Il diritto dell'Unione e nazionale in materia di protezione dei dati personali si applica a qualsiasi dato personale trattato in relazione al presente regolamento. In particolare, il presente regolamento non pregiudica i regolamenti (UE) 2016/679 e (UE) 2018/1725 e le direttive 2002/58/CE e (UE) 2016/680, anche per quando riguarda i poteri e le competenze delle autorità di controllo. In caso di conflitto tra il presente regolamento e il diritto dell'Unione in materia di protezione dei dati personali o il diritto nazionale adottato conformemente a tale diritto dell'Unione, prevale il pertinente diritto dell'Unione o nazionale in materia di protezione dei dati personali. Il presente regolamento non crea una base giuridica per il trattamento dei dati personali e non influisce sui diritti e sugli obblighi di cui ai regolamenti (UE) 2016/679 e (UE) 2018/1725 o alle direttive 2002/58/CE o (UE) 2016/680.

L'art. 1 par. 5 del *Data Act* prevede che:

5. Il presente regolamento fa salvo il diritto dell'Unione e nazionale in materia di protezione dei dati personali, della vita privata e della riservatezza delle comunicazioni e dell'integrità delle apparecchiature terminali, che si applica ai dati personali trattati in relazione ai diritti e agli obblighi, in particolare i regolamenti (UE) 2016/679 e (UE) 2018/1725 e la direttiva 2002/58/CE, nonché i poteri e le competenze delle autorità di controllo e i diritti degli interessati. Nella misura in cui gli utenti sono gli interessati, i diritti di cui al capo II del presente regolamento integrano i diritti di accesso da parte degli interessati e i diritti alla portabilità dei dati di cui agli articoli 15 e 20 del regolamento (UE) 2016/679. In caso di conflitto tra il presente regolamento e il diritto dell'Unione in materia di protezione dei dati personali o della vita privata o la legislazione nazionale adottata conformemente a tale diritto dell'Unione, prevale il pertinente diritto dell'Unione o nazionale in materia di protezione dei dati personali o della vita privata.

Dunque, qualora vi sia un conflitto fra una norma dei due regolamenti appena citati e il GDPR, prevarrà quest'ultimo. Questa regola è di particolare importanza in quanto diviene un criterio ermeneutico per l'interprete che deve coordinare i testi normativi ai fini della loro applicazione.

Tale criterio risulta utile anche in relazione alle definizioni previste dall'art. 2 del *Data Act* e dall'art. 2 del *Data Governance Act*, in quanto alcune di queste devono essere coordinate con quelle previste dal GDPR.

In particolare, sia il *Data Governance Act* che il *Data Act* all'art. 2, par. 1 prevedono la seguente definizione di «dati»: «qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva».

A tale definizione segue quella di dati personali (art. 2, par. 1, n. 3, sia del *Data Governance Act*, sia del *Data Act*), che rinvia a quella data dall'art. 4, par. 1, n. 1, GDPR (v. in questo capitolo il § 3), e la definizione di dati non personali, che vengono descritti come «i dati diversi dai dati personali».

Alcune altre nozioni, come quella di consenso nell'art. 2, par. 1, n. 5 del *Data Governance Act* e quella di interessato (art 2, par. 1, n. 11 *Data Act*; art 2, par. 1, n. 7 *Data Governance Act*) rinviano espressamente alle relative definizioni previste dal GDPR.

Rispetto invece alle qualificazioni di chi tratta i dati, non vi è corrispondenza fra il GDPR e i nuovi regolamenti. Di seguito è tracciato un quadro delle principali definizioni rilevanti nel contesto di questo manuale.

8.1. La definizione dei soggetti

Gli elementi di differenza fra le definizioni date dai due regolamenti ben si colgono attraverso il loro raffronto nella tabella che segue.

	Art. 2 del <i>Data Governance Act</i>	Art. 2 del <i>Data Act</i>
Titolare dei dati	Una persona giuridica, compresi gli enti pubblici e le organizzazioni internazionali, o una persona fisica che non è l'interessato rispetto agli specifici dati in questione e che, conformemente al diritto dell'Unione o nazionale applicabile, ha il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli (n. 8)	Una persona fisica o giuridica che ha il diritto o l'obbligo, conformemente al presente regolamento, al diritto applicabile dell'Unione o alla legislazione nazionale adottata conformemente al diritto dell'Unione, di utilizzare e mettere a disposizione dati, compresi, se concordato contrattualmente, dati del prodotto o di un servizio correlato che ha reperito o generato nel corso della fornitura di un servizio correlato (n. 13)
Utente dei dati	Una persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali e che <i>ha diritto</i> , anche a norma del GDPR in caso di dati personali, <i>a utilizzare tali dati a fini commerciali o non commerciali</i> (n. 9)	La definizione non è presente nel <i>Data Act</i> .
Utente	La definizione non è presente nel <i>Data Governance Act</i> .	Una persona fisica o giuridica che possiede un prodotto connesso o a cui sono stati trasferiti contrattualmente diritti temporanei di utilizzo di tale prodotto connesso o che riceve un servizio correlato (12)

	Art. 2 del <i>Data Governance Act</i>	Art. 2 del <i>Data Act</i>
Destinatario dei dati	La definizione non è presente nel <i>Data Governance Act</i> .	Una persona fisica o giuridica, che agisce per fini connessi alla sua attività commerciale, imprenditoriale, artigianale o professionale, diversa dall'utente di un prodotto connesso o di un servizio correlato, a disposizione della quale il titolare dei dati mette i dati, e che può essere un terzo in seguito a una richiesta da parte dell'utente al titolare dei dati o conformemente a un obbligo giuridico ai sensi del diritto dell'Unione o della legislazione nazionale adottata conformemente al diritto dell'Unione (14)

La tabella mostra infatti che alcune nozioni presenti nel *Data Act* non trovano una corrispondenza nel *Data Governance Act*. Seppur tale circostanza si può in linea generale spiegare in ragione della diversità delle funzioni e dell'oggetto della disciplina dettata dai due regolamenti, di certo non facilita lo sviluppo di un quadro sistematico chiaro e comune all'ambito del «diritto dei dati».

Un particolare elemento di criticità è la previsione di due definizioni diverse per la medesima nozione di «titolare dei dati» (in senso critico si veda anche EDPB-GEPD, *Parere congiunto EDPB-GEPD 2/2022 sulla proposta del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo*, 4 maggio 2022). Infatti, la coesistenza di due diverse definizioni della stessa nozione, all'interno della stessa materia e nella medesima area legislativa rende ancora più evidente la difficoltà nella costruzione di un sistema coerente all'interno del «diritto dei dati» e suggerisce una modifica legislativa che permetta un uso il più possibile univoco delle nozioni.

Inoltre, dal punto di vista del coordinamento fra il GDPR da una parte e il *Data Act* e il *Data Governance Act* dall'altra, si deve sottolineare che, come già ricordato in apertura di questo paragrafo, i recenti regolamenti non pregiudicano l'applicazione del GDPR.

Di conseguenza, quando i dati sono personali, è il GDPR che ne definisce lo statuto di base, e cioè i limiti del loro lecito trattamento, e dunque che in sostanza delinea anche i diritti di utilizzo e di circolazione alla base delle definizioni di «titolare dei dati» e «utente dei dati».

Rimane comunque un profilo critico, che corrisponde ad una discussione aperta in dottrina, legato alla qualificazione della situazione giuridica soggettiva di chi tratta i dati come «diritto» sia nel *Data Act* che nel *Data Governance Act*, qualificazione che non è per nulla scontata rispetto alla situazione giuridica soggettiva del titolare del trattamento che, se ricorrono le condizioni previste dalla disciplina in materia di protezione dei dati personali, può lecitamente trattare i dati personali su cui ha accesso, ma che, qualora non abbia accesso a dati personali non ha diritto – salvo che sia espressamente previsto da una norma di legge (v. cap. 6, *Le intersezioni fra disciplina in materia di dati personali e diritto dei consumatori*) – di ottenere tale accesso ai dati (Angiolini 2025).

Riferimenti bibliografici

- Angiolini, Chiara. 2025. "Titolari dei dati, utenti, destinatari dei dati: ambito soggettivo di applicazione." In Bachelet, Vittorio, Gianluigi Marino e Antonio Racano (a cura di). *Accesso equo ai dati e loro utilizzo: profili sistematici e applicativi nell'orizzonte del diritto privato*. Wolters Kluwer.
- Cerrina Feroni, Ginevra. 2025. "Data Act, accesso e riuso dei dati: quali sfide per la protezione dei dati personali?." In Morace Pinelli, Arnaldo (a cura di), *Data Act. Introduzione interdisciplinare e commentario al Regolamento (UE) 2023/2854*. Pisa: Pacini.
- Kuner, Christopher, Bygrave Lee A, Docksey, Christopher, Drechsler, Laura. (a cura di). 2020. *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford: Oxford University Press.
- Martial-Braz, Nathalie, Rochfeld, Judith (a cura di). 2019. *Droit des données personnelles. Les spécificités du droit français au regard du RGPD*. Paris: Dalloz.
- European Union Agency for Fundamental Rights. 2020. *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> (ultima consultazione: aprile 2025).
- Purtova, Nadezhda. 2018. "The law of everything. Broad concept of personal data and future of EU data protection law." *International Review of Law, Computers & Technology* 28, 2: 40-81.
- Rodotà, Stefano. 1995. *Tecnologie e diritti*. Bologna: Il Mulino.
- Zuboff, Shoshana. 2019. *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*. Roma: Luiss University Press.