Consiglio
dell'Unione europea

Bruxelles, 12 giugno 2019
(OR. en)

10253/19

TELECOM 260
COMPET 486
MI 519
DATAPROTECT 168
JAI 683

NOTA DI TRASMISSIONE

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	29 maggio 2019
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2019) 250 final
Oggetto:	COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union

Si trasmette in allegato, per le delegazioni, il documento COM(2019) 250 final.

All.: COM(2019) 250 final

COMMISSIONE
EUROPEA

Bruxelles, 29.5.2019
COM(2019) 250 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union

Indice

Il presente documento è fornito dalla Commissione europea esclusivamente a titolo informativo. Esso non contiene alcuna interpretazione autorevole del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, né costituisce una decisione o un'opinione della Commissione europea. Tale documento non pregiudica eventuali decisioni o opinioni della Commissione europea, né le competenze della Corte di giustizia dell'Unione europea per l'interpretazione del regolamento conformemente ai trattati dell'UE.

1 INTRODUZIONE

In una economia sempre più basata sui dati, i flussi di dati sono al centro dei processi aziendali nelle imprese di qualsiasi dimensione e in tutti i settori. Le nuove tecnologie digitali aprono nuove opportunità al grande pubblico, alle imprese e alle pubbliche amministrazioni dell'Unione europea (l'"UE").

Per potenziare ulteriormente lo scambio transfrontaliero dei dati e promuovere l'economia dei dati, a novembre 2018 il Parlamento europeo e il Consiglio hanno adottato il regolamento (UE) 2018/1807 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea[1] (il "regolamento sulla libera circolazione dei dati non personali") basato su una proposta avanzata dalla Commissione europea (la "Commissione"). Il regolamento si applica a decorrere dal 28 maggio 2019. Il principio della libera circolazione dei dati personali è già sancito nel regolamento (UE) 2016/679 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 (il "regolamento generale sulla protezione dei dati")[2]. Ne consegue che ora esiste un quadro globale per uno spazio comune europeo dei dati e per la libera circolazione di tutti i dati all'interno dell'Unione europea[3].

Il regolamento sulla libera circolazione dei dati non personali garantisce la certezza del diritto alle imprese per quanto concerne il trattamento dei loro dati in qualsiasi luogo dell'UE, accresce la fiducia nei servizi di trattamento di dati e contrasta le pratiche di "vendor lock-in". Questo accrescerà le possibilità di scelta dei consumatori, migliorerà l'efficienza e promuoverà l'adozione di tecnologie cloud, determinando ingenti risparmi per le imprese nell'UE. Da uno studio emerge che le imprese nell'UE possono risparmiare il 20-50 % dei loro costi IT passando al cloud[4].

Grazie ai due regolamenti, i dati possono circolare liberamente tra gli Stati membri, consentendo agli utenti dei servizi di trattamento di dati di utilizzare i dati raccolti nei diversi mercati dell'UE per migliorare la loro produttività e competitività. Gli utenti possono quindi beneficiare pienamente delle economie di scala create dal grande mercato dell'UE, migliorando la propria competitività globale e aumentando l'interconnettività dell'economia dei dati europea.

---

[1] Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea (GU L 303 del 28.11.2018, pag. 59).

[2] 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 (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

[3] Il regolamento generale sulla protezione dei dati si estende anche allo Spazio economico europeo (SEE), che include l'Islanda, il Liechtenstein e la Norvegia. Inoltre, il regolamento sulla libera circolazione dei dati non personali è indicato come rilevante ai fini del SEE.

[4] Deloitte: *Measuring the economic impact of cloud computing in Europe (Misurazione dell'impatto economico del «cloud computing» in Europa)*, SMART 2014/0031, 2016. Disponibile online al seguente indirizzo: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

Il regolamento sulla libera circolazione dei dati non personali è caratterizzato da tre aspetti significativi:

- vieta, di regola, agli Stati membri di imporre obblighi sui luoghi in cui i dati dovrebbero essere localizzati; eccezioni a questa regola possono essere giustificate solo per motivi di sicurezza pubblica nel rispetto del principio di proporzionalità;
- istituisce un meccanismo di cooperazione per garantire che le autorità competenti continuino a poter esercitare tutti i diritti di cui godono per quanto riguarda l'accesso ai dati trattati in un altro Stato membro;
- prevede incentivi per l'industria, con il sostegno della Commissione, nell'intento di sviluppare codici di autoregolamentazione sul cambio di fornitore di servizi e la portabilità dei dati.

Scopo delle presenti linee guida

Le presenti linee guida soddisfano l'articolo 8, paragrafo 3, del regolamento sulla libera circolazione dei dati non personali, che impone alla Commissione di pubblicare orientamenti sull'interazione tra questo regolamento e il regolamento generale sulla protezione dei dati, "in particolare per quanto concerne gli insiemi di dati composti sia da dati personali che da dati non personali".

Le presenti linee guida intendono aiutare gli utenti, specialmente le piccole e medie imprese, a comprendere meglio l'interazione tra il regolamento sulla libera circolazione dei dati non personali e il regolamento generale sulla protezione dei dati[5]. Pertanto, le linee guida vertono in modo particolare: i) sui concetti di dati personali e dati non personali; ii) sui principi della libera circolazione dei dati e del divieto di qualsiasi obbligo di localizzazione dei dati ai sensi di entrambi i regolamenti; iii) sulla nozione di portabilità dei dati secondo il regolamento sulla libera circolazione dei dati non personali. Esse riguardano anche i requisiti di autoregolamentazione stabiliti nei due regolamenti.

Il regolamento sulla libera circolazione dei dati non personali riguarda soltanto "i dati diversi dai dati personali" come definito dal regolamento generale sulla protezione dei dati. Il regolamento generale sulla protezione dei dati disciplina il trattamento dei dati personali, che costituisce un elemento fondamentale del quadro sulla protezione dei dati dell'UE[6]. Esso è

[5] Considerando 37 del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

[6]
- 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 (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).
- Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

entrato in vigore negli Stati membri il 25 maggio 2018. Il regolamento stabilisce norme armonizzate per proteggere le persone nell'UE/SEE con riguardo al trattamento dei dati di carattere personale e alla libera circolazione di tali dati. Fra le altre disposizioni, il regolamento generale sulla protezione dei dati: i) precisa quali informazioni costituiscono un dato personale; ii) stabilisce le basi giuridiche del trattamento; iii) definisce i diritti e gli obblighi che devono essere osservati nel trattare questi dati[7]. Per quanto riguarda il principio della libera circolazione dei dati personali, l'articolo 1, paragrafo 3, del regolamento generale sulla protezione dei dati prevede che "la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali".

Nella maggior parte delle situazioni della vita reale, un insieme di dati è generalmente composto sia da dati personali che da dati non personali. Per designare questo caso si utilizza di solito il termine "insieme di dati misti". La sezione 2.2 che segue spiega ulteriormente l'interazione tra il regolamento sulla libera circolazione dei dati non personali e il regolamento generale sulla protezione dei dati con riferimento agli insiemi di dati misti.

Per motivi di chiarezza, non vi sono obblighi contraddittori previsti dal regolamento generale sulla protezione dei dati e dal regolamento sulla libera circolazione dei dati non personali.

– Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89).

– Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento di dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37) (attualmente in fase di revisione).

[7] Per ulteriori indicazioni sui vari aspetti 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 (regolamento generale sulla protezione dei dati) e la normativa europea in materia di protezione dei dati, si prega di consultare il sito web del comitato europeo per la protezione dei dati, il quale ha emanato diverse linee guida conformemente all'articolo 70 del regolamento generale sulla protezione dei dati disponibili al seguente indirizzo: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_it. Il sito web in questione contiene anche riferimenti alle linee guida, alle raccomandazioni e ad altri documenti emanati dal predecessore del comitato europeo per la protezione dei dati, il gruppo di lavoro articolo 29. Inoltre, allo scopo di sensibilizzare maggiormente i cittadini e le imprese in merito al 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 (regolamento generale sulla protezione dei dati), la Commissione ha adottato una comunicazione sulla protezione dei dati - Orientamenti per l'applicazione diretta del regolamento generale sulla protezione dei dati (COM(2018) 43 final) disponibile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043.

2 L'interazione tra il regolamento sulla libera circolazione dei dati non personali e il regolamento generale sulla protezione dei dati - gli insiemi di dati misti

2.1 Il concetto di dati non personali nel regolamento sulla libera circolazione dei dati non personali

Il regolamento sulla libera circolazione dei dati non personali[8] intende garantire la libera circolazione dei dati diversi dai dati personali. Il regolamento utilizza in tutto il testo il termine "dati", il quale dovrebbe essere inteso come "dati diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679" [il regolamento generale sulla protezione dei dati][9]. Tali dati, che sono anche indicati in questo documento come "**dati non personali**", sono definiti in contrapposizione (*a contrario*) ai dati personali, come stabilito nel regolamento generale sulla protezione dei dati.

Dati personali

Il regolamento generale sulla protezione dei dati specifica che per "dato personale" si intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

L'ampia definizione di dati personali è intenzionale ed è rimasta sostanzialmente invariata nel regolamento generale sulla protezione dei dati rispetto alla normativa precedente[10]. Molti aspetti della definizione di dati personali, quali "qualsiasi informazione", "riguardante", "identificata o identificabile", sono già stati affrontati dal gruppo di lavoro articolo 29[11] nel suo parere 4/2007 sul concetto di dati personali adottato il 20 giugno 2007, WP 136.

---

8 Articolo 1 del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

9 Cfr. articolo 3, paragrafo 1, del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

10 Cfr. articolo 2, lettera a), della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (data di termine della validità: 24 maggio 2018, abrogata dal regolamento generale sulla protezione dei dati). Cfr. anche la giurisprudenza della Corte di giustizia sulla definizione di dati personali, che riconosce l'ampia interpretazione di tale nozione, ad esempio la sentenza della Corte di giustizia del 29 gennaio 2009, *Productores de Música de España (Promusicae)* contro *Telefónica de España SAU*, C-275/06, ECLI:EU:C:2008:54; la sentenza della Corte di giustizia del 24 novembre 2011, *Scarlet Extended SA* contro *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, ECLI:EU:C:2011:771; la sentenza della Corte di giustizia del 19 ottobre 2016, *Patrick Breyer* contro *Bundersrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779.

11 Il gruppo di lavoro articolo 29 era un organo consultivo che ha fornito pareri alla Commissione sulle questioni relative alla protezione dei dati e ha contribuito allo sviluppo di politiche armonizzate per la protezione dei dati nell'UE. Dopo l'entrata in vigore, il 25 maggio 2018, del regolamento generale sulla protezione dei dati, il gruppo di lavoro articolo 29 è stato sostituito dal comitato europeo per la protezione dei dati.

È pratica comune, in settori come la ricerca, ricorrere a pseudonimi per i dati personali al fine da nascondere l'identità di un soggetto. La **pseudonimizzazione** consiste nel trattamento dei dati personali in modo tale che non sia più possibile attribuirli a un interessato specifico senza l'utilizzo di informazioni aggiuntive. Queste informazioni aggiuntive sono conservate separatamente e protette da misure tecniche o organizzative (ad es. cifratura)[12,13]. Tuttavia, i dati pseudonimizzati sono comunque considerati informazioni su una persona identificabile, se possono essere attribuiti a questo soggetto utilizzando informazioni aggiuntive[14]. Secondo il regolamento generale sulla protezione dei dati, tali dati **sono considerati dati personali**.

Dati non personali

Laddove i dati non siano "dati personali", secondo quanto stabilito dal regolamento generale sulla protezione dei dati, essi costituiscono dati **non personali**. I dati non personali possono essere classificati in base alla loro origine come:

- in primo luogo, dati che in origine non si riferivano a una persona fisica identificata o identificabile, come i dati sulle condizioni meteorologiche prodotti da sensori installati sulle turbine eoliche o i dati sulle esigenze di manutenzione delle macchine industriali;

- in secondo luogo, dati che inizialmente erano dati personali, ma che poi sono stati resi **anonimi**[15]. L'"anonimizzazione" dei dati personali è diversa dalla pseudonimizzazione (cfr. sopra), in quanto i dati che sono stati resi anonimi in modo adeguato non possono essere attribuiti a una persona specifica, neppure ricorrendo a informazioni aggiuntive[16] e sono pertanto dati non personali.

---

12 Cfr. articolo 4, punto 5, 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 (regolamento generale sulla protezione dei dati), il quale definisce la "pseudonimizzazione".

13 Ad esempio, una ricerca sugli effetti di una nuova medicina potrebbe essere considerata come pseudonimizzazione, se i dati personali dei partecipanti allo studio fossero sostituiti da attributi univoci (ad es. numero o codice) nella documentazione della ricerca e i loro dati personali fossero conservati a parte, con gli attributi univoci assegnati, in un documento protetto (ad es. in una banca di dati protetta da password).

14 Cfr. considerando 26 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 (regolamento generale sulla protezione dei dati).

15 Cfr. considerando 26 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 (regolamento generale sulla protezione dei dati), il quale stabilisce che "…i principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato."

16 Cfr. sentenza della Corte di giustizia del 19 ottobre 2016, *Patrick Breyer* contro *Bundersrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779. La Corte di giustizia ha ritenuto che l'indirizzo di protocollo Internet (IP) dinamico possa rientrare nella nozione di dati personali, anche se un soggetto terzo (ad es. un fornitore di servizi Internet) è in possesso di dati supplementari che renderebbero possibile identificare il soggetto. La possibilità di identificare il soggetto deve rientrare tra i mezzi che possono essere ragionevolmente utilizzati per identificare la persona, direttamente o indirettamente.

La valutazione se i dati siano stati adeguatamente resi anonimi dipende dalle condizioni specifiche ed uniche di ogni singolo caso[17]. Diversi esempi di reidentificazione di insiemi di dati, che erano stati apparentemente resi anonimi, hanno evidenziato che tale valutazione può essere impegnativa[18]. Per stabilire se un soggetto è identificabile, si devono osservare tutti i mezzi che possono essere ragionevolmente utilizzati dal titolare del trattamento o da un altro individuo per identificare, direttamente o indirettamente, una persona[19].

Esempi di dati non personali

- I dati che sono aggregati fino a che i singoli eventi (quali i viaggi all'estero di una persona o i tipi di spostamenti che potrebbero costituire dati personali) non siano più identificabili possono essere considerati dati anonimi[20]. I dati anonimi sono, ad esempio, utilizzati nelle statistiche o nelle relazioni sulle vendite (ad esempio per valutare la popolarità di un prodotto e delle sue caratteristiche).
- I dati del trading ad alta frequenza nel settore finanziario o i dati sull'agricoltura di precisione che aiutano a monitorare e a ottimizzare l'uso di pesticidi, nutrienti e acqua.

Tuttavia, se i dati non personali possono essere associati in qualsiasi modo a una persona, facendo sì che essa sia direttamente o indirettamente identificabile, questi devono essere considerati dati personali.

Ad esempio, se una relazione di controllo della qualità su una linea di produzione rende possibile associare i dati a specifici operai (ad es. coloro che stabiliscono i parametri di produzione), i dati sarebbero considerati dati personali e si deve applicare il regolamento generale sulla protezione dei dati. Le stesse regole si applicano quando gli sviluppi della tecnologia e dell'analisi dei dati consentono di convertire i dati anonimi in dati personali. [21]

---

[17] L'anonimizzazione dei dati dovrebbe sempre essere effettuata utilizzando le tecniche di anonimizzazione più all'avanguardia.

[18] Per esempi di reidentificazione di dati apparentemente resi anonimi si veda lo studio sui futuri flussi di dati realizzato per la commissione ITRE del Parlamento europeo da Blackman, C., Forge, S.: *Data Flows — Future Scenarios: In-Depth Analysis for the ITRE Committee,* 2017, pag. 22, riquadro 2. Disponibile online al seguente indirizzo: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf.

[19] Cfr. considerando 26 del regolamento (UE) 2016/679, il regolamento generale sulla protezione dei dati, secondo cui ″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.″

[20] Cfr. gruppo di lavoro articolo 29: *parere 05/2014 sulle tecniche di anonimizzazione*, adottato il 10 aprile 2014, WP216, pag. 9: "Soltanto se il responsabile del trattamento aggrega i dati a un livello in cui i singoli eventi non sono più identificabili si può definire anonimo l'insieme di dati risultante. Ad esempio, se un'organizzazione raccoglie dati sugli spostamenti delle persone, i tipi di spostamenti individuali a livello di evento rientrano ancora tra i dati personali per tutte le parti coinvolte, fintantoché il responsabile del trattamento (o altri) ha ancora accesso ai dati non trattati originali, anche se gli identificatori diretti sono stati espunti dall'insieme dei dati forniti a terzi. Tuttavia, se il responsabile del trattamento cancella i dati non trattati e fornisce a terzi solamente statistiche aggregate ad alto livello, ad esempio "il lunedì sulla rotta X i passeggeri sono più numerosi del 160% rispetto al martedì", i dati possono essere definiti anonimi."

[21] Se i dati personali sono trattati illegalmente o il trattamento viola in altro modo il regolamento generale sulla protezione dei dati, gli interessati (persone fisiche) hanno diritto, in base a tale regolamento, di presentare

Poiché la definizione di dati personali si riferisce alle "persone fisiche", gli insiemi di dati che contengono i nomi e i dati di contatto delle persone giuridiche sono in linea di principio dati non personali[22]. Tuttavia, in alcuni casi specifici, possono costituire dati personali[23]. Questo si verifica se, ad esempio, il nome della persona giuridica corrisponde a quello della persona fisica che lo possiede o se le informazioni si riferiscono a una persona fisica identificata o identificabile[24].

2.2 Insiemi di dati misti

Il regolamento sulla libera circolazione dei dati non personali e il regolamento generale sulla protezione dei dati affrontano la libera circolazione dei dati nell'UE da due angolazioni differenti.

Il regolamento sulla libera circolazione dei dati non personali impone un divieto generale degli obblighi di localizzazione dei dati per i dati non personali. L'articolo 4, paragrafo 1, del regolamento vieta gli obblighi di localizzazione dei dati, a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità.

Il regolamento generale sulla protezione dei dati, oltre ad assicurare un alto livello di protezione dei dati personali, garantisce la libera circolazione dei dati personali. Ai sensi dell'articolo 1, paragrafo 3, del regolamento, la libera circolazione dei dati personali "non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali". Insieme, i due regolamenti dispongono la libera circolazione di "tutti" i dati nell'UE. Le disposizioni specifiche sono ulteriormente affrontate nelle sezioni 3.1 e 3.2.

Un insieme di dati misti è composto sia da dati personali che da dati non personali. Gli insiemi di dati misti rappresentano la maggior parte degli insiemi di dati utilizzati nell'economia dei dati e sono comuni a causa degli sviluppi tecnologici, come l'Internet delle cose (ad es. oggetti che si connettono digitalmente), l'intelligenza artificiale e le tecnologie che consentono l'analisi dei megadati.

---

un reclamo presso un'autorità di controllo nazionale (autorità competente per la protezione dei dati personali) nell'UE o di esercitare un effettivo ricorso giurisdizionale dinanzi a un tribunale nazionale. I compiti, le competenze e i poteri delle autorità di controllo nazionale sono disciplinati nel capo VI, sezione 2, del regolamento generale sulla protezione dei dati.

[22] Il considerando 14 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 (regolamento generale sulla protezione dei dati) afferma che "il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto". Tuttavia, ciò deve essere interpretato alla luce della definizione di dati personali contenuta nell'articolo 4, paragrafo 1, del regolamento generale sulla protezione dei dati.

[23] Cfr. sentenza della Corte di giustizia del 9 novembre 2010 nelle cause congiunte *Volker und Markus Schecke GbR* (C-92/09) e *Hartmut Eifert* (C-93/09) contro *Land Hessen*, ECLI:EU:C:2010:662, punto 52.

[24] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_it.

Esempi di insiemi di dati misti

- Un documento fiscale di un'impresa, che contiene il nome e il numero di telefono dell'amministratore delegato;
- insiemi di dati di una banca, in particolare quelli che contengono informazioni sui clienti e dettagli delle transazioni, come servizi di pagamento (carte di credito e di debito), applicazioni di partner relationship management (PRM) e contratti di prestito, documenti che includono dati misti relativi sia a persone fisiche che giuridiche;
- dati statistici resi anonimi di un istituto di ricerca e dati non trattati inizialmente raccolti, come le risposte dei singoli intervistati alle domande di un'indagine statistica;
- una banca dati di conoscenze di un'impresa riguardante i problemi IT e le loro soluzioni basate sulle singole relazioni degli incidenti informatici;
- dati relativi all'Internet delle cose, dove alcuni dati consentono di fare ipotesi sulle persone identificabili (ad es. presenza a un particolare indirizzo e modelli di utilizzo);
- analisi dei dati del registro operativo delle attrezzature di produzione nell'industria manifatturiera.

Esempio: servizi di gestione delle relazioni con i clienti

Alcune banche utilizzano servizi di gestione delle relazioni con i clienti (customer relationship management - CRM) forniti da soggetti terzi che richiedono di rendere disponibili i dati dei clienti nell'ambiente CRM. I dati del servizio CRM comprenderanno tutte le informazioni necessarie per gestire efficacemente le interazioni con i clienti, come il loro indirizzo postale ed email, il numero di telefono, i prodotti e i servizi che acquistano e le relazioni sulle vendite, tra cui i dati aggregati. Questi dati possono quindi includere sia dati personali che non personali dei clienti.

In riferimento agli insiemi di dati misti, il regolamento sulla libera circolazione dei dati non personali[25] dispone che:

"Nel caso di un insieme di dati composto sia da dati personali che da dati non personali, il presente regolamento si applica alla parte dell'insieme contenente i dati non personali. Qualora i dati personali e non personali all'interno di un insieme di dati siano indissolubilmente legati, il presente regolamento lascia impregiudicata l'applicazione del regolamento (UE) 2016/679."

Ciò significa che, in caso di un insieme di dati composto sia da dati personali che da dati non personali:

- il regolamento sulla libera circolazione dei dati non personali si applica alla parte dell'insieme contenente i dati non personali;

[25] Articolo 2, paragrafo 2, del regolamento stesso.

- la disposizione sulla libera circolazione dei dati del regolamento generale sulla protezione dei dati[26] si applica alla parte dell'insieme contenente i dati personali;
- se le parti di dati personali e di dati non personali sono "indissolubilmente legate", i diritti e gli obblighi in materia di protezione dei dati derivanti dal regolamento generale sulla protezione dei dati si applicano pienamente all'insieme di dati misti, anche quando i dati personali rappresentano soltanto una piccola parte dell'insieme di dati[27].

Questa interpretazione è conforme con il diritto alla protezione dei dati personali sancito dalla Carta dei diritti fondamentali dell'Unione europea[28] e con il considerando 8 del regolamento sulla libera circolazione dei dati non personali[29]. Il considerando 8 dispone che ″il quadro giuridico relativo alla protezione delle persone fisiche con riguardo al trattamento di dati personali... e segnatamente [il regolamento generale sulla protezione dei dati]..., nonché le direttive (UE) 2016/680 e 2002/58/CE…, non sono pregiudicati dal presente regolamento".

Esempio pratico

Una società che opera nell'UE offre i propri servizi tramite una piattaforma. Le imprese (clienti) caricano i loro documenti, che contengono insiemi di dati misti, sulla piattaforma. In qualità di "titolare del trattamento", l'impresa che carica i documenti deve assicurarsi che il trattamento rispetti il regolamento generale sulla protezione dei dati. Nel trattare l'insieme dei dati per conto del titolare del trattamento, la società che offre i servizi (il "responsabile del trattamento") deve memorizzare e trattare i dati conformemente al regolamento generale sulla protezione dei dati, ad esempio per essere certi che sia garantito un livello adeguato di sicurezza relativo ai dati, anche tramite la cifratura.

Il concetto di "indissolubilmente legato" non è definito da nessuno dei due regolamenti[30]. Ai fini pratici, esso può denotare una situazione in cui un insieme di dati contiene sia dati personali che dati non personali e separarli sarebbe impossibile o ritenuto dal titolare del trattamento economicamente inefficiente o non tecnicamente realizzabile. Ad esempio, quando la società acquista servizi di gestione delle relazioni con i clienti e sistemi di rendicontazione delle vendite, dovrebbe spendere altrettanto per comprare software separati per i CRM (dati personali) e per i sistemi di rendicontazione delle vendite (dati aggregati/non personali) basati sui dati CRM.

---

[26] Articolo 1, paragrafo 3, 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 (regolamento generale sulla protezione dei dati). Cfr. anche sezione 3.2.

[27] Come viene ricordato nel *documento di lavoro dei servizi della Commissione, valutazione d'impatto che accompagna il documento Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea,* SWD(2017) 304 final, parte 1.2, pag. 3, indipendentemente da quanti dati personali sono contenuti negli insiemi di dati misti, si deve garantire il pieno rispetto del GPDR [il regolamento generale sulla protezione dei dati] in relazione alla parte dell'insieme contenente i dati personali.

[28] Carta dei diritti fondamentali dell'Unione europea (GU C 362 del 26.10.2012, pag. 391).

[29] Considerando 8 del regolamento stesso.

[30] Il regolamento sulla libera circolazione dei dati non personali e il regolamento generale sulla protezione dei dati.

È altresì probabile che separare l'insieme di dati ne diminuisca sensibilmente il valore. Inoltre, la natura mutevole dei dati (cfr. sezione 2.1) rende ancora più difficile distinguere chiaramente e quindi separare le diverse categorie di dati.

Soprattutto, nessuno dei due regolamenti impone alle imprese di separare gli insiemi di dati per cui sono titolari o responsabili del trattamento.

Pertanto, un insieme di dati misti sarà di norma soggetto agli obblighi dei titolari e dei responsabili del trattamento e rispetterà i diritti degli interessati stabiliti dal regolamento generale sulla protezione dei dati.

Trattamento dei dati sanitari

I dati sanitari possono rientrare in un insieme di dati misti. Tra gli esempi figurano le cartelle cliniche elettroniche, le sperimentazioni cliniche o gli insieme di dati raccolti dalle varie applicazioni mobili per la salute e il benessere (come le applicazioni per misurare il proprio stato di salute, per ricordarci di prendere le medicine o per rilevare i progressi nella forma fisica)[31]. La divisione esatta tra dati personali e dati non personali in questi insiemi di dati sta diventando sempre più indistinta con gli sviluppi tecnologici. Pertanto, il loro trattamento deve essere conforme al regolamento generale sulla protezione dei dati, in particolare (dal momento che i dati sanitari rappresentano una categoria particolare di dati secondo il regolamento) all'articolo 9 che stabilisce un divieto generale di trattamento di categorie particolari di dati e le eccezioni a questo divieto.

I dati negli insiemi di dati misti contenenti dati sanitari possono essere una preziosa fonte d'informazione, ad es. per ulteriori ricerche mediche, per misurare gli effetti collaterali di un medicinale prescritto, per ottenere statistiche sulle malattie o per sviluppare nuovi servizi o trattamenti sanitari. Tuttavia, occorre ottemperare al regolamento generale sulla protezione dei dati quando si effettua il trattamento iniziale nonché ulteriori trattamenti dei dati. Pertanto, un qualsiasi trattamento simile di dati sanitari deve avere una base giuridica valida[32] e una motivazione adeguata, essere sicuro e fornire garanzie sufficienti.

Infine, è essenziale che le persone e le imprese abbiano certezza giuridica e fiducia nel trattamento dei dati. Questo è fondamentale anche per l'economia dei dati. I due regolamenti garantiscono tutto ciò ed entrambi perseguono l'obiettivo di non modificare la libera circolazione dei dati.

[31] Lo sviluppo e il funzionamento di applicazioni mobili per la salute richiedono un'osservanza rigorosa delle norme del regolamento generale sulla protezione dei dati. Questi obblighi saranno ulteriormente definiti nel codice di condotta sulla privacy delle applicazioni mobili per la salute, che è attualmente in corso di elaborazione. Per maggiori informazioni sullo stato del suo sviluppo si veda: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps.

[32] Cfr. articolo 6, paragrafo 1, 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 (regolamento generale sulla protezione dei dati).

3 Libera circolazione dei dati e rimozione degli obblighi di localizzazione dei dati

Questa sezione spiega più in dettaglio i concetti degli obblighi di localizzazione dei dati secondo il regolamento sulla libera circolazione dei dati non personali e del principio della libera circolazione nel regolamento generale sulla protezione dei dati. Sebbene queste disposizioni si rivolgano agli Stati membri, può essere utile per le imprese avere un quadro più preciso di come questi due regolamenti contribuiscano alla libera circolazione di tutti i dati nell'UE.

3.1 Libera circolazione dei dati non personali

Il regolamento sulla libera circolazione dei dati non personali[33] prevede che "gli obblighi di localizzazione di dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità".

Gli **obblighi di localizzazione dei dati** sono definiti[34] come "qualsiasi obbligo, divieto, condizione, limite o altro requisito, previsto dalle disposizioni legislative, regolamentari o amministrative di uno Stato membro o risultante dalle prassi amministrative generali e coerenti in uno Stato membro e negli organismi di diritto pubblico, anche nell'ambito degli appalti pubblici, fatta salva la direttiva 2014/24/UE, che impone di effettuare il trattamento di dati nel territorio di un determinato Stato membro o che ostacola il trattamento di dati in un altro Stato membro"[35].

Dalla definizione emerge che le misure che limitano la libera circolazione dei dati nell'UE possono assumere varie forme. Esse possono essere previste da disposizioni legislative, regolamentari o amministrative o anche risultare da prassi amministrative generali e coerenti. Inoltre, il divieto di qualsiasi obbligo di localizzazione dei dati riguarda le misure sia dirette che indirette che possano limitare la libera circolazione dei dati non personali.

Gli **obblighi di localizzazione dei dati diretti** possono, ad esempio, consistere nell'obbligo di conservare i dati in una specifica posizione geografica (ad es. i server devono essere situati in uno specifico Stato membro) o nell'obbligo di conformarsi a requisiti tecnici nazionali unici (ad es. i dati devono utilizzare specifici formati nazionali).

Gli **obblighi di localizzazione dei dati indiretti**, che ostacolerebbero il trattamento dei dati non personali in qualsiasi altro Stato membro, possono presentarsi in forme diverse. Essi possono includere l'obbligo di utilizzare dispositivi tecnologici che siano certificati o

---

33 Articolo 4, paragrafo 1, del regolamento stesso.

34 Articolo 3, paragrafo 5, del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

35 Si osservi che l'incertezza giuridica sulla portata degli obblighi giustificati o ingiustificati di localizzazione dei dati limita ulteriormente le scelte disponibili agli operatori del mercato e del settore pubblico per quanto riguarda la localizzazione dei dati trattati (cfr. considerando 4 del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea).

omologati in un determinato Stato membro o altri requisiti che producono l'effetto di rendere più difficile trattare dati al di fuori di un determinato territorio o area geografica all'interno dell'Unione[36,37].

Per valutare se una determinata misura rappresenti un obbligo di localizzazione dei dati indiretto si deve tenere conto delle circostanze specifiche di ogni caso.

Il regolamento sulla libera circolazione dei dati non personali[38] fa riferimento al concetto di **pubblica sicurezza** come indicato nella giurisprudenza della Corte di giustizia dell'Unione europea. La pubblica sicurezza riguarda la sicurezza sia interna che esterna di uno Stato membro[39], come pure le questioni di incolumità pubblica, in particolare al fine di agevolare le indagini, l'accertamento e il perseguimento di reati. Presuppone l'esistenza di una minaccia reale e sufficientemente grave a uno degli interessi fondamentali della società[40], quale il pregiudizio al funzionamento delle istituzioni e dei servizi pubblici essenziali nonché all'incolumità della popolazione, come il rischio di perturbazioni gravi dei rapporti internazionali o della coesistenza pacifica dei popoli, o ancora il pregiudizio agli interessi militari.

Inoltre, qualsiasi obbligo di localizzazione dei dati giustificato per motivi di sicurezza pubblica deve essere proporzionato. Conformemente alla giurisprudenza della Corte di giustizia dell'Unione europea, il principio di proporzionalità impone che le misure adottate siano atte a garantire il conseguimento dell'obiettivo perseguito e non vadano al di là di quanto necessario a tale scopo[41].

Per motivi di chiarezza, il divieto di qualsiasi obbligo di localizzazione dei dati non pregiudica le restrizioni già esistenti stabilite dal diritto dell'UE[42].

---

36 Considerando 4 del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

37 Cfr. due studi sugli obblighi di localizzazione dei dati svolti prima dell'adozione del regolamento sulla libera circolazione dei dati non personali: (1) Godel, M. et al.: *Facilitating cross border data flows in the Digital Single Market*, numero SMART 2015/2016, disponibile online al seguente indirizzo: http://ec.europa.eu/newsroom/document.cfm?doc_id=41185, e (2) Time.lex, Spark Legal Network e Tech4i2: *Cross-border data flow in the digital single market: study on data localisation restrictions*, numero SMART 2015/0054, disponibile online al seguente indirizzo: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695.

38 Considerando 19 del regolamento stesso.

39 Cfr. ad esempio la sentenza della Corte di giustizia del 23 novembre 2010, *Land Baden-Württemberg* contro *Tsakouridis*, C-145/09, ECLI:EU:C:2010:708, punto 43, e la sentenza del 4 aprile 2017, *Sahar Fahimian* contro *Bundesrepublik Deutschland*, C-544/15, ECLI:EU:C:2017:225, punto 39.

40 Cfr. ad esempio la sentenza della Corte di giustizia del 22 dicembre 2008, *Commissione delle Comunità europee* contro *Repubblica d'Austria*, C-161/07, ECLI:EU:C:2008:759, punto 35 e la giurisprudenza ivi citata, e la sentenza del 26 marzo 2009, *Commissione delle Comunità europee* contro *Repubblica italiana*, C-326/07, ECLI:EC:C:2009:193, punto 70 e la giurisprudenza ivi citata.

41 Cfr. ad esempio sentenza della Corte di giustizia dell'8 luglio 2010, *Afton Chemical Limited* contro *Secretary of State for Transport,* C-343/09, ECLI:EU:C:2010:419, punto 45 e anche giurisprudenza ivi citata.

42 Cfr. ad esempio l'articolo 245, paragrafo 2, della direttiva 2006/112/CE, del 28 novembre 2006, relativa al sistema comune d'imposta sul valore aggiunto, che stabilisce che "gli Stati membri possono esigere dal soggetto passivo stabilito nel loro territorio la comunicazione del luogo di archiviazione quando esso si trovi

Inoltre, il regolamento sulla libera circolazione dei dati non personali non impone alcun obbligo alle imprese né limita la loro libertà contrattuale nel decidere dove i loro dati devono essere trattati.

Gli Stati membri sono tenuti a rendere pubblico qualsiasi obbligo di localizzazione dei dati applicabile nel loro territorio su un **portale unico nazionale on line d'informazione** (siti web nazionali). Essi devono tenerlo aggiornato oppure fornire informazioni aggiornate a un punto informativo centrale istituito da un altro atto dell'UE[43]. Per comodità delle imprese e per garantire loro un facile accesso alle informazioni pertinenti in tutta l'UE, la Commissione pubblicherà collegamenti a questi punti d'informazione sul portale "La tua Europa"[44].

3.2 Libera circolazione dei dati personali

Il regolamento generale sulla protezione dei dati[45] stabilisce che "la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali".

Se uno Stato membro impone obblighi di localizzazione dei dati personali per ragioni diverse dalla protezione dei dati personali, questi dovranno essere valutati sulla base delle disposizioni relative alle libertà fondamentali e delle deroghe consentite a tali libertà previste nel trattato sul funzionamento dell'Unione europea[46,47] e nel diritto dell'UE pertinente, come la direttiva sui servizi[48] e la direttiva sul commercio elettronico[49].

---

fuori del loro territorio". Tuttavia, tale obbligo deve essere letto in conformità dell'articolo 249, il quale afferma che: "qualora un soggetto passivo archivi le fatture da esso emesse o ricevute tramite un mezzo elettronico che garantisca un accesso in linea ai dati e il luogo di archiviazione sia situato in uno Stato membro diverso da quello in cui è stabilito, le autorità competenti dello Stato membro in cui è stabilito hanno, ai fini della presente direttiva, il diritto di accedere a tali fatture per via elettronica, di scaricarle e di utilizzarle, nei limiti fissati dalla normativa dello Stato membro in cui il soggetto passivo è stabilito e nella misura in cui ciò sia loro necessario a fini di controllo."

[43] Articolo 4, paragrafo 4, del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

[44] https://europa.eu/youreurope/index.htm.

[45] Articolo 1, paragrafo 3, 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 (regolamento generale sulla protezione dei dati).

[46] Versione consolidata del trattato sul funzionamento dell'Unione europea (GU C 326 del 26.10.2012, pag. 47).

[47] Cfr. anche sentenza della Corte di giustizia del 19 giugno 2008, *Commissione delle Comunità europee* contro *Granducato di Lussemburgo*, C-319/06, ECLI:EU:C:2008:350, punti 90-91: la Corte ha ritenuto che l'obbligo di tenere a disposizione e conservare alcuni documenti in un particolare Stato membro costituisca una restrizione alla libera prestazione dei servizi; una giustificazione secondo cui "possa genericamente agevolare l'adempimento del compito di controllo delle autorità" non è sufficiente.

[48] Direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno (GU L 376 del 27.12.2006, pag. 36).

[49] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico") (GU L 178 del 17.7.2000, pag. 1).

Esempio

Una normativa nazionale prevede che la contabilità del personale sia situata in uno specifico Stato membro per ragioni riguardanti il controllo regolamentare, ad es. da parte dell'amministrazione fiscale nazionale. Tale normativa nazionale non rientrerebbe nell'ambito di applicazione dell'articolo 1, paragrafo 3, del regolamento generale sulla protezione dei dati, in quanto i motivi non riguardano la protezione dei dati personali. Questo obbligo dovrebbe invece essere valutato sulla base delle disposizioni relative alle libertà fondamentali e delle deroghe consentite a tali libertà previste nel trattato sul funzionamento dell'Unione europea.

Il regolamento generale sulla protezione dei dati[50] riconosce che gli Stati membri possono imporre condizioni, incluse limitazioni, sul trattamento dei dati genetici, biometrici o sanitari. Tuttavia, come stabilito nel considerando 53, tali limitazioni nazionali non dovrebbero ostacolare la libera circolazione dei dati personali all'interno dell'UE, quando queste condizioni si applicano al trattamento transfrontaliero di tali dati. Quanto detto è conforme all'articolo 16 del trattato sul funzionamento dell'Unione europea, che costituisce la base giuridica per l'adozione di norme relative al diritto di tutela dei dati personali e alla libera circolazione di tali dati.

3.3 Ambito di applicazione del regolamento sulla libera circolazione dei dati non personali

Come già menzionato, il regolamento sulla libera circolazione dei dati non personali intende garantire la libera circolazione dei dati non personali "all'interno dell'Unione"[51]. Esso non si applica pertanto ai servizi di trattamento di dati svolti al di fuori dell'UE e agli obblighi di localizzazione di dati relativi a tali trattamenti[52,53].

Ai sensi dell'articolo 2, paragrafo 1, l'ambito di applicazione del regolamento è limitato al trattamento dei dati elettronici non personali nell'UE che è:

(a) fornito come servizio ad utenti residenti o stabiliti nell'UE, indipendentemente dal fatto che il fornitore di servizi sia o non sia stabilito nell'Unione, oppure
(b) effettuato da una persona fisica o giuridica residente o stabilita nell'Unione per le proprie esigenze.

---

50 Articolo 9, paragrafo 4, 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 (regolamento generale sulla protezione dei dati).

51 Cfr. articolo 1 del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

52 Cfr. considerando 15 del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

53 Il termine "trattamento" è definito in termini generici (articolo 3, paragrafo 2, del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea) e, come evidenziato al considerando 17, il regolamento dovrebbe intendere i trattamenti di dati nell'accezione più ampia possibile, indipendentemente dal tipo di sistema IT utilizzato.

Esempi

Articolo 2, paragrafo 1, lettera a), del regolamento sulla libera circolazione dei dati non personali:

- Un fornitore di servizi cloud con sede negli USA fornisce servizi di trattamento di dati a clienti residenti o stabiliti nell'UE. Questi gestisce le sue attività tramite server situati nel territorio dell'UE, dove sono conservati o comunque trattati i dati dei suoi clienti europei. Il fornitore non deve essere in possesso di infrastrutture proprie situate nell'UE, ma può ad es. anche affittare lo spazio sul server nell'Unione. Il regolamento sulla libera circolazione dei dati non personali si applica a questi trattamenti di dati.
- Un fornitore di servizi cloud con sede in Giappone fornisce i propri servizi a clienti europei. Le capacità del fornitore sono situate in Giappone e tutte le attività di trattamento sono condotte in tale paese. In questo caso il regolamento sulla libera circolazione dei dati non personali non si applica, se tutte le attività di trattamento sono condotte al di fuori dell'UE[54].

Articolo 2, paragrafo 1, lettera b), del regolamento sulla libera circolazione dei dati non personali:

- Una piccola start-up europea dello Stato membro A decide di aumentare l'attività aprendo uno stabilimento nello Stato membro B. Per minimizzare i costi, la start-up sceglie di centralizzare l'archiviazione e il trattamento dei dati del nuovo stabilimento nel suo server situato nello Stato membro A. Gli Stati membri non possono vietare questa iniziativa di centralizzazione IT, tranne se giustificato da motivi di pubblica sicurezza nel rispetto del principio di proporzionalità.

Sebbene il regolamento sulla libera circolazione dei dati non personali non si applichi qualora tutte le attività di trattamento dei dati non personali siano condotte al di fuori dell'UE, il regolamento generale sulla protezione dei dati deve essere rispettato quando l'insieme di dati contiene dati personali. In particolare, le norme relative al trasferimento di dati personali verso paesi terzi o organizzazioni internazionali ai sensi del regolamento generale sulla protezione dei dati devono essere osservate in tutti i casi[55].

---

[54] Si osservi che il regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea non riguarda gli obblighi di localizzazione di dati imposti dagli Stati membri sull'archiviazione dei dati non personali in un paese terzo, che possono essere presenti negli ordinamenti giuridici nazionali. Per motivi di chiarezza, il regolamento generale sulla protezione dei dati si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato, oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione (cfr. articolo 3, paragrafo 2, del regolamento generale sulla protezione dei dati).

[55] In relazione al trasferimento dei dati personali verso paesi terzi, si prega di consultare il sito web della Commissione: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_it e la *Comunicazione*

3.4 Attività relative all'organizzazione interna degli Stati membri

Il regolamento sulla libera circolazione dei dati non personali non impone agli Stati membri di esternalizzare la prestazione di servizi riguardanti i dati non personali che essi intendono fornire direttamente od organizzare con mezzi diversi dagli appalti pubblici[56].

L'articolo 2, paragrafo 3, secondo comma, del regolamento sulla libera circolazione dei dati non personali afferma che:

"Il presente regolamento fa salve le disposizioni legislative, regolamentari e amministrative relative all'**organizzazione interna** degli Stati membri che attribuiscono tra autorità pubbliche e organismi di diritto pubblico quali definiti all'articolo 2, paragrafo 1, punto 4 della direttiva 2014/24/UE[57] poteri e responsabilità in materia di **trattamento dei dati, senza remunerazione contrattuale di soggetti privati**, nonché le disposizioni legislative, regolamentari e amministrative degli Stati membri che prevedono l'esercizio di tali poteri e responsabilità."[58]

Possono esservi interessi legittimi che giustificherebbero la scelta di questo tipo di "autofornitura" dei servizi di trattamento di dati, come l'"internalizzazione" o gli accordi reciproci tra amministrazioni pubbliche. Tra gli esempi tipici figurano l'uso di un "cloud della pubblica amministrazione" o l'assunzione da parte di un'amministrazione di una agenzia IT centralizzata per fornire servizi di trattamento di dati per le istituzioni e gli enti pubblici.

Tuttavia, il regolamento sulla libera circolazione dei dati non personali incoraggia gli Stati membri a considerare l'efficienza economica e gli altri vantaggi derivanti dall'utilizzo di fornitori esterni di servizi[59,60]. Nel momento in cui le autorità nazionali inizieranno ad

---

della Commissione al Parlamento europeo e al Consiglio — Scambio e protezione dei dati personali in un mondo globalizzato, COM(2017) 7 final, disponibile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=COM%3A2017 %3A7 %3AFIN. Per quanto riguarda il Giappone, il 23 gennaio 2019 la Commissione ha adottato la decisione di adeguatezza che permette la libera circolazione dei dati personali tra le due economie sulla base di solide garanzie di protezione.

[56] Considerando 14 del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

[57] L'articolo 2, paragrafo 1, punto 4), della direttiva 2014/24/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sugli appalti pubblici e che abroga la direttiva 2004/18/CE (GU L 94 del 28.3.2014, pag. 65) stabilisce che per "organismi di diritto pubblico" si intendono "gli organismi che hanno tutte le seguenti caratteristiche: a) sono istituiti per soddisfare specificatamente esigenze di interesse generale, aventi carattere non industriale o commerciale; b) sono dotati di personalità giuridica; e c) sono finanziati per la maggior parte dallo Stato, dalle autorità regionali o locali o da altri organismi di diritto pubblico; o la loro gestione è posta sotto la vigilanza di tali autorità o organismi; o il loro organo di amministrazione, di direzione o di vigilanza è costituito da membri più della metà dei quali è designata dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico".

[58] Il considerando 13 del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea specifica che il regolamento non pregiudica la direttiva 2014/24/UE.

[59] Considerando 14 del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

[60] Un fornitore esterno di servizi potrebbe essere qualsiasi entità, che non sia un "organismo di diritto pubblico" di cui all'articolo 2, paragrafo 1, punto 4), della direttiva 2014/24/UE del Parlamento europeo e del

"esternalizzare" il trattamento dei dati con remunerazione contrattuale di soggetti privati e il trattamento avrà luogo nell'UE, tale trattamento sarà disciplinato dal regolamento sulla libera circolazione dei dati non personali, il che significa che il principio della libera circolazione dei dati non personali si applicherà alle prassi generali e amministrative delle autorità nazionali. In particolare, si dovranno astenere dall'applicare restrizioni alla localizzazione dei dati, ad es. negli appalti pubblici[61].

4 Approcci di autoregolamentazione che sostengono la libera circolazione dei dati

L'autoregolamentazione contribuisce all'innovazione e alla fiducia tra gli operatori ed è potenzialmente più reattiva ai cambiamenti del mercato. La presente sezione offre una panoramica sulle iniziative di autoregolamentazione per il trattamento sia dei dati personali che dei dati non personali.

4.1 La portabilità dei dati e il cambio di fornitori di servizi cloud

Una delle finalità principali del regolamento sulla libera circolazione dei dati non personali è di evitare le pratiche di "vendor lock-in". Queste pratiche si verificano quando gli utenti non possono cambiare il fornitore di servizi, perché i loro dati sono "bloccati" nel sistema del fornitore, ad esempio a causa di uno specifico formato dei dati o di accordi contrattuali, e non possono essere trasferiti al di fuori del suo sistema informatico. La portabilità dei dati senza impedimenti è uno degli elementi fondamentali che consente agli utenti di scegliere liberamente tra i fornitori di servizi di trattamento di dati e garantisce quindi la concorrenza effettiva nei mercati.

La portabilità dei dati tra le imprese sta acquisendo un'importanza crescente in numerose industrie digitali, tra cui i servizi cloud.

Secondo l'articolo 6 del regolamento sulla libera circolazione dei dati non personali, la Commissione incoraggia e facilita l'elaborazione di codici di condotta di autoregolamentazione a livello dell'Unione ("codici di condotta"), al fine di contribuire a un'economia dei dati competitiva. Esso offre all'industria una base per sviluppare codici di autoregolamentazione sul cambio di fornitore di servizi e la portabilità dei dati tra i diversi sistemi informatici.

Quando si sviluppano tali codici di condotta sulla portabilità dei dati si dovrebbe tenere conto di numerosi aspetti, vale a dire:

- le **migliori prassi** per agevolare il cambio di fornitore di servizi e la portabilità dei dati in un formato strutturato, di uso comune e leggibile elettronicamente;

Consiglio, del 26 febbraio 2014, sugli appalti pubblici e che abroga la direttiva 2004/18/CE (GU L 94 del 28.3.2014, pag. 65).

[61] Considerando 13 del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

- gli **obblighi d'informazione minimi** per garantire che gli utenti professionali ricevano informazioni sufficientemente dettagliate e chiare prima della conclusione di un contratto, per quanto riguarda le procedure e i requisiti tecnici, i tempi e gli oneri applicati nel caso in cui un utente professionale intenda cambiare fornitore di servizi o ritrasferire i dati nei propri sistemi informatici;
- gli **approcci in materia di sistemi di certificazione** per consentire un miglior confronto dei servizi cloud;
- le **tabelle di marcia in materia di comunicazione** per sensibilizzare a proposito dei codici di condotta.

Nel mercato dei servizi cloud, la Commissione ha iniziato a facilitare le attività dei gruppi di lavoro dei portatori di interesse cloud del mercato unico digitale, che riuniscono esperti e utenti professionali cloud, tra cui le piccole e le medie imprese. In questa fase, un sottogruppo sta elaborando codici di autoregolamentazione sulla portabilità dei dati e sul cambio di fornitore di servizi cloud (gruppo di lavoro SWIPO), [62] mentre un altro sottogruppo sta lavorando allo sviluppo della certificazione di sicurezza dei servizi cloud (gruppo di lavoro CSPCERT)[63].

Il gruppo di lavoro SWIPO sta sviluppando codici di condotta che riguardano l'intero spettro dei servizi cloud: Infrastruttura come servizio (IaaS), Piattaforma come servizio (PaaS) e Software come servizio (SaaS).

La Commissione auspica che i diversi codici di condotta siano integrati da **clausole contrattuali tipo**[64]. Queste consentiranno una sufficiente specificità tecnica e giuridica nell'attuazione e nell'applicazione pratiche dei codici di condotta, che rivestiranno particolare importanza per le piccole e medie imprese. L'elaborazione delle clausole contrattuali tipo è prevista dopo lo sviluppo dei codici di condotta (che dovrebbe essere portato a termine entro il 29 novembre 2019).

Conformemente all'articolo 8 del regolamento sulla libera circolazione dei dati non personali, la Commissione valuterà l'attuazione del regolamento entro il 29 novembre 2022. Ciò consentirà di valutare: i) l'impatto sulla libera circolazione dei dati in Europa; ii) l'applicazione del regolamento, in particolare per quanto riguarda gli insiemi di dati misti; iii) la misura in cui gli Stati membri hanno efficacemente abrogato le attuali restrizioni ingiustificate in materia di localizzazione di dati; iv) l'efficacia dei codici di condotta sul mercato nell'ambito della portabilità dei dati e del cambio di fornitore di servizi cloud.

---

62 Gruppo di lavoro sul cambio di fornitore di servizi cloud e sulla portabilità dei dati.

63 Gruppo di lavoro sulla certificazione europea dei fornitori di servizi cloud. Cfr. anche la sezione 4.3.

64 Cfr. considerando 30 del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

La nozione di portabilità e l'interazione con il regolamento generale sulla protezione dei dati

Entrambi i regolamenti[65] fanno riferimento alla portabilità dei dati e hanno lo scopo di agevolare il loro trasferimento da un ambiente IT a un altro, ad es. verso un altro sistema del fornitore o verso sistemi in loco. Ciò impedisce le pratiche di "vendor lock-in" e promuove la concorrenza tra i fornitori di servizi. Tuttavia, i regolamenti hanno un diverso approccio alla portabilità per quanto concerne il legame tra i gruppi d'interesse a cui si rivolgono e la natura giuridica delle disposizioni.

Il diritto alla portabilità dei dati personali ai sensi dell'articolo 20 del regolamento generale sulla protezione dei dati si concentra sul rapporto tra l'interessato e il titolare del trattamento. Esso riguarda il diritto dell'interessato di ricevere i dati personali che ha fornito al titolare del trattamento in un formato strutturato, di uso comune e leggibile elettronicamente e di trasmettere tali dati a un altro titolare del trattamento o alle proprie capacità di stoccaggio senza impedimenti da parte del titolare del trattamento cui li ha forniti[66]. Generalmente, gli interessati in questo rapporto sono i fruitori di vari servizi online che desiderano cambiare il fornitore di questi servizi.

L'articolo 6 del regolamento sulla libera circolazione dei dati non personali non prevede il diritto degli utenti professionali di trasferire i dati, ma introduce un approccio di autoregolamentazione con codici volontari di condotta per il settore. Al contempo, esso è rivolto ai casi in cui un utente professionale ha esternalizzato il trattamento dei suoi dati a terzi che offrono un servizio di trattamento di dati[67]. Conformemente all'articolo 3, punto 8, del regolamento sulla libera circolazione dei dati non personali, un "utente professionale" può comprendere "una persona fisica o giuridica, compreso un'autorità pubblica e un organismo di diritto pubblico, che utilizza o richiede servizi di trattamento di dati per fini connessi alla sua attività commerciale, industriale, artigianale, professionale o a una sua funzione".

In pratica, la portabilità dei dati ai sensi dell'articolo 6 del regolamento sulla libera circolazione dei dati non personali riguarda le interazioni business-to-business tra un utente professionale (il quale, nei casi che includono il trattamento dei dati personali, può qualificarsi come "titolare del trattamento" in conformità al regolamento generale sulla protezione dei dati) e un fornitore di servizi (analogamente, da considerarsi in alcuni casi il "responsabile del trattamento").

---

65 Articolo 6 del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea e articolo 20 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 (regolamento generale sulla protezione dei dati).

66 Cfr. gruppo di lavoro articolo 29: *Linee guida sul diritto alla portabilità dei dati*. WP 242 rev.01, adottato il 13 dicembre 2016, rivisto e adottato da ultimo il 5 aprile 2017.

67 Il considerando 29 del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea afferma che, mentre i consumatori singoli traggono vantaggi dal vigente diritto dell'Unione [ad es. regolamento generale sulla protezione dei dati], la portabilità dei dati "non facilita gli utenti che intendono cambiare fornitore di servizi nell'ambito della loro attività imprenditoriale o professionale".

Nonostante le differenze, possono verificarsi situazioni in cui la portabilità dei dati rientrerebbe nel campo di applicazione sia del regolamento sulla libera circolazione dei dati non personali sia del regolamento generale sulla protezione dei dati per quanto riguarda gli insiemi di dati misti.

Esempio

Un'impresa che usa un servizio cloud decide di cambiare il fornitore di tale servizio e di trasferire tutti i dati a un nuovo fornitore. Il cambio del fornitore e la portabilità dei dati sono disciplinati dal contratto tra il cliente e il fornitore di servizi cloud. Se il precedente fornitore di servizi cloud aderisce al codice di condotta sviluppato nel quadro del regolamento sulla libera circolazione dei dati non personali, la portabilità dei dati deve avvenire nel rispetto degli obblighi ivi previsti.

Se tra gli insiemi di dati da trasferire vi sono anche dati personali, la portabilità deve osservare tutte le disposizioni pertinenti del regolamento generale sulla protezione dei dati, in particolare garantire che il nuovo fornitore di servizi cloud rispetti gli obblighi applicabili, quali la sicurezza[68].

Esempio

Qualora una banca decida di cambiare il proprio fornitore di servizi di gestione delle relazioni con i clienti (CRM), è possibile che alcuni dati (personali e non personali) debbano essere trasferiti dal vecchio al nuovo fornitore. Questi dati saranno poi soggetti a obblighi regolamentari diversi, alcuni derivanti dal regolamento generale sulla protezione dei dati e altri dal regolamento sulla libera circolazione dei dati non personali.

4.2 Codici di condotta e sistemi di certificazione in materia di protezione dei dati personali

Per dimostrare la conformità con gli obblighi previsti dal regolamento generale sulla protezione dei dati (cfr. articolo 24, paragrafo 3, e articolo 28, paragrafo 5) possono essere utilizzati codici di condotta e sistemi di certificazione.

In conformità all'articolo 40, paragrafo 1, e all'articolo 42, paragrafo 1, del regolamento generale sulla protezione dei dati, gli Stati membri, le autorità di controllo, il comitato europeo per la protezione dei dati e la Commissione dovrebbero incoraggiare il settore a sviluppare codici di condotta e stabilire meccanismi di certificazione in materia di protezione dei dati.

Le associazioni o altre organizzazioni rappresentanti categorie specifiche di titolari del trattamento o di responsabili del trattamento possono elaborare codici di condotta per il

[68] Cfr. gruppo di lavoro articolo 29: *Parere 05/2012 sul cloud computing*, WP196, adottato l'1 luglio 2012, che definisce in modo più preciso la posizione e gli obblighi degli utenti cloud e dei fornitori di servizi cloud riguardo al trattamento dei dati personali.

settore in questione. Un progetto del codice deve essere presentato alla rispettiva autorità di controllo competente per essere approvato[69]. Se il progetto riguarda attività di trattamento in diversi Stati membri, l'autorità di controllo deve sottoporlo al comitato europeo per la protezione dei dati prima di approvarlo. Il comitato si pronuncerà riguardo alla conformità del progetto del codice di condotta al regolamento generale sulla protezione dei dati.

Il comitato europeo per la protezione dei dati ha pubblicato le sue linee guida 1/2019 sui codici di condotta e gli organismi di controllo ai sensi del regolamento generale sulla protezione dei dati[70]. Queste linee guida comprendono informazioni sull'elaborazione dei codici di condotta e sui criteri per la loro approvazione e altre informazioni utili. Analogamente, le linee guida 1/2018 sulla certificazione e identificazione dei criteri di certificazione in conformità degli articoli 42 e 43 del regolamento generale sulla protezione dei dati forniscono informazioni sulla certificazione ai sensi di questo regolamento e sullo sviluppo e l'approvazione dei criteri di certificazione[71].

Esempi di codici di condotta sviluppati dal settore cloud

Il codice di condotta per il cloud dell'UE, il cui sviluppo è stato agevolato dalla Commissione, è stato elaborato in collaborazione con il Cloud Select Industry Group (C-SIG) sulla base della direttiva sulla protezione dei dati[72] e successivamente del regolamento generale sulla protezione dei dati. Questo codice riguarda l'intero spettro dei servizi cloud — Infrastruttura come servizio (IaaS), Piattaforma come servizio (PaaS) e Software come servizio (SaaS)[73].

Il codice di condotta dei fornitori di servizi di infrastrutture cloud in Europa (CISPE)[74] è rivolto ai fornitori IaaS. Il codice di condotta CISPE contiene obblighi per i fornitori IaaS che operano come responsabili del trattamento dei dati ai sensi del regolamento generale sulla

---

69 Cfr. articolo 40, paragrafo 5, e articolo 55 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 (regolamento generale sulla protezione dei dati).

70 Comitato europeo per la protezione dei dati: *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 (Linee guida 1/2019 sui codici di condotta e gli organismi di controllo di cui al regolamento 2016/679)*, documento adottato il 12 febbraio 2019, versione per consultazione pubblica, disponibile al seguente indirizzo: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_it.

71 Comitato europeo per la protezione dei dati: *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 (Linee guida 1/2018 sulla certificazione e identificazione dei criteri di certificazione in conformità degli articoli 42 e 43 del regolamento (UE) 2016/679)*, adottate il 23 gennaio 2019, disponibili al seguente indirizzo: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_it.

72 Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (data di termine della validità: 24 maggio 2018).

73 Per maggiori informazioni sul codice di condotta per il cloud dell'UE, si veda: https://eucoc.cloud/en/home.html.

74 Per maggiori informazioni sul codice di condotta CISPE, si veda: https://cispe.cloud/code-of-conduct/.

protezione dei dati. Esso stabilisce inoltre disposizioni sulla struttura di governance per l'attuazione e l'applicazione del codice.

Il codice di condotta di Cloud Security Alliance (CSA) per la conformità al GPDR si rivolge a tutte le parti interessate nell'ambito del cloud computing e della legislazione europea sui dati personali, come i fornitori di servizi cloud, i clienti e i potenziali clienti cloud, i revisori e gli intermediari cloud. Il codice di condotta riguarda l'intero spettro dei fornitori di servizi cloud[75].

4.3 Rafforzare la fiducia nel trattamento transfrontaliero dei dati - certificazione di sicurezza

Come indicato al considerando 33 del regolamento sulla libera circolazione dei dati non personali, rafforzare la fiducia nella sicurezza del trattamento transfrontaliero dei dati dovrebbe ridurre la tendenza degli operatori del mercato e del settore pubblico a servirsi della localizzazione dei dati come sostituto della sicurezza dei dati. Insieme al pacchetto sulla cibersicurezza proposto dalla Commissione nel 2017[76], il gruppo di lavoro CSPCERT sta sviluppando raccomandazioni allo scopo di elaborare un sistema di certificazione cloud europeo che sarà presentato alla Commissione e che dovrebbe contribuire ad agevolare la libera circolazione dei dati, a consentire un miglior confronto dei servizi cloud e a promuovere la diffusione del cloud. La Commissione può richiedere all'ENISA (l'agenzia dell'Unione europea per la cibersicurezza) di preparare un sistema candidato in conformità alle disposizioni pertinenti del regolamento sulla cibersicurezza[77]. Un tale sistema può riguardare sia i dati personali che i dati non personali. Oltre al regolamento sulla cibersicurezza e come evidenziato alla sezione 4.2, il GDPR può essere anche utilizzato per dimostrare l'esistenza di garanzie adeguate per la sicurezza dei dati[78].

Osservazioni conclusive

La certezza giuridica e la fiducia nel trattamento dei dati sono essenziali per mettere l'UE in grado di sfruttare pienamente le potenzialità dei dati laddove si possono sviluppare catene di valore tra i vari settori e paesi. I due regolamenti garantiscono tutto ciò ed entrambi perseguono l'obiettivo della libera circolazione dei dati. Insieme, il regolamento sulla libera circolazione dei dati non personali e il regolamento generale sulla protezione dei dati gettano le fondamenta per la libera circolazione di tutti i dati nell'Unione europea e per un'economia dei dati europea altamente competitiva.

---

[75] Per maggiori informazioni sul codice di condotta di CSA, si veda: https://gdpr.cloudsecurityalliance.org/.

[76] Per maggiori informazioni, cfr.: https://ec.europa.eu/digital-single-market/en/cyber-security.

[77] Regolamento del Parlamento Europeo e del Consiglio relativo all'ENISA, l'agenzia dell'Unione europea per la cibersicurezza, che abroga il regolamento (UE) n. 526/2013, e relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione ("regolamento sulla cibersicurezza").

[78] Cfr. considerando 74 del regolamento sulla cibersicurezza.