PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Linee guida sulle questioni etiche e legali della protezione dei dati nella ricerca e nell'innovazione delle TIC

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (GDPR) - PRINCIPI

Questo progetto è stato finanziato dal programma di ricerca e innovazione Horizon 2020 dell'Unione Europea con l'accordo di sovvenzione n. 788039. Il presente documento riflette esclusivamente il punto di vista degli autori e l'Agenzia non può essere ritenuta responsabile per l'uso che può essere fatto delle informazioni in esso contenute.

1 Principi

Bud P. Bruegger (ULD)

Ringraziamenti: Gli autori ringraziano la revisione e i suggerimenti di Giuseppe D'Acquisto, Senior Technology Advisor, Garante per la Protezione dei Dati Personali.

Questa sezione delle Linee guida è stata convalidata da José Luis Piñar, ex presidente dell'Agenzia spagnola di protezione dei dati e attualmente Cattedratico dell'insegnamento universitario Google: Privacy, Società e Innovazione della Universidad CEU-San Pablo, Madrid

La sezione *Capire la protezione dei dati: il Regolamento UE in poche parole* ha fornito una panoramica del GDPR. Ha quindi anche introdotto i *principi* della protezione dei dati, come contenuto nel Capitolo 2 "Principi" del GDPR e lì in particolare nell'Art. 5 "Principi relativi al trattamento dei dati personali". Mentre *Understanding data protection: the EU regulation in a nutshell* ha scelto una struttura che motiva il contenuto del GDPR in termini di potere, la presente sezione segue la struttura dell'Art. 5 GDPR. Essa discute ogni principio in modo più dettagliato.

I principi esprimono la seguente struttura:

- **Condizioni sulle finalità** del trattamento: che tipo di *scopi* perseguiti dal trattamento dei dati personali sono consentiti è descritto nell'**Art. 5(1)(a)** e **5(1)(b)** GDPR. Il trattamento dei dati personali per finalità che non soddisfa queste condizioni non è consentito. Le condizioni sono:
    - ***Liceità*** (art. 5(1)(a) GDPR);
    - ***Legittimità*** (art. 5(1)b) GDPR).
- **Condizioni per l'attuazione del** trattamento: Quando la finalità soddisfa i criteri di cui sopra, per essere consentita, l'attuazione del trattamento deve inoltre soddisfare alcune condizioni. Queste sono descritte nell'Art. 5(1)(a) sebbene 5(1)(f); in particolare l'attuazione:
    - deve essere ***equo*** (art. 5(1)(a) GDPR);
    - deve essere ***trasparente*** (art. 5(1)(a) GDPR);
    - deve essere ***limitato agli scopi dichiarati*** (art. 5(1)(b) GDPR);
    - deve utilizzare il **minimo di dati** che è necessario per gli scopi (art. 5(1)(c) GDPR);
    - deve utilizzare **solo dati precisi** (art. 5(1)(d) GDPR);
    - deve utilizzare il **grado minimo di identificazione** degli interessati che è necessario per le finalità (art. 5(1)(e) GDPR);
    - deve essere **sicuro** (art. 5(1)(f) GDPR).

Inoltre, secondo l'art. 5(2) GDPR, per i titolari del trattamento di **rispettare il** GDPR significa che il loro **trattamento**:

- **soddisfa tutte le condizioni di cui sopra** e
- i titolari del trattamento sono in grado di **dimostrarlo**.

Per aiutare i lettori a capire il GDPR, la discussione dettagliata dei principi di cui sopra utilizza la struttura fornita dalla legge. Ciò significa che un punto del GDPR viene discusso alla volta. **Ogni punto** dell'Art. 5(1) e Art. 5(2) sono quindi chiamati un ***principio***. Il nome del principio che è previsto dal GDPR corrisponde ai titoli utilizzati per le sezioni seguenti. In alcuni casi, diverse condizioni di cui sopra rientrano in un unico principio.

Ci sono due eccezioni alla strutturazione della seguente discussione per paragrafo dell'art. 5 GDPR. Sono motivate da una maggiore chiarezza e discutono le dichiarazioni fornite in un paragrafo del GDPR sotto il principio (cioè, il significato principale) fornito in un altro paragrafo. Vale a dire, le eccezioni sono che:

- il requisito che le finalità debbano essere *specificate*, *esplicite* e *legittime* (previsto dall'art. 5(1)(b) GDPR) viene discusso insieme alla *liceità, correttezza e trasparenza* (dell'art. 5(1)(a) GDPR). 5(1)(a) GDPR), e
- la dichiarazione sul periodo di conservazione relativo a certi tipi di trattamento (prevista dall'art. 5(1)(e) GDPR) viene discussa insieme alla minimizzazione dei dati (dell'Art. 5(1)(c) GDPR) poiché, probabilmente, il periodo di conservazione è pertinente al fatto che i dati siano (temporalmente) "*limitati a quanto necessario in relazione alle finalità*".

La seguente tabella fornisce una panoramica di come i principi si riferiscono alle lettere dell'articolo 5 GDPR.

	Arte. 5(1)(a)	**Arte. 5(1)(b)**	**Arte. 5(1)(c)**	**Arte. 5(1)(d)**	**Arte. 5(1)(e)**	**Arte. 5(1)(f)**	**Arte. 5(2)**
Legittimità e **legalità**							
Equità							
Trasparenza							
Limitazione dello scopo							
Minimizzazione dei dati							
Precisione							
Limitazione della conservazione (minimizzazione del potenziale di identificazione)							
Integrità e **riservatezza**							

Responsabilità							

La discussione di ogni principio è strutturata come segue:

- Una **descrizione** astratta del principio,
- una breve discussione degli **articoli correlati e dei considerando del GDPR** adatti a fornire una comprensione più profonda del principio, e
- esempi di **misure tecniche o organizzative** concrete che possono essere utilizzate per attuare il principio.

La descrizione cerca di catturare l'essenza del principio. La sezione sugli articoli correlati e i considerando indica i punti del GDPR che descrivono più in dettaglio come il principio deve essere applicato concretamente. Questa sezione può essere in una prima lettura e consultata quando si desidera una comprensione più profonda. La sezione sulle misure fornisce una lista non esaustiva di esempi di come ogni principio può essere implementato nella pratica.

Il resto di questo capitolo descrive i principi elencati nell'Art. 5 GDPR utilizzando la struttura descritta.

1.1 Legalità, equità e trasparenza

Bud P. Bruegger (ULD)

Ringraziamenti: Gli autori riconoscono con gratitudine il contributo di Iñigo de Miguel Beriain (UPV/EHU) che ha scritto un'analisi di questo principio come input alla descrizione qui presentata.

Di seguito si discute il principio di *liceità, equità e trasparenza* che è definito nell'art. 5(1)(a) GDPR.

***Legalità, equità e trasparenza* in un colpo d'occhio:**

Secondo il GDPR, il trattamento deve essere *legittimo* e perseguire *scopi legittimi*. Inoltre deve essere *equo* e *trasparente*.

La liceità è definita molto precisamente nel GDPR ed è raggiunta se lo scopo del trattamento rientra in una delle sei categorie (alias *basi legali*) elencate nell'Art. 6(1) GDPR.

Legittimo è un concetto molto più ampio, che significa conformità alla lettera della legge, allo spirito della legge, ai valori della società (in particolare, la *Carta europea dei diritti fondamentali*) e ai principi dell'*etica*.

L'equità è usata nel suo significato comune. Proibisce per esempio pratiche manipolative da parte del titolare del trattamento, come il nudging. Probabilmente, la maggior parte degli articoli del GDPR riguardano la correttezza. Nominare il principio in modo esplicito può essere un ripiego per il caso in cui una conseguenza della correttezza potrebbe non essere espressa esplicitamente nel GDPR. Questo evita qualsiasi scappatoia.

La trasparenza del trattamento è una strategia principale per equilibrare il potere tra il titolare del trattamento e il soggetto dei dati. Funziona mettendo in luce l'eversione e quindi aprendola al controllo. È indicata nel GDPR tra i requisiti dettagliati delle informazioni che devono essere fornite dal titolare del trattamento a entrambi, interessati e autorità di controllo.

1.1.1 Descrizione

In *Capire la protezione dei dati: il regolamento UE in poche parole*, la maggior parte delle proprietà richieste in questo principio sono state discusse in termini di bilanciamento del potere tra il titolare del trattamento e gli interessati. Questo è riassunto nel seguente: Sia la *liceità* che la *legittimità* delle finalità è presentata come un pre-requisito perché il trattamento sia ammissibile. Vedere *1.5 Per quali scopi è permesso il trattamento per i dettagli*. La *correttezza* non è stata discussa nell'introduzione. Probabilmente, bilanciando il potere tra il titolare del trattamento e gli interessati, l'intero GDPR riguarda l'equità. La *trasparenza* è stata presentata come un pre-requisito per la responsabilità. Vedi *1.6.1 I titolari del trattamento sono pienamente responsabili* dei dettagli.

Il GDPR definisce il principio come segue:

Definizione nell'art. 5(1)(a) GDPR:

I dati personali devono essere trattati in modo **legale**, **equo** e **trasparente nei confronti** della persona interessata ("*liceità, equità e trasparenza"*);

La legalità, l'equità e la trasparenza sono discusse più in dettaglio nel seguito.

1.1.1.1 Prerequisito per la legittimità: scopi specifici ed espliciti

La liceità è un requisito per le finalità del trattamento[1]. È quindi impossibile ragionare su di essa senza prima conoscere le precise finalità che vengono perseguite dal trattamento. Per questo motivo, il requisito dell'**art. 5(1)(b)** che le finalità devono essere specificate ed esplicite è discusso qui come un prerequisito:

I dati personali sono raccolti per **scopi specifici, espliciti** e legittimi

Scopi specifici:

Il *gruppo di lavoro sulla protezione dei dati dell'articolo 29* scrive[2]:

> "La **specificazione delle finalità è al centro del quadro giuridico** stabilito **per la protezione dei dati personali**. Per **determinare se il trattamento dei dati è conforme alla legge**, e per stabilire quali garanzie di protezione dei dati devono essere

1 Non rientra nello scopo di questo documento fornire un'analisi giuridica approfondita del concetto di finalità al di là del suo significato nel linguaggio comune. Si deve solo sottolineare che le finalità del trattamento di solito sono legate a un obiettivo che il titolare persegue. Tali obiettivi dovrebbero essere concreti (molto più che teorici) ed è spesso possibile determinare se l'obiettivo è stato raggiunto o misurare in che misura è stato raggiunto.

2 Evidenziazione aggiunta dall'autore, per la citazione si veda la pagina 15 di: Gruppo di lavoro articolo 29 sulla protezione dei dati, 00569/13/IT, WP203, Parere 03/2013 sulla limitazione delle finalità, adottato il 2 aprile2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (ultima visita 27/05/2020).

applicate, è una **precondizione necessaria per identificare lo o gli scopi specifici** per i quali è richiesta la raccolta di dati personali."

La specificazione può essere vista come il primo compito della concettualizzazione di un'attività di elaborazione che guida tutte le decisioni successive:

- se il **trattamento è lecito**, cioè legittimo,
- **cosa comporta l'attuazione** del trattamento necessario per raggiungere gli scopi, e
- quali **garanzie di** protezione dei dati dovrebbero essere applicate.

Il *gruppo di lavoro* afferma[3] inoltre:

> "Lo **scopo** della raccolta deve essere **chiaramente** e **specificamente** identificato: deve essere sufficientemente **dettagliato** per determinare quale tipo di trattamento è e non è incluso nello scopo specificato, e per permettere che la conformità con la legge possa essere valutata e le garanzie di protezione dei dati applicate."

e

> Per queste ragioni, **uno scopo vago o generale**, come per esempio "migliorare l'esperienza degli utenti", "scopi di marketing", "scopi di sicurezza informatica" o "ricerca futura", senza maggiori dettagli, di solito **non soddisfa i criteri di *specificità*".**

Scopi espliciti:

Il gruppo di lavoro afferma inoltre[4]:

> "I dati personali devono essere raccolti per **scopi espliciti**. Gli scopi della raccolta **non** devono essere **solo** specificati **nella mente** delle persone responsabili della raccolta dei dati. Devono anche essere resi espliciti. In altre parole, devono essere **chiaramente rivelati, spiegati o espressi in qualche forma intelligibile**".

Si noti che l'obbligo di rendere esplicite le finalità è strettamente legato all'informazione degli interessati sulle finalità del trattamento (cfr. art. 13(1)(c) e 14(1)(c) GDPR).

Sulla base del prerequisito degli scopi espliciti specificati, la legittimità e la liceità possono essere discusse.

1.1.1.2 Legittimità e legalità

Mentre l'art. 5(1)(a) GDPR parla solo di *legittimità*, il requisito strettamente correlato della *legittimità* è indicato nell'Art. 5(1)(b) GDPR. Poiché entrambi esprimono requisiti relativi alle finalità del trattamento, sono discussi qui insieme.

L'art. 5(1)(b) GDPR afferma:

> I dati personali sono raccolti per **scopi** *determinati, espliciti* e **legittimi** e [...]

Il GDPR non fornisce una definizione di *legittimità*, ma il *gruppo di lavoro dell'articolo 29 sulla protezione dei dati* fornisce quanto segue: [5]

> Il requisito della ***legittimità*** significa che gli scopi devono essere **"conformi alla legge" nel senso più ampio**. Questo include **tutte le forme di diritto scritto e comune**, la **legislazione**

3 WP203, pagina 15, evidenziazione aggiunta dall'autore.
4 WP203, pagina 17, evidenziazione aggiunta dall'autore.
5 WP203, pagina 20, , evidenziazione aggiunta dall'autore.

primaria e secondaria, i **decreti municipali**, i **precedenti** giudiziari, i **principi costituzionali**, i **diritti fondamentali**, **altri principi giuridici**, così come la **giurisprudenza**, come tale "diritto" sarebbe interpretato e preso in considerazione dai tribunali competenti.

La legittimità è quindi un **requisito** molto **ampio**. Questo diventa ancora più significativo se si considera che alcune legislazioni, come la *Clinical Trial Regulation*[6], includono anche ***requisiti etici***. Ma anche quando l'etica non è prescritta dalla legge, c'è il pericolo che scopi chiaramente non etici possano essere considerati anche illegittimi. Per esempio, questo può essere il caso in cui il trattamento avviene in spregio a una disapprovazione da parte di un comitato etico di ricerca.

A differenza della *legittimità*, la ***liceità*** è effettivamente definita nel GDPR. Vale a dire, l'**art. 6(1)** GDPR recita:

Il trattamento è **lecito** solo se e nella misura in cui si applica almeno una delle seguenti condizioni: [...]

Nell'omissione rappresentata da [...], sono elencate sei possibili cosiddette *basi giuridiche.* Esse possono essere viste come categorie di scopi. Queste sono descritte più dettagliatamente nella sezione seguente.

1.1.1.3 Equità

Probabilmente, tutta la protezione dei dati e quindi il GDPR riguarda l'equità verso gli interessati. Il GDPR può essere visto nello spiegare cosa significa concretamente l'*equità.*

Quindi la sua menzione esplicita come principio può essere considerata come una "clausola di ripiego" per il caso in cui un requisito concreto di equità non sia stato esplicitamente dichiarato nel GDPR. Anche in questo caso, il principio di *equità* impedirebbe qualsiasi "scappatoia" nel GDPR.

Mentre l'intero GDPR può essere considerato una questione di equità, la sezione di seguito fornisce alcuni esempi in cui la correttezza è particolarmente evidente.

1.1.1.4 Trasparenza

La trasparenza è un concetto ben compreso ed è un pre-requisito chiave per la responsabilità nel GDPR. L'obiettivo principale della trasparenza è quello di informare in anticipo[7] **gli interessati** dell'esistenza del trattamento e delle sue caratteristiche principali. Altre informazioni (come i dati sulla persona interessata) sono disponibili su richiesta. Gli interessati devono anche essere informati di alcuni eventi, in particolare le violazioni dei dati (nel caso in cui l'interessato sia esposto a un rischio elevato). La trasparenza è anche supportata dai titolari del trattamento che designano un responsabile della protezione dei dati (DPO) che agisce come unico punto di contatto per le preoccupazioni degli interessati. Nel GDPR, gli interessati sono autorizzati ad essere i principali guardiani dei loro diritti e delle loro libertà. Evidentemente, la trasparenza è un prerequisito per individuare e intervenire in caso di non conformità.

---

6 REGOLAMENTO (UE) N. 536/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 16 aprile 2014 sulla sperimentazione clinica di medicinali ad uso umano e che abroga la direttiva 2001/20/CE, https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/reg_2014_536/reg_2014_536_en.pdf (ultima visita 27/05/2020).

7 Up-front qui significa che gli interessati dovrebbero essere consapevoli del trattamento prima che abbia luogo. Non implica un certo metodo di fornire informazioni o esclude modi dinamici di fornire le informazioni necessarie.

Le autorità di controllo, come ovvio dal loro nome, sono anche custodi del rispetto del GDPR, anche se il loro coinvolgimento è spesso innescato da reclami presentati dagli interessati[8]. Ci sono requisiti di trasparenza per i titolari del trattamento che sono specificamente rivolti ai titolari del trattamento di vigilanza, tra cui le registrazioni del trattamento (vedi *Documentazione del trattamento* nella sezione "*Strumenti e azioni principali" della Parte II*) e le valutazioni d'impatto sulla protezione dei dati (vedi la sezione con lo stesso nome in "*Strumenti e azioni principali",* Parte II di queste Linee guida). Il fatto che i titolari del trattamento debbano rispondere[9] alle autorità di controllo e che debbano permettere indagini e audit in loco[10] implementa [11]ulteriormente la trasparenza.

1.1.2 Articoli e Considerando correlati

1.1.2.1 Legalità

La definizione di legalità è data nell'art. 6(1) GDPR. Essa recita come segue:

> Il trattamento è ***lecito* solo se e nella misura in cui** si applica almeno una delle seguenti condizioni:
>
> (a) l'interessato ha dato il **consenso** al trattamento dei suoi dati personali per una o più *finalità* specifiche;
>
> (b) il trattamento è necessario per l'**esecuzione di un contratto di cui l'**interessato è parte o per prendere provvedimenti su richiesta dell'interessato prima della conclusione di un contratto;
>
> (c) il trattamento è necessario per il **rispetto di un obbligo legale al quale** è soggetto il titolare del trattamento;
>
> (d) il trattamento è necessario per **proteggere gli interessi vitali** della persona interessata o di un'altra persona fisica;
>
> (e) il trattamento è necessario per l'esecuzione di un compito di **interesse pubblico** o per l'esercizio dei poteri pubblici conferiti al titolare del trattamento;
>
> (f) il trattamento è necessario ai *fini* dei **legittimi interessi perseguiti dal titolare del trattamento** o da un terzo, **tranne quando su** tali interessi **prevalgono gli interessi o i diritti e le libertà fondamentali della persona interessata** che richiedono la protezione dei dati personali, in particolare se la persona interessata è un bambino.
>
> La lettera f) del primo comma non si applica ai trattamenti effettuati dalle autorità pubbliche nell'esercizio delle loro funzioni.

Mentre le finalità del trattamento devono essere specificate ed esplicite (vedi Art. 5(1)(b), e quindi anche sufficientemente ristrette e specifiche, le suddette sono chiaramente **categorie di finalità**. (Dove la parola finalità è stata usata esplicitamente, è quindi scritta in corsivo). Essi sono comunemente chiamati ***basi[12] giuridiche*** e sono riferimenti dalla loro posizione nell'articolo 6; per esempio, il *consenso* sarebbe quindi la *base giuridica* dell'art. 6(1)(a).

---

8 Vedi l'art. 57(1)(f) GDPR.
9 Vedi l'art. 58(1)(a) GDPR.
10 Vedi l'art. 58(1)(f) GDPR.
11 Vedi l'art. 58(1)(b) GDPR.
12 Il termine *base giuridica* è usato estesamente nel GDPR ed è raccomandato qui come termine preferenziale. In alternativa, il GDPR contiene anche il termine *legal ground*. In letteratura si usa anche il termine *base legale.*

Il GDPR prevede due articoli che indicano **ulteriori requisiti di liceità** per due casi diversi: **dati sensibili** e dati relativi a **condanne penali**. In particolare questi sono i seguenti:

L'art. 9 GDPR afferma che il trattamento di dati particolarmente sensibili è in linea di principio vietato ed elenca 10 eccezioni a questa regola. Le eccezioni sono paragonabili nella struttura alle basi giuridiche dell'Art. 6. L'articolo specifica che i dati sono particolarmente sensibili, se rivelano:

- origine razziale o etnica,
- opinioni politiche,
- credenze religiose o filosofiche,
- l'iscrizione al sindacato,

o sono:

- dati genetici,
- dati biometrici allo scopo di identificare in modo univoco una persona fisica,
- dati relativi alla salute, o
- dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica.

Per questi dati, si applicano requisiti più rigorosi affinché il loro trattamento sia considerato legittimo. Per esempio, invece del semplice consenso dell'art. 6(1)(a), il trattamento di tali dati sensibili richiede un livello di consenso più esigente chiamato ***consenso esplicito*** (vedi Art. 9(2)(a) GDPR).

Come l'art. 9 per i dati particolarmente sensibili, l'**art. 10 GDPR** limita ulteriormente il trattamento dei "dati relativi a **condanne penali e reati** o misure di sicurezza correlate". In particolare, per essere legittimo, il trattamento deve essere "effettuato solo sotto il **controllo dell'autorità ufficiale** o quando [è] autorizzato dal diritto dell'Unione o degli Stati membri che prevede garanzie adeguate per i diritti e le libertà degli interessati".

Ci sono diversi articoli e considerando nel GDPR che specificano il **concetto di consenso** (dell'art. 6(1)(a) GDPR) in modo più dettagliato. I più importanti sono i seguenti:

- **Art. 4(11)** che **definisce il consenso**;
- **Art. 7** che elenca le **condizioni per il consenso**; e
- **L'art. 8** che regola le **condizioni applicabili al consenso del bambino in relazione ai servizi della società dell'informazione.**

Considerando che il consenso è un concetto complesso, il **Comitato europeo per la protezione dei dati** ha emesso ***Linee guida*** autorevoli *05/2020* ***sul consenso*** *ai sensi del regolamento 2016/679*[13].

Oltre al *consenso*, anche il concetto di ***interesse legittimo perseguito dal titolare del trattamento*** (dell'art. 6(1)(f) GDPR) è difficile da comprendere appieno. Ciò che è cruciale qui è la restrizione di "**tranne** quando tali interessi sono prevalenti rispetto agli interessi o ai diritti e alle libertà fondamentali della persona interessata". Ciò significa che l'interesse legittimo del titolare del trattamento deve essere bilanciato con gli interessi degli interessati. Per determinare se questo è il caso, il titolare del trattamento deve realizzare un cosiddetto

13 EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.0, Adopted on4 May2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (ultima visita 22/05/2020).

balancing test. Come farlo è descritto in "Strumenti e azioni principali" nella Parte II di queste Linee guida. Si basa principalmente sull'autorevole *parere 06/2014* del Gruppo dell'*articolo 29 sulla nozione di legittimo interesse del titolare del trattamento dei dati ai sensi dell'articolo 7 della direttiva 95/46/CE*[14]. Anche se questo parere si basa sulla direttiva sulla protezione dei dati che è precedente al GDPR, è in generale applicabile all'interpretazione dell'art. 6(1)(f) GDPR. È raccomandato per **ulteriori letture** sull'argomento.

1.1.2.2 Equità

Probabilmente, l'intero GDPR riguarda l'equità. Qui di seguito si segnalano alcuni articoli del GDPR che illustrano particolarmente bene questo aspetto.

Un'area in cui l'equità è evidente riguarda i requisiti di trasparenza. Qui, l'**art. 12(1)** afferma che i titolari del trattamento devono fornire informazioni "all'interessato in una forma **concisa**, trasparente, **intelligibile** e **facilmente accessibile**, utilizzando un **linguaggio chiaro e semplice**, in particolare per qualsiasi informazione rivolta specificamente a un minore". Evidentemente, questo proibisce la pratica sleale di fornire le informazioni richieste in una forma che è inaccessibile agli interessati.

Allo stesso modo, il **consenso** non può essere implicito, ma richiede piuttosto un'esplicita "dichiarazione o una **chiara azione affermativa**" (vedi **Art. 4(11)** GDPR). Lo stesso articolo afferma inoltre che il consenso deve essere **dato liberamente**, **specifico**, **informato** e **non ambiguo**". Inoltre, **in qualsiasi momento**, senza bisogno di giustificazione, una persona interessata deve essere in grado di **ritirare il** consenso **con la stessa facilità con cui è stato dato**. Questi requisiti rigorosi per il consenso proibiscono direttamente molte pratiche manipolative, compreso il "nudging"[15] degli interessati.

Diversi **diritti degli interessati** possono essere direttamente associati all'equità. Questi includono:

- Il **diritto alla rettifica** (art. 16 GDPR) per evitare che gli interessati subiscano conseguenze negative a causa di dati inesatti;
- Il **diritto alla limitazione del trattamento** (art. 18 GDPR) che impedisce ai titolari del trattamento di utilizzare ulteriormente i dati che sono stati segnalati come inesatti o che riguardano il trattamento a cui l'interessato si è opposto;
- Il **diritto alla portabilità dei dati** (art. 20 GDPR) che impedisce situazioni di lock-in e una possibile perdita (ad esempio di investimenti[16]) quando gli utenti cambiano il loro rapporto con il titolare del trattamento;
- Il **diritto di opposizione** (art. 21 GDPR) dove nel caso di una base giuridica dell'art. 6(1)(f) GDPR, gli interessati possono presentare le **loro situazioni specifiche** in cui il loro interesse prevale sugli interessi legittimi del titolare del trattamento;
- Il **diritto di non essere sottoposto a una decisione basata unicamente su un trattamento automatizzato** (art. 22 GDPR), che prevede anche il **diritto di ottenere l'intervento umano da** parte del titolare del trattamento (vedi paragrafo 3).

---

14 Gruppo di lavoro articolo 29 per la protezione dei dati, 844/14/IT, WP217, parere 06/2014 sulla nozione di interessi legittimi del titolare del trattamento dei dati ai sensi dell'articolo 7 della direttiva 95/46/CE, adottato il 9 aprile 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (ultima visita 22/05/2020).

15 Vedi per esempio, Weinmann, M., Schneider, C. & Brocke, J.v. Digital Nudging. Bus Inf Syst Eng 58, 433-436 (2016). https://doi.org/10.1007/s12599-016-0453-1 (ultima visita 22/05/2020).

16 Un primo esempio per una possibile perdita di investimento è la collezione di foto personali.

Un'altra indicazione di equità è quando il titolare del trattamento deve prendere in considerazione il punto di vista degli interessati. Questo è per esempio evidente nel considerando 50 del GDPR che richiede di considerare le ragionevoli aspettative degli interessati quando si determina se uno scopo è compatibile secondo l'art. 6(4). Appare anche nelle valutazioni d'impatto sulla protezione dei dati (art. 35 GDPR), dove i titolari del trattamento, eventualmente, devono chiedere il parere degli interessati o dei loro rappresentanti (art. 35(9) GDPR).

1.1.2.3 Trasparenza

Diversi articoli del GDPR forniscono ulteriori dettagli sul principio di *trasparenza*. Essi includono quanto segue:

- **Gli articoli da 12 a 14** descrivono in dettaglio le **informazioni** che i titolari del trattamento devono fornire **in anticipo** agli interessati.
- **L'art. 15** descrive le informazioni che devono essere fornite su richiesta degli interessati, compreso l'accesso completo ai loro dati.
- **L'art. 34** descrive come gli interessati devono essere informati delle violazioni dei dati, quando è probabile che ciò comporti un rischio elevato.
- **L'art. 38(4)** designa il *Responsabile della protezione dei dati (DPO)* presso il titolare del trattamento come punto di accesso per gli interessati.
- **Gli artt. 12** e **19** descrivono le informazioni che i titolari del trattamento devono fornire agli interessati che esercitano uno dei loro diritti.
- **L'art. 30** ***registri di trattamento*** e **35** ***valutazione d'impatto sulla protezione dei dati*** descrivono le informazioni che devono essere fornite alle autorità di controllo. (Quest'ultimo solo se il trattamento può comportare un rischio elevato).
- **L'art. 58(1)** specifica come i titolari del trattamento debbano essere trasparenti nei confronti delle autorità di controllo rispondendo (punto a), permettendo ispezioni e audit (punto b), e concedendo l'accesso ai loro locali (punto f).
- **L'art. 33** descrive le notifiche di violazione verso le autorità di vigilanza.

Considerando l'importanza della trasparenza nel GDPR, il ***Comitato europeo per la protezione dei dati*** ha fornito un'interpretazione autorevole dei relativi obblighi nelle loro **Linee guida sulla trasparenza** ai sensi del regolamento 2016/679 (wp260rev.01)[17]. Questo è raccomandato per ulteriori letture.

1.1.3 Misure tecniche e organizzative correlate

Esempi di misure per implementare diversi aspetti del principio sono forniti di seguito.

1.1.3.1 Legittimità e legalità

- Almeno laddove la verifica e la dimostrazione della **legittimità** richiedono **passi formali**, questi possono essere considerati misure organizzative a sostegno della

17 EDPB, Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 (ultima visita 22/05/2020).

legittimità. Un primo esempio sono la **richiesta e l'approvazione** di certe ricerche mediche attraverso il **comitato etico di ricerca** competente.

- Un pre-requisito per valutare sia la legittimità che la liceità è la specificazione **di scopi espliciti**. Questo di per sé può essere considerato una misura, in particolare quando va di pari passo con le **considerazioni** su come rendere la specificazione il più **specifica** e **ristretta possibile**. In questo caso, anche tale analisi può essere considerata parte di questa misura.
- La principale misura a sostegno della liceità è identificare una o più **basi giuridiche** dell'**art. 6(1)** GDPR. In molti casi, un'attività di trattamento utilizza più basi giuridiche. Un caso d'uso [18]pubblicato dal *Data Privacy Vocabulary Community Group* del W3C fornisce un esempio facilmente accessibile.
- Laddove l'art. **6(1)(a)** GDPR, cioè il *consenso, è* stato scelto come base giuridica, un'**analisi** che giustifichi che i **requisiti** rigorosi del GDPR **per il consenso (liberamente dato e informato)** siano stati soddisfatti è una misura importante. Questo può per esempio includere test se le informazioni fornite come base per il consenso sono effettivamente comprensibili per gli interessati e se la revoca del consenso è davvero facile come darlo.
    - Inoltre, laddove sono interessati i **bambini** o altri **soggetti vulnerabili**, questa analisi dovrebbe porre particolare attenzione alle garanzie relative all'art. 7 GDPR.
- Laddove l'art. **6(1)(f)** GDPR, cioè il *consenso legittimo da parte del titolare del trattamento, è* stato scelto come base giuridica, le misure includono una precisa specificazione degli interessi legittimi, nonché un ***test di bilanciamento*** (si veda la sezione omonima in "Strumenti e azioni principali" nella Parte II di queste Linee guida) per accertare che questi prevalgano effettivamente sugli interessi, i diritti e le libertà degli interessati.
- Con qualsiasi base giuridica, se i titolari del trattamento intendono **trattare ulteriormente** alcuni dati**,** al di là delle finalità iniziali, per **finalità compatibili** (cfr. art. 5(1)(b) GDPR), l'analisi basata sui criteri dell'Art. 6(4) per dimostrare che queste finalità aggiuntive sono effettivamente compatibili, è una misura che dimostra la liceità di tale trattamento.
- Se vengono trattate categorie speciali di dati (cioè dati sensibili) o dati relativi a condanne penali, devono essere adottate ulteriori misure oltre a quelle relative all'art. 6(1) GDPR. In particolare, nel primo caso, la condizione dell'art. 9(2) GDPR, per cui si applica un'eccezione al divieto di trattamento dei dati sensibili, deve essere trovata e documentata. Nel secondo caso, le condizioni che rendono ammissibile il trattamento secondo l'art. 10 GDPR devono essere attuate e documentate.

1.1.3.2 Equità

- Come è stato argomentato sopra, tutti i requisiti del GDPR possono essere considerati una questione di equità; diversi diritti degli interessati sono stati presentati come particolarmente rilevanti, tuttavia. Le prime misure a sostegno dell'equità sono quindi un'adeguata **attuazione dei diritti degli interessati**.

18 Bruegger, Schlehahn & Zwingelberg, Data Privacy Vocabulary Community Group, Data Protection Aspects of Online Shopping - A Use Case, https://www.w3.org/community/dpvcg/2019/12/12/data-protection-aspects-of-online-shopping-a-use-case/ (ultima visita 25/05/2020).

1.1.3.3 Trasparenza

- L'attuazione dei requisiti degli artt. Da 12 a 14 GDPR per fornire **informazioni** adeguate e facilmente comprensibili **agli interessati** è una misura primaria per sostenere la trasparenza.
- Lo stesso vale per i documenti preparati per informare le autorità di controllo, in particolare i ***registri di trattamento*** (secondo l'articolo 30 GDPR) e una ***valutazione d'impatto sulla protezione dei dati*** (secondo l'articolo 35 GDPR). Un'ulteriore misura è la pubblicazione parziale di questa valutazione d'impatto.
- Qualsiasi analisi che valuti l'efficacia e l'accessibilità dell'informazione fornita - possibilmente in relazione a categorie speciali di soggetti come i bambini - può essere considerata una misura in sé.
- La nomina di un Responsabile della protezione dei dati (DPO) può essere vista in parte come una misura per aumentare la trasparenza sia verso gli interessati che verso l'autorità di controllo.

1.2 Limitazione dello scopo

Bud P. Bruegger (ULD)

Ringraziamenti: Gli autori riconoscono con gratitudine il contributo di Iñigo de Miguel Beriain (UPV/EHU) che ha scritto un'analisi di questo principio come input alla descrizione qui presentata.

Di seguito si discute il principio di *limitazione delle finalità* che è definito nell'art. 5(1)(b) GDPR.

***Limitazione dello scopo* in sintesi:**

I dati che sono stati **raccolti per determinati scopi "iniziali" sono trattati solo ulteriormente**:

- per questi **scopi iniziali**, o per
- **scopi compatibili**.

Per il caso generale, il GDPR dà dei **criteri** per **determinare la compatibilità** delle finalità (vedi Art. 6(4)). Inoltre, alcune finalità sono **pre-approvate come compatibili** dal GDPR (vedi Art. 5(1)(b)) a condizione che siano attuate le opportune garanzie (vedi Art. 89). Vale a dire, questi sono:

- **l'archiviazione** nell'**interesse pubblico,**
- **ricerca scientifica o storica**, e
- **statistiche**.

1.2.1 Descrizione

In *Capire la protezione dei dati: il regolamento UE in poche parole*, la *limitazione delle finalità* è stata motivata limitando l'uso del potere acquisito esclusivamente al raggiungimento degli scopi dichiarati e legittimi. (Vedi *1.6.4 Limitare i titolari del trattamento a usare il potere esclusivamente per raggiungere gli scopi legittimi dichiarati* per i dettagli).

Il GDPR definisce il principio come segue:

Definizione nell'art. 5(1)(b) GDPR:

I dati personali sono raccolti per finalità determinate, esplicite e legittime e **non sono ulteriormente trattati** in **modo incompatibile con tali finalità**; [...] ("*limitazione delle finalità*");

Si noti che la prima metà di questa frase è già stata discussa sotto il principio precedente. In particolare, il requisito che i fini debbano essere ***specificati*** **ed** ***espliciti*** era un **prerequisito per** poter parlare di ***legittimità***; il requisito della legittimità riguarda i fini ed è stato quindi discusso insieme alla *legittimità*.

Ciò che viene discusso qui più in dettaglio è l'essenza di questo principio, vale a dire la **limitazione al trattamento compatibilmente con le finalità**. Questo è un requisito che riguarda l'attuazione dell'attività di trattamento, non le finalità.

1.2.1.1 Non trattate in modo incompatibile con questi scopi

La parte essenziale di questo principio è quindi contenuta nella mezza frase "non ulteriormente trattati in modo incompatibile con questi scopi". Di seguito si analizza questa frase in modo più dettagliato.

La frase parla di compatibilità con gli **scopi**. È chiaro dalla prima metà della frase che questi sono gli scopi **che sono stati esplicitamente specificati**[19] (vedi sezione 1.1.1.1 sopra). La parte dell'art. 5(1)(b) che è stata rappresentata da [...] e di cui si parlerà in seguito utilizza anch'essa il concetto di "compatibilità con le ***finalità iniziali"***. Le *finalità iniziali* sembrano quindi essere le stesse specificate (durante la concezione dell'attività di trattamento).

L'art. 5(1)(b) esprime quindi che il trattamento deve essere compatibile con:

- gli **scopi iniziali stessi**, o
- **altri scopi** che sono **compatibili** con questi scopi iniziali.

La prima segue dal ragionamento che i fini sono sempre compatibili con se stessi.

La formulazione dell'art. 5(1)(b) parla di "**ulteriore** trattamento". Mentre questo potrebbe essere inteso temporalmente, cioè nel senso di "dopo che gli scopi iniziali sono stati raggiunti", l'aspetto temporale sembra essere irrilevante per questo principio. Invece, "ulteriormente" ha il significato di "oltre" senza significato temporale e si riferisce puramente agli scopi.

La situazione è visualizzata in Figura 1:

19 Queste sono anche le finalità che vengono comunicate agli interessati come richiesto dall'art. 13 e 14 GDPR).

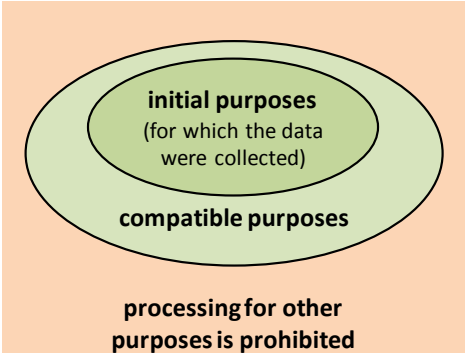

Figura 1: L'elaborazione è consentita per gli scopi iniziali e compatibili.

È importante sapere che non è necessaria alcuna base giuridica aggiuntiva per un ulteriore trattamento per scopi compatibili. Questo è dichiarato esplicitamente nel considerando 50 del GDPR (2ª frase). Riferendosi all'ulteriore trattamento per scopi compatibili, afferma che:

> In tal caso, non è richiesta alcuna base giuridica diversa da quella che ha permesso la raccolta dei dati personali.

1.2.1.2 Uso per scopi incompatibili

Questo solleva la questione di come può accadere di trattare dati personali per scopi incompatibili e quali sono le sue conseguenze.

Capire come l'elaborazione può avvenire è importante per poterla evitare. I tre esempi seguenti illustrano la questione senza pretesa di completezza:

- **Function creep**: è comune che le attività di trattamento si evolvano nel tempo. È anche comune che poi acquisiscano nuove funzionalità o "caratteristiche" che corrispondono a un trattamento aggiuntivo o modificato. Nei casi in cui il titolare del trattamento non riesce ad esercitare un controllo sufficiente su tale evoluzione, il trattamento può andare inosservato oltre gli scopi iniziali o compatibili.
- **Mancanza di separazione**: Supponiamo che un titolare del trattamento gestisca più attività di trattamento indipendenti che perseguono scopi distinti. Se il titolare del trattamento non implementa misure adeguate per separare le diverse attività di trattamento, è facile che i dati raccolti per una serie di scopi siano usati per altri scopi. Questo è illustrato in Figura 2 e Figura 1.

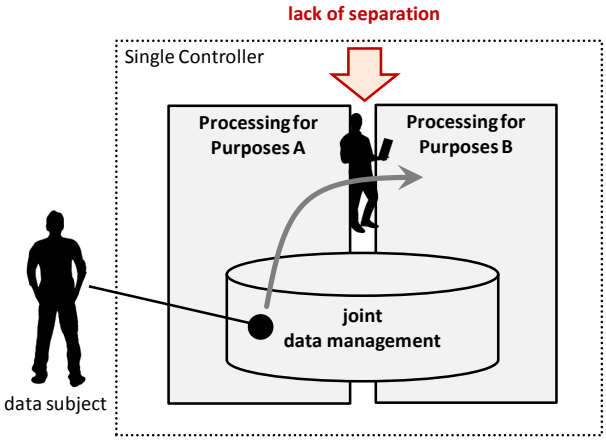

Figura 2: Una mancanza di separazione porta all'uso di dati per scopi incompatibili.

- **Destinatari che perseguono finalità proprie**: I destinatari sono persone o organizzazioni a cui vengono comunicati dati personali (vedi definizione nell'art. 4(9) GDPR). I destinatari possono essere ad esempio:
    - **dipendenti** che accedono *legittimamente* ai dati su istruzione del titolare del trattamento per adempiere alle finalità compatibili del trattamento, o
    - **attaccanti esterni** che accedono illegittimamente ai dati attraverso una violazione[20].

  In quest'ultimo caso, è ovvio che il destinatario utilizza i dati personali per altri scopi. Sono proprio questi scopi che probabilmente hanno motivato l'attacco in primo luogo. Ma anche i dipendenti possono avere altri interessi nei dati rispetto al perseguimento degli scopi dichiarati dal loro datore di lavoro. Un primo esempio è quello in cui il dipendente conosce già la persona interessata e viene a conoscenza di informazioni che altrimenti non sarebbero accessibili.

Con la comprensione acquisita da questi esempi che illustrano come i dati possono essere utilizzati per altri scopi, si deve porre la questione delle possibili conseguenze.

In tutti i casi, i principi **fondamentali** di *legalità* e *legittimità* sono probabilmente **violati**. Secondo questi principi, il trattamento è vietato a meno che non sia giustificato da una dimostrata liceità e legittimità delle finalità. Questo ovviamente non è il caso quando il trattamento avviene per scopi incompatibili, e quindi ingiustificati.

L'uso dei dati al di fuori e oltre gli scopi giustificati **permette** anche ai **titolari del trattamento** disonesti di **accumulare potere**. Questo può accadere, ad esempio, quando i titolari del trattamento combinano le serie di dati delle persone in attività di trattamento distinte, conservano e accumulano i dati quando non sono più necessari per gli scopi, ed eventualmente anche acquisiscono dati da altre fonti al fine di ottenere più potere sui loro interessati. Tale potere accumulato supera evidentemente il guadagno di potere che era giustificato da una dimostrata liceità e legittimità delle finalità iniziali.

È evidente che al di là della sola violazione dei principi della protezione dei dati, a seconda degli scopi per i quali i dati vengono (ab)usati, le **persone interessate** possono subire anche **danni materiali o immateriali**. Per esempio, la conoscenza di certi dati sulla salute può influenzare significativamente le relazioni quando sono accessibili a conoscenti o impedire opportunità di lavoro quando sono accessibili a potenziali datori di lavoro. Se usati per scopi criminali, alcuni tipi di dati possono essere la base per un ricatto.

1.2.1.3 Quando gli scopi sono compatibili?

Quanto segue discute come determinare se potenziali scopi aggiuntivi sono considerati compatibili. Si basa principalmente sull'art. 6(4) GDPR.

Nel caso in cui una **base giuridica** del ***consenso*** (vedi Art. 6(1)(a) GDPR) è stato scelto per il trattamento, un ulteriore trattamento per **scopi aggiuntivi** diversi da quelli compatibili pre-approvati (vedi sotto) sono **considerati incompatibili**[21]. Questo perché il consenso è sempre specifico per le finalità specificate[22]. "Ampliare" le finalità del trattamento oltre a quelle

20 I titolari non sono responsabili delle azioni degli attaccanti, ma solo di prevenire gli attacchi attraverso adeguate misure di sicurezza.

21 Si noti che l'art. 6(4) GDPR sugli scopi compatibili esclude esplicitamente che sia applicabile quando la base giuridica è il consenso.

22 In particolare, questi scopi sono specificati nel dialogo che chiede il consenso e la specificazione è un aspetto importante dell'informazione del consenso.

specificate a cui l'interessato ha acconsentito, sarebbe chiaramente ingiusto e poco trasparente.

L'art. 6(4) prevede poi i seguenti **criteri che** i titolari del trattamento devono utilizzare per determinare se uno scopo aggiuntivo è compatibile (riformulato leggermente rispetto al GDPR):

> (a) Qualsiasi **legame tra** gli **scopi iniziali** e gli **scopi aggiuntivi** in esame;
>
> (b) il **contesto in cui i dati** personali **sono stati raccolti**, in particolare per quanto riguarda la **relazione** tra gli **interessati** e il **titolare del trattamento**;
>
> (c) la **natura dei dati personali**, in particolare se comprendono **categorie speciali di dati** personali (cioè, sensibili) o se vengono trattati dati personali relativi a **condanne penali** e **reati;**
>
> (d) le **possibili conseguenze** dell'ulteriore trattamento previsto **per gli interessati**;
>
> (e) l'**esistenza di garanzie adeguate**, che possono includere la **pseudonimizzazione**.

Ulteriori indicazioni, compresi esempi di applicazione di questi criteri, sono disponibili presso il *gruppo*[23] *di lavoro dell'articolo 29 sulla protezione dei dati*. Mentre questo parere si riferisce alla *direttiva sulla protezione dei dati* (cioè il predecessore o il GDPR), molti aspetti sono ancora ugualmente applicabili oggi.

Per semplificare la determinazione se gli scopi aggiuntivi sono compatibili, il **GDPR pre-approva alcuni** degli **scopi** aggiuntivi più comuni perseguiti nel trattamento successivo. Vale a dire, l'art. 5(1)(b) include quanto segue:

> [Un ulteriore trattamento a fini di **archiviazione nel pubblico interesse**, di **ricerca scientifica o storica** o a fini **statistici** non è considerato incompatibile con le finalità iniziali, conformemente all'articolo 89, paragrafo 1.

Il citato Art. 89(1) richiede la presenza di garanzie aggiuntive.

Qui, il citato Art. 89 GDPR impone che l'ulteriore trattamento per questi scopi pre-approvati è ammissibile solo se ci sono garanzie adeguate.

1.2.2 Articoli e Considerando correlati

L'**essenza** del principio di limitazione delle finalità è descritta nell'**art. 5(1)(b)** GDPR e contiene anche l'elenco delle **finalità compatibili pre-approvate**.

L'art. 5(1)(e) GDPR fornisce ulteriori dettagli sul possibile **periodo di conservazione** dei dati relativi all'ulteriore trattamento **per le finalità compatibili pre-approvate**.

Il considerando 50 del GDPR fornisce una guida per l'interpretazione dell'ulteriore trattamento per scopi compatibili. Di particolare interesse è la seconda frase che afferma che **non è richiesta alcuna base giuridica aggiuntiva** separata da quella che ha permesso la raccolta dei dati personali.

L'art. 89 GDPR impone che quando il trattamento prosegue per **scopi compatibili pre-approvati**, i titolari del trattamento devono attuare **garanzie adeguate**. Apre anche alla possibilità che in questo contesto, il diritto dell'Unione o degli Stati membri possa prevedere **deroghe a certi diritti degli interessati**.

---

23 Gruppo di lavoro articolo 29 sulla protezione dei dati, 00569/13/EN, WP203, Parere 03/2013 sulla limitazione delle finalità, adottato il 2 aprile 2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (ultima visita 28/05/2020).

1.2.3 Misure tecniche e organizzative correlate

Quanto segue fornisce esempi di misure tecniche e organizzative a sostegno della *limitazione degli scopi*:

- Una precisa e chiara specificazione degli scopi iniziali e potenzialmente compatibili è un prerequisito per qualsiasi ragionamento sulla separazione degli scopi.
- Comprendere la protezione dei dati come un processo che include **revisioni regolari** durante l'intero ciclo di vita dell'attività di trattamento è importante per evitare il trattamento dei dati per scopi incompatibili, ad esempio, a causa del **function creep**. Si noti che la revisione regolare è obbligatoria nel contesto della *protezione dei dati mediante progettazione* (art. 25(1) GDPR), delle *valutazioni d'impatto sulla protezione dei dati* (art. 35(11) GDPR) e della *sicurezza* (art. 32(1)(d) GDPR).
- La **verifica della compatibilità delle finalità** secondo l'art. 6(4) può essere considerata una misura organizzativa a sostegno della limitazione delle finalità.
- L'**analisi di** come il **personale autorizzato** può utilizzare i dati personali **per altri scopi** è un'altra misura organizzativa. Tale analisi mira a identificare possibili **motivazioni**, **conflitti d'interesse** (come il personale che tratta i dati di parenti e conoscenti), e misure per **prevenire** [24] **o mitigare** tali situazioni (ad esempio, la possibilità che un dipendente possa segnalare un conflitto d'interesse per un caso assegnato e passarlo a un altro dipendente senza conflitto d'interesse).
- Un'altra misura è un'analisi delle **motivazioni** che **gli attaccanti esterni** possono avere per ottenere i dati per altri scopi. Questa è una parte importante della valutazione del rischio e un prerequisito per implementare adeguate salvaguardie a sostegno della limitazione dello scopo.
- Qualsiasi misura organizzativa o tecnica per implementare la **separazione tra attività di trattamento distinte** perseguite dallo stesso titolare del trattamento sono a sostegno diretto della limitazione delle finalità.
- Qualsiasi misura (come la crittografia) a sostegno della **riservatezza** impedisce che parti non autorizzate possano utilizzare i dati per scopi illegittimi.
- Qualsiasi misura per garantire che il **personale autorizzato** agisca **solo su istruzione e secondo le istruzioni** del titolare del trattamento (cfr. Art. 29 e 32(4) GDPR) garantisce che il trattamento non vada oltre quanto necessario per raggiungere gli scopi specificati.
- Una misura secondaria che mitiga i danni dopo una violazione è la **pseudonimizzazione**. La possibilità drasticamente ridotta di identificare i soggetti dei dati e il collegamento ad altri set di dati può in molti casi impedire efficacemente l'uso dei dati trapelati per altri scopi.

1.3 Minimizzazione dei dati

Bud P. Bruegger (ULD)

24 Un altro esempio per prevenire i conflitti d'interesse è quando una grande azienda elabora in uffici lontani dagli interessati per ridurre la probabilità che i dipendenti elaborino dati di conoscenti.

*Ringraziamenti: L'*autore ringrazia il contributo di Andrès Chomczyk Penedo (VUB) che ha scritto un'analisi di questo principio come input alla descrizione qui presentata.

Di seguito si discute il principio di *minimizzazione dei dati* che è definito nell'art. 5(1)(c) GDPR.

***Minimizzazione dei dati* in sintesi:**

La minimizzazione dei dati limita i dati che vengono raccolti e utilizzati a quelli **adeguati**, **pertinenti** e **limitati** alla **necessaria realizzazione degli scopi**. La limitazione al necessario ha due aspetti:

- volume di dati (o più precisamente, contenuto di informazioni) e
- durata della conservazione.

Di conseguenza, viene elaborato (compreso l'immagazzinamento) il minor numero di dati possibile per un periodo di tempo più breve possibile, pur raggiungendo gli scopi dichiarati.

1.3.1 Descrizione

In *Capire la protezione dei dati: il regolamento UE in poche parole*, la *minimizzazione dei dati* era motivata dal minimizzare il guadagno di potere del titolare del trattamento a quello che è minimamente necessario per soddisfare le finalità dichiarate e legittime. In particolare, ha affrontato la minimizzazione del contenuto informativo presente nei dati personali trattati. Questo completa la minimizzazione del grado di associazione che i dati hanno con la persona interessata, e la limitazione dell'accesso al potere. Vedi *Minimizzazione del potere a ciò che è necessario per soddisfare le finalità dichiarate* per il dettaglio.

Il GDPR definisce il principio come segue:

Definizione nell'art. 5(1)(c) GDPR:

I dati personali devono essere **adeguati**, **pertinenti e limitati a ciò che è necessario in relazione alle finalità** per le quali sono trattati ("*minimizzazione dei dati*");

Evidentemente, questo è possibile solo se queste finalità sono specificate ed esplicite (come richiesto dall'art. 5(1)(b) GDPR).

1.3.1.1 Adeguato, pertinente e limitato

Adeguato e ***pertinente*** sono facili da capire: I dati inadeguati, cioè inadatti agli scopi, non possono essere raccolti o trattati; i dati devono anche essere pertinenti, cioè devono servire agli scopi.

Per comprendere l'aspetto della ***limitazione***, è necessario uno sguardo più preciso su ciò che i *dati* significano effettivamente. In particolare, è intuitivo che non si tratta solo del numero di elementi di dati, ma del **contenuto informativo** effettivo dei dati. Di seguito lo illustreremo in relazione agli scopi:

- **Selezione**: Quando un insieme di possibili elementi di dati è in considerazione, **selezionare** quelli che sono necessari per gli scopi. Si noti che se i dati sono già

memorizzati, la selezione può anche essere intesa come **cancellazione** di elementi di dati non necessari. Altrimenti riguarda i dati che vengono effettivamente raccolti.

- **Risoluzione**: Quando i dati sono disponibili a più risoluzioni possibili, **limitare la risoluzione** a ciò che è minimamente necessario per lo scopo. Per esempio:
    - **Valori**: esprimere i **valori** alla **scala più grossolana** che ancora supporta gli scopi,
        - per esempio, utilizzare una **categoria di età** (40-59 anni, risoluzione di 20 anni) **invece di** una **data di nascita** (risoluzione di un giorno),
    - **Località**: esprimere le **località** in termini di suddivisione geografica più grossolana possibile,
        - per esempio, utilizzare **unità amministrative** come zone di codice postale o province o **celle di griglia** invece di coordinate precise (di metri di risoluzione),
    - **Serie temporali**: esprimono **serie temporali** di dati alla frequenza di campionamento più grossolana che ancora supporta gli scopi,
        - questo può richiedere un ri-campionamento dei dati ottenuti da qualche sensore,
    - **Impronte digitali**: Se avete bisogno di confrontare **solo** insiemi di dati per l'**uguaglianza**, considerate di elaborare solo qualche "**impronta digitale**" dei dati.
        - Per esempio, un "valore di hash crittografico" (alias "digest") dei dati può essere sufficiente per rilevare il cambiamento[25].
- **Livello di aggregazione**: Dove possibile, scegliete un adeguato **livello di aggregazione**. La maggior parte dei valori di dati con cui abbiamo a che fare sono una forma di aggregazione, anche se questo può non essere evidente poiché può essere fatto "invisibilmente" da qualche sensore o metodo di raccolta dati. L'aggregazione è un modo di **sostituire diversi elementi di dati con uno solo**. I primi esempi vengono dalla statistica e includono la media, la mediana, il minimo e il massimo. Nel contesto della protezione dei dati, si devono distinguere due tipi di aggregazione:
    - **Persona singola**: Aggregazione di elementi di dati relativi a una **singola persona**:
        - Prendendo per esempio il reddito medio di una persona in un anno, si riduce il contenuto informativo relativo a quella persona.
    - **Persone multiple**: Aggregazione di elementi di dati relativi a una **moltitudine di persone**:
        - Prendere per esempio il reddito medio annuo su un gruppo di persone riduce anche il contenuto informativo complessivo (minimizzazione dei dati). Inoltre, indebolisce anche il grado di associazione tra un elemento di dati e una data persona. Questo tipo di aggregazione è quindi anche pertinente alla limitazione della conservazione (vedi sezione 1.5)

25 Per ulteriori informazioni sui digest crittografici, vedere per esempio, https://en.wikipedia.org/wiki/Cryptographic_hash_function (ultima visita 15/5/2020).

1.3.1.2 Aspetto temporale

La minimizzazione dei dati ha chiaramente anche un **aspetto temporale**. Soprattutto, "limitato a ciò che è necessario in relazione agli scopi" significa anche che non è più giustificato conservare i dati quando gli scopi sono già stati soddisfatti. I dati devono quindi essere **cancellati non appena non sono più necessari**.

In pratica, questo può essere ancora **più diversificato**: Delle finalità (plurale), alcune possono essere soddisfatte prima di altre. Inoltre, dopo il "trattamento principale"[26], [27]possono aver luogo "ulteriori trattamenti per scopi di archiviazione nel pubblico interesse, scopi di ricerca scientifica o storica o scopi statistici". Per modellare questo, distinguiamo diverse **fasi di trattamento**. La figura seguente cerca di visualizzare questa situazione.

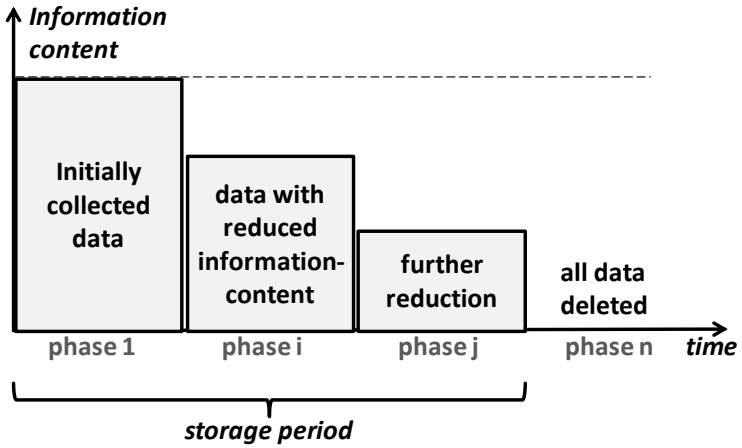

Figura 3: Riduzione del contenuto informativo in più fasi.

In particolare, la figura mostra un esempio con quattro fasi. Qualsiasi numero di fasi è possibile. Poiché ogni fase è associata a un sottoinsieme di scopi, alla fine di ogni fase, quando i rispettivi scopi sono stati soddisfatti, certi dati non sono più necessari. Di conseguenza, alla **fine di ogni fase**, certi dati possono essere **cancellati** (selezione), o il loro **contenuto informativo può essere ridotto** (riduzione della risoluzione o aumento del livello di aggregazione). È evidente che un tale approccio diversificato minimizza ulteriormente i dati, rispetto a un approccio monofase che mantiene l'intero contenuto informativo fino a quando tutti gli scopi sono stati soddisfatti.

1.3.2 Articoli e Considerando correlati

Al di là della definizione di *minimizzazione dei dati* data nell'art. 5(1)(c), la seconda parte dell'art. 5(1)(e) "limitazione della conservazione" GDPR afferma esplicitamente che:

> [I dati personali possono essere conservati per periodi più lunghi nella misura in cui i dati personali saranno trattati esclusivamente a fini di archiviazione nel pubblico interesse, a fini di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione delle misure tecniche e organizzative adeguate richieste dal presente regolamento per salvaguardare i diritti e le libertà della persona interessata;

26 Il termine "elaborazione principale" è usato qui per distinguere dalla "elaborazione successiva".
27 La formulazione è stata copiata direttamente dall'art. 5(1)(b) GDPR.

Questo si riferisce all'ulteriore trattamento per scopi compatibili dopo aver soddisfatto gli scopi iniziali descritti nell'Art. 5(1)(b) GDPR[28].

Poiché riguarda la conservazione dei dati personali, è considerato qui pertinente alla minimizzazione dei dati poiché l'affermazione "limitato a ciò che è necessario in relazione alle finalità" non è limitata solo al volume dei dati, ma chiaramente deve essere intesa anche per affrontare l'aspetto temporale dei dati. Inoltre, la minimizzazione dei dati riguarda tutti gli aspetti del trattamento (come la *raccolta* e la *divulgazione*) e quindi anche la *conservazione*.

Per questi motivi, la seconda parte dell'art. 5(1)(e) GDPR è qui considerato per fornire una guida su come interpretare il principio di minimizzazione dei dati nel contesto di un ulteriore trattamento per scopi compatibili dopo aver soddisfatto gli scopi iniziali.

Oltre a questo, il GDPR sottolinea l'importanza del principio in vari contesti:

Nell'art. 25(1) GDPR sulla ***protezione dei dati mediante progettazione***, si sottolinea come la ***minimizzazione dei dati*** deve essere **considerata in ogni fase del ciclo di vita** di un'attività di trattamento. Questo include per esempio la fase di analisi e concezione di un'attività di trattamento in cui vengono determinate le finalità del trattamento: Evidentemente, più precise e ristrette sono le finalità specificate, più chiaro diventa quali dati sono effettivamente necessari e più dati possono essere riconosciuti come non necessari. Allo stesso modo, in una fase successiva del ciclo di vita, si possono adottare misure per attuare un'effettiva cancellazione o riduzione del contenuto delle informazioni.

L'art. 89(1) e il Considerando 156 GDPR sottolineano l'**importanza della *minimizzazione dei dati*** per il caso in cui, dopo aver soddisfatto le finalità iniziali, i dati vengono trattati ulteriormente per "finalità compatibili"[29]. In particolare, "gli scopi di **archiviazione** nell'interesse pubblico, gli scopi di **ricerca scientifica** o **storica** o gli **scopi statistici** non sono considerati incompatibili con gli scopi iniziali, conformemente all'articolo 89, paragrafo 1"[30]. Art. 89(1) GDPR (2ª frase) impone esplicitamente che per questo ulteriore trattamento, "le misure tecniche e organizzative sono in atto in particolare al fine di garantire il rispetto del principio di minimizzazione dei dati".

1.3.3 Misure tecniche e organizzative correlate

Quanto segue fornisce esempi di misure tecniche o organizzative a sostegno della minimizzazione dei dati. Non vuole essere completo, ma piuttosto rendere il principio più concreto:

- **Sapere quali dati sono necessari per gli scopi**: Sapere quali dati sono effettivamente necessari è possibile solo con una definizione precisa e ristretta delle finalità. Scoprire ciò che è realmente necessario è una misura a sostegno della minimizzazione dei dati che è generalmente attuata durante la fase di concezione o progettazione di un'attività di trattamento.
- **Raccogliere solo i dati necessari**: Durante la fase di progettazione e la selezione, l'implementazione e/o la configurazione del software, l'acquisizione dei dati, per esempio attraverso moduli di input o finestre di dialogo, deve essere progettata in modo da raccogliere solo i dati necessari al necessario livello di dettaglio.

---

28 Vale a dire, l'art. 5(1)(b) contiene la seguente dichiarazione: "l'ulteriore trattamento a fini di archiviazione nel pubblico interesse, a fini di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali, conformemente all'articolo 89, paragrafo 1".

29 Vedi l'art. 5(1)(b) GDPR.

30 Testo tratto dall'art. 5(1)(b) GDPR.

- **Cancellare i dati e ridurre il contenuto informativo tra le fasi di elaborazione**[31]: Pianificare e implementare la funzionalità per eliminare i dati non necessari alla fine delle fasi di elaborazione o ridurre in altro modo il loro contenuto informativo.
- **Proteggersi dal superamento del periodo massimo di archiviazione**: Come seconda linea di difesa, definite un *periodo massimo di conservazione*[32] e implementate una procedura che vi avverta della presenza di dati che hanno superato questo periodo. Questa misura protegge dai fallimenti della cancellazione, per esempio quelli causati da un bug del software che si manifesta in certi casi, un crash del sistema durante l'operazione di cancellazione, o il ripristino dei dati da un backup dopo un crash del sistema anche se i dati erano già stati precedentemente cancellati.

1.4 Precisione

Bud P. Bruegger (ULD)

*Ringraziamenti: L'*autore ringrazia il contributo di Frédéric Tronnier (GUF) che ha scritto un'analisi di questo principio come input alla descrizione qui presentata.

Di seguito si discute il principio di *accuratezza* che è definito nell'art. 5(1)(d) GDPR.

***Precisione* in sintesi:**

L'accuratezza dei dati riguarda sia la **correttezza dei fatti** che l'essere **aggiornati**. È vietato utilizzare dati inesatti che non siano adatti allo scopo o che abbiano conseguenze negative per le persone interessate. La misura principale per attuare questo principio è quella di sostenere adeguatamente il **diritto di rettifica degli** interessati.

1.4.1 Descrizione

In *Capire la protezione dei dati: il regolamento UE in poche parole*, l'*accuratezza* (insieme all'integrità) è stata motivata dal fatto che l'accuratezza dei dati è necessaria per essere adatti agli scopi dichiarati. Qualsiasi elaborazione che non sia adatta allo scopo non può giustificare un guadagno di potere su un soggetto di dati. Vedi *Divieto di trattamento che non è adatto allo scopo* per i dettagli.

Oltre all'idoneità allo scopo, il trattamento di dati inesatti può avere conseguenze negative per gli interessati. Queste possono andare da un maggiore sforzo necessario per esercitare i propri diritti, alla negazione di diritti e opportunità, fino a conseguenze finanziarie o legali negative. Mentre il trattamento che è affetto da tali difetti non è

31 Si noti che questa dichiarazione è relativa all'insieme dei dati in possesso del titolare. Si presume anche qui che i dati siano raccolti solo una volta da/sui soggetti interessati e che non vi sia una raccolta successiva di dati (ad esempio, in caso di necessità). La dichiarazione non esclude che fasi diverse o fasi di trattamento utilizzino solo un sottoinsieme dei dati complessivi.

32 Si noti che questo potrebbe essere direttamente "il periodo per il quale i dati personali saranno conservati" secondo l'Art. 13(2)(a) o se il periodo di conservazione dipende da criteri, il tempo massimo in cui ci si può aspettare che queste condizioni siano state soddisfatte.

probabilmente adatto allo scopo, in aggiunta violerebbe il principio di *equità* (vedi sopra).

Il GDPR definisce il principio come segue:

Definizione nell'art. 5(1)(d) GDPR:

I dati personali devono essere **esatti** e, se necessario, **aggiornati**; devono essere adottate **tutte le misure ragionevoli** per garantire che i **dati personali inesatti, tenuto conto** delle finalità per le quali sono trattati, siano **cancellati o rettificati** senza indugio ("*accuratezza*");

Di seguito vengono discussi vari aspetti dell'*accuratezza in modo* più dettagliato:

1.4.1.1 Come si può valutare la precisione?

Il concetto di accuratezza deve essere oggettivo. Deve essere possibile verificare se i dati sono accurati o meno senza dubbi e diversi verificatori devono arrivare alla stessa valutazione. Questo è possibile solo quando i dati rappresentano **fatti verificabili**. Questo non è per esempio il caso dei dati che rappresentano un'espressione o un'opinione di una persona.

La verifica dell'accuratezza dei dati comporta quindi generalmente la verifica dei fatti che stanno alla base dei dati. Per esempio, per verificare che un numero di telefono cellulare appartenga effettivamente a una persona, si potrebbe inviare e ricevere un messaggio di prova con un codice casuale su un altro canale.

In alcune situazioni, può essere l'interessato a fornire al titolare del trattamento la necessaria documentazione dei fatti che permettono una verifica. Ad esempio, una persona interessata può fornire un certificato di residenza rilasciato da un'autorità di fiducia al fine di sostenere la verifica di un indirizzo di residenza.

1.4.1.2 Cosa significa "aggiornato"?

Nel valutare se i dati sono aggiornati, si deve tener conto delle finalità del trattamento. Per esempio, un venditore può memorizzare l'indirizzo di consegna di una persona interessata, mentre la persona interessata si è trasferita nel frattempo in una nuova residenza. Se lo scopo del trattamento è quello di consegnare effettivamente la merce alla persona interessata, l'indirizzo è evidentemente obsoleto e i dati non sono idonei allo scopo. Se invece lo scopo del trattamento è la fatturazione di merci già consegnate, il vecchio indirizzo deve essere considerato aggiornato.

1.4.1.3 Come si scopre l'imprecisione dei dati?

I dati inesatti (compresi quelli non aggiornati) devono essere rettificati o cancellati dal titolare del trattamento senza indugio. Ma come si scopre effettivamente l'inesattezza dei dati e quali titolarità hanno i titolari del trattamento?

Il meccanismo probabilmente più importante per i titolari del trattamento per rilevare l'inesattezza dei loro dati è la **notifica da parte della persona**[33] **interessata**. In particolare, la persona interessata deve essere a conoscenza del trattamento (vedi art. 13 e 14 GDPR) e può accedere ai dati utilizzati dal titolare del trattamento (vedi art. 15 GDPR). Su questa base, possono verificare l'esattezza dei loro dati e, se necessario, invocare il loro **diritto di** chiedere

33 Altri meccanismi includono per esempio i controlli di coerenza, la varianza eccessiva o la mancanza di correlazione attesa.

la **rettifica** dei loro dati (cfr. art. 16 GDPR). In questo caso, un titolare del trattamento adempie all'obbligo di accertare l'esattezza sostenendo adeguatamente il diritto di rettifica nel loro trattamento.

Quando i dati sono raccolti direttamente dagli interessati, è per lo più ragionevole per un titolare del trattamento presumere che i dati ottenuti siano accurati (almeno al momento della raccolta). La situazione può essere diversa quando i dati sono raccolti da un'altra fonte. In questo caso, è obbligo del titolare del trattamento verificare l'accuratezza dei dati ottenuti, almeno per quanto riguarda l'idoneità agli scopi dichiarati del trattamento e alle eventuali conseguenze negative che le imprecisioni possono avere per gli interessati.

Per alcuni elementi di dati, il fatto che siano stati raccolti direttamente dalle persone interessate può non essere sufficiente per un titolare del trattamento per presumere l'accuratezza. Questo è in particolare il caso quando una richiesta potenzialmente imprecisa porta a benefici per l'interessato. In questi casi, il titolare del trattamento può avere bisogno di realizzare una verifica dei dati in anticipo come parte integrante della raccolta dei dati. Questo è possibile per esempio chiedendo agli interessati di fornire una certificazione da parte di un'autorità fidata dei fatti dichiarati.

1.4.2 Articoli e Considerando correlati

L'articolo del GDPR più strettamente legato al principio di *accuratezza* è il **16 *diritto di rettifica***. La sua rilevanza è già stata discussa nella sezione 1.4.1.3 precedente. Un'adeguata **informazione** che crea consapevolezza del trattamento tra gli interessati (**art. 13 e 14 GDPR**) e il **diritto di accedere ai** dati in possesso del titolare del trattamento (**art. 15**) possono essere considerati necessari per consentire il diritto di rettifica.

Quando un titolare del trattamento non può agire immediatamente su una richiesta di rettifica (secondo l'art. 16 GDPR), ma richiede un tempo adeguato per verificare l'accuratezza dei dati in discussione, può essere necessario **limitare il trattamento dei** dati (vedi **art. 18(1)(a)** GDPR). Dopo la verifica dell'esattezza e la rettifica effettuata, il titolare del trattamento deve **informare l'interessato** secondo l'**art. 12(3)** GDPR. Se il titolare del trattamento dovesse constatare che i dati sono effettivamente esatti e non necessitano di rettifica, l'**interessato** deve essere **informato ai sensi dell'art. 12(4))** GDPR. Se il trattamento è stato limitato, l'interessato può allora **acconsentire alla revoca della limitazione** anche senza rettifica (cfr. **art. 18(2)** GDPR). In assenza di tale consenso, il titolare del trattamento può **cancellare i dati** (cfr. **art. 5(1)(d)** GDPR) o fare in modo che il suo Responsabile della protezione dei dati (DPO) **consulti l'Autorità di controllo** sulla questione (cfr. **Art. 39(1)(e)** GDPR).

Nel caso in cui il titolare del trattamento abbia comunicato i dati ai **destinatari**, questi **devono anche essere messi a conoscenza** dell'inesattezza (secondo l'**art. 19** GDPR). In particolare, i titolari del trattamento sono obbligati a notificare ai destinatari le rettifiche che sono state effettuate. Considerando che la verifica dell'accuratezza può dipendere dalle finalità del trattamento (vedi sopra), può essere utile e più tempestivo notificare volontariamente ai destinatari già la richiesta di rettifica. Tale approccio esteso copre poi anche il caso in cui i dati sono esatti per il titolare del trattamento, ma richiedono una rettifica presso uno dei destinatari.

Gli interessati hanno anche il **diritto di richiedere informazioni su tali notifiche** (vedi 2ª frase dell'**art. 19** GDPR). Queste informazioni includono il nome dei singoli destinatari[34].

34 Questo è interessante, dato che negli artt. 13(1)(e) e 14(1)(e), è sufficiente informare sulle categorie di destinatari.

1.4.3 Misure tecniche e organizzative correlate

Qualsiasi organizzazione o misura tecnica per sostenere l'individuazione di imprecisioni o la tempestiva rettifica (o cancellazione) dei dati sostiene il principio di *accuratezza*. Per capire quando l'accuratezza è particolarmente importante e sono necessarie misure più forti, è necessaria un'analisi su come le imprecisioni si riferiscono all'idoneità allo scopo e come possono influenzare negativamente gli interessati.

Esempi di possibili misure a sostegno della precisione sono:

- una misura organizzativa al momento della progettazione è l'analisi del livello minimo di precisione richiesto per essere adatti allo scopo;
- una misura organizzativa al momento della progettazione è l'analisi dei possibili impatti negativi che dati imprecisi possono avere sugli interessati;
- una misura di design-time è l'analisi dell'accuratezza dei dati ottenuti da fonti diverse dagli stessi soggetti dei dati;
- un'altra è l'analisi se certi elementi di dati richiedono una verifica preliminare (vedi sopra);
- Un'altra misura progettuale è quella di formulare requisiti per il sostegno dei diritti all'informazione (art. 13 o 14 GDPR), il diritto di accesso (art. 15 GDPR) e, soprattutto, il diritto alla rettifica (art. 16 GDPR);
- lo stesso vale per l'attuazione delle notifiche ai destinatari (art. 19 GDPR) sull'inesattezza e la rettifica;
- al momento di operare l'attività di trattamento, la designazione del personale per eventuali interventi manuali necessari per verificare l'esattezza o effettuare la rettifica è una possibile misura organizzativa;
- lo stesso vale per la preparazione del Responsabile della protezione dei dati (DPO) a trattare efficacemente le richieste di rettifica.

1.5 Limitazione della conservazione

Bud P. Bruegger (ULD)

Qui di seguito si discute il principio di *limitazione della conservazione* che è definito nell'art. 5(1)(e) GDPR.

La limitazione della conservazione **in sintesi:**

La limitazione della conservazione (anche se non è implicita nel suo nome) considera il grado in cui le persone interessate sono **identificate** dai dati, cioè, quanto è facile che le persone interessate possano essere associate ai dati. I gradi di identificazione previsti dal GDPR sono ***dati direttamente identificabili*** che contengono *identificatori*, ***dati pseudonimi*** e ***dati anonimi***. I dati devono essere raccolti con il più basso grado di identificazione possibile e la pseudonimizzazione e l'anonimizzazione devono essere utilizzate per ridurre ulteriormente l'identificazione il prima possibile nel tempo.

1.5.1 **Descrizione**

In *Capire la protezione dei dati: il regolamento UE in poche parole*, la *limitazione della conservazione* era motivata dalla minimizzazione del guadagno di potere del titolare del trattamento a quello che è minimamente necessario per soddisfare le finalità dichiarate e legittime. In particolare, ha affrontato la minimizzazione del grado in cui i dati personali sono associati al soggetto dei dati. Questo completa la minimizzazione del contenuto dell'informazione e la limitazione dell'accesso al potere. Vedi *Minimizzazione del potere a ciò che è necessario per soddisfare le finalità dichiarate* per il dettaglio.

Il GDPR definisce il principio come segue:

> **Definizione** nell'art. 5(1)(e) GDPR:
>
> I dati personali sono **conservati in una forma che consenta l'identificazione delle persone interessate per un tempo non superiore a quello necessario per le finalità per le quali** i dati personali sono trattati; [...]
>
> ("*limitazione della conservazione*");

Chiaramente, il concetto principale di questo principio riguarda l'***identificazione***, cioè l'associazione dei dati personali con la persona interessata. Il resto di questa sezione analizza quindi principalmente cosa significa effettivamente l'identificazione.

Si noti che nel riquadro di definizione di cui sopra, la parte omessa che è rappresentata da [...] è stata discussa sotto il principio di *minimizzazione dei dati* (vedi *1.3*). Essa riguarda la **limitazione temporale della memorizzazione** che è probabilmente un aspetto del **concetto** generale **di limitazione** espresso per i dati nel principio di *minimizzazione dei dati.*

Da questo punto di vista, il nome di *limitazione della conservazione* è fuorviante poiché implica solo l'aspetto temporale della minimizzazione dei dati ma non si riferisce all'identificazione. Chiamarla *minimizzazione del potenziale di identificazione* potrebbe essere più chiaro.

1.5.1.1 Identificazione delle persone interessate

Per capire meglio cosa si intende per identificazione, facciamo riferimento all'art. 4(1) GDPR. La seconda metà[35] della frase recita come segue:

> [Una persona fisica identificabile è una persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento a un identificatore come un nome, un numero di identificazione, dati relativi all'ubicazione, un identificatore online o a uno o più fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale persona fisica;

Per una migliore comprensione, questa frase è divisa nelle due parti seguenti:

Identificazione diretta con riferimento a un identificatore:

> [Una persona fisica identificabile è una persona che può essere identificata, **direttamente** ~~o indirettamente~~, in particolare mediante riferimento a un **identificatore** come un *nome*, un *numero di identificazione*, *dati relativi all'ubicazione*, un *identificatore online* ~~o a uno o più~~

35 Una parte di frase che è separata dal resto con punti e virgola è qui chiamata "mezza frase".

~~fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale persona fisica~~;

Identificazione indiretta con riferimento a uno o più fattori specifici dell'identità di una persona fisica:

[Una persona fisica identificabile è una persona che può essere identificata, ~~direttamente o~~ **indirettamente**, in particolare mediante riferimento ~~a un identificatore come un nome, un numero di identificazione, dati relativi all'ubicazione, un identificatore online o~~ a uno **o più fattori specifici dell'identità** *fisica*, *fisiologica*, *genetica*, *mentale*, *economica*, *culturale* o *sociale* **di tale persona fisica**;

Gli **esempi per gli identificatori** sono[36]:

- Un nome,
- un numero di identificazione,
- dati di localizzazione,
- un identificatore online.

Si noti in particolare i *dati di localizzazione* che molti non sono comunemente pensati come un identificatore che supporta l'identificazione diretta, anche se il suo carattere altamente identificativo è effettivamente intuitivo.

Gli esempi di **fattori specifici dell'identità di una persona fisica** riguardano i seguenti aspetti:

- Fisico
- Fisiologico
- Genetico
- Mentale
- Economico
- Culturale
- Sociale

Questa distinzione di identificazione diretta e indiretta permette ora di diversificare il concetto *di forma che permette l'identificazione degli interessati*.

1.5.1.2 Tipi di dati distinti nel GDPR

Il GDPR distingue tre tipi di dati con diversi gradi di associazione con gli interessati:

(i) identificare direttamente i dati personali[37]

(ii) dati personali pseudonimi

(iii) dati anonimi

36 Si noti che il considerando 30 del GDPR fornisce inoltre esempi di "identificatori online": indirizzi di protocollo internet, identificatori di cookie o altri identificatori come i tag di identificazione a radiofrequenza.

37 Il termine "*dati personali che identificano direttamente*" non è usato nel GDPR ma clonato dall'autore.

(i) Dati personali che identificano direttamente: Il primo deve evidentemente contenere **identificatori**, poiché permette l'identificazione diretta degli interessati. Tuttavia, la maggior parte delle serie di dati personali non contiene solo identificatori. Gli altri dati devono poi essere considerati tutti **fattori specifici dell'identità di una persona fisica**, poiché tutti descrivono aspetti diversi che sono legati all'identità della persona interessata.

(ii) Dati personali pseudonimi: L'art. 4(5) GDPR definisce il relativo concetto di "pseudonimizzazione". La sua formulazione può essere adattata come segue per definire i dati personali pseudonimi:

I dati personali pseudonimi sono dati personali che **non possono più essere attribuiti a un soggetto specifico senza l'uso di informazioni aggiuntive**.

Questo deve essere interpretato nel modo seguente:

- I dati personali pseudonimi **non possono supportare l'identificazione diretta**.
- **Non deve** quindi **contenere identificatori**.
- **I dati aggiuntivi**, in questo contesto, sono dati che permettono di **associare agli identificatori fattori specifici dell'identità di una persona fisica.**

(iii) Dati anonimi: Le informazioni anonime sono definite nel considerando 26 del GDPR (quinta frase). Usando *informazioni* e *dati* come sinonimi, la sua formulazione può essere adattata come segue:

I dati anonimi sono

- dati che non si riferiscono a una persona fisica identificata o identificabile o
- dati personali resi anonimi in modo tale che la persona interessata non sia o non sia più identificabile.

Si noti che l'identificabile comprende sia l'identificazione diretta che quella indiretta. Anche con informazioni aggiuntive, non è possibile attribuire dati anonimi a un soggetto specifico.

Si noti che secondo il considerando 26 (frase 6), il GDPR non si applica ai dati anonimi. Questo è chiaro anche perché non corrisponde alla definizione di dati personali (vedi Art. 4(1) e il considerando 26 del GDPR).

Avendo distinto questi tipi di dati, "conservati in una forma che permetta l'identificazione delle persone interessate per un tempo non superiore a quello necessario alle finalità" può essere ora inteso in modo più preciso, considerando anche l'aspetto temporale del principio.

1.5.1.3 Aspetto temporale

L'art. 5(1)(e) affronta chiaramente l'aspetto temporale imponendo che un modulo che permette l'identificazione **non** sia conservato **più a lungo** di quanto sia necessario per gli scopi. Questo aspetto temporale è discusso qui in modo diversificato. I due criteri seguenti definiscono questa diversificazione:

- **L'identificazione** può essere **diretta** o **indiretta**.
- **L'identificazione** può essere **accessibile a tutti** o a **un gruppo ristretto di persone.**

Sulla base di queste distinzioni, è possibile distinguere quattro casi diversi. Questi sono mostrati in Figura 4 rappresentati come "fasi". È possibile passare da una fase a qualsiasi fase successiva. Questo può essere fatto sia in modo sequenziale, sia omettendo le fasi intermedie. In ogni fase, il grado di identificazione dei dati con la persona interessata si riduce. Il

principio di *limitazione della memorizzazione* afferma che in ogni momento, solo il **grado minimo di identificazione che è necessario per soddisfare gli scopi deve essere utilizzato**.

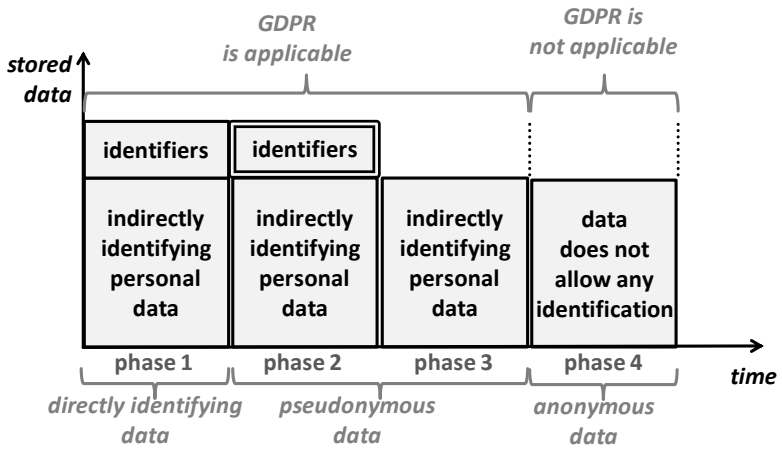

Figura 4: Dati con diversi gradi di associazione con il soggetto dei dati.

Si noti che il principio della *limitazione della conservazione* è mostrato nella sua forma pura: il grado di associazione con il soggetto dei dati è ridotto tra fasi consecutive. In pratica, la limitazione della memorizzazione è generalmente combinata con la *minimizzazione dei dati*. In uno scenario combinato, anche l'altezza delle caselle mostrate in figura sarebbe ridotta.

Le fasi della figura sono descritte più in dettaglio nel seguito:

La fase 1 mostra i dati che contengono entrambi, **identificatori** e **fattori specifici dell'identità di una persona fisica**. Per brevità, questi ultimi sono chiamati *dati personali indirettamente identificativi*. Gli identificatori supportano l'identificazione diretta. Sono **accessibili** a **tutti coloro ai quali i dati vengono divulgati**.

La fase 2 mostra una modalità di trattamento chiamata "**pseudonimizzazione**"[38]. Qui, gli **identificatori** sono ancora memorizzati, ma **tenuti separati** e **protetti** in un modo che consente l'**accesso solo** in **condizioni ben specificate,** utilizzando **procedure predefinite**, per raggiungere **scopi precisamente definiti**, con accesso limitato a un **insieme predefinito di persone**[39] **autorizzate**. Queste restrizioni sono rappresentate da un doppio bordo intorno agli identificatori. L'**accesso all'identificazione diretta** è quindi **strettamente controllato** e disponibile solo a poche persone designate.

L'identificazione indiretta che utilizza informazioni aggiuntive è ancora possibile sulla base dei dati personali che identificano indirettamente. Richiede tuttavia informazioni aggiuntive. Il titolare del trattamento implementa misure per prevenire la disponibilità di tali informazioni aggiuntive alle persone che accedono a questi dati durante l'attività di trattamento. Ciò significa che **per la maggior parte dei trattamenti** (e un importante sottoinsieme di scopi), e la maggior parte dei dipendenti, l'**identificazione non è più possibile**.

La fase 3 mostra la situazione in cui le **finalità non richiedono più la possibilità di identificazione diretta** degli interessati, nemmeno in casi eccezionali. In questo caso, gli *identificatori* che permettono l'identificazione diretta possono essere cancellati del tutto. Di conseguenza, con adeguate misure di protezione in atto, **il titolare del trattamento stesso** (compreso tutto il personale) **non è più in grado di identificare gli interessati**. Questo evidentemente riduce ulteriormente il grado di identificazione rispetto alla fase 2.

38 Vedi articolo 4(5) GDPR.
39 Vedi considerando 29 GDPR, 2ªfrase.

La fase 4 mostra che vengono utilizzati solo **dati anonimi. La** figura implica che questi sono il risultato di un'anonimizzazione dei dati della fase 3 (o delle fasi precedenti). Per definizione[40], i dati anonimi non possono essere attribuiti a una persona interessata, nemmeno con l'uso di informazioni aggiuntive. Questi dati non sono quindi più dati personali e quindi non sono soggetti al GDPR (e l'anonimizzazione riuscita ha quindi lo stesso effetto della cancellazione). I **dati anonimi eliminano quindi completamente la possibilità di identificazione**.

Alcuni lettori potrebbero conoscere il concetto di "***unlinkability***"[41] che è strettamente legato a quello di limitazione della conservazione. Questo diventa chiaro quando si considera che l'identificazione diretta può essere vista come un identificatore che stabilisce un legame con il soggetto dei dati; e che l'uso di informazioni aggiuntive per l'identificazione indiretta richiede di collegare i record di dati che appartengono alla stessa persona nelle due serie di dati.

1.5.2 Articoli e Considerando correlati

Come è stato dimostrato, diversi concetti che sono definiti al di fuori dell'articolo 5 GDPR sono rilevanti per la comprensione del principio di limitazione della conservazione. In particolare, questi sono:

- *Identificazione diretta* e *indiretta* definita nell'art. 4(1) GDPR
- *Pseudonimizzazione* che è definita nell'art. 4(5) GDPR
- *Dati anonimi* che sono definiti nel considerando 26 del GDPR

Nell'art. 11(1), il GDPR afferma che:

> Se le finalità per le quali un titolare del trattamento tratta dati personali non richiedono o non richiedono più l'identificazione di un interessato da parte del titolare del trattamento, quest'ultimo non è obbligato a mantenere, acquisire o trattare informazioni supplementari per identificare l'interessato al solo scopo di rispettare il presente regolamento.

Questo fornisce una guida sull'importanza che il principio di limitazione della conservazione ha rispetto ad altri concetti nel GDPR: La limitazione della conservazione ha una chiara precedenza su altri obblighi del GDPR nel senso che un titolare del trattamento non deve raccogliere o conservare identificatori al solo scopo di rispettare questi obblighi.

Nell'articolo 11(2) GDPR[42], questo è poi dichiarato esplicitamente per gli obblighi dei diritti degli interessati degli articoli da 15 a 20:

> 2. Se, nei casi di cui al paragrafo 1 del presente articolo, il titolare del trattamento può dimostrare di non essere in grado di identificare l'interessato, ne informa l'interessato, se possibile. In tali casi, gli articoli da 15 a 20 non si applicano, tranne quando l'interessato, al fine di esercitare i suoi diritti ai sensi di tali articoli, fornisce informazioni supplementari che ne consentano l'identificazione.

Oltre a questo, il GDPR sottolinea l'importanza della pseudonimizzazione in vari contesti:

L'art. 89(1) sottolinea l'**importanza della *pseudonimizzazione*** per il caso in cui, dopo aver soddisfatto le finalità iniziali, i dati siano trattati ulteriormente per "finalità compatibili"[43]. In

40 Vedi il considerando 26 del GDPR.

41 Conferenza tedesca delle autorità indipendenti di protezione dei dati della Federazione e dei Länder, 17. Aprile 2020, Il modello standard di protezione dei dati, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V20b_EN.pdf (ultima visita 28/05/2020).

42 Vedi anche l'art. 12(2) GDPR che discute ulteriormente questo caso.

43 Vedi l'art. 5(1)(b) GDPR.

particolare, "gli scopi di **archiviazione** nell'interesse pubblico, gli scopi di **ricerca scientifica** o **storica** o gli **scopi statistici** non sono considerati incompatibili con gli scopi iniziali, conformemente all'articolo 89, paragrafo 1"[44]. Art. 89(1) GDPR (2nd frase) impone esplicitamente che per questo ulteriore trattamento, "misure tecniche e organizzative devono essere in atto ed elenca la pseudonimizzazione come unico esempio di tali misure (3rd frase). Inoltre afferma (4th frase): "Se queste finalità possono essere soddisfatte da un ulteriore trattamento che non permette o non permette più l'identificazione degli interessati, queste finalità sono soddisfatte in quel modo." Questo sembra essere un'applicazione diretta del principio di limitazione della conservazione.

L'art. 6(4)(e) sottolinea ulteriormente il ruolo della pseudonimizzazione quando un titolare del trattamento determina se uno scopo aggiuntivo è compatibile con gli scopi per cui i dati sono stati raccolti.

L'art. 25(1) elenca la pseudonimizzazione come unico esempio di una misura che può essere attuata durante la protezione dei dati mediante progettazione.

Anche l'art. 32(1)(a) elenca la pseudonimizzazione insieme alla crittografia come una misura a sostegno della sicurezza. Mentre questo sottolinea ulteriormente l'importanza della pseudonimizzazione e quindi la limitazione della memorizzazione, ci si può chiedere tuttavia se la pseudonimizzazione sostenga effettivamente uno degli obiettivi di protezione comuni della sicurezza informatica, vale a dire *riservatezza*, *integrità* e *disponibilità*.

1.5.3 Misure tecniche e organizzative correlate

Quanto segue fornisce alcuni esempi di misure concrete che sostengono il principio della limitazione della conservazione:

- Al momento di progettare una data attività di trattamento, una misura organizzativa è quella di **verificare se i dati di identificazione** diretta **devono essere raccolti** per soddisfare le finalità dichiarate.
- **La pseudonimizzazione** e l'**anonimizzazione** dei dati tra le fasi di trattamento sono misure tecniche primarie. Richiedono la verifica se gli scopi rimanenti dopo il completamento della fase di trattamento richiedono ancora lo stesso grado di identificazione degli interessati.
- Quando si pianifica di emettere credenziali di autenticazione agli interessati, una misura organizzativa è quella di verificare se è sufficiente **emettere credenziali pseudonime**. Per esempio, l'emissione di una password casuale una tantum durante la raccolta dei dati può essere sufficiente per sostenere in seguito il diritto di ritirare il consenso.
- Progettare un sito web in modo che **si astenga dall'impostare i cookie** al di fuori delle aree che richiedono l'autenticazione **evita un modo di identificare gli interessati** attraverso le sessioni e può essere considerato una misura a sostegno della limitazione della memorizzazione. (Vedi Impostare i cookie e scrivere una politica sui cookie). Concretamente, questo può essere fatto attraverso una configurazione appropriata dell'applicazione web (come un sistema di gestione dei contenuti e i suoi plugin) o del server web.
- Il funzionamento di un servizio basato su Internet in un modo che **permette agli** utenti di connettersi attraverso una **rete anonima come TOR**[45] evita di identificare i soggetti

44 Testo tratto dall'art. 5(1)(b) GDPR.
45 Vedi per esempio, https://en.wikipedia.org/wiki/Tor_(anonymity_network) (ultimo accesso 18/5/2020).

dei dati attraverso il loro indirizzo IP (di rete) e quindi è una misura a sostegno della limitazione della conservazione.

- Dotare un **dispositivo utente abilitato al WiFi** di una **randomizzazione[46] dell'indirizzo MAC** tale da impedire che l'oggetto dei dati trasmetta degli identificatori unici.

1.6 Integrità e riservatezza

Bud P. Bruegger (ULD)

*Ringraziamenti: L'*autore ringrazia il contributo di Frédéric Tronnier (GUF) che ha scritto un'analisi di questo principio come input alla descrizione qui presentata.

Di seguito si discute il principio di *integrità e riservatezza* che è definito nell'art. 5(1)(f) GDPR.

***Integrità e riservatezza* in sintesi:**

Il principio si riferisce ai classici obiettivi di protezione della **sicurezza** informatica, cioè ***riservatezza***, ***integrità*** e ***disponibilità*** (CIA). La ***resilienza*** può essere considerata un aspetto della disponibilità. L'obiettivo principale è quello di proteggere le *risorse* dai *rischi* causati da *eventi indesiderati*. In netto contrasto con la sicurezza informatica, queste risorse **e i rischi** non sono quelli del titolare del trattamento (un'organizzazione), ma quelli degli **interessati**. Da questo punto di vista, è anche chiaro perché la *portabilità dei dati* si adatta alla *disponibilità* all'interno di questo principio: protegge le persone interessate dalla perdita di una risorsa (rappresentata dai dati) quando si cambia titolare del trattamento (soprattutto fornitore).

1.6.1 Descrizione

In *Capire la protezione dei dati: il regolamento UE in poche parole*, l'*integrità* (insieme all'accuratezza) è stata motivata dal fatto che l'accuratezza dei dati è necessaria per essere adatti agli scopi dichiarati. Qualsiasi elaborazione che non sia adatta allo scopo non può giustificare un guadagno di potere su un soggetto di dati. Vedi *Divieto di trattamento che non è adatto allo scopo* per i dettagli. La *riservatezza* invece è stata motivata dalla limitazione dell'accesso al potere. Vedi *1.6.5.3 Limitazione dell'accesso al potere* per i dettagli. La *disponibilità* era motivata dalla protezione del patrimonio dell'interessato. Vedere *1.6.6 Protezione del patrimonio dell'interessato per* i dettagli.

Il GDPR definisce il principio come segue:

Definizione nell'art. 5(1)(f) GDPR:

46 Vedi per esempio, https://en.wikipedia.org/wiki/MAC_spoofing#MAC_Address_Randomization_in_WiFi (ultimo accesso 18/5/2020).

I dati personali sono trattati in modo da **garantire un'adeguata sicurezza** dei dati personali, compresa la protezione contro il **trattamento non autorizzato** o **illegale** e contro la **perdita accidentale, la distruzione** o il **danneggiamento**, utilizzando misure tecniche o organizzative adeguate ("*integrità e riservatezza*").

1.6.1.1 La struttura dell'art. 5(1)(f) e rischi per la sicurezza

Ciò che è evidente dalla formulazione dell'art. 5(1)(f) è che il GDPR parla di **eventi indesiderati**, cioè:

- trattamento non autorizzato o illegale, e
- perdita accidentale, distruzione o danno.

Chiaramente, questi eventi non fanno parte dell'elaborazione come previsto; idealmente, dovrebbero essere evitati del tutto. Poiché nella sicurezza questo non è mai possibile con il 100% di certezza, c'è una **probabilità** residua **che tali eventi si verifichino**.

È anche evidente che il verificarsi di tali eventi ha **conseguenze indesiderabili**.

I lettori che hanno familiarità con la sicurezza informatica avranno riconosciuto che questa discussione ha introdotto gli elementi utilizzati nella definizione di *rischio*. Ciò è reso esplicito in quanto segue:

Rischio di sicurezza = probabilità di un evento indesiderabile * gravità delle conseguenze indesiderabili

Questo è un rischio "individuale" e il rischio totale è quindi una somma su tutti i rischi individuali applicabili.

I lettori attenti avranno notato che la terminologia usata qui differisce un po' da quella comune nella sicurezza[47] informatica. In particolare, è stato usato il termine "rischio di sicurezza", molto più che solo "rischio" e allo stesso modo, è stata usata la "gravità delle conseguenze indesiderabili" invece di "danno". La motivazione di questa scelta di termini è spiegata nel seguito:

1.6.1.2 Differenza principale da altri rischi nel GDPR e dai rischi nella sicurezza informatica

Il GDPR si riferisce ad almeno due tipi di rischio fondamentalmente diversi (ma senza rendere esplicita questa distinzione). Di seguito si introducono quindi due termini diversi per rendere esplicita questa distinzione. Vale a dire, sono il *rischio di sicurezza* e il *rischio di protezione dei dati*.

Nel GDPR, il ***rischio di sicurezza*** è implicito in entrambi gli articoli 5(1)(f) e 32. Come risulta dalla sottosezione precedente, la sua definizione deriva dall'esistenza di **eventi indesiderabili** che **non fanno parte delle operazioni di trattamento previste**.

Al contrario, il GDPR considera chiaramente anche i rischi derivanti dal trattamento dei dati stesso - in assenza di eventi indesiderati – cioè durante il trattamento indisturbato come previsto. Chiamiamo questo tipo di rischio: *rischio di protezione dei dati.* È presente anche se la sicurezza fosse perfetta e tutti i possibili eventi indesiderati potessero essere evitati con il 100% di certezza.

47 Vedi per esempio https://en.wikipedia.org/wiki/IT_risk#Measuring_IT_risk (ultima visita 19/05/2020).

Quindi è importante capire che i *rischi di sicurezza* sono solo un sottoinsieme dei rischi che i titolari del trattamento sono obbligati a mitigare attraverso l'implementazione di misure tecniche e organizzative appropriate.

Dopo aver distinto i rischi di sicurezza dai rischi di protezione dei dati, confrontiamo i rischi di sicurezza del GDPR con quelli della sicurezza informatica. Dato che la sua definizione fornita nel riquadro della sottosezione precedente ha la stessa struttura, si può concludere che i *rischi di sicurezza* nel GDPR sono gli stessi della sicurezza informatica?

Questo indica la scelta del secondo termine, cioè la *gravità delle conseguenze indesiderabili* invece del *danno*.

Nella **sicurezza informatica**, il ***danno*** è una quantificazione delle conseguenze indesiderabili rispetto alla **missione e ai valori dell'organizzazione** che gestisce l'attività di elaborazione. È spesso quantificato in termini di **valore monetario**, **coerente con** un'organizzazione la cui missione è produrre **profitto**.

In netto contrasto con questo, c'è la **gravità delle conseguenze indesiderabili** inerenti al principio di integrità e riservatezza **nel GDPR.** Questa misura **si riferisce** ai **diritti e alle libertà delle persone fisiche** come sono definiti nella Carta europea dei diritti fondamentali. L'effetto indesiderato può quindi consistere nell'impedire o negare il libero esercizio dei propri diritti e libertà[48]. Tali effetti non possono generalmente essere misurati in termini di valori monetari. È anche generalmente impossibile quantificarli, e possono essere espressi solo su una scala di misura ordinale (per esempio quella composta da *basso*, *medio* e *alto*).

Quindi la **differenza** tra la **sicurezza informatica** e la **sicurezza secondo l'art. 5(1)(f)** GDPR è la **valutazione delle conseguenze indesiderate**, anche se gli eventi indesiderati possono essere gli stessi. In molti casi, un evento che infligge solo conseguenze minori per la missione dell'organizzazione del titolare del trattamento, può infliggere gravi interferenze nei diritti e nelle libertà di un individuo interessato (e viceversa).

1.6.1.3 Obiettivi di protezione inerenti all'art. 5(1)(f)

Il GDPR nomina questo principio definito nell'art. 5(1)(f) solo ***integrità*** *e* ***riservatezza***. Questi sono due dei tre noti obiettivi di protezione della sicurezza informatica. Il terzo è la ***disponibilità***. Questa trinità di obiettivi di protezione è spesso indicata semplicemente con l'acronimo *CIA*.

Mentre il nome del principio dato nel GDPR sembra suggerire che la disponibilità sia esclusa, sia l'esatta formulazione dell'art. 5(1)(f) che l'art. 5(1)(f) del GDPR sono stati modificati. 5(1)(f) che dell'Art. 32 "*Sicurezza del trattamento*" suggeriscono il contrario. In particolare:

- la dicitura "protezione contro le perdite accidentali" può essere chiaramente associata alla *disponibilità*, e
- L'art. 32(1)(b) impone ai titolari del trattamento di "assicurare la costante *riservatezza*, *integrità*, *disponibilità* e ***resilienza*** dei sistemi e dei servizi di trattamento".

La resilienza è nominata qui come quarto obiettivo di protezione. È anche chiaramente accettato come un obiettivo della sicurezza informatica, spesso trattato come un aspetto della *disponibilità*.

In conclusione, l'art. 5(1)(f) GDPR fa riferimento all'intero spettro di obiettivi di protezione conosciuti dalla sicurezza informatica. Saranno tutti discussi qui senza limitare la discussione solo ai due che fanno parte del nome del principio.

---

48 Felix Bieker, Benjamin Bremert, Identifizierung von Risiken für die Grundrechte von Individuen, in : ZD, 2020, p. 7 e seguenti. (in tedesco, abstract in inglese).

Per una discussione approfondita, vedere le pubblicazioni dell'ENISA sull'argomento[49].[50] Qui di seguito verrà data solo una breve descrizione di ogni obiettivo di protezione.

1.6.1.4 Integrità

L'integrità si riferisce all'aspetto dell'art. 5(1)(f) che richiede la protezione dei dati personali "contro i danni accidentali", per esempio a causa di un errore di trasmissione. Mira quindi a prevenire qualsiasi tipo di evento che possa "corrompere" i dati in un modo che li renda inadatti alle finalità del trattamento.

1.6.1.5 Riservatezza

La riservatezza si riferisce all'aspetto dell'art. 5(1)(f) che richiede la protezione dei dati personali "contro il trattamento non autorizzato o illegale". È importante notare che nel GDPR, il *trattamento* comprende anche la *divulgazione* dei dati (vedi art. 4(2) GDPR). Quindi la riservatezza richiede di proteggere i dati personali dalla divulgazione indesiderata mentre sono a riposo, in transito e in uso[51]. Inoltre, richiede che nessuna persona non autorizzata possa interagire con l'operazione di trattamento, ad esempio inserendo decisioni che riguardano una persona, modificando o cancellando dati personali, o innescando qualsiasi altra operazione che è riservata al personale autorizzato che lavora secondo precise istruzioni del titolare del trattamento.

1.6.1.6 Disponibilità, resilienza e portabilità

La disponibilità si riferisce all'aspetto dell'Art. 5(1)(f) che richiede la protezione dei dati personali "contro la perdita o la distruzione accidentale", per esempio a causa del guasto di un componente di memorizzazione.

La resilienza sembra essere definita nell'art. 32(1)(c) come "la capacità di ripristinare la disponibilità e l'accesso ai dati personali in modo tempestivo in caso di incidente fisico o tecnico". Si tratta quindi chiaramente di un aspetto della disponibilità ed è legato alla nota misura del *Disaster Recovery*.

Probabilmente, un altro aspetto della *disponibilità* è la *portabilità* dei dati come viene definita nell'art. 20 GDPR. Mentre la disponibilità è di solito intesa a proteggere gli interessati dalla perdita dei loro dati mentre sono trattati da un determinato titolare del trattamento, la *portabilità dei dati* protegge gli interessati dalla perdita quando si spostano da un titolare del trattamento (ad esempio, nel ruolo di fornitore di servizi) ad un altro. La portabilità comporta che gli interessati possano ottenere i loro dati in un formato leggibile da una macchina (vedi Art. 20(1) GDPR) e, se fattibile, di farli trasmettere direttamente da un titolare del trattamento a un altro (vedi Art. 20(2) GDPR).

1.6.2 Articoli e Considerando correlati

Mentre l'art. 5(1)(f) GDPR afferma astrattamente che "misure tecniche o organizzative appropriate" devono essere utilizzate per attuare i suddetti obiettivi di protezione della sicurezza, l'**Art. 32 GDPR fornisce ulteriori dettagli.**

---

49 ENISA, Linee guida per le PMI sulla sicurezza del trattamento dei dati personali, 27 gennaio 2017, https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing (ultima visita 19/05/2020).

50 ENISA, Handbook on Security of Personal Data Processing, 29 gennaio 2018, https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing (ultima visita 19/05/2020).

51 L'art. 32(2) GDPR utilizza l'espressione "trasmesso, memorizzato o altrimenti trattato".

L'art. 32(1), afferma che nel decidere sulle misure appropriate, i titolari del trattamento devono tenere conto "del **livello di sviluppo** e dei **costi di attuazione**", così come "della natura, della portata, del **contesto** e delle finalità **del trattamento**". In particolare il contesto del trattamento è rilevante qui, poiché si può sostenere che l'attuale **panorama delle minacce** ne è un aspetto. Come previsto, il titolare del trattamento deve anche prendere in considerazione "**i rischi per i** diritti e le libertà delle **persone fisiche**".

Quindi il livello di protezione richiesto dipende chiaramente dalla gravità delle possibili conseguenze indesiderabili a cui sono esposti gli interessati e da un modello di minaccia che stima la probabilità di eventi indesiderabili. La sicurezza è quindi solo un mezzo, non un obiettivo in sé. Il livello di sicurezza è sufficiente quando i rischi per le persone interessate sono ridotti a un livello accettabile. La selezione delle misure dipende sia da ciò che il mercato ha da offrire, sia da quanto queste misure siano convenienti.

L'art. 32(1)(d) GDPR afferma il concetto ben accettato che **la sicurezza è un processo**, non un obiettivo che viene raggiunto una volta. In particolare, il GDPR richiede "un processo per testare, esaminare e valutare regolarmente l'efficacia delle misure tecniche e organizzative per garantire la sicurezza del trattamento".

L'art. 32(2) GDPR fornisce **ulteriori dettagli** marginali **su ciò che gli obiettivi di protezione comportano**, elencando "la distruzione accidentale o illegale, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o altrimenti trattati".

L'articolo 32(3) GDPR suggerisce che "l'adesione a un **codice di condotta approvato** o a un **meccanismo di certificazione approvato** può essere usato come elemento per **dimostrare il rispetto**" del principio di *integrità e riservatezza*.

L'art. 32(4) GDPR chiarisce che un elemento importante della sicurezza è **garantire che i dipendenti agiscano solo su istruzione e secondo le istruzioni del titolare del trattamento**. Questo è necessario per stabilire chiaramente la responsabilità e l'affidabilità. È anche necessario per garantire il requisito dell'art. 5(1)(f) alla "protezione contro il trattamento non autorizzato o illegale".

Dall'**art. 25** GDPR, ne consegue che tutti i requisiti posti dal GDPR, compresa la sicurezza, devono essere considerati **durante tutto il ciclo di vita dell'**attività di trattamento. Il GDPR richiede quindi anche la **sicurezza per progettazione e per impostazione predefinita**. La sicurezza deve quindi essere considerata anche all'inizio del ciclo di vita, per esempio attraverso i requisiti utilizzati per una gara d'appalto; e alla fine del ciclo di vita, per esempio quando si migra le operazioni a un nuovo sistema di trattamento e si smantella quello vecchio.

L'art. 30(1)(g) GDPR richiede di elencare specificamente le ***misure di sicurezza*** tecniche e organizzative nei ***registri di trattamento*** che sono destinati alle autorità di vigilanza.

1.6.3 Misure tecniche e organizzative correlate

I seguenti esempi di misure tecniche e organizzative concretizzano ulteriormente il concetto di sicurezza nel GDPR.

1.6.3.1 Misure a sostegno dell'integrità

- Una delle misure tecniche classiche per sostenere l'integrità è l'**elaborazione transazionale**. È meglio conosciuta dai sistemi di gestione di basi di dati, ma è

possibile anche in altre impostazioni[52]. Le transazioni sono importanti quando un'operazione che porta il sistema da uno stato coerente ad un altro è composta da più passi di elaborazione (cioè, non è "atomica"). Una transazione fa in modo che tutti questi passi o nessuno siano applicati, anche se il sistema dovesse bloccarsi nel mezzo. Garantisce quindi che il sistema rimanga sempre in uno stato coerente.

- Le incongruenze possono sorgere a causa di errori di trasmissione in linee di comunicazione rumorose. La misura tecnica di **correzione[53] degli errori in avanti** che è incorporata nei moderni protocolli di comunicazione supporta quindi l'integrità dei dati durante il trasferimento.
- Una misura tecnica comune per rilevare cambiamenti indesiderati negli insiemi di dati utilizza **i checksum** (alias hash o digest). In particolare, un checksum di un insieme di dati viene calcolato quando si sa che è in uno stato coerente. In momenti successivi, il checksum dell'insieme di dati può essere nuovamente calcolato e confrontato con quello iniziale per rilevare cambiamenti e corruzione.
- L'integrità è una questione importante nella distribuzione del software, in particolare se il software viene scaricato automaticamente su una rete. Gli aggiornamenti automatici dei sistemi operativi sono un primo esempio. Per supportare l'integrità del software, vengono spesso utilizzate misure tecniche come l'**autenticazione delle fonti** sulla rete e la **firma digitale del software.** La firma digitale è spesso usata anche per i file di dati.

1.6.3.2 Misure a sostegno della riservatezza

- Una misura organizzativa progettuale a sostegno della riservatezza è un'**analisi** delle **conseguenze che le** divulgazioni indesiderate a varie parti possono avere **per gli interessati**. Questo è paragonabile alla sicurezza informatica dove si identificano gli asset critici dell'organizzazione che hanno bisogno di una protezione particolare.
- La riservatezza impone al titolare del trattamento di attuare misure di protezione contro il trattamento non autorizzato (cfr. art. 5(1)(f) GDPR). Come sottolineato negli artt. 29 e 32(4) GDPR, questo include che i dipendenti trattino i dati personali solo su istruzione e secondo le istruzioni del titolare del trattamento. Ci sono una moltitudine di misure organizzative che supportano questo requisito, tra cui le seguenti:
    - **Verifica** dei nuovi dipendenti per garantire le competenze necessarie per eseguire le istruzioni dei titolari del trattamento;
    - Il mezzo legale "garantisce che **le persone autorizzate** a trattare i dati personali **si** siano **impegnate alla riservatezza** o siano sottoposte a un adeguato obbligo di riservatezza per legge". (La formulazione è tratta dall'art. 28(3)(b) che si riferisce alle persone che lavorano per i responsabili del trattamento, ma è ugualmente applicabile alle persone che lavorano per il titolare del trattamento).

52 Per esempi di elaborazione transazionale al di fuori dei DBMS, vedere per esempio https://en.wikipedia.org/wiki/Tuxedo_(software) e https://docs.oracle.com/cd/E13222_01/wls/docs81/jta/trxejb.html (entrambi visitati l'ultima volta il 20/05/2020).

53 Vedi per esempio, https://en.wikipedia.org/wiki/Forward_error_correction (ultima visita 20/05/2020).

- In questo senso, anche i **contratti con eventuali responsabili del trattamento** (vedi Art. 28(3) GDPR) che trasmettono i requisiti di riservatezza devono essere considerati come misure.
- **Formazione** dei dipendenti su come eseguire le istruzioni;
- **Punti di contatto interni** per i dipendenti che vogliono chiarire come eseguire le istruzioni;
- Manuali che descrivono le istruzioni (**manuali di processo**);
- **Supervisione** e **controllo della qualità**.

- Ciò che vale per le istruzioni alle risorse umane vale anche per **le istruzioni alle risorse tecniche**, cioè al software. L'attuazione di misure di protezione contro il trattamento non autorizzato significa che i titolari del trattamento devono accertare che il software corrisponda effettivamente alle loro istruzioni. Ci sono diverse misure per questo scopo, tra cui le seguenti:
  - **Specificazione di requisiti precisi** come input per offerte o sviluppo personalizzato di software;
  - **Test di accettazione** formale da parte del titolare del trattamento;
  - **Analisi delle nuove versioni** del software per accertare che la funzionalità cambiata corrisponda ancora alle istruzioni del titolare del trattamento e che non si sia insinuata una funzionalità aggiuntiva (**function creep**) che corrisponde a un'elaborazione non autorizzata dal titolare del trattamento.
- Un'importante misura tecnica è il **controllo dell'accesso** che fa sì che solo il personale autorizzato possa accedere ai sistemi e ai dati per scopi autorizzati. Il controllo degli accessi può comportare una moltitudine di misure, tra cui le seguenti:
  - Emissione di **credenziali di autenticazione**.
  - Configurazione dei **diritti** e delle condizioni di **accesso.**
  - Gestione del **ciclo di vita delle credenziali** e dei **diritti di accesso**, compresa la scadenza e il rinnovo, la revoca (ad esempio, quando i dipendenti vanno via), la concessione e la revoca dei diritti di accesso temporanei (ad esempio, quando i dipendenti sono malati).
  - **Audit** regolari dell'efficacia generale del sistema di controllo degli accessi.
- Esiste un'ampia gamma di misure tecniche volte a impedire a persone non autorizzate (interne o esterne) di accedere ai dati. Di solito si parla di **protezione dei dati a riposo, in transito e in uso. I** primi due aspetti richiedono generalmente la **crittografia**.
- C'è una grande quantità di misure per impedire alle persone non autorizzate di accedere a sistemi e reti. Alcuni esempi sono i seguenti:
  - **Hardening** dei sistemi operativi;
  - Applicazione tempestiva di **patch e aggiornamenti critici per la sicurezza;**
  - **Firewall**;
  - Installazione di software **anti-malware**;
  - Funzionamento dei **sistemi di rilevamento delle intrusioni**;

- Quando si **sviluppa il software**, sono disponibili molte misure per prevenire l'accesso non autorizzato al software e ai sistemi, tra cui la sanificazione dell'input, le misure di prevenzione per i tipi noti di attacchi come il cross site scripting, i metodi che impediscono i buffer overflow, la randomizzazione della memoria, ecc.
- Alcune misure non sono in grado di prevenire direttamente l'elaborazione non autorizzata, ma agiscono come **deterrenti** aiutando a **rilevare** tali azioni, **determinare** chiaramente **la responsabilità** e consentire di **ritenere responsabili le persone** che hanno agito senza autorizzazione. Tali misure comportano generalmente la **registrazione** o la creazione di **audit trail**.
- Una misura importante associata alla **fine della vita** dei componenti di archiviazione include la **distruzione** completa e **sicura di** tutti i dati prima dello **smaltimento**.

1.6.3.3 Misure a sostegno della disponibilità e della resilienza

- Una misura organizzativa a tempo di progettazione è l'analisi dell'impatto della perdita accidentale sui soggetti dei dati. Questo mira a identificare gli asset che devono essere protetti da misure di disponibilità.
- Un'altra misura di design-time riguarda la portabilità dei dati e studia la disponibilità di adeguati formati standardizzati leggibili dalla macchina che sono disponibili e le possibilità di trasferire automaticamente i dati a un altro titolare del trattamento (vedi Art. 20(2) GDPR). 20(2) GDPR).
- Un tipo molto comune di misure a sostegno della disponibilità è la **ridondanza dello storage**. Esempi ben noti sono i seguenti:
    - Archiviazione RAID;
    - Backups;
    - Storage remoto a supporto del *disaster recovery*.
- Oltre alla memorizzazione dei dati, la **ridondanza** può essere importante anche **nei sistemi di elaborazione**. Le misure di ridondanza includono quanto segue:
    - Configurazioni Master/Slave con fail-over;
    - Server farm e configurazioni cloud;
    - Strategie di migrazione dei processi basate sulla virtualizzazione.

1.7 Responsabilità

Bud P. Bruegger (ULD)

Ringraziamenti: L'autore ringrazia il contributo di Johann Čas e Walter Peissl (entrambi OEAW) che hanno scritto un'analisi di questo principio come input alla descrizione qui presentata.

Di seguito si discute il principio di *responsabilità* che è definito nell'art. 5(2) GDPR.

***La responsabilità* in sintesi:**

La responsabilità consiste in due requisiti per i titolari del trattamento:

- **Rispetto** dei principi del GDPR;
- **Dimostrazione di conformità.**

La conformità si ottiene implementando ***misure tecniche e organizzative*** che sono adeguate rispetto ai rischi per i diritti e le libertà degli interessati, corrispondono allo stato della tecnologia e sono economicamente efficaci. Ogni descrizione dei principi ha fornito esempi di tali misure tecniche e organizzative. Per un'applicazione sistematica di queste misure, i titolari del trattamento possono creare ***politiche di protezione dei dati***. I ***codici di condotta approvati***, dove disponibili, sono simili, ma sono pre-approvati e di solito si rivolgono a un intero settore. La conformità non è uno stato che viene raggiunto una volta per tutte, ma **un processo continuo** che abbraccia l'intero ciclo di vita di un'attività di trattamento.

La dimostrazione della conformità si ottiene principalmente attraverso la **documentazione** (si veda la sezione *Documentazione della elaborazione* in "Strumenti e azioni principali"). La documentazione dovrebbe essere continua come il processo di conformità. Ogni misura attuata, comprese le considerazioni e le decisioni rilevanti per la protezione dei dati, dovrebbe essere documentata. Il GDPR richiede due documenti formali come parte della dimostrazione di conformità nei confronti delle *autorità di controllo*: il ***registro del trattamento*** (vedi *Documentazione del trattamento* per i dettagli) e, dove i rischi sono probabilmente elevati, una ***valutazione d'impatto sulla protezione dei dati*** (vedi la sezione con lo stesso nome in "*Strumenti e azioni principali" nella Parte II* per i dettagli). La *certificazione* può supportare la dimostrazione della conformità.

1.7.1 Descrizione

In *Capire la protezione dei dati: il regolamento UE in poche parole*, la piena *responsabilità* dei titolari del trattamento è stata dichiarata come la prima delle diverse misure adottate dal GDPR per limitare il potere ottenuto dal titolare del trattamento attraverso il trattamento e bilanciarlo con il potere degli interessati. Vedi *1.6.1 I titolari del trattamento sono pienamente responsabili* per maggiori dettagli.

Il GDPR definisce il principio come segue:

Definizione nell'art. 5(2) GDPR:

Il **titolare del trattamento** è **responsabile** ed è in grado di **dimostrare il rispetto** del paragrafo 1 ("*responsabilità"*).

Il paragrafo 1 qui si riferisce ai principi che sono stati discussi nelle sei sezioni precedenti, vale a dire

- Legalità, equità e trasparenza;
- Limitazione dello scopo;
- Minimizzazione dei dati;
- Precisione;
- Limitazione della conservazione; e
- Integrità e riservatezza.

Per riformulare l'art. 5(2), un **titolare del trattamento** è pienamente **responsabile di due cose**:

- **Il rispetto** di questi sei principi,
- **Dimostrare la conformità**.

La responsabilità non è quindi un nuovo principio che i titolari del trattamento devono rispettare, ma istruisce i titolari del trattamento **su come i sei principi devono essere applicati**.

Si noti che dover essere in grado di dimostrare la conformità è un grande passo avanti rispetto al semplice obbligo di conformità. In particolare, mette "l'onere della prova" sul titolare del trattamento; un titolare del trattamento che non è in grado o non vuole dimostrare la conformità, è in violazione del GDPR.

1.7.1.1 Cosa significa conformarsi?

Mentre l'art. 5(2) parla solo del rispetto dei sei principi, in realtà questo deve essere esteso a **tutto il GDPR**. Questo è motivato dal fatto che tutti gli altri articoli sono destinati a fornire dettagli ai principi o a descrivere più in dettaglio come devono essere attuati.

C'è un modo dichiarato in tutto il GDPR su come la conformità deve essere raggiunta; vale a dire, attraverso l'attuazione di **misure tecniche o organizzative**. Nell'art. 24 che descrive gli obblighi di un titolare del trattamento, il primo paragrafo afferma esplicitamente che questo è il modo in cui i titolari del trattamento si conformano (e dimostrano la conformità) al GDPR; l'Art. 25(1) afferma che la protezione dei dati fin dalla progettazione si riduce all'attuazione di tali misure durante l'intero ciclo di vita dell'attività di trattamento; l'art. 25(2) sottolinea analogamente l'uso di tali misure per la protezione dei dati per impostazione predefinita; l'art. 28(1) afferma che anche i responsabili del trattamento sono tenuti a rispettare le misure organizzative. 28(1) afferma che anche i responsabili del trattamento devono attuare tali misure; l'Art. 32 afferma che anche il rispetto dei requisiti di sicurezza si ottiene attraverso l'attuazione di tali misure; e l'Art. 89(1) afferma che le garanzie necessarie per il "trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici" assicurano che tali misure siano in atto.

Dato che le misure tecniche e organizzative sono così centrali per raggiungere la conformità, la discussione di ognuno dei sei principi di cui sopra è finita con esempi di tali misure.

Il rispetto dei requisiti di protezione dei dati può essere visto come un processo. Seguendo il concetto di *protezione dei dati mediante progettazione* (cfr. Art. 25(1) GDPR), in ogni fase del ciclo di vita dell'attività di trattamento, vengono valutati i rischi per i diritti e le libertà delle persone fisiche e vengono attuate adeguate misure di mitigazione. Il GDPR usa una definizione molto ampia del termine *misure tecniche e organizzative*. Include fondamentalmente tutto ciò che un titolare del trattamento fa per conformarsi al GDPR. Pertanto, anche la fase di valutazione di cui sopra può essere considerata una misura in sé.

1.7.1.2 Cosa significa dimostrare la conformità?

Considerando che la conformità si ottiene attraverso l'attuazione di misure appropriate, non è sorprendente che la **dimostrazione di conformità documenti tali misure**.

Questo è per esempio evidente dall'Art. 30(1)(g) che obbliga a elencare le misure pertinenti alla sicurezza nei ***registri di trattamento***. È anche centrale nell'Art. 35 sulla ***valutazione d'impatto sulla protezione dei dati*** che è probabilmente lo strumento principale previsto dal GDPR per dimostrare la conformità. In particolare, l'Art. 35(7)(d) chiede ai titolari del

trattamento di dichiarare le misure che hanno attuato per garantire la protezione dei dati personali e per dimostrare la conformità al GDPR.

Una **discussione più dettagliata** sulla ***Documentazione del Trattamento*** in generale, e sulle *Valutazioni di Impatto sulla Protezione dei Dati* in particolare, può essere trovata nei "Principali Strumenti e *Azioni"* più avanti. Entrambe queste sezioni sottolineano ulteriormente l'importanza delle misure tecniche e organizzative.

1.7.1.3 Economia di scala per la conformità e la sua dimostrazione

Come argomentato sopra, la conformità si ottiene implementando misure tecniche e organizzative. È evidente dalla discussione di cui sopra che la conformità può richiedere un numero significativo di tali misure. Questo può rendere più difficile valutare l'effettiva protezione offerta da queste misure e se questa protezione è applicata in modo uniforme e coerente.

Per mitigare questa difficoltà, il GDPR offre alcuni tipi di "meccanismi di astrazione" che permettono di considerare un insieme di misure correlate come una singola unità. In particolare, il GDPR prevede due meccanismi di questo tipo nel suo Art. 24 che descrive la "Responsabilità del titolare del trattamento":

- ***Politiche di protezione dei dati*** (cfr. art. 24(2) GDPR), e
- ***codici di condotta approvati*** (vedi art. 24(3) e 40).

Una ***politica di protezione dei dati*** è un meccanismo per rendere sistematica l'applicazione delle misure. Questo garantisce un insieme uniforme e coerente di misure in situazioni simili. Per esempio, invece di dover valutare quali misure di sicurezza sono appropriate per ciascuno di molti server molto simili, un'unica politica può essere scritta una volta e applicata a tutti i server. Evidentemente, soprattutto in operazioni di elaborazione complesse ed estese, questo porta un'economia di scala potenzialmente molto significativa che può anche estendersi a più attività di elaborazione indipendenti dello stesso titolare del trattamento.

Il meccanismo dei ***codici di condotta approvati*** estende questa economia di scala al di là di un singolo titolare del trattamento ad un intero settore di trattamento. Questi codici di condotta sono preparati da **associazioni** e altri organismi **che rappresentano categorie di titolari del trattamento o responsabili del trattamento** (vedi art. 40(2) GDPR). Se un codice di condotta non riguarda attività di trattamento in più Stati membri, l'*autorità di controllo* competente può **approvarlo** (cfr. art. 40(5) GDPR) e successivamente registrarlo e pubblicarlo (vedi Art. 40(6) GDPR). Se un progetto di codice di condotta si riferisce ad attività di trattamento in più Stati membri, viene utilizzato un processo simile che coinvolge il *comitato europeo per la protezione dei dati* (cfr. art. 40(7) GDPR). 40(7) GDPR). I codici di condotta forniscono evidentemente anche un'economia di scala alle autorità di controllo che devono monitorare il rispetto del GDPR.

Sia i *codici di condotta approvati* che la *certificazione* (secondo l'art. 42 GDPR) possono aiutare i titolari del trattamento nella dimostrazione della conformità (vedi art. 24(3) GDPR). 24(3) GDPR).

1.7.2 Articoli e Considerando correlati

La responsabilità riguarda la conformità e la dimostrazione della conformità. Si riferisce direttamente ai sei principi di protezione dei dati definiti nell'art. 5(1) ma indirettamente si estende a tutto il GDPR.

L'art. 24 GDPR fornisce dettagli su come un titolare del trattamento deve raggiungere la conformità e dimostrarla. L'art. 25(1) sulla protezione dei dati per progettazione illustra come

la conformità (e di conseguenza anche la sua dimostrazione) deve essere considerata un processo continuo che attraversa tutti i cicli di vita di un'attività di trattamento. I *codici di condotta* e la *certificazione* che possono aiutare la conformità e la sua certificazione sono descritti negli artt. 40 e 42 GDPR, rispettivamente.

Gli articoli particolarmente pertinenti per la dimostrazione della conformità sono 30 *record di trattamento* e 35 *valutazione d'impatto sulla protezione dei dati*.

1.7.3 Misure tecniche e organizzative correlate

Le misure pertinenti all'*accountability* riguardano il modo di andare verso la conformità e la sua dimostrazione, molto più che ciò che deve essere fatto per conformarsi.

Le seguenti "meta-misure" riguardano i modi per **raggiungere la conformità**:

- ***Protezione dei dati per progettazione e default*** (vedi art. 25 GDPR),
- La ***valutazione d'impatto sulla protezione dei dati*** (cfr. art. 35 GDPR) nella sua funzione di processo continuo che guida il titolare del trattamento nella valutazione dei rischi e nell'identificazione delle misure tecniche e organizzative appropriate per la loro mitigazione.
- La creazione e l'applicazione di ***politiche di protezione dei dati*** (vedi Art. 24(2) GDPR).
- L'adesione a ***codici di condotta approvati*** (vedi art. 24(3) GDPR).
- L'adesione a ***meccanismi di certificazione approvati*** (vedi Art. 24(3) GDPR).

Le seguenti "meta-misure" riguardano i modi di **documentare la conformità**:

- La ***valutazione d'impatto sulla protezione dei dati*** (vedi art. 35 GDPR) nella sua funzione di rapporto. Se il rischio non è verosimilmente elevato e tale valutazione d'impatto non è quindi richiesta, la documentazione di come è stata stabilita questa stima del rischio dovrebbe essere documentata (si veda la sezione "Valutazione d'impatto sulla protezione dei dati″ in "Strumenti e azioni principali" nella parte II di queste Linee guida per i dettagli).
- I ***registri del trattamento*** (vedi art. 30 GDPR).