

# UE-RGDP

## Guida tascabile

Alan Calder

# UE-RGDP

## Guida tascabile

Documenti e dati



# UE-RGDP

Guida tascabile

ALAN CALDER



**IT Governance Publishing**



**Documents**

Document Sharing Hub

Copyright IT Governance Ltd

Provided by IHS Markit under license with IT Governance Ltd. See /, User=,

No reproduction or networking permitted without license from IHS.

**Full document details: ITG 2017**

È stato fatto ogni possibile sforzo per garantire che le informazioni contenute in questo libro siano accurate al momento della stampa. L'editore e l'autore declinano qualsiasi responsabilità in caso di errori od omissioni, qualunque sia la loro origine. Le opinioni espresse in questo libro sono quelle dell'autore, non dell'editore. I siti Web identificati sono forniti solo a scopo informativo e non costituiscono approvazioni da parte nostra. La visita dei medesimi è a esclusivo rischio del lettore. L'editore e l'autore declinano qualsiasi responsabilità derivante da eventuali perdite o danni subiti da un soggetto che agisce, od omette di agire, come conseguenza dei presenti contenuti.

Fatto salvo il trattamento equo per scopi di ricerca o studio privato, critica o revisione, come contemplato dal Copyright, Designs and Patents Act 1988, è rigorosamente vietato riprodurre, conservare o trasmettere, in qualsivoglia forma e con qualsiasi mezzo, la presente pubblicazione senza il previo consenso scritto dell'editore. L'attività di reprografia è soggetta alle condizioni delle licenze rilasciate dalla Copyright Licensing Agency. Per qualsiasi domanda sulla riproduzione dei contenuti della pubblicazione al di fuori dei suddetti termini, si prega di contattare l'editore al seguente indirizzo:

IT Governance Publishing  
IT Governance Limited  
Unit 3, Clive Court  
Bartholomew's Walk  
Cambridgeshire Business Park  
Ely, Cambridgeshire  
CB7 4EA  
United Kingdom

[www.itgovernance.co.uk](http://www.itgovernance.co.uk)

© Alan Calder 2017

L'autore ha affermato i diritti di autore ai sensi del Copyright, Designs and Patents Act, 1988, per essere identificato come autore di questo lavoro.

Prima pubblicazione nel Regno Unito nel 2017  
da IT Governance Publishing.

ISBN 978-1-84928-880-4

## L'AUTORE

Alan Calder è fondatore e presidente esecutivo di IT Governance Ltd ([www.itgovernance.co.uk](http://www.itgovernance.co.uk)), una società di informazione e consulenza che assiste i Consigli di amministrazione delle imprese nella gestione di tutti gli aspetti relativi a governance informatica, gestione del rischio, conformità e sicurezza dell'informazione.

IT Governance Ltd opera siti Web in tutto il mondo distribuendo una gamma di libri, strumenti e altre pubblicazioni sui temi di IT governance, gestione del rischio, conformità e sicurezza dell'informazione.

Copyright IT Governance Ltd

# INDICE

|                                                                   |           |
|-------------------------------------------------------------------|-----------|
| <b>Introduzione .....</b>                                         | <b>8</b>  |
| <b>Capitolo 1: Breve storia della protezione dei dati .....</b>   | <b>11</b> |
| <b>Capitolo 2: Terminologia e definizioni .....</b>               | <b>19</b> |
| <b>Capitolo 3: Il regolamento .....</b>                           | <b>32</b> |
| Principi .....                                                    | 36        |
| Applicabilità .....                                               | 38        |
| Diritti degli interessati .....                                   | 40        |
| Consenso .....                                                    | 41        |
| Diritto all'oblio .....                                           | 44        |
| Portabilità dei dati .....                                        | 45        |
| Liceità del trattamento .....                                     | 46        |
| Conservazione dei dati.....                                       | 47        |
| Uno "sportello unico" .....                                       | 48        |
| Registro delle attività di trattamento dei dati ..                | 50        |
| Valutazioni d'impatto sulla protezione dei dati .....             | 50        |
| Protezione dei dati fin dalla progettazione e di default.....     | 51        |
| Contratti fra il titolare e il responsabile del trattamento ..... | 53        |
| Responsabile della protezione dei dati.....                       | 54        |
| Responsabilizzazione del Consiglio di amministrazione.....        | 57        |
| Violazioni dei dati.....                                          | 58        |
| Cifratura.....                                                    | 59        |
| Trasferimenti internazionali.....                                 | 61        |
| Norme vincolanti d'impresa .....                                  | 62        |
| Considerazioni aggiuntive .....                                   | 64        |
| Modifiche alla "legge sui cookie" .....                           | 65        |
| Indirizzi IP .....                                                | 67        |

## Indice

|                                                                           |           |
|---------------------------------------------------------------------------|-----------|
| Direttiva sulla sicurezza delle reti e dell'informazione.....             | 68        |
| <b>Capitolo 4: Osservanza al regolamento.....</b>                         | <b>70</b> |
| Ripercussioni .....                                                       | 70        |
| Comprendere i dati dell'organizzazione: dove sono e come sono usati ..... | 72        |
| Documentazione .....                                                      | 74        |
| Misure tecniche e organizzative adeguate e ISO/IEC 27001 .....            | 75        |
| Standard, programmi e marchi di protezione..                              | 78        |
| Proteggere le relazioni con il fornitore.....                             | 79        |
| <b>Capitolo 5: Indice del regolamento.....</b>                            | <b>82</b> |
| <b>Appendice 1: Autorità nazionali di protezione dei dati .....</b>       | <b>89</b> |
| <b>Appendice 2: Risorse sull'UE-RGDP .....</b>                            | <b>90</b> |
| <b>Risorse su ITG .....</b>                                               | <b>94</b> |

## INTRODUZIONE

Nell'ultimo decennio, la cibersecurity è diventato un problema sempre più importante per le organizzazioni in tutta l'UE. Anche se le minacce informatiche hanno target estremamente diversi (come l'infrastruttura nazionale critica, la proprietà intellettuale, i segreti commerciali e le informazioni finanziarie), uno dei principali bersagli dei criminali informatici sono le informazioni di identificazione personale (PII, Personally Identifiable Information).

Queste informazioni, che includono nomi, indirizzi, identificativi fiscali o della sicurezza sociale, dati della carta di pagamento, ecc. hanno un particolare valore perché aprono la porta a un'ampia serie di illeciti, incluso il furto economico e il furto di identità.

La preoccupazione del privato (che nella legislazione sulla protezione dei dati è chiamato l'interessato) va ben oltre il crimine informatico. Oggi gli Stati e le grandi organizzazioni raccolgono volumi enormi di informazioni personali per monitorare l'attività del singolo utente nello spazio informatico. Le società di marketing digitale continuano a sviluppare metodi nuovi e sempre più efficaci per monitorare i consumatori. Le società di social media prosperano sulla pubblicazione dei dati personali. Se da un lato questa attività offre certamente numerosi vantaggi, è anche vero che rappresenta un rischio per la privacy dell'individuo.

## *Introduzione*

L'Unione europea è sempre stata in prima linea nella difesa dei diritti dei cittadini relativamente ai loro dati personali. Il regolamento generale sulla protezione dei dati (RGDP), che è diventato legge ed entrerà in vigore nel maggio 2018, è probabilmente il più grande passo avanti compiuto da un'autorità eletta a livello mondiale nell'impegno a garantire una protezione adeguata della vita privata e dei dati personali dei suoi cittadini.

L'RGDP crea una base uniforme per la protezione dei dati in tutti gli Stati membri dell'Unione europea. Questo significa che i cittadini dell'Unione saranno trattati in modo equo, presumibilmente, ovunque si trovino nel territorio dell'Unione e che le organizzazioni conformi ai requisiti del regolamento in una giurisdizione lo saranno in tutti gli altri Stati membri.

Anche le organizzazioni al di fuori dell'UE, così come i fornitori nell'Unione, rientrano nel campo di applicazione del regolamento. L'RGDP copre nello specifico gli accordi attuali in materia di trasferimento dei dati da un paese UE verso paesi terzi. Ancora più importante, punisce le violazioni con sanzioni "che devono essere proporzionali e dissuasive", fino a un massimo di 20 milioni di euro o del 4% del fatturato globale dell'organizzazione, a seconda del valore superiore fra i due.

Il periodo di transizione a disposizione della aziende per adeguare le proprie pratiche in materia di trattamento dei dati ai requisiti dell'RGDP termina nel maggio 2018. Da quel momento, le

## Introduzione

organizzazioni che violano la nuova legislazione sono punibili con sanzioni pecuniarie particolarmente elevate.

Questa Guida tascabile vuole fornire una panoramica del nuovo regolamento, illustrare i principi generali della protezione dei dati e spiegare cosa significa l'RGDP per le imprese UE e non-UE, affinché possano prosperare sotto il nuovo quadro normativo.

Per capire a fondo il regolamento, è importante fare luce sul significato di alcuni termini chiave utilizzati in questo libro, per cui si rimanda al Capitolo 2 - Terminologia e definizioni.

## CAPITOLO 1: BREVE STORIA DELLA PROTEZIONE DEI DATI

La percezione comune della protezione dei dati è un concetto molto moderno. In genere si pensa ai database e ai dati archiviati in formato digitale, concordando sull'importanza di proteggere queste informazioni. È chiaro a tutti che i dati digitali non hanno un peso fisico e possono essere smarriti o rubati senza intaccare l'originale. Inutile dire che una perdita di questo tipo potrebbe interessare grandi volumi di informazioni. Se è vero che in passato le cose erano diverse, è anche vero che tutt'oggi ci sono informazioni in altri formati che è importante proteggere.

Forse le prime forme di protezione dei dati e della vita privata risalgono alle professioni più che alla legge codificata. Ad esempio, il principio di riservatezza fra un avvocato e il suo cliente (il cosiddetto segreto professionale dell'avvocato) è nato come forma di accordo fra il rappresentante legale e il suo cliente molti decenni, se non secoli, prima di essere codificato in legge. La legge sul segreto professionale è stata introdotta per assicurare che gli avvocati potessero rappresentare debitamente gli interessi dei propri assistiti senza temere future conseguenze legali.

Allo stesso modo, la riservatezza della professione medica riguardo alle informazioni di carattere sanitario dei pazienti si è instaurata nella pratica molti decenni fa ed è riuscita a garantire una protezione abbastanza efficace delle informazioni.

## Capitolo 1: Breve storia della protezione dei dati

eccetto nei casi in cui la divulgazione è imposta per legge. Anche in questo secondo esempio, la protezione dei dati è nata nella professione molto prima che nel diritto.

Pratiche di questo genere hanno consentito di tutelare montagne di informazioni personali in funzione degli interessi della singola attività: se una professione vedeva un valore nella protezione delle informazioni, allora le proteggeva. Con la diffusione della conservazione dei dati in formato digitale anziché cartaceo e l'introduzione di metodi di manipolazione dei dati personali (anche nei loro elementi minimi) sempre più potenti, è emersa la necessità di cambiare le regole, perché tutte queste informazioni erano improvvisamente a rischio e proprio per questo acquisivano un valore particolare. Le campagne politiche, per citare un esempio etico *ragionevole*, si servono di enormi volumi di dati per raggiungere meglio i segmenti di popolazione di loro interesse, per definire le politiche e modellare l'immagine dei loro candidati. All'altro estremo, il furto di identità è oggi un problema gravissimo e la gravità di questa minaccia si alimenta proprio dell'enorme volume di informazioni disponibili.

Pensando alla situazione europea, una delle prime forme di tutele legali delle informazioni personali è stata introdotta con l'articolo 8 della convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU, 1953). Seppure non nella forma che ci aspetteremmo di vedere oggi in una legge sulla protezione della vita privata, l'articolo 8 ha gettato le basi per le

## Capitolo 1: Breve storia della protezione dei dati

moderne leggi europee sulla privacy. L'articolo 8 dice:

1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.
2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

Per alcuni questa è una clausola aperta e inconcludente, che le persone senza scrupolo possono interpretare per porre limitazioni ai diritti delle persone (applicando leggi che eludono ad alcune protezioni); per imporre un peso normativo non necessario su terzi (applicando leggi che usano un linguaggio altrettanto generico); e per limitare il potere dello Stato di perseguire la giustizia (perché la Corte europea dei diritti dell'uomo si opporrebbe a qualsiasi legge che viola il diritto alla vita privata<sup>1</sup>). Emergendo opinioni

---

<sup>1</sup> In particolare, nel caso in cui suddette leggi sembrano contravvenire o ledere altri articoli del CEDU, come

## *Capitolo 1: Breve storia della protezione dei dati*

così contrastanti, è rimasto generalmente equilibrato negli interessi di tutte le parti.

Indipendentemente da come venga interpretato, il retaggio del CEDU in materia di diritto alla privacy si è tramandato nei decenni fino al quadro legislativo attuale.

Nel 1981, il Consiglio d'Europa ha definito alcune norme per assicurare la libera circolazione delle informazioni tra tutti i paesi membri dell'UE senza che fosse violata la privacy personale. La convenzione che ha applicato questi standard (la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale) è stata promulgata in risposta all'uso sempre più diffuso dei computer per archiviare e trattare i dati personali. Gli standard minimi definiti dalla convenzione sono serviti da base per il primo giro di normative europee sulla vita privata.

Tuttavia, come sappiamo, la potenza e la disponibilità dei computer è letteralmente esplosa negli anni '80 e '90. Per fare un esempio, nel 1995, più di 1 milione di persone nel Regno Unito usavano Internet regolarmente. Con il passare degli anni, le normative sulla protezione dei dati nei paesi UE si sono diversificate, creando ostacoli

---

l'articolo 10, che disciplina il diritto alla libertà di espressione e all'informazione.

~~~~~

## *Capitolo 1: Breve storia della protezione dei dati*

alla libera circolazione dei dati a livello di Unione e, di conseguenza, alle attività delle imprese. Era chiaro che le norme esistenti sulla protezione dei dati in Europa non erano più adeguate per supportare gli articoli 8 e 10 del CEDU. Così venne promulgata la direttiva sulla protezione dei dati di carattere personale (direttiva 95/46/CE, 1995).

La direttiva imponeva agli Stati membri di sviluppare leggi proprie per soddisfare i nuovi e rigorosi criteri minimi, tenendo conto della diffusione di computer e dispositivi elettronici sempre più potenti, facilmente disponibili ed economici. A livello pratico, la direttiva è stata come una "reimpostazione" nel settore della tutela dei dati, perché obbligava tutti gli Stati membri ad allinearsi ai suoi requisiti, e quindi a migliorare la protezione dei dati personali abbattendo al contempo le barriere alla libera circolazione dei dati a livello di Unione.

La direttiva 95/46/CE introduceva anche delle regole per il trasferimento dei dati personali al di fuori dell'UE. Ciò è stato ripreso nel quadro normativo "Safe Harbor" fra Stati Uniti e Unione europea, in cui si asseriva che le norme in materia di protezione dei dati negli Stati Uniti erano sufficienti per garantire la tutela dei dati personali di provenienza UE, a patto che il destinatario basato negli Stati Uniti osservasse una serie di principi di tutela dei dati auto-controllati. Anche se tale quadro legislativo è stato dichiarato non conforme alla direttiva 95/46/CE nel 1995, è stato comunque il riferimento per un'ingente volume di attività per oltre 15 anni.

## *Capitolo 1: Breve storia della protezione dei dati*

Nel Regno Unito, il Data Protection Act 1998, con i suoi otto principi cardine, ha applicato i requisiti della direttiva 95/46/CE. Questi principi definivano in modo chiaro gli obiettivi generali della legge, rendendo ragionevolmente semplice determinare se un'organizzazione fosse o meno ottemperante ai propri obblighi. Tuttavia, a causa di alcune sue complessità di base, il Data Protection Act 1998 ha subito innumerevoli modifiche e aggiornamenti, diventando con il tempo sempre più complesso e voluminoso.

In quegli anni, la tutela dei dati in Germania era regolamentata primariamente dalla legge federale sulla protezione dei dati (Bundesdatenschutzgesetz, BDSG), supportata da una serie di norme settoriali a vari livelli di autorità federale e statale. La legge tedesca, mirando a soddisfare i requisiti della direttiva 95/46/CE, era in linea di massima paragonabile a quella britannica, seppure con notevoli differenze di dettaglio.

La Francia ha anticipato di gran lunga tutti gli altri paesi europei nella protezione dei dati poiché la sua legge in materia (Loi informatique et libertés, LIL) venne introdotta nel 1978, coprendo l'intero arco di vita della Convenzione UE e della direttiva 95/46/CE. Anziché promulgare una nuova legge per rispondere alle pressioni dell'Unione, la Francia decise di emendare la normativa esistente. Nonostante ciò, la LIL attuale è incredibilmente concisa.

Anche se in tutta l'Unione vennero introdotte leggi abbastanza simili, a causa delle differenze nei

## *Capitolo 1: Breve storia della protezione dei dati*

tempi e negli interessi di ogni Stato, non esistevano due legislazioni nazionali sufficientemente simili perché un'organizzazione potesse risultare conforme alla legge nazionale e a quella di tutti gli altri paesi UE allo stesso tempo. Ossia, la libera circolazione delle informazioni risultava di fatto inibita, perché i diversi contesti normativi collidevano nei dettagli, obbligando imprese e governi a mettere in atto processi specifici per un numero sempre crescente di scenari. Questa situazione, combinata agli incalzanti sviluppi tecnologici, creò l'ambiente propizio per la nascita dell'RGDP.

È opportuno discutere perché l'UE abbia deciso di promulgare un regolamento anziché una direttiva (come era la direttiva 95/46/CE). Nel diritto dell'UE, una direttiva definisce le condizioni o i requisiti minimi, senza indicare però misure specifiche da eseguire. Ciò significa che la direttiva non ha un effetto diretto sulle persone fisiche e le persone giuridiche. Gli Stati membri hanno invece l'obbligo di approvare leggi proprie per conformarsi ai requisiti minimi della direttiva. Sono proprio tali leggi che le persone fisiche e giuridiche devono osservare.

Un regolamento, invece, è di fatto una legge ed entra in vigore in tutta l'Unione nello stesso momento. Gli Stati membri non devono promulgare leggi supplementari perché il regolamento entri in vigore, né il regolamento è soggetto all'interpretazione di autorità di governo o tribunali locali. Per il suo peso legale, un regolamento deve attraversare tipicamente un iter legislativo molto più lungo. Tuttavia, un

**Documents**

## *Capitolo 1: Breve storia della protezione dei dati*

regolamento è più efficace nel garantire coerenza normativa nell'Unione.

L'RGDP ha percorso una strada particolarmente lunga e tortuosa prima di ottenere l'approvazione del Parlamento europeo e del Consiglio, e sicuramente non priva di controversie. Il testo è rimasto per molti anni a livello di comitato, dove è stato scritto e riscritto più volte, per le migliaia di proposte di emendamento che spingevano per più o meno privacy dei dati, finché le divergenze più aspre sono state gradualmente appianate e risolte.

AVAShare - Documenti e dati

## CAPITOLO 2: TERMINOLOGIA E DEFINIZIONI

Prima di entrare nella vera e propria analisi del regolamento e come osservarlo, è importante fare luce sulle definizioni di alcuni termini chiave di uso comune. Ove il regolamento include una definizione, questa è stata riportata di seguito, con eventuali commenti aggiuntivi.

### *Norme vincolanti d'impresa*

le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro dell'Unione al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo di imprese;<sup>2</sup>

Le norme vincolanti d'impresa sono state sviluppate in origine dal Gruppo di lavoro "Articolo 29" (un gruppo all'interno dell'Unione che elabora e promuove buone pratiche in materia di protezione dei dati) per permettere alle grandi organizzazioni o ai gruppi di organizzazioni di

---

<sup>2</sup> UE-RGDP, articolo 4, paragrafo 20.

## *Capitolo 2: Terminologia e definizioni*

trasferire i dati in altri paesi in modo sicuro, riducendo al contempo gli ostacoli burocratici. L'RGDP pone le condizioni per cui i singoli Stati membri possano definire le proprie norme vincolanti d'impresa per agevolare i trasferimenti internazionali.

### *Dati biometrici*

I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;<sup>3</sup>

I dati biometrici sono usati sempre più come metodo di autenticazione, spesso insieme ad altre informazioni che è importante tutelare (ad esempio le password e qualsiasi informazione che diventa accessibile in seguito all'uso delle password). Gli Stati membri possono introdurre ulteriori limitazioni o condizioni sul trattamento dei dati biometrici.

### *Consenso*

Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante

---

<sup>3</sup> UE-RGDP, articolo 4, paragrafo 14.

## Capitolo 2: Terminologia e definizioni

dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;<sup>4</sup>

Il consenso è un concetto estremamente importante nel regolamento e verrà affrontato in dettaglio in questo libro.

### *Trattamento transfrontaliero*

- (a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
- (b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.<sup>5</sup>

Questo articolo si riferisce ai trasferimenti dei dati entro il territorio UE. In questi casi, il regolamento prevede delle clausole che permettono di determinare l'autorità di controllo competente.

---

<sup>4</sup> UE-RGDP, articolo 4, paragrafo 11.

<sup>5</sup> UE-RGDP, articolo 4, paragrafo 23.

## Capitolo 2: Terminologia e definizioni

### *Data relativi alla salute*

I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;<sup>6</sup>

I dati relativi alla salute sono oggetto di tutele particolari sotto l'RGDP, al fine di tutelare i soggetti vulnerabili. Tutti i dati personali devono essere protetti, ma alcune forme di dati, ad esempio quelli sulla salute, sono soggetti a limitazioni supplementari su come e quando possono essere trattati e sul tipo di consenso che occorre ottenere prima di procedere al trattamento. Gli Stati membri possono introdurre ulteriori limitazioni o condizioni sul trattamento dei dati relativi alla salute.

### *Titolare del trattamento*

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

---

<sup>6</sup> UE-RGDP, articolo 4, paragrafo 15.

## Capitolo 2: Terminologia e definizioni

sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;<sup>7</sup>

Si tratta in genere delle entità che si interfacciano direttamente con gli interessati e alle quali gli interessati forniscono le proprie informazioni personali. Ad esempio, un ospedale potrebbe usare un modulo online per immettere le informazioni sulla salute dei pazienti. Anche se il modulo online è fornito da un terzo, l'ospedale (che determina lo scopo del trattamento dei dati) è il titolare del trattamento.

### *Responsabile del trattamento*

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;<sup>8</sup>

In molti casi, il titolare del trattamento e il responsabile del trattamento sono la stessa entità. Nell'esempio precedente, l'organizzazione che fornisce il modulo online sarà il responsabile del trattamento, poiché l'atto di raccogliere i dati è incluso nella definizione di "trattamento".<sup>9</sup> Un singolo titolare del trattamento può avere più responsabili del trattamento.

---

<sup>7</sup> UE-RGDP, articolo 4, paragrafo 7.

<sup>8</sup> UE-RGDP, articolo 4, paragrafo 8.

<sup>9</sup> UE-RGDP, articolo 4, paragrafo 2.

## Capitolo 2: Terminologia e definizioni

### *Interessato*

The Regulation defines a data subject as “an identified or identifiable natural person”.<sup>10</sup> Non vi è restrizione sulla nazionalità o il luogo di residenza di un interessato, il quale può trovarsi in qualsiasi parte nel mondo: il regolamento non fa distinzione. Equally, however, a data subject has to be a *person*; a corporation or other entity cannot be a data subject, and information on those subjects has no protection under the Regulation.

### *Archivio*

Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;<sup>11</sup>

Questo è un termine generico che include tutti i metodi con cui i dati personali possono essere raccolti, conservati, trasmessi e trattati.

### *Dati genetici*

I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche

---

<sup>10</sup> UE-RGDP, articolo 4, paragrafo 1.

<sup>11</sup> UE-RGDP, articolo 4, paragrafo 6.

## Capitolo 2: Terminologia e definizioni

sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;<sup>12</sup>

Alla luce del crescente interesse nella genetica e nell'ingegneria genetica, ma anche della preoccupazione del pubblico riguardo allo statuto giuridico dei dati genetici, il regolamento considera questi dati come dati personali, dotandoli di tutele almeno equivalenti a quelle degli altri dati personali. Gli Stati membri possono introdurre ulteriori limitazioni o condizioni sul trattamento dei dati genetici.

### *Stabilimento principale*

- (a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte

---

<sup>12</sup> UE-RGDP, articolo 4, paragrafo 13.

## Capitolo 2: Terminologia e definizioni

decisioni è considerato essere lo stabilimento principale;

- (b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;<sup>13</sup>

È importante determinare lo "stabilimento principale" di un'organizzazione con presenza in più Stati membri, perché ciò permette di definire l'autorità di controllo competente e individuare le possibili limitazioni e condizioni specifiche nel trattamento di alcuni tipi di dati personali (ad esempio i dati biometrici, genetici e relativi alla salute).

### *Dati personali*

Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la

---

<sup>13</sup> UE-RGDP, articolo 4, paragrafo 16.

## Capitolo 2: Terminologia e definizioni

persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;<sup>14</sup>

Si noti che questo elenco di caratteristiche non è completo: *any information that could be used to identify the data subject is personal data, and this information can be in any format.* Ciò include fotografie, corrispondenza, mezzi fisici, ecc.

### *Violazione dei dati personali*

Una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;<sup>15</sup>

Il regolamento si occupa principalmente delle violazioni dei dati personali. Le violazioni dei dati in senso più generale diventano di interesse solo se la perdita dei dati è in qualche modo ricollegabile a una violazione dei dati personali.

---

<sup>14</sup> UE-RGDP, articolo 4, paragrafo 1.

<sup>15</sup> UE-RGDP, articolo 4, paragrafo 12.

## Capitolo 2: Terminologia e definizioni

### *Trattamento*

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;<sup>16</sup>

Questa è una definizione estremamente ampia e, ancora una volta, non esaustiva. A livello pratico, il trattamento può includere qualsiasi interazione che avete con i dati personali, in qualunque forma. Pertanto, individuare tutte le opzioni di trattamento che utilizzate nella vostra attività è fondamentale per garantire la conformità all'RGDP.

### *Profilazione*

Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la

---

<sup>16</sup> UE-RGDP, articolo 4, paragrafo 2.

## Capitolo 2: Terminologia e definizioni

situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;<sup>17</sup>

Gli interessati devono essere sempre informati degli eventuali processi di profilazione realizzati sui loro dati personali perché possano esprimere il consenso.

### *Pseudonimizzazione*

Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;<sup>18</sup>

Se da un lato il regolamento considera la pseudonimizzazione una cosa positiva in termini generali, dall'altro precisa che i dati sottoposti a pseudonimizzazione "attribuibili a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una

---

<sup>17</sup> UE-RGDP, articolo 4, paragrafo 4.

<sup>18</sup> UE-RGDP, articolo 4, paragrafo 5.