Il Regolamento Generale sulla Protezione dei Dati

Prof. Avv. Pierluigi Perri
Università degli Studi di Milano
pierluigi.perri@unimi.it

La Direttiva 95/46/EC

- Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati.

La Direttiva 2002/58/EC

- Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

I problemi della Direttiva 95/46

Direttiva vs. Regolamento

- Direttiva = Una direttiva è un atto legislativo che stabilisce un obiettivo che tutti i paesi dell'UE devono realizzare. Tuttavia, spetta ai singoli paesi definire attraverso disposizioni nazionali come tali obiettivi vadano raggiunti. Un esempio è quello della direttiva sui diritti dei consumatori dell'UE, che rafforza i diritti dei consumatori in tutta l'Unione, ad esempio eliminando spese e costi nascosti in Internet, ed estendendo il periodo entro il quale i consumatori possono recedere da un contratto d'acquisto.
- Regolamento = Un regolamento è un atto legislativo vincolante. Deve essere applicato in tutti i suoi elementi nell'intera Unione europea. Ad esempio, quando l'Unione ha deciso che dovevano esservi garanzie comuni sui beni importati dall'esterno dell'UE, il Consiglio ha adottato un regolamento.

Obiettivi

- La Direttiva è lo strumento legislativo che viene adoperato per **armonizzare** una determinata disciplina tra gli Stati europei, il Regolamento invece è lo strumento adoperato per **uniformare** una determinata disciplina tra tutti gli Stati membri.

Efficacia

Il regolamento ha effetto a decorrere dal **25 maggio 2018**, data in cui **ha abrogato** la direttiva UE sulla protezione dei dati (95/46/CE), conferendo **nuovi diritti** alle persone fisiche, estendendo la portata delle **responsabilità** del titolare e del responsabile del trattamento dei dati e potenziando il regime di applicazione con l'introduzione di **sanzioni** molto elevate.

Cosa cambia?

I cambiamenti chiave comprendono:

- un nuovo **principio di territorialità** che governa l'ambito di applicazione del Regolamento;
- la necessità di applicare i principi di "**data proteciton by design**" e di "**data protection by default**" nei processi di sviluppo e lancio di nuove tecnologie, prodotti, servizi, ecc.;
- il nuovo obbligo di effettuare il c.d. **data protection impact assessment**;
- i nuovi diritti alla **portabilità dei dati** e il **limitazione del trattamento**;
- l'estensione dell'obbligo di comunicare alle Autorità di controllo competenti (Autorità Garanti) eventuali **violazioni di dati personali**;
- Le Autorità di controllo ora possono avere un ruolo di "**capofila**" nella determinazione delle controversie, per cui vengono attivate direttamente dall'interessato e la loro competenza si può espandere in tutta Europa;
- sanzioni amministrative per inosservanza delle norme che possono arrivare fino a un massimo di EUR 20 milioni o (se superiore) al 4% del fatturato globale annuo dell'organizzazione;
- norme speciali sulla **profilazione** e sul consenso dei **minori** per i servizi della società dell'informazione.

Dato personale

- Art. 4 RGPD
- "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, **dati relativi all'ubicazione**, **un identificativo online** o a uno o più **elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale**;"

Dato ex sensibile

- Art. 9 RGPD
- "[...]dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati **genetici**, dati **biometrici** intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'**orientamento sessuale** della persona".

Dato giudiziario

Art. 10 RGPD

- "[...] dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza".

Trattamento

Art. 4 RGPD

- "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;"

Dati particolari

- Art. 4 RGPD

- «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- «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;
- «dati 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;"

Il Titolare e il Responsabile del trattamento

Fare clic per inserire il sottotitolo

Titolare

Art. 4 RGPD

- "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;"

Responsabilità del titolare

Art. 24 RGPD

- "1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto **misure tecniche e organizzative adeguate** per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono **riesaminate** e **aggiornate** qualora necessario.

- 2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di **politiche adeguate** in materia di protezione dei dati da parte del titolare del trattamento.

- 3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento."

Accountability

- Il principio dell'*accountability* o "responsabilizzazione" rientra tra i principi cardine del GDPR

- Esso è contenuto nel Considerando 85 e nell'art. 5 comma 2

Considerando 85

- "[...] *non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di* ***dimostrare*** *che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.*"

Accountability

- Il principio dell'*accountability* o "responsabilizzazione" rientra tra i principi cardine del GDPR

- Esso è contenuto nel Considerando 85 e nell'art. 5 comma 2

Responsabilità del titolare

Art. 24 RGPD

- "1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto **misure tecniche e organizzative adeguate** per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono **riesaminate** e **aggiornate** qualora necessario.

- 2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di **politiche adeguate** in materia di protezione dei dati da parte del titolare del trattamento.

- 3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento."

Art. 5 comma 2

- Principi applicabili al trattamento di dati personali

- *"2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di* ***comprovarlo*** *(«responsabilizzazione»)."*

Il senso dell'accountability

- Esso può essere riassunto nell'obbligo, in capo al titolare, di essere in grado di **dimostrare** la conformità del trattamento ai principi e alle regole contenute nel GDPR e di **affermare** esplicitamente che assicurare tale conformità rientra tra i suoi compiti

Responsabile del trattamento

Art. 4 RGPD

- "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo **che tratta dati personali per conto del titolare del trattamento**"

Responsabile del trattamento

Art. 28 RGPD

- "1.Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino **garanzie sufficienti** per mettere in atto **misure tecniche e organizzative adeguate** in modo tale che il trattamento soddisfi i requisiti del presente regolamento e **garantisca la tutela dei diritti dell'interessato**."

Rapporto contrattuale

- Art. 28 RGPD

- "3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento."

Incaricato del trattamento

- Art. 4 RGPD

- "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile"

Il Responsabile della protezione dei dati (data protection officer)

Fare clic per inserire il sottotitolo

Titolare e DPO

- 1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:
  - a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
  - b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
  - c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.
- La nomina del DPO, quindi, è sempre compito del titolare e del responsabile nell'ambito delle loro politiche di *governance*.

I compiti

- I compiti minimi del DPO sono specificati nell'art. 39 del GDPR
- a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
- d) cooperare con l'autorità di controllo; e
- e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

I compiti

- Riassumendo, i suoi compiti sono: **informare**, **sorvegliare**, **fornire consulenza**, **cooperare** con l'attività di controllo e fungere da **punto di contatto**

- Eventuali compiti aggiuntivi possono essere i seguenti:
  - tenuta del registro dei trattamenti;
  - formazione per il personale che tratta i dati sotto l'autorità del titolare o del responsabile del trattamento;
  - sovrintendere all'esercizio dei diritti degli interessati;
  - prestare assistenza qualificata in caso di notifica per violazione di dati personali;
  - condurre delle attività di *audit*;
  - presentare una relazione annuale delle attività svolte.

Come svolge le sue mansioni?

- Nello svolgimento delle sue mansioni, il titolare e il responsabile del trattamento:
  - si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
  - sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
  - si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.
  - Si assicurano che altri compiti e funzioni non diano adito a un conflitto di interessi.

Indipendenza

- Il DPO non deve ricevere alcuna istruzione per lo svolgimento dei suoi compiti (es. approccio da seguire nel caso specifico, interpretazioni da dare a una specifica questione) ma non può comunque travalicare i limiti previsti dall'articolo 39.
- Il DPO riferisce al vertice amministrativo (es. il CdA), il quale non è tenuto a seguire le sue indicazioni. È tuttavia indispensabile conservare una traccia di questo "dialogo" tra titolare o responsabile e DPO.
- Il DPO deve avere un lasso temporale d'azione contrattualmente definito che sia compatibile con lo sviluppo di una politica di protezione dei dati all'interno dell'organizzazione ("quanto maggiore è la stabilità del contratto e maggiori le tutele previste contro l'ingiusto licenziamento, tanto maggiore sarà la probabilità che l'azione del DPO si svolga in modo indipendente").

Conflitto d'interessi

- Il DPO può svolgere altre funzioni nella misura in cui queste non diano adito a un conflitto d'interessi (art. 38 comma 6 GDPR).

- Nel nostro sistema giuridico, in generale si ravvisa il conflitto d'interessi quando vi è una correlazione diretta o indiretta tra un interesse personale di un soggetto, o di suoi parenti o affini, e gli interessi dell'organo o dell'ente che rappresenta. Tale interesse è sufficiente che sia divergente, non essendo necessario che sia conflittuale.

- Il conflitto d'interessi resta tale anche nel momento in cui la decisione finale presa sia quella più conveniente od opportuna per l'organo o ente.

Informativa e consenso per il RGPD

Fare clic per inserire il sottotitolo

Informativa

Art. 13 RGPD

- "1.In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni: a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
- c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione"

Altre informazioni aggiuntive che bisogna specificare

- **Periodo di conservazione** dei dati personali o criteri utilizzati per determinare tale periodo
- **Indicazione dei diritti per gli interessati** (ivi compresi i "nuovi" diritti di limitazione di trattamento e di portabilità dei dati)
- **Indicazione del diritto di revocare il consenso** senza però pregiudicare i trattamenti precedentemente avvenuti
- **Indicazione del diritto di proporre reclamo innanzi al Garante**
- **Conferimento obbligatorio o facoltativo** dei dati e conseguenze derivanti dal diniego a conferire i dati personali
- **Indicazione dell'esistenza di un processo decisionale automatizzato**, ad es. per profilazione, e informazioni **significative** sulla logica utilizzata e sull'importanza e le conseguenze di tale trattamento.

Particolarità del consenso nel RGPD

- Art. 7 del RGPD

1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento **deve essere in grado di dimostrare** che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata **in modo chiaramente distinguibile** dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. **La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca**. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali **non necessario** all'esecuzione di tale contratto.

Condizioni applicabili al consenso dei minori

- Per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia **almeno 16 anni**. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.
- Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché **non inferiore ai 13 anni**.
- 2. Il titolare del trattamento si adopera **in ogni modo ragionevole** per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.

I diritti degli interessati

Fare clic per inserire il sottotitolo

Diritto di accesso dell'interessato

- Art. 15 RGPD
- 1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
  - a) le **finalità** del trattamento;
  - b) le **categorie** di dati personali in questione;
  - c) i **destinatari** o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
  - d) quando possibile, il **periodo di conservazione** dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
  - e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la **rettifica** o la **cancellazione** dei dati personali o la **limitazione del trattamento** dei dati personali che lo riguardano o di opporsi al loro trattamento;

Diritto di accesso dell'interessato /2

- f) il diritto di proporre reclamo a un'autorità di controllo;
- g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

- 2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

Diritto di rettifica

- Art. 16 RGPD
- L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Diritto alla cancellazione

- 1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
  - a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
  - b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
  - c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
  - d) i dati personali sono stati trattati illecitamente;
  - e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
  - f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

Modalità

- 2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della **tecnologia disponibile** e dei **costi di attuazione** adotta le **misure ragionevoli**, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

- Ragionevolezza = tecnologia disponibile + costi d'attuazione

Eccezioni

- esercizio del diritto alla libertà di espressione e di informazione;
- adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- per motivi di interesse pubblico nel settore della sanità pubblica;
- a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Diritto di limitazione del trattamento

- Art. 18 RGPD
- È possibile richiedere al titolare la limitazione del trattamento quando:
  - l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
  - il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
  - benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
  - l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Obbligo di notifica del titolare

- Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Diritto alla portabilità dei dati

- Art. 20 RGPD
- 1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso **comune** e **leggibile** da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento **senza impedimenti** da parte del titolare del trattamento cui li ha forniti qualora :
  - a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
  - b) il trattamento sia effettuato con mezzi automatizzati

Diritto di opposizione

- Art. 21 RGPD
- 1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la **profilazione** sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
- 2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.
- 3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

Diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato

- Art. 22 RGPD
- 1. L'interessato ha il diritto di non essere sottoposto a una decisione basata **unicamente** sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
- 2. Il paragrafo 1 non si applica nel caso in cui la decisione:
  - a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
  - b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
  - c) si basi sul consenso esplicito dell'interessato.

Sicurezza dei dati

- Art. 32 del Regolamento
- Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
  - la **pseudonimizzazione** e la **cifratura** dei dati personali;
  - la capacità di assicurare su base permanente la **riservatezza**, l'**integrità**, la **disponibilità** e la **resilienza** dei sistemi e dei servizi di trattamento;
  - la capacità di **ripristinare tempestivamente** la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
  - una **procedura** per **testare**, **verificare** e **valutare** regolarmente l'**efficacia** delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

La sicurezza nel Regolamento europeo

Fare clic per inserire il sottotitolo

Le misure tecniche e organizzative "adeguate" nel Regolamento 679/2016

- Ancora una volta si fa leva sull'*accountability* dei titolare.
- Non più parametri per individuarle ma "suggerimenti" non esaustivi quali:
  - pseudonimizzazione e cifratura;
  - assicurare su base permanente la riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento;
  - capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente;
  - una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative.

Pseudonimizzazione

- Art. 4 n. 5)
- "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".