REGOLAMENTO UE 2016/679

OBIETTIVI, ORGANIZZAZIONE, ADEMPIMENTI E ATTORI DEL NUOVO REGOLAMENTO UE 2016/679

Giovanni Cortelezzi giovanni@serviziinformatici.com

servizi informatici
software & consulenza

REGOLAMENTO UE 2016/679 Articolo **1**

1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Direttiva UE 2016/680 Articolo 1

1. La presente direttiva stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica.

2. Ai sensi della presente direttiva gli Stati membri:

   1) tutelano i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali; e
   2) garantiscono che lo scambio dei dati personali da parte delle autorità competenti all'interno dell'Unione, qualora tale scambio sia richiesto dal diritto dell'Unione o da quello dello Stato membro, non sia limitato né vietato per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

3. La presente direttiva non pregiudica la facoltà degli Stati membri di prevedere garanzie più elevate di quelle in essa stabilite per la tutela dei diritti e delle libertà dell'interessato con riguardo al trattamento dei dati personali da parte delle autorità competenti.

OBIETTIVI

- Rafforzamento dei diritti e dei doveri
- Sburocratizzazione
- Uniformità delle tutele

- Regolamento generale, non Direttiva
- Proattività Titolare/Rresponsabile
- Privacy by design Accountability
- Sportello unico (One-Stop-Shop)

IN SINTESI

- **«Accountability»**
  - proattività: approccio basato sul rischio del trattamento
  - privacy by design/default
  - valutazione di impatto
  - RPD/DPO
  - registro dei trattamenti
  - certificazione trattamenti/codici di condotta
- **Nuovi diritti interessati**: «oblio», limitazione, portabilità
- **Ruolo Autorità di controllo**: «sportello unico» e meccanismo di coerenza
- **Sistema sanzionatorio**: sanzioni tendenzialmente uniformi in Ue

REGOLAMENTO UE 2016/679

Accountability

parole chiave: Responsabilizzazione Rischio

Obbligo incombente su titolari

- **Fattori da considerare**: natura, ambito, contesto, finalità del trattamento + rischi per diritti e libertà fondamentali dell'interessato
- **Risultato**: misure tecniche e organizzative adeguate
- **Obiettivo**: garantire ed essere in grado di dimostrare Conformità → Documentabilità dei processi
- Permanente, NON una tantum

Strumenti e obblighi

privacy by design privacy by default	(art. 25)
misure di sicurezza	(art. 32) adeguate, in base al rischio, per obiettivi (riservatezza, integrità, disponibilità, resilienza) + processo di revisione continua → NO MISURE «MINIME»
valutazione di impatto privacy	(artt. 35-36) trattamenti a rischio elevato - consultazione preventiva Autorità → NO AUTORIZZAZIONE PREVENTIVA
designazione di un RPD/DPO	(artt. 37-39) criteri nomina, requisiti soggettivi, compiti (vigilanza DPIA, interfaccia con Autorità e interessati)
codici di condotta certificazione trattamenti	(artt. 40-43) strumenti per dimostrare la conformità
Contitolari e responsabili del trattamento	(artt. 26, 28) disciplina della contitolarità e rafforzamento obbligo di garanzie contrattuali fra titolare e responsabile (che può nominare direttamente sub-responsabili)
Registro delle attività di trattamento	(art. 30) importante ai fini della gestione protezione dati (esenzioni per PMI < 250 dipendenti)
Data breach	(artt. 33, 34) notifica violazioni di dati ad Autorità/agli interessati (criteri di soglia basati sul rischio)

ATTORI E RUOLI

- Titolare del trattamento
- Contitolare del trattamento
- Responsabile del trattamento
- Persone autorizzate al trattamento
- Responsabile della protezione dei dati
- Interessato

Titolare del trattamento (data controller)

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 (art. 4, par. 7) (**ed è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa)**

Co-Titolare del trattamento

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento (art 26)

Co-Titolarità

La disciplina della contitolarità del trattamento impone ai titolari di definire specificamente il rispettivo ambito di responsabilità e i compiti con particolare riguardo all’esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari che operano congiuntamente

• I contitolari determinano con accordo interno le rispettive responsabilità in merito all’osservanza degli obblighi, all’esercizio dei diritti dell’interessato e all’informativa

• L’accordo interno (nel contenuto essenziale) è messo a disposizione degli interessati

Responsabile del trattamento (data processor)

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4, par. 8; art. 28)

Il responsabile può nominare sub-responsabili per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e «responsabile primario»
Il «responsabile primario» risponde dinanzi al titolare dell'inadempimento del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento

Necessità di un contratto (o altro atto giuridico) che disciplini:
• materia e durata del trattamento;
• natura e finalità del trattamento;
• tipo di dati personali e categorie di interessati;
• obblighi e diritti del titolare del trattamento.

In base al contratto il responsabile si impegna a:

- trattare dati soltanto su istruzione documentata del titolare;
- consentire i trattamenti solo a persone autorizzate con impegno alla riservatezza che abbiano un adeguato obbligo legale di riservatezza;
- adottare tutte le misure di sicurezza (es. cifratura; pseudonimizzazione; recupero da backup);
- rispettare le condizioni per ricorrere a un sub-responsabile del trattamento;
- assistere il titolare per dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- cancellare o restituire tutti i dati e cancellare le copie esistenti;
- mettere a disposizione del titolare le informazioni per dimostrare il rispetto dei suddetti obblighi e consentire le ispezioni.

- *La Commissione può stabilire clausole contrattuali tipo per le materie oggetto del contratto tra titolare e responsabile*
- *L'autorità di controllo può adottare clausole contrattuali tipo per le materie oggetto del contratto tra titolare e responsabile, in conformità del meccanismo di coerenza di cui all'articolo 63*

Persone autorizzate al trattamento

È definito «terzo» la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia la persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile (art. 4, par. 10)

TRATTAMENTO SOTTO L'AUTORITÀ DEL TITOLARE O DEL RESPONSABILE (art. 29)
Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali **non può trattare tali dati se non è istruito** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri

SICUREZZA DEL TRATTAMENTO (art. 32, par. 4)
Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali **non tratti tali dati se non è istruito** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri

RESPONSABILE DELLA PROTEZIONE DEI DATI (art. 37, 38, 39; cons. 97)

La designazione del RPD è obbligatoria se:
• il trattamento è effettuato da autorità pubbliche o organismi pubblici (eccezione: Autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali)
• si svolgono trattamenti su larga scala
• monitoraggio regolare e sistematico degli interessati
• categorie particolari di dati personali (art. 9) e dati relativi a condanne penali e a reati (art. 10)

v. "Linee guida sui Responsabili della Protezione dei Dati (RPD)" del 13 dicembre 2016, del "Gruppo di lavoro art. 29",WP 243 rev. 01 Linee guida 5 aprile 2017
REGOLAMENTO 2016/679

Più autorità pubbliche o organismi pubblici possono designare un unico RPD tenuto conto delle dimensioni e della struttura organizzativa (art. 37, par. 3)
REGOLAMENTO 2016/679

Requisiti richiesti al Responsabile della Protezione dei Dati

- Qualità professionali (esperienza professionale, formazione specialistica, certificazioni, etc.)
- Conoscenza specialistica - Normativa e prassi in materia di protezione dati - disciplina di settore
- Capacità di assolvere i compiti previsti
- Autonomia e assenza di conflitto di interessi

Il Responsabile della Protezione dei Dati può essere:

- INTERNO: dipendente del Titolare del trattamento
- ESTERNO: contratto di servizio (professionista o società di consulenza)

GRAZIE PER L'ATTENZIONE

Giovanni Cortelezzi **giovanni@serviziinformatici.com**

Definizioni (Art. 4)

Articolo 4 - Ai fini del presente regolamento s'intende per:

1) «dato personale»: 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;

2) «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;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «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 situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) «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;

6) «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;

7) «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 sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «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;

9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «violazione dei dati personali»: la 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;

13) «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;

14) «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;

15) «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;

16) «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 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;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «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 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 imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:
a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
c) un reclamo è stato proposto a tale autorità di controllo;

23) «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;

24) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (19);

26) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

REGISTRO DEI TRATTAMENTI

Articolo 30 Registri delle attività di trattamento

1. Ogni titolare del trattamento e, se del caso, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
a) il nome e i dati di contatto del titolare del trattamento e, se del caso, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) se del caso, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle appropriate garanzie;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
2. Ogni responsabile del trattamento e, se del caso, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:
a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, se del caso, del responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) se del caso, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.
4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, se del caso, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.
5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

REGOLAMENTO UE 2016/679

Valutazione d´impatto sulla protezione dei dati

Articolo 35

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

………

Chi la deve fare: il Titolare del trattamento

Cosa deve fare (Art.35 paragrafo 7):

- Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- Una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- Una valutazione dei rischi per i diritti e le libertà degli interessati; e
- Le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento di cui si tratta, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.