# Le novità del Nuovo Regolamento Europeo in materia di privacy


Clusit
Education

# Agenda

- Gli obblighi di sicurezza previsti dalla normativa vigente
- Il nuovo Regolamento europeo

# GLI OBBLIGHI DI SICUREZZA PREVISTI DALLA NORMATIVA VIGENTE

# Misure di sicurezza idonee e preventive

## MISURE IDONEE

- I titolari del trattamento, al fine di **ridurre al minimo**, i rischi di:
  - distruzione o perdita, anche accidentale, dei dati
  - accesso non autorizzato ai dati
  - trattamento dei dati non consentito o non conforme alle finalità della raccolta

**DEVONO ADOTTARE MISURE DI SICUREZZA PREVENTIVE ED IDONEE A PROTEGGERE I DATI STESSI.**

L'adozione di tali misure è correlata:

- alla natura dei dati
- alle specifiche caratteristiche del trattamento
- al progresso tecnico

(art. 31 Codice della Privacy)

# Misure minime di sicurezza

**MISURE MINIME**

- I titolari del trattamento **sono comunque tenuti ad adottare** le **misure minime previste** dall'allegato B al d.lgs 196/2003 per i:

  a) **Trattamenti effettuati con l'ausilio di strumenti elettronici**

  b) **Trattamenti effettuati senza l'ausilio di strumenti elettronici**

(art. 33 Codice della Privacy)

# Misure minime di sicurezza

## a) Trattamenti effettuati con l'ausilio di strumenti elettronici

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

## b) Trattamenti effettuati senza l'ausilio di strumenti elettronici

- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

# Misure minime di sicurezza

| MISURE MINIME DI SICUREZZA - ALLEGATO B AL D.LGS 196/2003 | | |
|---|---|---|
| TRATTAMENTO DEI DATI PERSONALI EFFETTUATO CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI | | |
| | **TIPOLOGIA DI DATI A CUI APPLICARE LA MISURA** | **SPECIFICHE** |
| **Individuazione degli Incaricati** | Tutti | Per iscritto |
| **Sistema di autenticazione informatica** | Tutti | Applicare punti da 1 a 11 dell'allegato B al D.lgs 196/03 |
| **Attribuzione User-Id e Password a ciascun incaricato** | Tutti | Applicare il punto 2 dell'allegato B al D.lgs 196/03 |
| **Unicità User-Id** | Tutti | Individuale e non riutilizzato |
| **Password** | Tutti | Segreta<br>Min 8 caratteri<br>Non contiene riferimenti riconducibili all'incaricato |
| **Sostituzione Password** | Tutti | Autonoma<br>Al primo utilizzo<br>Dati comuni ogni sei mesi<br>Dati sensibili o giudiziari ogni tre mesi |
| **Istruzioni in merito alla custodia del personal computer** | Tutti | Per iscritto |

# Misure minime di sicurezza

| MISURE MINIME DI SICUREZZA - ALLEGATO B AL D.LGS 196/2003 | | |
|---|---|---|
| TRATTAMENTO DEI DATI PERSONALI EFFETTUATO CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI | | |
| | **TIPOLOGIA DI DATI A CUI APPLICARE LA MISURA** | **SPECIFICHE** |
| **Custodia delle credenziali di autenticazione**<br>**Accesso al computer dell'incaricato in caso di prolungata assenza o impedimento** | Tutti | Applicare il punto 10 dell'allegato B al D.lgs 196/03 |
| **Sistema di autorizzazione informatica** | Tutti | Applicare punti da 12 a 14 dell'allegato B al D.lgs 196/03 |
| **Aggiornamento almeno annuale dell'individuazione dell'ambito dei trattamenti consentiti ai singoli incaricati** | Tutti | Per iscritto |
| **Installazione Software antivirus** | Tutti | Semestrale |
| **Software di sicurezza** | Tutti | Aggiornamento annuale per dati comuni<br>Aggiornamenti semestrali per dati sensibili |
| **Backup** | Tutti | Settimanali |

# Misure aggiuntive

**MISURE AGGIUNTIVE**

Il Garante Privacy ha individuato

**ulteriori misure di sicurezza** che

**devono essere adottate in specifici settori**

per trattare dati.

# I provvedimenti del Garante

- Linee guida del Garante per posta elettronica e internet (2007)
- Provvedimento del Garante sugli Amministratori di Sistema (2008)
- Sicurezza dei dati di traffico telefonico e telematico (c.d. Data Retention) – (2008)
- Provvedimento generale prescrittivo in tema di biometria (2014)

# IL NUOVO REGOLAMENTO EUROPEO

# La rivoluzione privacy in Europa: cosa sta cambiando?

- **La Commissione Europea ha presentato una proposta per la tutela uniforme in materia di protezione dei dati personali:**
  - Il nuovo Regolamento UE sostituirà la direttiva 95/46/CE.
  - A differenza della direttiva, il Regolamento sarà legge direttamente applicabile in ogni Stato membro, quindi anche in Italia.
  - Il Codice Privacy ne sarà fortemente impattato.
  - La Privacy avrà regole comuni in tutti gli Stati membri
  - Alcune norme contenute nel Regolamento renderanno estremamente pesanti ed onerosi gli adempimenti per le imprese e gli enti.

# La rivoluzione privacy in Europa: cosa sta cambiando?

- Le norme nazionali che regolano la protezione dei dati personali nell'Unione Europea sono spesso numerose e costose; l'intento è quello di favorire la crescita economica.
- Il quadro legale oggi non consente alle aziende di approfittare di un mercato unico.
- In questo quadro «l'Europa è un pacthwork di legislazioni nazionali» che complica il lavoro delle imprese nel tentativo di espandersi all'estero.
- In Italia si è molto criticato, in passato, l'obbligo di redigere il DPS: se fossero confermati gli obblighi introdotti dal Regolamento sarebbero richiesti sforzi di compliance e di documentazione molto superiori.

# La rivoluzione privacy in Europa: cosa sta cambiando?

- **Il Comitato Scientifico dell'Istituto Italiano per la Privacy, ha evidenziato gli aspetti principali caratterizzanti questa operazione normativa:**
  - allargamento dell'ambito di applicazione delle norme privacy che in un prossimo futuro potranno tutelare le informazioni dei residenti europei anche se presenti in Internet o nel cloud computing.
  - sarà imposta alle imprese l'adozione di un vero modello organizzativo per la tutela dei dati, con l'introduzione del principio di responsabilità (accountability). In concreto, saranno le aziende a dover dimostrare la conformità del loro operato alle regole comunitarie, in caso di controlli.
  - infine, colpisce l'adozione di un impianto sanzionatorio di fonte comunitaria, a garanzia dell'efficacia di quanto prescritto, con livelli massimi di rilievo, parametrati al fatturato globale annuo dell'impresa penalizzata.

# La rivoluzione privacy in Europa: cosa sta cambiando?

- Gli operatori nazionali continueranno ad operare, applicando dei principi omogenei in ambito europeo. **Saranno previste più garanzie e più tutele per le persone fisiche:**

  - **Gli obiettivi infatti sono di garantire trasparenza e sicurezza**

  - **Attualmente il 72% dei cittadini europei ritieni di non aver il pieno controllo dei dati personali.**

# Iter legislativo ordinario


http://www.europarl.europa.eu/external/html/legislativeprocedure/default_it.htm

# Iter legislativo ordinario


http://www.europarl.europa.eu/external/html/legislativeprocedure/default_it.htm

# Iter legislativo ordinario

25 gennaio 2012

**Commissione europea**

presenta proposta di regolamento

al Parlamento ed al Consiglio

**TESTO UFFICIALE REPERIBILE ALLA URL**
**http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:IT:PDF**

# Iter legislativo ordinario

14 marzo 2014

**Parlamento**

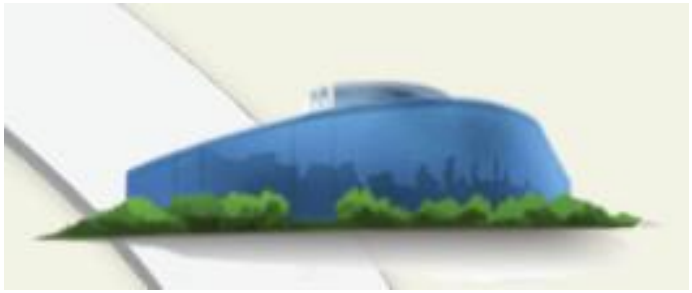
presenta al Consiglio

un testo emendato

**TESTO UFFICIALE REPERIBILE ALLA URL**
**http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//IT**

# Iter legislativo ordinario

11 giugno 2015

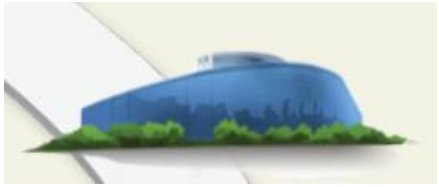


**Consiglio**

adotta un orientamento generale

**TESTO UFFICIALE REPERIBILE ALLA URL**
**http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/it/pdf**

# Iter legislativo ordinario



24 giugno 2015

**Parlamento, Commissione**

**e Consiglio**

avviano procedura di codecisione nota come "consultazione a tre" o "trilogo"

# La proposta di Regolamento UE

Articolo 22

**Responsabile del Trattamento**

Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità del rischio per i diritti e le libertà delle persone fisiche, **il responsabile del trattamento mette in atto opportune misure ed è in grado di dimostrare che il trattamento dei dati personali è effettuato conformemente al presente regolamento**.

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

L'adesione a **codici di condotta** approvati, ai sensi dell'articolo 38, **o un meccanismo di certificazione** approvato, ai sensi dell'articolo 39, può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del responsabile del trattamento.

# La proposta di Regolamento UE

Articolo 26

**Incaricato del Trattamento**

Il responsabile del trattamento **ricorre unicamente a incaricati del trattamento che presentino garanzie sufficienti per mettere in atto opportune misure tecniche ed organizzative in modo tale che il trattamento soddisfi i requisiti del presente regolamento**.

**L'incaricato del trattamento non ricorre ad un altro incaricato senza il previo consenso specifico o generale per iscritto del responsabile del trattamento**. In quest'ultimo caso l'incaricato del trattamento dovrebbe sempre informare il responsabile del trattamento di eventuali modifiche intenzionali riguardanti l'aggiunta o la sostituzione di altri incaricati del trattamento, dando così l'opportunità al responsabile del trattamento di obiettare a tali modifiche.

# La proposta di Regolamento UE

Articolo 26

**Incaricato del Trattamento**

**L'esecuzione dei trattamenti su commissione è disciplinata da un contratto o da altro atto giuridico** a norma del diritto dell'Unione o di uno Stato membro **che vincoli l'incaricato del trattamento al responsabile del trattamento**, in cui sono stipulati 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 e i diritti del responsabile del trattamento e che preveda in particolare che l'incaricato del trattamento:

a) tratti i dati personali soltanto su istruzione del responsabile del trattamento, salvo che lo richieda il diritto dell'Unione o dello Stato membro cui è soggetto l'incaricato del trattamento; in tal caso, l'incaricato del trattamento informa il responsabile del trattamento circa tale obbligo giuridico prima del trattamento dei dati, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) prenda tutte le misure richieste ai sensi dell'articolo 30;

c) rispetti le condizioni per ricorrere ad un altro incaricato del trattamento, come un requisito di autorizzazione preventiva specifica del responsabile del trattamento;

d) tenuto conto della natura del trattamento, assista il responsabile del trattamento nel dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

e) assista il responsabile del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 30 a 34;

f) restituisca o cancelli, a scelta del responsabile del trattamento, i dati personali al cessare della prestazione dei servizi di trattamento di dati precisati nel contratto o altro atto giuridico, salvo che il diritto dell'Unione o dello Stato membro cui è soggetto l'incaricato del trattamento preveda un requisito di conservazione dei dati;

g) metta a disposizione del responsabile del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca agli audit realizzati dal responsabile del trattamento.

# La proposta di Regolamento UE

Articolo 26

**Incaricato del Trattamento**

**L'incaricato del trattamento informa immediatamente il responsabile del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o le disposizioni dell'Unione o dello Stato membro concernenti la protezione dei dati**.

Fatto salvo un contratto individuale tra il responsabile del trattamento e l'incaricato del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 2 e 2 bis può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 2 ter e 2 quater o su clausole contrattuali tipo che sono parte di una certificazione concessa al responsabile del trattamento o all'incaricato del trattamento ai sensi degli articoli 39 e 39 bis.

La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 2 e 2 bis e in conformità della procedura d'esame di cui all'articolo 87, paragrafo 2.

Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 2 e 2 bis in conformità del meccanismo di coerenza di cui all'articolo 57.

Il contratto o altro atto giuridico cui si fa riferimento ai paragrafi 2 e 2 bis sono tenuti in forma scritta, anche in formato elettronico.

# La proposta di Regolamento UE

Articolo 23

**Protezione fin dalla progettazione e protezione di default**

Tenuto conto della tecnologia disponibile e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche della probabilità e della gravità del rischio per i diritti e le libertà delle persone fisiche costituite dal trattamento, i responsabili del trattamento mettono in atto **misure tecniche e organizzative adeguate** all'attività di trattamento in corso e ai suoi obiettivi, quali la **minimizzazione e la pseudonimizzazione dei dati**, in modo tale che il trattamento soddisfi i requisiti del presente regolamento e tuteli i diritti degli interessati.

Il responsabile del trattamento mette in atto opportune misure per **garantire che siano trattati, di default, solo i dati personali necessari per ogni specifica finalità del trattamento; ciò vale per la quantità dei dati raccolti, l'estensione del trattamento, il periodo di conservazione e la loro accessibilità**.
Quando il trattamento non è finalizzato a fornire informazioni al pubblico, detti meccanismi garantiscono che, **di default, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento umano**.

Un meccanismo di **certificazione** approvato ai sensi dell'articolo 39 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2

# La proposta di Regolamento UE

Articolo 30

**Misure di sicurezza**

Tenuto conto della tecnologia disponibile e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche della probabilità e della gravità del rischio per i diritti e le libertà delle persone fisiche, il responsabile del trattamento e l'incaricato del trattamento mettono in atto opportune **misure tecniche e organizzative quale la pseudonimizzazione dei dati personali per garantire un livello di sicurezza adeguato al rischio**.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei **rischi presentati da trattamenti di dati derivanti in particolare dalla distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso, in modo accidentale o illegale, a dati personali trasmessi, memorizzati o comunque elaborati**.

# La proposta di Regolamento UE

Articolo 30

**Misure di sicurezza**

L'adesione a **codici di condotta** approvati, ai sensi dell'articolo 38, o un meccanismo di certificazione approvato, ai sensi dell'articolo 39, può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1.

Il responsabile del trattamento e l'incaricato del trattamento fanno sì che chiunque agisca sotto l'autorità del responsabile del trattamento o dell'incaricato del trattamento e abbia accesso a dati personali **non tratti tali dati se non è istruito in tal senso** dal responsabile del trattamento, salvo che lo richieda il diritto dell'Unione o di uno Stato membro.

# La proposta di Regolamento UE

Articolo 31

**Notificazione delle violazioni di dati personali all'autorità di controllo**

In caso di **violazione dei dati personali suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche**, ad esempio discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto professionale o qualsiasi altro danno economico o sociale importante, **il responsabile del trattamento notifica la violazione all'autorità di controllo competente** ai sensi dell'articolo 51 **senza ritardo ingiustificato, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza. Qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo è corredata di una giustificazione motivata**.

La notifica prevista al paragrafo 1 non è richiesta se, ai sensi dell'articolo 32, paragrafo 3, lettere a) e b), non è richiesta una comunicazione all'interessato.

**L'incaricato del trattamento informa il responsabile del trattamento senza ingiustificato ritardo dopo aver accertato la violazione dei dati personali.**

# La proposta di Regolamento UE

Articolo 31

**Notificazione delle violazioni di dati personali all'autorità di controllo**

La notifica di cui al paragrafo 1 deve come minimo:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile e appropriato, le categorie e il numero di interessati approssimativi in questione nonché le categorie e il numero approssimativo di registrazioni dei dati in questione;
b) indicare l'identità e le coordinate di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le possibili conseguenze della violazione dei dati personali individuate dal responsabile del trattamento;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del responsabile del trattamento per porre rimedio alla violazione dei dati personali; e
e) ove opportuno, indicare le misure intese ad attenuare i possibili effetti pregiudizievoli della violazione dei dati personali.

Qualora e nella misura in cui non sia possibile fornire le informazioni di cui al paragrafo 3, lettere d), e) ed f), contestualmente alle informazioni di cui ai punti a) e b), il responsabile del trattamento trasmette dette informazioni senza ulteriore ingiustificato ritardo.

Il responsabile del trattamento documenta la violazione dei dati personali di cui ai paragrafi 1 e 2, incluse le circostanze in cui si è verificata, le sue conseguenze e i provvedimenti adottati per porvi rimedio. La documentazione deve consentire all'autorità di controllo di verificare il rispetto del presente articolo.

# La proposta di Regolamento UE

Articolo 32

**Comunicazione delle violazioni di dati personali all'autorità di controllo**

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ad esempio discriminazione, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, decifratura non autorizzata della pseudonimizzazione, perdita di riservatezza dei dati protetti da segreto professionale o qualsiasi altro danno economico o sociale importante, **il responsabile del trattamento comunica la violazione all'interessato senza ingiustificato ritardo**.

La comunicazione all'interessato di cui al paragrafo 1 descrive la natura della violazione dei dati personali e contiene almeno le informazioni e le raccomandazioni di cui all'articolo 31, paragrafo 3, lettere b), e) ed f).

Non è richiesta la comunicazione all'interessato ai sensi del paragrafo 1 se:
a. il responsabile del trattamento ha utilizzato le opportune misure tecnologiche ed organizzative di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; oppure
b. il responsabile del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c. detta comunicazione richiederebbe sforzi sproporzionati, in particolare a motivo del numero di casi in questione. In una simile circostanza, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia;
d. avrebbe ripercussioni negative su un interesse pubblico rilevante.

# La proposta di Regolamento UE

Articolo 33

**Valutazione d'impatto sulla protezione dei dati**

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, ad esempio discriminazione, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, decifratura non autorizzata della pseudonimizzazione, perdita di riservatezza dei dati protetti da segreto professionale o qualsiasi altro danno economico o sociale importante, **il responsabile del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto delle operazioni di trattamento previste sulla protezione dei dati personali**

**Il responsabile del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, chiede un parere al responsabile della protezione dei dati**, qualora ne sia designato uno.

# La proposta di Regolamento UE

Articolo 33

**Valutazione d'impatto sulla protezione dei dati**

La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei seguenti casi:
a) una valutazione sistematica e globale di aspetti della personalità degli interessati, basata sulla profilazione e da cui discendono decisioni che hanno effetti giuridici sugli interessati o incidono gravemente sugli interessati;
b) il trattamento di categorie particolari di dati personali ai sensi dell'articolo 9, paragrafo 1, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza, qualora i dati siano trattati per prendere decisioni su larga scala riguardanti persone fisiche;
c) la sorveglianza di zone accessibili al pubblico su larga scala, in particolare se effettuata mediante dispositivi ottico-elettronici.

L'autorità di controllo redige e rende pubblico un elenco delle tipologie di operazioni di trattamento soggette al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato europeo per la protezione dei dati.

L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di operazioni di trattamento per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato europeo per la protezione dei dati.

# La proposta di Regolamento UE

Articolo 33

**Valutazione d'impatto sulla protezione dei dati**

Prima di adottare gli elenchi di cui ai paragrafi 2 bis e 2 ter, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 57 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al controllo del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

La valutazione contiene almeno una descrizione generale delle operazioni di trattamento previste, una valutazione del rischio di cui al paragrafo 1, le misure previste per affrontare il rischio, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e dei legittimi interessi degli interessati e delle altre persone in questione.

Nella valutazione della liceità e dell'impatto del trattamento compiuto dai relativi responsabili o incaricati si tiene debito conto del rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 38, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

# La proposta di Regolamento UE

Articolo 33

**Valutazione d'impatto sulla protezione dei dati**

Il responsabile del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza delle operazioni di trattamento

Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il responsabile del trattamento è soggetto un fondamento giuridico attraverso un atto legislativo che disciplina l'operazione di trattamento specifica o l'insieme di operazioni in questione, i paragrafi 1, 2 e 3 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

# La proposta di Regolamento UE

Articolo 79

**Sanzioni amministrative**

Ogni autorità di controllo garantisce che le **sanzioni amministrative pecuniarie** irrogate ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui all'articolo 79 bis siano in ogni singolo caso **effettive, proporzionate e dissuasive**.

Le sanzioni amministrative pecuniarie sono irrogate, in funzione delle **circostanze di ogni singolo caso**, oltre alle misure di cui all'articolo 53, paragrafo 1 ter , lettere da a) a f) o in luogo di tali misure.

Al momento di decidere se irrogare una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

a) **la natura, la gravità e la durata della violazione considerate la natura, la portata o la finalità del trattamento** in questione nonché il **numero di interessati lesi dal danno e il livello del danno da essi subito**;

b) il **carattere doloso o colposo** della violazione;

c) le **misure prese dal responsabile del trattamento o dall'incaricato del trattamento per attenuare il danno** subito dagli interessati;

# La proposta di Regolamento UE

Articolo 79

**Sanzioni amministrative**

d) il **grado di responsabilità del responsabile del trattamento o dell'incaricato del trattamento** considerate le misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 23 e 30;

e) eventuali **precedenti violazioni** pertinenti commesse dal responsabile del trattamento o dall'incaricato del trattamento;

f) la **maniera in cui l'autorità di controllo ha preso conoscenza della violazione**, in particolare se e in che misura il responsabile del trattamento o l'incaricato del trattamento ha notificato la violazione;

h) qualora siano stati precedentemente imposti provvedimenti di cui all'articolo 53, paragrafo 1 ter , lettere a), d), e) e f), nei confronti del responsabile del trattamento o dell'incaricato del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

i) l'adesione ai codici di condotta approvati ai sensi dell'articolo 38 o ai meccanismi di certificazione approvati ai sensi dell'articolo 39;

j) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso.

# La proposta di Regolamento UE

Articolo 79

**Sanzioni amministrative**

**Ciascuno Stato membro può prevedere norme che dispongano se e in quale misura possano essere irrogate sanzioni amministrative pecuniarie a autorità pubbliche e organismi pubblici istituiti in tale Stato membro**.

# La proposta di Regolamento UE

Articolo 79 bis

**Sanzioni amministrative pecuniarie**

1. L'autorità di controllo può irrogare **sanzioni amministrative pecuniarie non superiori a 250 000 EUR** o, per le imprese, **allo 0,5 % del fatturato mondiale totale annuo dell'esercizio precedente**, al responsabile del trattamento che, con dolo o colpa:

- non risponde entro il termine di cui all'articolo 12, paragrafo 2 alle richieste dell'interessato;
- fa pagare un contributo in violazione dell'articolo 12, paragrafo 4, prima frase.

# La proposta di Regolamento UE

Articolo 79 bis

**Sanzioni amministrative pecuniarie**

2. L'autorità di controllo può irrogare **sanzioni amministrative pecuniarie non superiori a 500 000 EUR** o, per le imprese, **all'1 % del fatturato mondiale totale annuo dell'esercizio precedente**, al responsabile del trattamento o all'incaricato del trattamento che, con dolo o colpa:

- non fornisce le informazioni o fornisce informazioni incomplete o non fornisce le informazioni per tempo o in modo sufficientemente trasparente all'interessato, in violazione dell'articolo 12, paragrafo 3, e degli articoli 14 e 14 bis;
- non dà l'accesso all'interessato o non rettifica i dati personali, in violazione degli articoli 15 e 16;
- non cancella i dati personali in violazione del diritto alla cancellazione e "all'oblio" a norma dell'articolo 17, paragrafo 1, lettere a), b), d) oppure e);
- tratta dati personali in violazione del diritto di limitazione di trattamento a norma dell'articolo 17 bis oppure non informa l'interessato prima che la limitazione di trattamento sia revocata a norma dell'articolo 17 bis, paragrafo 4;

# La proposta di Regolamento UE

Articolo 79 bis

**Sanzioni amministrative pecuniarie**

- non comunica a ciascuno dei destinatari cui il responsabile del trattamento ha trasmesso i dati personali le eventuali rettifiche, cancellazioni o limitazioni di trattamento, in violazione dell'articolo 17 ter;
- non fornisce all'interessato i dati personali che lo riguardano in violazione dell'articolo 18;
- tratta i dati personali dopo l'obiezione da parte dell'interessato a norma dell'articolo 19, paragrafo 1, e non dimostra l'esistenza di motivi legittimi preminenti 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;
- non fornisce all'interessato informazioni relative al diritto di opporsi al trattamento per finalità di marketing diretto a norma dell'articolo 19, paragrafo 2 o continua a trattare i dati per finalità di marketing diretto dopo l'obiezione da parte dell'interessato in violazione dell'articolo 19, paragrafo 2 bis;
- omette di determinare o non determina in modo sufficiente le rispettive responsabilità dei corresponsabili del trattamento, in violazione dell'articolo 24;
- omette di conservare o non conserva in modo sufficiente la documentazione di cui all'articolo 28 e all'articolo 31, paragrafo 4.

# La proposta di Regolamento UE

Articolo 79 bis

**Sanzioni amministrative pecuniarie**

3. L'autorità di controllo può irrogare **sanzioni amministrative pecuniarie non superiori a 1 000 000 EUR** o, per le imprese, al **2 % del fatturato mondiale totale annuo dell'esercizio precedente**, al responsabile del trattamento o all'incaricato del trattamento che, con dolo o colpa:

- tratta dati personali senza una base giuridica a tal fine o non rispetta le condizioni relative al consenso, in violazione degli articoli 6, 7, 8 e 9;
- non rispetta le condizioni relative al processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione di cui all'articolo 20;
- non attua misure adeguate o non è in grado di dimostrare la conformità del trattamento, in violazione degli articoli 22 e 30;
- non designa un rappresentante, in violazione dell'articolo 25; tratta o dà istruzione di trattare dati personali in violazione dell' articolo 26;
- omette di allertare o notificare all'autorità di controllo o all'interessato una violazione di dati personali, oppure non la notifica [tempestivamente o] integralmente, in violazione degli articoli 31 e 32;

# La proposta di Regolamento UE

Articolo 79 bis

**Sanzioni amministrative pecuniarie**

- non effettua una valutazione d'impatto sulla protezione dei dati in violazione dell'articolo 33 o tratta dati personali senza la consultazione preventiva dell'autorità di controllo, in violazione dell'articolo 34, paragrafo 2;
- fa un uso illecito di un sigillo o marchio di protezione dei dati di cui all'articolo 39 o non rispetta le condizioni e le procedure di cui agli articoli 38 bis e 39 bis;
- effettua o dà istruzione di effettuare un trasferimento di dati a un destinatario in un paese terzo o un'organizzazione internazionale in violazione degli articoli da 41 a 44;
- non si conforma a un ordine, a una limitazione provvisoria o definitiva di trattamento o a un ordine di sospensione dei flussi di dati dell'autorità di controllo, di cui all'articolo 53, paragrafo 1, o non dà l'accesso in violazione dell'articolo 53, paragrafo 2.

# La proposta di Regolamento UE

Articolo 79 bis

**Sanzioni amministrative pecuniarie**

**Se un responsabile del trattamento o un incaricato del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento elencate nei paragrafi 1, 2 o 3, l'importo totale della sanzione amministrativa pecuniaria non può superare l'importo precisato per la violazione più grave**

# La proposta di Regolamento UE

Articolo

**Sanzioni penali**

Per le violazioni del presente regolamento, in particolare per violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 79 bis, **gli Stati membri determinano le sanzioni per violazione di tali disposizioni e prendono tutti i provvedimenti necessari per la loro applicazione. Tali sanzioni sono effettive, proporzionate e dissuasive**.

**Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate** ai sensi del paragrafo 1 entro la data di cui all'articolo 91, paragrafo 2, **e comunica senza ritardo ogni successiva modifica**.

Gli Stati membri possono astenersi dal prevedere norme relative alle sanzioni amministrative pecuniarie a norma dell'articolo 79 bis, paragrafi 1, 2 e 3 se il loro sistema giudiziario non le prevede e le violazioni ivi enumerate sono già soggette a sanzioni penali nella loro legislazione nazionale entro [data di cui all'articolo 92, paragrafo 2], **assicurandosi nel contempo che tali sanzioni penali siano effettive, proporzionate e dissuasive in considerazione del livello di sanzioni amministrative pecuniarie previste dal presente regolamento**.
In questo caso, gli Stati membri comunicano alla Commissione le pertinenti norme di diritto penale.

# Il Data Protection Officer

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 35<br>**Designazione del Responsabile della protezione dei dati** | 1. Il responsabile del trattamento e l'incaricato del trattamento **designano sistematicamente** un responsabile della protezione dei dati quando:<br>a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, oppure<br>b) il trattamento è effettuato da un'impresa con 250 o più dipendenti, oppure<br>c) le attività principali del responsabile del trattamento o dell'incaricato del trattamento consistono in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il controllo regolare e sistematico degli interessati.<br><br>2. Nei casi di cui al paragrafo 1, lettera b), **un gruppo di imprese** può nominare **un unico responsabile** della protezione dei dati. | 1. Il responsabile del trattamento **o** l'incaricato del trattamento **possono designare** o, **se previsto dal diritto dell'Unione o degli Stati membri, designano** (…) un responsabile della protezione dei dati.<br><br>2. Un **gruppo di imprese** può nominare un **unico responsabile** della protezione dei dati. |

# Il Data Protection Officer

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 35<br>**Designazione del Responsabile della protezione dei dati** | 3. Qualora il responsabile del trattamento o l'incaricato del trattamento sia un'autorità pubblica o un organismo pubblico, **il responsabile della protezione dei dati può essere designato per più enti**, tenuto conto della struttura organizzativa dell'autorità pubblica o dell'organismo pubblico.<br><br>4. Nei **casi diversi** da quelli di cui al paragrafo 1, il responsabile del trattamento, l'incaricato del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di responsabili del trattamento o di incaricati del trattamento **possono designare un responsabile della protezione dei dati**. | 3. Qualora il responsabile del trattamento o l'incaricato del trattamento sia un'autorità pubblica o un organismo pubblico, un **unico responsabile della protezione dei dati** può essere designato per **più autorità pubbliche o organismi pubblici**, tenuto conto della loro struttura organizzativa e dimensione.<br><br>4. (…). |

# Il Data Protection Officer

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 35<br>**Designazione del Responsabile della protezione dei dati** | 5. Il responsabile del trattamento o l'incaricato del trattamento designa il responsabile della protezione dei dati **in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, e della capacità di adempiere ai compiti di cui all'articolo 37**. Il livello necessario di conoscenza specialistica **è determinato in particolare in base al trattamento di dati effettuato e alla protezione richiesta per i dati personali trattati** dal responsabile del trattamento o dall'incaricato del trattamento. | 5. Il (…) responsabile della protezione dei dati è designato **in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, e della capacità di adempiere ai compiti di cui all'articolo 37**, in particolare **l'assenza di conflitto di interessi**. (…). |

# Il Data Protection Officer

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 35<br>**Designazione del Responsabile della protezione dei dati** | 6. Il responsabile del trattamento o l'incaricato del trattamento si assicura che ogni altra funzione professionale del responsabile della protezione dei dati **sia compatibile con i compiti e le funzioni dello stesso in qualità di responsabile della protezione dei dati e non dia adito a conflitto di interessi**.<br><br>7. Il responsabile del trattamento o l'incaricato del trattamento designa un responsabile della protezione dei dati **per un periodo di almeno due anni. Il mandato del responsabile della protezione dei dati è rinnovabile**. Durante il mandato può essere destituito solo se non soddisfa più le condizioni richieste per l'esercizio delle sue funzioni. | 6. (…)<br><br>7. (…). Durante il mandato il responsabile della protezione dei dati può essere destituito, **oltre che per gravi motivi i quali, a norma del diritto dello Stato membro interessato, giustifichino la destituzione di un dipendente o di un funzionario pubblico**, solo se non soddisfa più le condizioni richieste per l'esercizio delle sue funzioni a norma dell'articolo |

# Il Data Protection Officer

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 35<br>**Designazione del Responsabile della protezione dei dati** | 8. Il responsabile della protezione dei dati può essere **assunto** dal responsabile del trattamento o dall'incaricato del trattamento **oppure adempiere ai suoi compiti in base a un contratto di servizi**.<br><br>9. Il responsabile del trattamento o l'incaricato del trattamento **comunica il nome e le coordinate di contatto del responsabile della protezione dei dati all'autorità di controllo e al pubblico**.<br><br>10. Gli interessati hanno il diritto di **contattare** il responsabile della protezione dei dati **per tutte le questioni relative al trattamento dei loro dati personali e presentare richieste per esercitare i diritti riconosciuti dal presente regolamento**. | 8. Il responsabile della protezione dei dati **può essere un membro del personale** del responsabile del trattamento o dell'incaricato del trattamento oppure **adempiere ai suoi compiti in base a un contratto di servizi**.<br><br>9. Il responsabile del trattamento o l'incaricato del trattamento **pubblica le coordinate di contatto del responsabile della protezione dei dati e le comunica all'autorità di controllo (…).**<br><br>10. Gli interessati possono **contattare** il responsabile della protezione dei dati **per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti riconosciuti dal presente regolamento**. |

# Il Data Protection Officer

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 35<br>**Designazione del Responsabile della protezione dei dati** | 11. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 86 al fine di **precisare i criteri e i requisiti concernenti le attività principali del responsabile del trattamento o dell'incaricato del trattamento** di cui al paragrafo 1, lettera c), e **i criteri relativi alle qualità professionali del responsabile della protezione dei dati** di cui al paragrafo 5. | 11. (…) |

# Il Data Protection Officer

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 36<br>**Posizione del responsabile della protezione dei dati** | 1. Il responsabile del trattamento o l'incaricato del trattamento si assicura che il responsabile della protezione dei dati **sia prontamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali**.<br><br>2. Il responsabile del trattamento o l'incaricato del trattamento **si assicura che il responsabile della protezione dei dati adempia alle funzioni e ai compiti in piena indipendenza e non riceva alcuna istruzione per quanto riguarda il loro esercizio. Il responsabile della protezione dei dati riferisce direttamente ai superiori gerarchici del responsabile del trattamento o dell'incaricato del trattamento.** | 1. Il responsabile del trattamento o l'incaricato del trattamento si assicura che il responsabile della protezione dei dati sia **prontamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.**<br><br>2. Il responsabile del trattamento o l'incaricato del trattamento **sostiene il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 37 fornendogli (…) le risorse necessarie per adempiere a tali compiti nonché l'accesso ai dati personali e alle operazioni di trattamento.** |

# Il Data Protection Officer

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 36<br>**Posizione del responsabile della protezione dei dati** | 3. Il responsabile del trattamento o l'incaricato del trattamento **sostiene il responsabile della protezione dei dati nell'esecuzione dei suoi compiti e gli fornisce personale, locali, attrezzature e ogni altra risorsa necessaria per adempiere alle funzioni e ai compiti di cui all'articolo 37.** | 3. Il responsabile del trattamento o l'incaricato del trattamento **si assicura che il responsabile della protezione dei dati possa agire in maniera indipendente nell'adempimento dei propri compiti e non riceva alcuna istruzione per quanto riguarda il loro esercizio**. Il responsabile della protezione dei dati **non è penalizzato dal responsabile del trattamento o dall'incaricato del trattamento per l'adempimento dei propri compiti**. **Il responsabile della protezione dei dati riferisce direttamente ai massimi superiori gerarchici del responsabile del trattamento o dell'incaricato del trattamento.**<br><br>4. Il responsabile della protezione dei dati **può svolgere altri compiti e funzioni**. Il responsabile del trattamento o l'incaricato del trattamento **si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.** |

# Il Data Protection Officer

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 37<br>**Compiti del Responsabile della protezione dei dati** | 1. Il responsabile del trattamento o l'incaricato del trattamento conferisce al responsabile della protezione dei dati almeno i seguenti compiti:<br><br>a) **informare e consigliare** il responsabile del trattamento o l'incaricato del trattamento in merito **agli obblighi derivanti dal presente regolamento e conservare la documentazione relativa a tale attività e alle risposte ricevute**;<br><br>b) sorvegliare l'attuazione e l'applicazione delle **politiche del responsabile del trattamento o dell'incaricato del trattamento in materia di protezione dei dati personali**, compresi l'attribuzione delle responsabilità, la formazione del personale che partecipa ai trattamenti e gli audit connessi; | 1. Il (…) responsabile della protezione dei dati è (...) incaricato delle seguenti funzioni:<br><br>a) **informare e consigliare** il responsabile del trattamento o l'incaricato del trattamento **nonché i dipendenti che trattano dati personali** in merito **agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati** (…);<br><br>b) sorvegliare **l'osservanza del presente regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati** nonché delle **politiche del responsabile del trattamento o dell'incaricato 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 gli audit connessi; |

# Il Data Protection Officer

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 37<br>**Compiti del Responsabile della protezione dei dati** | c) sorvegliare **l'attuazione e l'applicazione del presente regolamento**, **con particolare riguardo ai requisiti concernenti la protezione fin dalla progettazione, la protezione di default, la sicurezza dei dati, l'informazione dell'interessato e le richieste degli interessati di esercitare i diritti riconosciuti dal presente regolamento**;<br><br>d) garantire **la conservazione della documentazione** di cui all'articolo 28;<br><br>e) controllare **che le violazioni dei dati personali siano documentate, notificate e comunicate ai sensi degli articoli** 31 e 32;<br><br>f) controllare **che il responsabile del trattamento o l'incaricato del trattamento effettui la valutazione d'impatto sulla protezione dei dati e richieda l'autorizzazione preventiva o la consultazione preventiva** nei casi previsti dagli articoli 33 e 34; | c) (...)<br><br>d) (...)<br><br>e) (...)<br><br>f) fornire, se richiesto, **un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento** ai sensi dell'articolo 33; |

# Il Data Protection Officer

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 37<br>**Compiti del Responsabile della protezione dei dati** | g) controllare che **sia dato seguito alle richieste dell'autorità di controllo** e, nell'ambito delle sue competenze, **cooperare con l'autorità di controllo** di propria iniziativa o su sua richiesta;<br><br>h) fungere **da punto di contatto per l'autorità di controllo** per questioni connesse al trattamento e, se del caso, **consultare l'autorità di controllo di propria iniziativa**. | g) controllare che **sia dato seguito alle richieste dell'autorità di controllo** e, nell'ambito delle sue competenze, **cooperare con l'autorità di controllo** di propria iniziativa o su sua richiesta;<br><br>h) fungere **da punto di contatto per l'autorità di controllo** per questioni connesse al trattamento di dati personali, tra cui **la consultazione preventiva** di cui all'articolo 34 e, se del caso, **effettuare consultazioni su qualunque altra questione**. |

# Il Data Protection Officer

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 37<br>**Compiti del Responsabile della protezione dei dati** | 2. Alla Commissione è conferito il potere di adottare **atti delegati** conformemente all'articolo 86 al fine di precisare **i criteri e i requisiti concernenti i compiti, la certificazione, lo status, i poteri e le risorse del responsabile della protezione** dei dati di cui al paragrafo 1. | 2. (...)<br><br>2 bis. Nell'eseguire i propri compiti il responsabile della protezione dei dati **considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento**. |

# La Certificazione

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 39<br>**Certificazione** | 1. Gli Stati membri e la Commissione **incoraggiano**, in particolare a livello europeo, **l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati garantito** dai responsabili del trattamento e dagli incaricati del trattamento. I meccanismi di certificazione della protezione dei dati **contribuiscono alla corretta applicazione del presente regolamento, in funzione delle specificità settoriali e dei diversi trattamenti**. | 1. Gli Stati membri, **il comitato europeo per la protezione dei dati** e la Commissione incoraggiano, in particolare a livello unionale, **l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento delle operazioni di trattamento effettuate** dai responsabili del trattamento e dagli incaricati del trattamento. Si tiene conto delle **esigenze specifiche delle micro, piccole e medie imprese.** |

# La Certificazione

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 39<br>**Certificazione** | | **1 bis.** I meccanismi, i sigilli e i marchi approvati ai sensi del paragrafo 2 bis, **oltre ad essere stabiliti affinché vengano applicati** dai responsabili del trattamento e dagli incaricati del trattamento **soggetti al presente regolamento**, possono essere stabiliti anche **al fine di dimostrare la previsione di adeguate garanzie** da parte dei responsabili del trattamento o incaricati del trattamento **non soggetti al presente regolamento ai sensi dell'articolo 3, nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali** alle condizioni di cui all'articolo 42, paragrafo 2, lettera e). Detti responsabili del trattamento o incaricati del trattamento assumono **l'impegno vincolante ed esecutivo, mediante strumenti contrattuali o di altro genere, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati**. |

# La Certificazione

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 39<br>**Certificazione** | 2. Alla **Commissione** è conferito il potere di adottare **atti delegati** conformemente all'articolo 86 **al fine di precisare i criteri e i requisiti concernenti i meccanismi di certificazione della protezione dei dati** di cui al paragrafo 1, comprese le condizioni di rilascio e ritiro e i requisiti per il riconoscimento nell'Unione e in paesi terzi. | 2. La **certificazione** ai sensi del presente articolo **non riduce la responsabilità** del responsabile del trattamento o dell'incaricato del trattamento **riguardo alla conformità al presente regolamento** e **lascia impregiudicati le funzioni e i poteri dell'autorità di controllo competente** a norma dell'articolo 51 o 51 bis.<br><br>2 bis. La **certificazione** ai sensi del presente articolo è rilasciata **dagli organismi di certificazione** di cui all'articolo 39 bis o, se del caso, **da parte dell'autorità di controllo competente** in base ai **criteri** approvati **dall'autorità di controllo competente** o, ai sensi dell'articolo 57, **dal comitato europeo per la protezione dei dati**. |

# La Certificazione

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 39<br>**Certificazione** | 3. La Commissione può stabilire **norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscere i meccanismi di certificazione e i sigilli e marchi di protezione dei dati**. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 87, paragrafo 2. | 3. Il responsabile del trattamento o l'incaricato del trattamento che sottopone il trattamento effettuato al meccanismo di certificazione **trasmette all'organismo di certificazione** previsto all'articolo 39 bis o, se del caso, **all'autorità di controllo competente tutte le informazioni e gli consente l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione.**<br><br>4. La certificazione viene rilasciata al responsabile del trattamento o incaricato del trattamento **per un periodo massimo di 3 anni e può essere rinnovata alle stesse condizioni purché continuino ad essere soddisfatti i requisiti pertinenti**. Viene **revocata dagli organismi di certificazione** di cui all'articolo 39 bis o, se del caso, **dall'autorità di controllo competente**, **qualora non siano o non siano più soddisfatte i requisiti pertinenti.**<br><br>5. Il comitato europeo per la protezione dei dati **raccoglie in un registro tutti i meccanismi di certificazione e i sigilli** di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato, ad esempio tramite il portale europeo della giustizia elettronica. |

# La Certificazione

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 39 bis **Organismo di certificazione e relativa procedura** | | 1. Fatti salvi le funzioni e i poteri dell'autorità di controllo competente, di cui agli articoli 52 e 53, la certificazione viene rilasciata e rinnovata **da un organismo di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati**. Ogni Stato membro stabilisce se tali organismi di certificazione siano accreditati:<br>a) **dall'autorità di controllo competente** ai sensi dell'articolo 51 o 51 bis, e/o<br>b) **dall'organismo nazionale di accreditamento** designato in virtù del regolamento (CE) 765/2008 del Parlamento europeo e del Consiglio che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti conformemente alla norma EN-ISO/IEC 17065/2012 **e ai requisiti aggiuntivi stabiliti dall'autorità controllo competente** ai sensi dell'articolo 51 o 51 bis. |

# La Certificazione

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 39 bis **Organismo di certificazione e relativa procedura** | | 2. L'organismo di certificazione di cui al paragrafo 1 può essere accreditato a tal fine solo se:<br>a) riguardo al contenuto della certificazione ha **dimostrato in modo convincente alla competente autorità di controllo di essere indipendente e competente**;<br>a bis) **si è impegnato a rispettare i criteri di cui al paragrafo 2 bis dell'articolo 39** e approvati dall'autorità di controllo competente ai sensi dell'articolo 51 o 51 bis o, ai sensi dell'articolo 57, dal comitato europeo di protezione dei dati;<br>b) ha istituito **procedure per il rilascio, il riesame periodico e il ritiro dei sigilli e dei marchi di protezione dei dati**;<br>c) ha istituito **procedure** e strutture atte a trattare **i reclami concernenti violazioni della certificazione o il modo in cui la certificazione è stata o è attuata** dal responsabile del trattamento o dall'incaricato del trattamento ed ha gli strumenti necessari a rendere dette procedure e strutture trasparenti per gli interessati e il pubblico;<br>d) dimostra **in modo convincente per l'autorità di controllo competente che i compiti e le funzioni da esso svolti non danno adito a conflitto di interessi**. |

# La Certificazione

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 39 bis **Organismo di certificazione e relativa procedura** | | 3. L'accreditamento degli organi di certificazione di cui al paragrafo 1 **ha luogo in base ai criteri approvati dall'autorità di controllo competente** ai sensi dell'articolo 51 o 51 bis o, ai sensi dell'articolo 57, **dal comitato europeo di protezione dei dati**. In caso di accreditamento ai sensi del paragrafo 1, lettera b), tali requisiti integrano quelli previsti dal regolamento 765/2008 nonché **le norme tecniche che definiscono i metodi e le procedure degli organismi di certificazione**.<br><br>4. **L'organismo di certificazione** di cui al paragrafo 1 è **responsabile della corretta valutazione che comporta la certificazione o la revoca di quest'ultima**, fatta salva la responsabilità del responsabile del trattamento o dell'incaricato del trattamento riguardo alla conformità al presente regolamento. **L'accreditamento è rilasciato per un periodo massimo di 5 anni e può essere rinnovato alle stesse condizioni purché l'organismo soddisfi i requisiti.**<br><br>5. **L'organismo di certificazione** di cui al paragrafo 1 **trasmette all'autorità di controllo competente i motivi del rilascio o della revoca della certificazione richiesta.** |

# La Certificazione

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 39 bis **Organismo di certificazione e relativa procedura** | | 6. I **requisiti** di cui al paragrafo 3 e i criteri di cui al paragrafo 2 bis dell'articolo 39 **sono resi pubblici dall'autorità di controllo in forma facilmente accessibile**. Le autorità di controllo provvedono a **trasmetterli anche al comitato europeo per la protezione dei dati**. Il **comitato europeo per la protezione dei dati raccoglie in un registro tutti i meccanismi di certificazione e i sigilli di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato,** ad esempio tramite il portale europeo della giustizia elettronica.<br><br>6 bis. Fatte salve le disposizioni del capo VIII, **l'autorità di controllo competente o l'organismo nazionale di accreditamento revoca l'accreditamento rilasciato all'organismo di certificazione**, di cui al paragrafo 1, **se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate dall'organismo non sono conformi al presente regolamento**.<br><br>7. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 86 **al fine di precisare i criteri e i requisiti da tenere conto per i meccanismi di certificazione della protezione dei dati** di cui al paragrafo 1 (…). |

# La Certificazione

| | Testo Commissione Europea | Testo Consiglio dei Ministri |
|---|---|---|
| Art. 39 bis<br>**Organismo di certificazione e relativa procedura** | | 7 bis. **Il comitato europeo per la protezione dei dati fornisce alla Commissione pareri sui criteri e i requisiti** di cui al paragrafo 7.<br><br>8. La **Commissione può stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscere i meccanismi di certificazione e i sigilli e marchi di protezione dei dati**. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 87, paragrafo 2. |

# Grazie per l’attenzione!