Il nuovo Regolamento europeo sulla protezione dei dati personali

ITASEC19 - Pisa, 12 febbraio 2019

Ing. Dorotea Alessandra de Marco

Ing. Marco Coppotelli

Garante per la protezione dei dati personali
Dipartimento tecnologie digitali e sicurezza informatica

Agenda

- GDPR: elementi di continuità e principali novità
- Accountability di titolari e responsabili
- Diritti degli interessati
- Sicurezza del trattamento
- Gestione dei data breach
- Certificazioni e codici di condotta

GDPR: elementi di continuità e principali novità (1/2)

Elemento	Direttiva 95/46/CE	Regolamento (UE) 2016/679
Relazione titolare-interessato	bipolare	multipolare
Estensione geografica	nazionale	sovranazionale
Quadro giuridico	prevalentemente prescrittivo	valutazione del rischio
Costi	elevati	commodity
Controllo	enforcement	accountability

GDPR: elementi di continuità e principali novità (2/2)

Attori del trattamento (titolare, responsabile, interessato)

Presupposti di liceità (consenso, contratto, interesse vitale, obbligo di legge, interesse pubblico, interesse legittimo)

Requisiti di qualità dei dati/dei trattamenti

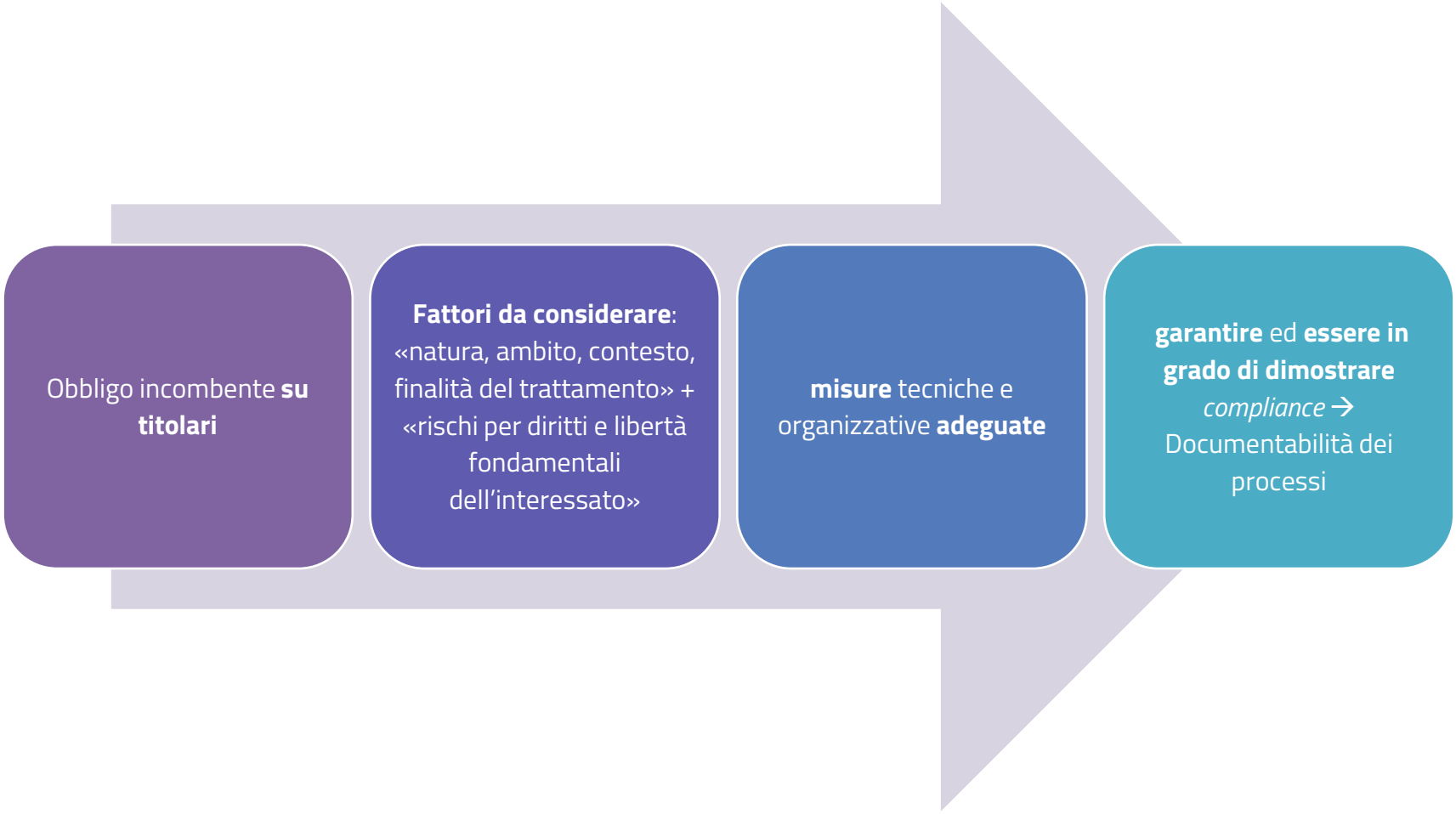
Approccio a dati sensibili e giudiziari (estensione a dati biometrici e genetici)

Informativa sul trattamento dei dati personali

Diritti dell'interessato

Trasferimento dei dati verso Paesi terzi (decisione di adeguatezza o garanzie adeguate di natura contrattuale o pattizia, quali binding corporate rules, clausole contrattuali tipo o ad-hoc, codici di condotta, certificazioni)

Accountability di titolari e responsabili (1/4)



Accountability di titolari e responsabili (2/4)
Data protection officer

Designazione

Obbligatoria
(pubbliche amministrazioni, monitoraggio regolare e sistematico su larga scala, trattamenti su larga scala di categorie particolari di dati o di dati giudiziari)

Sulla base di una valutazione del rischio

Caratteristiche

Trasparenza (noto all'autorità e agli interessati)

Indipendenza

Autorevolezza

Competenze manageriali

Qualità professionali

Risorse necessarie per assolvere compiti

Compiti

Consulenza al titolare o al responsabile del trattamento

Sorveglianza sul rispetto del GDPR

Parere su DPIA

Cooperazione con DPA

Punto di contatto con le DPA e con gli interessati

Accountability di titolari e responsabili (3/4)

Data protection impact assessment

Procedura che mira a descrivere un trattamento di dati per valutarne la **necessità** e la **proporzionalità** nonché i relativi **rischi**, allo scopo di approntare misure idonee ad affrontarli

Perché?

- strumento di accountability
- aiuta il titolare a rispettare le prescrizioni del RGPD e ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni
- permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali

Quando?

- in tutti i casi in cui un trattamento presenta un rischio elevato
- prima di procedere al trattamento
- riesame continuo della DPIA a intervalli regolari

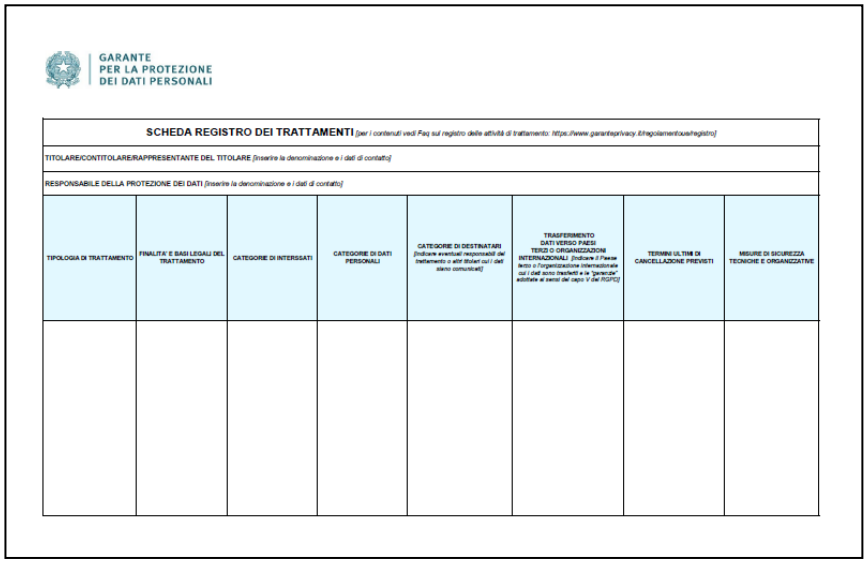
Chi?

- responsabilità del titolare
- conduzione materiale può essere affidata a un altro soggetto, interno o esterno
- titolare monitora lo svolgimento consultandosi con il DPO, il responsabile della sicurezza dei sistemi informativi e il responsabile IT

Accountability di titolari e responsabili (4/4)
Registro delle attività di trattamento

Registro dei trattamenti

- strumento per avere un quadro aggiornato dei trattamenti e per la valutazione e analisi del rischio
- parte integrante di un sistema di corretta gestione dei dati personali
- forma scritta, anche elettronica
- esibito su richiesta al Garante



GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*

TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*

RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*

TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASI LEGALI DEL TRATTAMENTO	CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e la "garanzia" adottata ai sensi del capo V del RGPD]*	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

Diritti degli interessati
Alcune delle principali novità

Cancellazione / Oblio

- diritto alla cancellazione dei propri dati personali in forma rafforzata
- obbligo per i titolari di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati
- limitazioni (es. accertamento, esercizio o difesa di un diritto in sede giudiziaria)

Limitazione al trattamento

- sospensione temporanea del trattamento in corso
- diverso e più ampio rispetto al «blocco» del trattamento (es. in attesa della rettifica dei dati, o in caso di opposizione al trattamento)
- necessità di «contrassegnare» i dati personali memorizzati

Portabilità

- diritto di ottenere i dati forniti in un formato interoperabile e di trasferirli ad altro titolare (o di farli trasferire direttamente da titolare iniziale)
- rispetto di presupposti specifici (solo a dati trattati con il consenso dell'interessato o sulla base di un contratto, dati forniti dall'interessato)

Sicurezza del trattamento (1/5)
Misure tecniche e organizzative

Principi applicabili (integrità e riservatezza)

Garanzia di trattamento conforme (responsabilità del titolare del trattamento)

Data protection by design e by default (protezione dei dati fin dalla progettazione e protezione per impostazione predefinita)

Scelta del responsabile del trattamento (soggetto che fornisce "garanzie sufficienti" per mettere in atto misure tecniche e organizzative adeguate)

Sicurezza del trattamento (2/5)
Approccio basato sul rischio

Sicurezza del trattamento (3/5)
Alcune misure di sicurezza indicate dal GDPR

Pseudonimizzazione e **cifratura** dei dati personali

Capacità di assicurare su base permanente la **riservatezza**, **l'integrità**, la **disponibilità** e la **resilienza** dei sistemi e dei servizi di trattamento

Capacità di **ripristinare** tempestivamente la **disponibilità** e **l'accesso** dei dati personali in caso di incidente fisico o tecnico

Procedure per **testare, verificare e valutare regolarmente** l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

Sicurezza del trattamento (4/5)
Rischi da tenere in considerazione

Nel valutare l'adeguato livello di sicurezza

si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare

- distruzione
- perdita
- modifica
- divulgazione non autorizzata
- accesso, accidentale o illegale

a dati personali trasmessi, conservati o comunque trattati

Sicurezza del trattamento (5/5)
Data protection by design e by default

Data protection by design

Misure volte a integrare nel trattamento le tutele per gli interessati

Elementi da considerare
(natura, ambito di applicazione, contesto e finalità del trattamento, rischi potenziali per i diritti e le libertà degli interessati, stato dell'arte, costi di attuazione)

Minimizzazione e pseudonimizzazione dei dati

Data protection by default

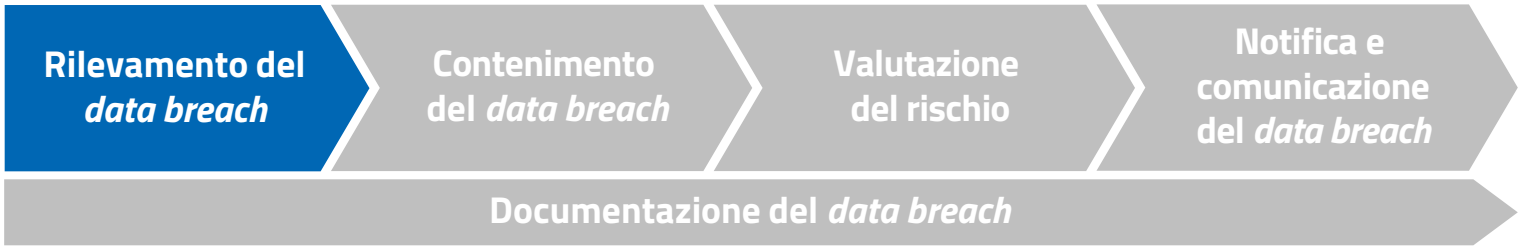
Trattamento di dati personali strettamente necessari a una determinata finalità

Limitazione quantitativa e qualitativa dei dati raccolti

Periodo di conservazione

Accessibilità dei dati

Gestione dei data breach (1/6)



Cos'è un *data breach*?

"*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*"

(art. 4, punto 12), del GDPR)

- Il titolare del trattamento è tenuto a attuare le misure tecniche e organizzative necessarie per rilevare immediatamente un *data breach*
- È inoltre opportuno che il titolare del trattamento includa, negli accordi con i responsabili del trattamento, specifici obblighi informativi in caso di rilevamento di un *data breach* da parte degli stessi responsabili del trattamento

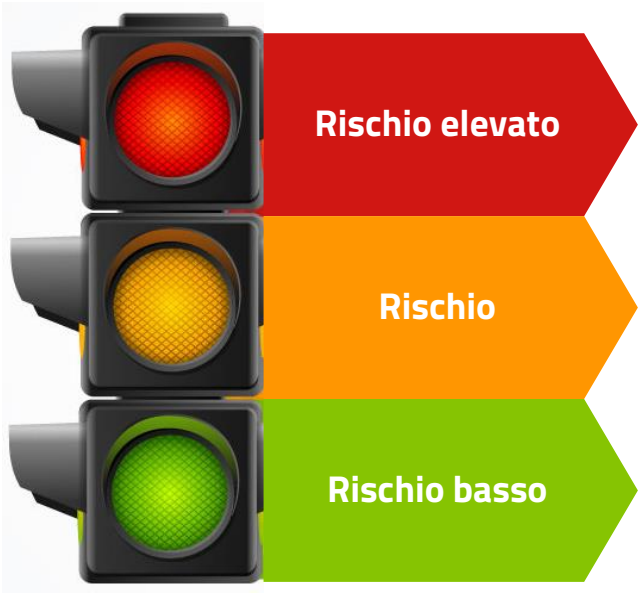
Gestione dei data breach (2/6)

- Rimuovere le cause che hanno determinato il *data breach*
- Identificare e mettere in atto quelle misure volte a contenere il *data breach* o a attenuarne gli effetti negativi per gli interessati (es. cambio delle *password*, sospensione di un servizio, blocco del traffico di rete)
- Ripristinare la normale operatività dei sistemi
- Raccogliere e conservare eventuali prove digitali
- Attivare procedure di *escalation*

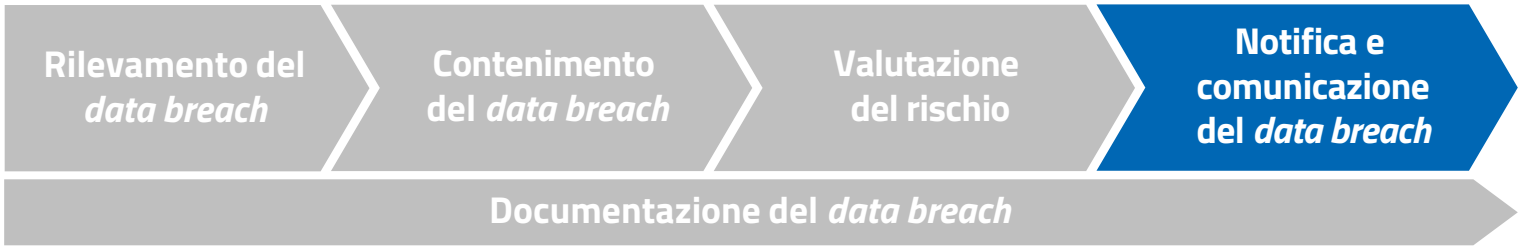
Gestione dei data breach (3/6)

Fattori da tenere in considerazione

- Tipo di *data breach*
- Natura e volume dei dati personali
- Numero di interessati
- Caratteristiche particolari degli interessati
- Facilità di identificazione degli interessati
- Gravità delle conseguenze per gli interessati
- Caratteristiche del titolare del trattamento



Gestione dei data breach (4/6)



Notifica all'autorità di controllo

- **In quali casi?** Quando il *data breach* presenta rischi per i diritti e le libertà delle persone fisiche
- **In che tempi?** Senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il titolare del trattamento è a conoscenza del *data breach*
- **Come?** Notifica completa o per fasi (quando il titolare non è in grado di fornire con immediatezza tutte le informazioni richieste); in caso di data breach ripetuti, ravvicinati e di simile natura è possibile effettuare una notifica differita

Contenuto della notifica

- Descrizione della natura della violazione
- Numero e categorie di interessati
- Numero e categorie di dati personali
- Punto di contatto (responsabile della protezione dei dati o altro soggetto)
- Misure adottate per porre rimedio al *data breach*
- Misure adottate per attenuarne gli effetti negativi

Gestione dei data breach (5/6)

Rilevamento del *data breach* → Contenimento del *data breach* → Valutazione del rischio → **Notifica e comunicazione del *data breach***

Documentazione del *data breach*

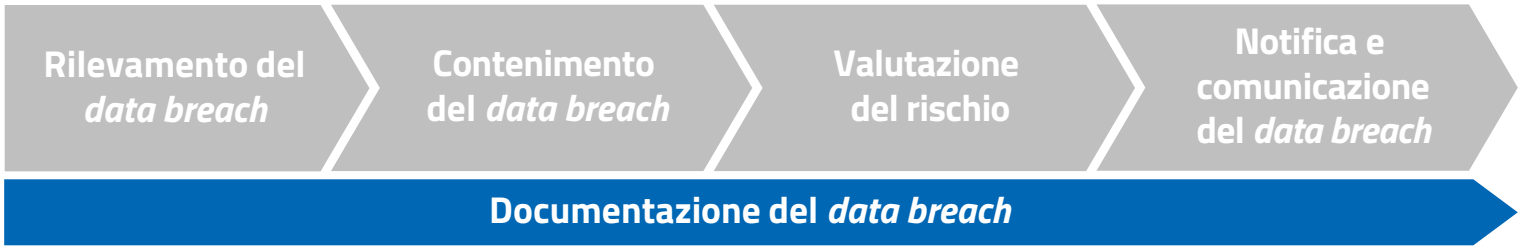
Comunicazione agli interessati

- **In quali casi?** Quando il *data breach* presenta rischi elevati per i diritti e le libertà delle persone fisiche
- **In che tempi?** Senza ingiustificato ritardo dal momento in cui il titolare del trattamento è a conoscenza del *data breach*
- **Come?** Preferibilmente tramite canali di comunicazione diretti (es. e-mail, sms), utilizzando un linguaggio semplice e chiaro

Contenuto della comunicazione

- Descrizione della natura della violazione
- Punto di contatto (responsabile della protezione dei dati o altro soggetto)
- Misure adottate per porre rimedio al *data breach*
- Misure adottate per attenuarne gli effetti negativi

Gestione dei data breach (6/6)



Contenuto del registro dei *data breach*

- Data e ora del *data breach*
- Momento in cui il titolare è venuto a conoscenza del *data breach*
- Documentazione relativa al *data breach*
- Conseguenze del *data breach* per gli interessati
- Misure adottate per porre rimedio al *data breach*

- Il titolare del trattamento deve conservare la documentazione di tutti i *data breach* occorsi (ad esempio in un apposito registro dei *data breach*)
- Nel registro dei *data breach* dovrebbero essere annotate anche le ragioni alla base delle decisioni prese dal titolare del trattamento (es. valutazione del rischio per gli interessati), i motivi dell'eventuale ritardo nella notifica all'autorità di controllo nonché la comunicazione agli interessati

Certificazioni e codici di condotta (1/6)

Considerando 77

«**dimostrare la conformità** da parte del titolare del trattamento»

Considerando 81

«garantire che siano **rispettate le prescrizioni** del presente regolamento riguardo al trattamento che il responsabile del trattamento deve eseguire per conto del titolare del trattamento»

«l'applicazione da parte del responsabile del trattamento di un **codice di condotta** approvato o di un **meccanismo di certificazione** approvato può essere utilizzata come elemento per **dimostrare il rispetto degli obblighi** da parte del titolare del trattamento»

Considerando 100

«al fine di **migliorare la trasparenza** e il rispetto del presente regolamento dovrebbe essere incoraggiata l'istituzione di **meccanismi di certificazione e sigilli** nonché **marchi di protezione dei dati** che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi»

Certificazioni e codici di condotta (2/6)

Art. 24 (3) **Responsabilità del titolare del trattamento** - elemento per dimostrare il rispetto degli obblighi del titolare del trattamento

Art. 25 (3) **Protezione dei dati "by design" e "by default"** - elemento per dimostrare la conformità ai requisiti PbDD

Art. 28 (5) **Responsabile del trattamento** - elemento per dimostrare le garanzie sufficienti

Art. 32 (3) **Sicurezza del trattamento** - elemento per dimostrare la conformità ai requisiti sicurezza

Art. 35 (8) **Valutazione di impatto** - tenuto in debito conto il rispetto da parte di titolari e responsabili dei codici di condotta approvati

Art. 46 (2) **Trasferimento dati verso paesi terzi** - garanzie adeguate

Art. 83 (2) **Sanzioni amministrative pecuniarie** - elemento di cui si tiene debito conto

Certificazioni e codici di condotta (3/6)

Codici di condotta

Strumenti per contribuire alla **corretta applicazione** del Regolamento

Elaborati da **associazioni** e altri **organismi rappresentanti** le categorie di titolari del trattamento o responsabili del trattamento

Soggetti all'**approvazione** dell'autorità di controllo competente che esprime un parere della conformità al Regolamento e, in caso positivo, li inoltra al Comitato

Registro dei i codici di condotta approvati

Controllo della **conformità** effettuato da un organismo in possesso del livello adeguato di competenze riguardo al contenuto del codice e accreditato dall'autorità di controllo competente

Certificazioni e codici di condotta (4/6)

Codici di condotta

Le associazioni e le categorie di titolari o responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del regolamento relativamente a:

a) il **trattamento corretto** e trasparente dei dati

b) i **legittimi interessi** perseguiti dal responsabile del trattamento in contesti specifici

c) la **raccolta** dei dati personali

d) la **pseudonimizzazione** dei dati personali

e) **l'informazione** fornita al **pubblico e agli interessati**

f) **l'esercizio dei** diritti degli interessati

g) **l'informazione** fornita e la protezione del **minore** e le modalità con cui è ottenuto il **consenso** dei titolari della responsabilità genitoriale sul minore

h) le **misure e le procedure** di cui agli artt. 24 e 25 e le misure volte a garantire la sicurezza del trattamento di cui all'art. 32

i) la **notifica di una violazione** dei dati personali alle autorità di controllo e la comunicazione di tali violazioni all'interessato

j) il **trasferimento** di dati personali verso paesi terzi o organizzazioni internazionali

k) le **procedure stragiudiziali** e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento

Certificazioni e codici di condotta (5/6)

Codici di condotta

Codici di condotta nazionali

- **Autorità di controllo nazionale**

Codici di condotta sovranazionali

- **Comitato europeo per la protezione dei dati**

Codici di condotta europei

- **Commissione europea**

Certificazioni e codici di condotta (6/6)

Lavori in corso presso l'EDPB

Guidelines to identify common criteria to accredit certification bodies under Regulation 2016/679

requisiti aggiuntivi per l'accreditamento ai sensi dell'art. 43, par. 1, lett. b), del Regolamento

Guidelines to identify common criteria to certify processing under Regulation 2016/679

criteri di certificazione di cui all'art. 42 del Regolamento (punto 3)

Guidelines on Codes of Conduct and Monitoring Bodies under Regulation 2016/679