

Il nuovo regolamento sulla privacy: quali obblighi per le associazioni e società sportive?

Avv. Mario Vigna
Ancona 15 giugno 2018
Sala Riunioni del Comitato Regionale CONI Marche



Il 4 maggio 2016 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il **Regolamento Generale sulla data protection (GDPR) 2016/679**, applicabile in tutti gli stati membri a partire dal **25 maggio 2018**

Il Regolamento disciplina solamente il trattamento dei dati relativi a **persone fisiche** (no riferimenti a dati di persone giuridiche)

Ambito di applicazione



SI APPLICA

A tutte le organizzazioni pubbliche e private che trattano dati personali



NON SI APPLICA

al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale.

Il principio di accountability (Responsabilità)



Responsabilizzazione del titolare e del responsabile → sono loro a decidere modalità e limiti del trattamento, nonché le garanzie per la loro protezione, nel rispetto del Regolamento

Tenuto conto di:

- natura del trattamento*
 - ambito di applicazione,*
 - contesto del trattamento*
 - finalità del trattamento,*
 - rischi aventi probabilità e gravità diverse*
- per i diritti e le libertà delle persone fisiche*

il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento



Gli obblighi legati alla *accountability*

- *privacy by design e by default*
- nomina di un DPO
- i registri del trattamento
- valutazione dell'impatto
- misure di sicurezza e *data breach*

Privacy by design e privacy by default

Privacy by design (progettazione)

protezione dei dati fin dalla progettazione (siti WEB, applicativi, APP, gestionali, database) ovvero riduzione al minimo del trattamento dei dati mediante misure tecniche ed organizzative quali, ad esempio, la pseudonimizzazione dei dati.

Privacy by default (impostazioni predefinite)

la tutela della protezione del dato deve diventare l'impostazione predefinita, pertanto il titolare del trattamento dovrà adottare misure tecniche ed organizzative adeguate per garantire che siano trattati per impostazione predefinita solo i dati personali necessari per ogni specifica finalità del trattamento, che questi ultimi vengano conservati solo per il tempo strettamente necessario e resi accessibili al solo personale espressamente autorizzato.

La nozione di “dato personale”



*"Qualsiasi informazione riguardante una persona fisica **identificata o identificabile**"*

Esempi di dati personali:

- ✓ Nome e cognome
- ✓ Data e luogo di nascita
- ✓ Codice fiscale
- ✓ Indirizzo di casa
- ✓ Indirizzo e-mail
- ✓ Numero di telefono
- ✓ Numero di passaporto o patente
- ✓ Numero indirizzo IP
- ✓ Volto, impronta digitale, calligrafia

Identificazione= possibilità di distinguere la persona da qualsiasi altro soggetto/ all'interno di una categoria

Tipologie di dati personali

➤ Dati particolari

quelli che rivelano origine razziale o etnica, opinioni politiche, convinzioni religiose/filosofiche, appartenenza sindacale, dati relativi alla salute, dati relativi alla vita sessuale e all'orientamento sessuale ("dati sensibili" secondo il codice della *privacy*).

Ad esempio i dati dei PAZIENTI

Tipologie di dati personali

➤ 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'indicazione univoca, quali l'immagine facciale o i dati dattiloscopici

➤ Dati genetici

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

Il trattamento dei dati personali

Trattamento

- Qualsiasi operazione compiuta con o senza l'ausilio di processi automatizzati e applicate a dati personali

- ✓ **Raccolta**
- ✓ Registrazione
- ✓ Organizzazione
- ✓ Strutturazione
- ✓ **Conservazione**
- ✓ Adattamento/modifica
- ✓ **Estrazione**
- ✓ **Consultazione**
- ✓ Utilizzo
- ✓ Comunicazione mediante trasmissione
- ✓ **Cancellazione o distruzione**

Particolari tipologie di trattamento

Pseudonimizzazione

- il trattamento dei dati personali in modo tale che i dati non possano più essere attribuiti ad 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 non siano attribuiti ad una persona fisica identificata o identificabile

Particolari tipologie di trattamento

Profilazione

- qualsiasi forma di **trattamento automatizzato** di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali (ad es. rendimento professionale, situazione economica, salute, preferenze personali, interessi, affidabilità).

Obiettivi: analizzare/prevedere aspetti riguardanti situazione economica della persona, suo rendimento, salute, interessi, ubicazione...

2 caratteristiche:

- 1 trattamento automatizzato (es. online)
- 2 scopo di valutazione degli aspetti personali della persona fisica

Nb è considerata attività invasiva e può portare ad abusi



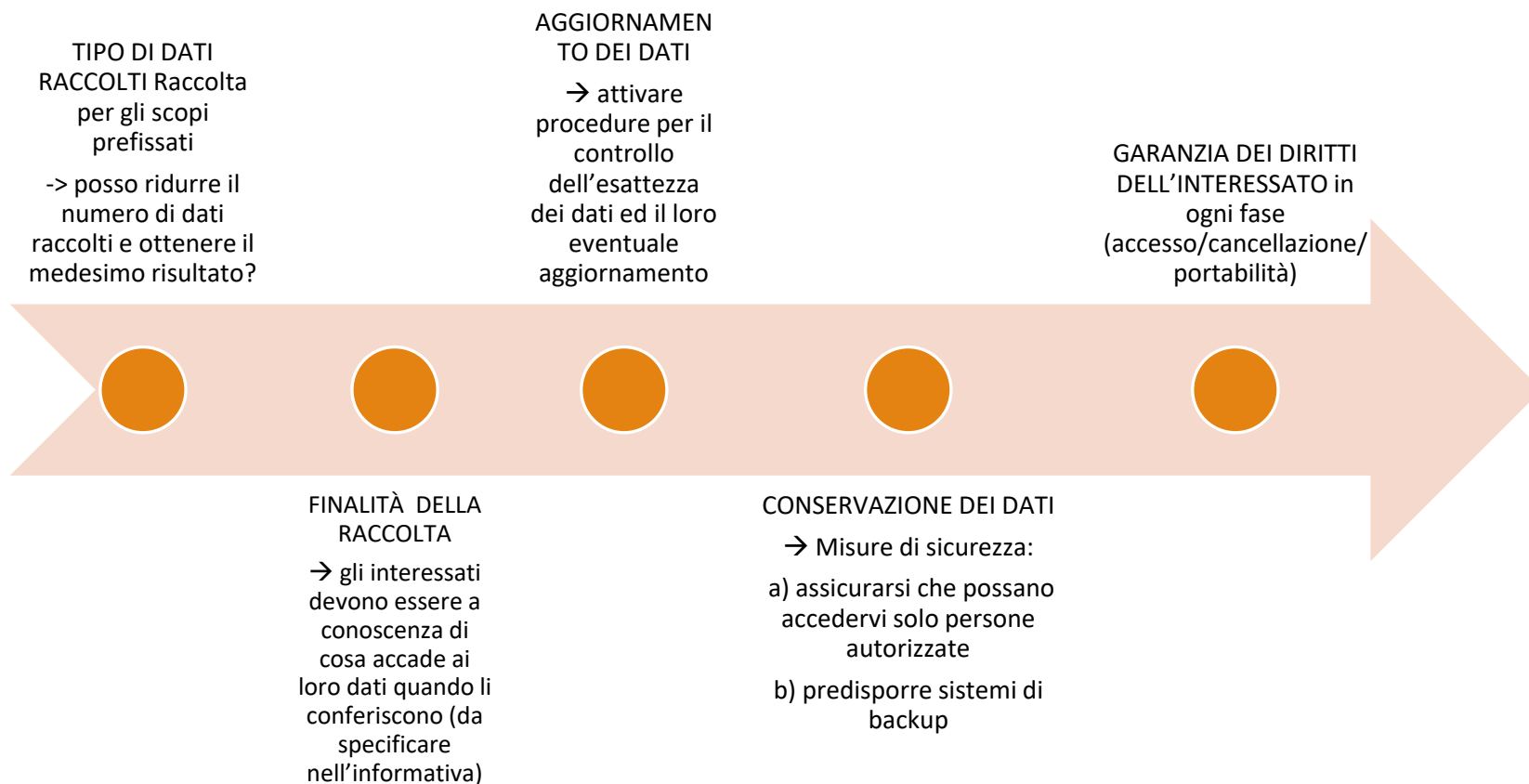
La profilazione

In caso di profilazione vige l'obbligo di informare l'interessato (all'interno dell'informativa) specificando:

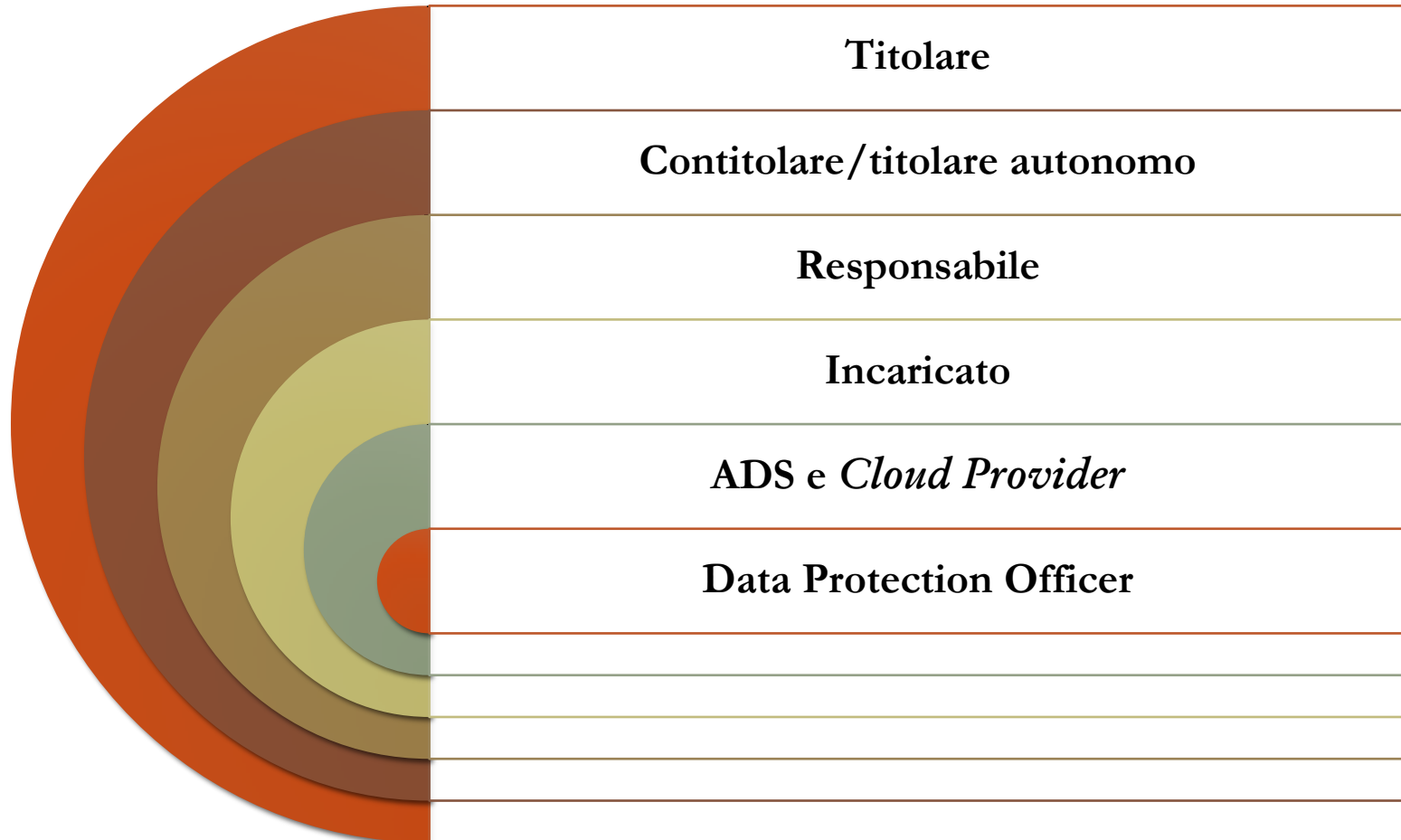
- a) modalità del trattamento;
- b) finalità del trattamento;
- c) logica del trattamento;
- d) conseguenze del trattamento sull'interessato



Flusso del trattamento



I soggetti



Il *Data Protection Officer* (D.P.O.)

Chi è?

Il *data protection officer* (**Responsabile della protezione dati**) è un **professionista che possieda un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali**, che sia in grado di adempiere alle proprie funzioni in piena indipendenza ed in assenza di conflitti di interesse e può essere tanto un **soggetto interno** all'organizzazione del titolare (es. un dipendente) quanto un **soggetto esterno**

I compiti

- informare e consigliare il titolare o il responsabile del trattamento nonché i dipendenti in merito agli obblighi derivanti dal Regolamento e dalle norme interne in materia di *data protection*.
- Sorvegliare l'osservanza del Regolamento e/o di altre normative vigenti, nonché delle *policy* interne del titolare (incluse attribuzioni delle responsabilità, formazione del personale ed i relativi audit)

Il *data protection officer* QUANDO LA NOMINA E' OBBLIGATORIA

se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico

le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala

le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati

L'informativa – cosa scrivere

L'obiettivo: «garantire la lealtà del trattamento»

Meglio per iscritto → ne provo l'esistenza, la completezza e la correttezza

Anche per tipologie di dati per cui il consenso non è richiesto

l'identità e i dati di contatto del titolare del trattamento (e del responsabile della protezione dei dati, ove applicabile);

Obbligatorietà o facoltatività del conferimento (quando posso rifiutare il consenso? Che conseguenze ha il rifiuto?)

le finalità del trattamento nonché le modalità e la base giuridica del trattamento (basato su consenso o giustificato da leggi/legittimo interesse, che va specificato)

Eventuali trattamenti automatizzati (profilazione)

destinatari dei dati personali

ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo

il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati

L'informativa – cosa scrivere

il diritto dell'interessato all'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati

l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca

il diritto di proporre reclamo a un'autorità di controllo

se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

L'informativa – come scrivere

- Forma concisa
- Chiarezza
- Facile accessibilità e intelligibilità per l'interessato
- Richiesta di consenso chiaramente distinguibile
- Previsione di revocabilità del consenso in qualsiasi momento



Consenso da parte dei minori

Valido ed efficace a partire dai 16 anni di età

→ raccolta del consenso di genitori (o chi ne fa le veci) per i minori di 16 anni

Presupposti di liceità del trattamento

presupposti

CONSENSO

ESECUZIONE DI UN CONTRATTO

OBBLIGO LEGALE

SALVAGUARDIA INTERESSI VITALI
DELL'INTERESSATO O ALTRA PERSONA

ESECUZIONE COMPITO DI INTERESSE PUBBLICO

LEGITTIMO INTERESSE DEL TITOLARE

il consenso

Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali

Ad esempio nell'attività di raccolta fondi, profilazione dei donatori, ecc.

Tutela dei diritti dell'interessato

➤ Accesso ai dati

Regola: gratuità

- Diritto di ricevere copia dei dati oggetto del trattamento
- Diritto di sapere periodo di conservazione (o perlomeno i criteri per determinarlo)
- Possibilità di consentire la consultazione diretta e da remoto

Eccezioni: previsione di un contributo da parte dell'interessato in caso di:

- Richieste manifestamente infondate
- Richieste ripetitive
- Richieste tese all'ottenimento di più copie

Tutela dei diritti dell'interessato

➤ **Diritto di cancellazione (diritto all'oblio)**

L'interessato può richiedere e ottenere la cancellazione dei dati in caso di:

- Ipotesi previste dalla legge
- Dati non necessari rispetto alle finalità del trattamento
- Trattamento illecito
- Opposizione dell'interessato
- Revoca del consenso dell'interessato

Tutela dei diritti dell'interessato

➤ Diritto di limitazione del trattamento

Esempi:

- I dati personali sono necessari all'interessato per accertare o esercitare un diritto in sede giudiziaria (purché non siano più necessari al titolare)
- L'interessato contesta l'esattezza dei dati → il trattamento viene limitato per il periodo necessario a controllare l'esattezza di tali dati
- Trattamento illecito (l'interessato non chiede la cancellazione ma solo la limitazione)

➤ Diritto alla portabilità dei dati (in caso di trattamento automatizzato)

- L'interessato ha il diritto di ricevere i dati in formato di uso comune su supporto automatico
- Il Titolare dev'essere in grado di trasferire direttamente i dati portabili a altro titolare indicato dall'interessato

esempi pratici

Collaboratori con partita IVA che emettono fattura per le loro prestazioni?



Il Titolare del trattamento deve rivolgersi a fornitori che applichino misure nel rispetto del Regolamento, nel caso si renda necessario esternalizzare il trattamento

Registri del trattamento

Cosa inserire


Nome e contatti del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del DPO;
le finalità del trattamento;
le categorie di interessati e dei dati personali;
le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;
i termini ultimi previsti per la cancellazione delle diverse categorie di dati; una descrizione generale delle misure di sicurezza tecniche e organizzative.

Registri del trattamento

Quando è obbligatorio?

Il dovere di tenuta dei registri non si applica 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 (nello specifico dati sensibili e biometrici o dati personali relativi a condanne penali e reati)

Ma è bene adottarlo a prescindere dalle dimensioni, in quanto garantisce una corretta gestione dei dati personali



- Più efficienza (meno sprechi di tempo o rischio di duplicazione)
- Meno rischi di trattamenti illeciti

E' una valutazione che va fatta prima del trattamento per soppesare la **particolare probabilità e gravità del rischio**. La valutazione d'impatto è richiesta per i trattamenti su larga scala e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato

Quale rischio? Impatti negativi su libertà e diritti degli interessati

Quando è obbligatoria

la sorveglianza sistematica su larga scala di una zona accessibile al pubblico

Il trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali

Una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche

Misure di sicurezza

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per **garantire un livello di sicurezza adeguato al rischio**, che comprendono, tra le altre, se del caso:

la pseudonimizzazione e la cifratura dei dati personali

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

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

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

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati

Notifica del *data breach*

Il Regolamento prevede che non appena viene a conoscenza di una avvenuta violazione dei dati personali trattati, il titolare deve notificarla all'autorità di controllo competente, **senza ingiustificato ritardo** e – se possibile – entro **72 ore** dal momento in cui ne è venuto a conoscenza. L'obbligo di notifica non scatta nel caso in cui il titolare del trattamento sia in grado di dimostrare che è improbabile che la **violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche**.

Oltre che all'Autorità Garante, il titolare del trattamento deve comunicare la violazione anche all'interessato, **in caso di rischio elevato** per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le necessarie precauzioni



Chi decide?

Il Titolare, dopo aver valutato il rischio per gli interessati
Non è necessario se la comunicazione richiederebbe sforzi sproporzionati (in questo caso, basta una comunicazione pubblica o altre modalità simili)

Il contenuto della notifica



- ✓ Descrizione della violazione, compreso, se possibile, il numero di interessati in questione
- ✓ Indicazione di categorie e numero approssimativo di dati personali interessati dalla violazione
- ✓ Comunicazione dei dati del titolare o di altro punto di contatto da cui avere maggiori informazioni
- ✓ Descrizione delle probabili conseguenze della violazione dei dati personali
- ✓ Descrivere le misure già adottate o proposte dal titolare per porre rimedio alla violazione e/o attenuarne i possibili effetti negativi

Esempi di data breach?

→ Divulgazione (intenzionale o meno), perdita, distruzione, accesso non autorizzato

- Perdita del faldone contenente i certificati medici
- Involontaria cancellazione di un file contenente i dati di
- Perdita di file in backup
- Attacco informatico



➤ Nota bene

Anche se il data breach non è rilevante, occorre documentarlo per poter presentare tale documentazione in sede di accertamento

✓ È più semplice se si adotta il registro del trattamento

Responsabilità del titolare e del responsabile

A) Il titolare

- danno cagionato da trattamento svolto in violazione del Regolamento

B) Il responsabile

Solo se:

- non ha adempiuto agli obblighi che il Regolamento pone in capo al responsabile
- agisce in modo contrario o difforme rispetto alle indicazioni (legittime) del titolare

Le Sanzioni di carattere economico

Inosservanza dei principi base del trattamento; inosservanza dei diritti degli interessati; inosservanza delle disposizioni sul trasferimento dei dati personali in paesi terzi o verso organizzazioni internazionali; inosservanza di un ordine, limitazione provvisoria o definitiva o di un ordine di sospensione dei flussi da parte dell'autorità di controllo:

fino a 20 milioni di Euro, o per le imprese, fino al 4% del fatturato annuo mondiale dell'esercizio precedente



COCCIA DE ANGELIS VECCHIO

A S S O C I A T I

Studio Legale e Tributario



Grazie per l'attenzione!

Avv. Mario Vigna

Associate di:

Coccia De Angelis Vecchio & Associati

**Studio Legale e Tributario
Piazza Adriana, 15
00193 Roma, Italia**

Web: www.cdaa.it

**Tel: +39 06.6880.3025
Fax: +39 06.6880.9416
E-mail: m.vigna@cdaa.it**