



Unione Province d'Italia
Unione Province d'Italia
UPI



Provincia
di Ancona



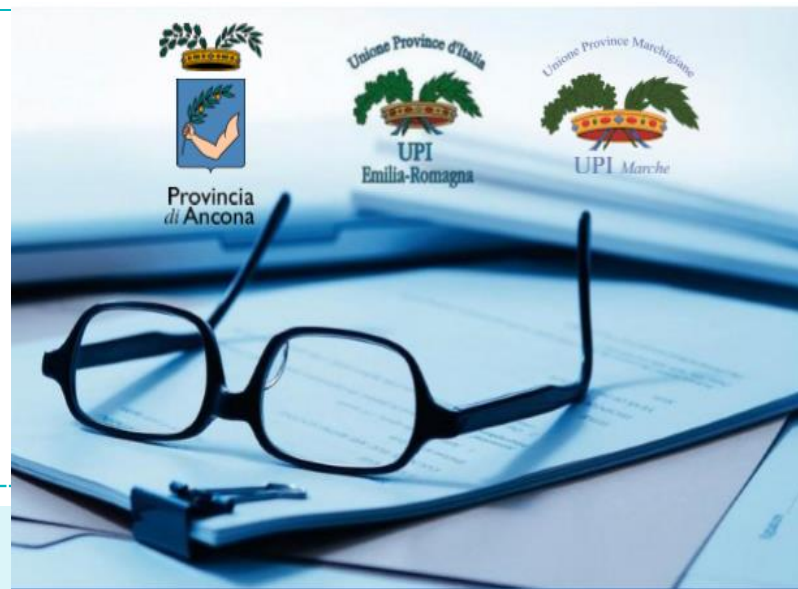
Unione Province d'Italia
UPI
Emilia-Romagna



Unione Province Marchigiane
UPI
Marche



CENTRO STUDI
PRIVACY E NUOVE
TECNOLOGIE



Corso in house

GDPR e nuovo Codice Privacy:
novità e profili applicativi

Data:
13 giugno 2019

DOTT. RICCARDO ACCIAI

***DIRETTORE DIPARTIMENTI LMPC E RTM
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI***



1. GDPR – Il cambio di impostazione

- Privacy, riservatezza e protezione dei dati personali
- Venti anni di protezione dati in Italia
- GDPR e normativa di attuazione
- I nuovi principi
- Le figure organizzative: conferme e novità
- I presupposti di legittimità dei trattamenti



Privacy, riservatezza e protezione dei dati personali

- Privacy
- Riservatezza
- Protezione dei dati personali



20 anni di protezione dati in Italia

- La prima elaborazione giuridica
- USA-Europa
- I primi atti normativi internazionali
- La legge n. 675/1996 e la legge n. 676/1996
- I decreti integrativi e modificativi
- Il Codice e gli «aggiustamenti» successivi



- Le ragioni di un Regolamento comunitario
- Il «pacchetto» protezione dati:
 - un Regolamento che sostituisce la Direttiva n. 95/46/CE (per settori pubblico e privato)
 - una Direttiva (per settori della prevenzione contrasto e repressione crimini nonché per esecuzione sanzioni penali)



Il cammino del GDPR



- Presentato da Commissione UE il 25.1.2012
- Processo di co-legislazione con Parlamento europeo e Consiglio UE
- Percorso:
 - presentati numerosi emendamenti
 - pubblicato GUUE 4.5.2016
 - entrata in vigore 24.5.2016
 - applicazione 25.5.2018



Il Regolamento



- Si articola in: 11 Capi, 99 articoli e 173 «considerando»
- Caratteristiche del regolamento comunitario
- Valutazione d'insieme:
 - il livello di definizione
 - i margini per gli stati membri
 - il «linguaggio»
 - il coordinamento con l'esistente



Il Regolamento: ambito di applicazione

- Materiale: si applica ai trattamenti, automatizzati e non, di dati personali contenuti in un archivio o destinati a confluirci (no trattamenti a fini personali o per prevenzione e accertamento dei reati)
- Territoriale: si applica ai trattamenti: *a)* effettuati nell'ambito delle attività di uno stabilimento nell'UE, indipendentemente dal fatto che questi siano concretamente effettuati o meno nell'UE; *b)* di dati personali di interessati che si trovano nell'UE da un tit o resp non stabilito nell'Unione se: 1. l'offerta di beni e servizi è effettuata nell'UE; 2. il monitoraggio del loro comportamento è effettuato nell'UE



Il trattamento di dati personali



- **Trattamento:** qualunque operazione o insieme di operazioni, effettuati anche senza ausilio di processi automatizzati come la raccolta, la registrazione, l'organizzazione, la messa a disposizione ... la distruzione di dati
- **Dato personale:** qualunque informazione relativa a persona fisica (*,giuridica, ente o associazione*) identificata o identificabile



Il trattamento di dati personali



Categorie di dati «particolari»

- (dati “sensibili): dati *che rivelino* origine etnica o razziale; convinzioni religiose, filosofiche, politiche, sindacali, stato di salute e vita sessuale
- + dati genetici e dati biometrici
- (dati giudiziari) dati relativi a condanne penali e a reati o a connesse misure di sicurezza

Dati «comuni»: gli altri



Il completamento del quadro normativo

- Legge di delegazione europea 25.10.2017, n. 163
- Istituzione Commissione esperti nominata il 14.12.2017; insediata il 4.1.2018
- Schema di decreto legislativo approvato dal Governo Gentiloni il 21.3.2018
- Le obiezioni e le consultazioni
- D.lgs. 10 Agosto 2018, n. 101 (entrato in vigore 19.9.2018)



completamento del quadro normativo



Il Codice emendato dal d.lgs. n. 101/2018

- La forma
- Le abrogazioni e le conferme
- I passi successivi:
 - i codici di condotta
 - le autorizzazioni generali
 - i regolamenti interni



completamento del quadro normativo



I codici deontologici A.5 e A.7

(per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti per il trattamento dei dati personali effettuato a fini di informazione commerciale)

- Entro 19.3.2018 proposta al Garante da parte organismi interessati di trasformazione in codici di condotta
- Entro i 6 mesi successivi il Garante approva o meno
- Durante tale procedimento i codici deontologici rimangono in vigore
- La scadenza di uno dei termini sopra indicati fa cessare efficacia ai codici deontologici



completamento del quadro normativo



I codici deontologici A.1, A.2, A.3, A.4, A.6
(giornalismo, storici, statistici-Sistan; statistico-scientifici,
investigazioni difensive)

- Entro 19.12.2018 il Garante ne verifica la conformità con Regolamento e dispone la pubblicazione in *G.U.* di quelle ritenute compatibili ridenominandole «Regole deontologiche»
- Successivamente sono riportate nell'allegato A al Codice (emendato) con decreto del Ministro della Giustizia
- Il Garante promuove la revisione delle disposizioni di tali codici con le modalità di cui all'art 2-*quater* Codice



Le Autorizzazioni generali

- Entro 19.12.2018 il Garante ne verifica la conformità con Regolamento ed eventualmente procede al loro aggiornamento; avvia una consultazione pubblica e dopo 60 gg. adotta il relativo provvedimento
- Le originarie autorizzazioni da tale momento cessano di avere effetto al pari di quelle non ritenute compatibili
- Autorizzazione n. 7 (dati a carattere giudiziario) - sostituita da adottande misure da parte del Ministro della Giustizia (art. 2-*octies*)
- Le autorizzazioni emendate restano in vigore fino all'adozione delle corrispondenti regole deontologiche e delle misure di garanzia ex artt. 2-*quater* e 2-*septies* Codice



Il completamento del quadro comunitario

Le necessarie indicazioni del EDPB

- Sulla DPIA
- Sulla *lead authority* e la procedura di cooperazione
- Sulle sanzioni
- Sulle strategie e misure di «enforcement»
- Altri interventi, linee guida e pareri....

Le necessarie indicazioni della Commissione

- Sui requisiti per meccanismi di certificazione pdp
- Sulle icone di cui art. 12, par. 7



I nuovi principi



- Approccio basato sul rischio
- *Accountability*
- *Privacy by design*
- *Privacy by default*



I soggetti



- Il titolare: la persona fisica, giuridica, l'autorità pubblica, ente associazione, organismo che singolarmente o con altri determina le finalità e i mezzi del trattamento (è l'entità nel suo complesso (non la persona che la rappresenta) che esercita potere decisionale autonomo su finalità e mod.)
- Il responsabile: la persona fisica, giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare
Interni e/o esterni? - sub-responsabili
- Gli incaricati ????



Fondamento di liceità del trattamento

- Consenso libero, specifico e informato, manifestato attraverso «dichiarazione o azione positiva inequivocabile» - Non è ammesso il consenso tacito o presunto (no caselle pre-spuntate)
- Per i dati sensibili il consenso deve essere «esplicito»
Portabilità dei dati
- Onere dimostrativo a carico del Titolare (v. consid. n. 42)
- Alternative al consenso: adempimento obblighi contrattuali; interessi vitali dell'interessato o di un III; obblighi di legge, interesse pubblico, esercizio pubblici poteri; interesse legittimo prevalente del titolare
- Consenso dei minori valido dopo i 16 anni



Trattamento da parte dei soggetti pubblici

Base giuridica (Regolamento UE art. 6/1/c/e – 6/3/b)

- Il trattamento è lecito solo se e nella misura in cui è necessario:
 - a) per adempiere ad un obbligo legale al quale è soggetto il titolare del trattamento;
 - b) per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento

La base su cui si fonda il trattamento di tali dati è stabilita dal diritto dell'Unione o dello Stato membro



Trattamento da parte dei soggetti pubblici

Base giuridica dati comuni (d.lgs. 101/2018 - art. 2ter)

- La base giuridica richiesta dal Regolamento (v. slide prec.) è costituita esclusivamente da una norma di legge o, nei casi da questa previsti, di regolamento
- La comunicazione di dati comuni fra titolari che esercitano un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa in presenza della norma di cui sopra, ovvero quando risulti necessaria per lo svolgimento delle finalità istituzionali e previa comunicazione al Garante (45 gg poi silenzio-accoglimento)



Trattamento da parte dei soggetti pubblici

Base giuridica dati comuni (d.lgs. 101/2018 - art. 2ter)

- La diffusione o la comunicazione di dati comuni trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri a soggetti che intendono trattarli per altre finalità sono ammesse solo in presenza della norma di cui sopra



Trattamento da parte dei soggetti pubblici

Base giuridica dati particolari (Regol. UE, art. 9/2/g)

- Il trattamento di dati particolari è consentito quando è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi degli interessati

(d.lgs. 101/2018 - art. 2-*sexies*)

Trattamento da parte dei soggetti pubblici

Base giuridica dati particolari (d.lgs. 101/2018 - art. 2-*sexies*)

- I trattamenti di dati particolari per motivi di interesse pubblico rilevante sono ammessi quando sono previsti dal diritto dell'Unione o nell'ordinamento interno da disposizioni di legge o (nei casi previsti dalla legge) di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato



Trattamento da parte dei soggetti pubblici

Base giuridica dati particolari (d.lgs. 101/2018)

- Elenco finalità (d.lgs. 101/2018 - art. 2-*sexies*)
- Misure di garanzia per trattamenti dati genetici, biometrici e relativi alla salute (d.lgs. 101/2018 - art. 2-*septies*)
- Principi relativi al trattamento di dati «giudiziari» (d.lgs. 101/2018 - art. 2-*octies*)



2 I principali adempimenti per l'ente locale

- ❑ **La nomina del DPO e il suo ruolo**
- ❑ **I registri dei trattamenti e di data breach**
- ❑ **DPIA e consultazione preventiva**
- ❑ **Misure di sicurezza**
- ❑ **Diritti degli interessati ed obblighi del titolare**



I rapporti all'interno dell'Ente



Le figure: titolare, responsabile e incaricati

- Maggiori dettagli e definizione rispettive responsabilità nel caso di contitolarità
- Incarico specifico per responsabili (contratto o altro)
- Possibilità di nomina di sub-responsabili di cui il Responsabile risponde al Titolare
- Obblighi specifici a carico del Responsabile (tenuta registro dei trattamenti; adozione misure tecniche e org.ve per sicurezza trattamenti; designazione del DPO)
- Incaricati? Non sono esclusi (persone autorizzate al trattamento sotto l'autorità diretta del Resp. o del Tit.)
- Requisiti per la nomina



I principali adempimenti per l'ente locale

Obblighi del titolare

- Approccio basato sul rischio
- *Accountability*
- *Privacy by design e privacy by default*
- Nomina DPO
- Valutazione di impatto obbligatoria
- Fine della notificazione e del *prior checking*



I principali adempimenti per l'ente locale

Obblighi del titolare

- Registro dei trattamenti (obbligatorio per soggetti con più di 250 dipendenti o che effettuano trattamenti «a rischio»)
- Analisi del rischio
- Misure di sicurezza: lista «aperta e non esaustiva» all'art. 32; cade obbligo di «misure minime»
- Codici di condotta e schemi di certificazione per attestare adeguatezza misure sicurezza adottate
- Documentazione *data breach* e eventuale notifica a Garante (entro 72 h) se si ritiene che da questa possano derivare rischi per interessati
- Nomina DPO in caso di trattamenti su larga scala basati su monitoraggio degli interessati o su dati sensibili/giudiziari



Il DPO



Nomina del DPO

- **chi vi è tenuto?** soggetti pubblici (tutti, tranne autorità giurisdizionali) e soggetti privati che effettuino su larga scala trattamenti di dati particolari o che prevedono monitoraggio regolare degli interessati)
- **più titolari un solo DPO?** (tenere conto dimensioni e struttura org.va)
- **scelto fra chi?** (interni/esterni ma con conoscenze e capacità...)
- **con quale forma?**
- **posizione** (no istruzioni; risponde al vertice; no rimozione o penalizzazione per sua attività; ok altri compiti, ma no conflitto interessi)
- **compiti** (informare e fornire consulenza alla struttura; sorvegliare osservanza disciplina privacy, fornire parere su DPIA, coop. con DPA, punto di contatto per consultazioni)



Prepararsi



Predisporre per:

- DPIA
- Consultazione preventiva
- *Data Breach*
- Reclamo al Garante
- Richieste di informazioni o ispezioni



DPIA

La Valutazione d'impatto (DPIA)

- **Quando?** Se il trattamento allorché preveda l'uso di nuove tecnologie può comportare un rischio elevato per diritti e libertà delle persone
- **E, in particolare?** Quando il trattamento implichi una valutazione sistematica e globale di dati personali, compresa profilazione; trattamento su larga scala dati particolari; sorveglianza sistematica su larga scala di zona accessibile al pubblico. Elenco pubblico DPA
- **Chi la fa?** Il Titolare o il Resp. con parere del DPO
- **Cosa contiene?** Descrizione dei trattamenti e loro finalità; valutazione necessità e proporzionalità; valutazione dei rischi; misure per ridurre i rischi
Software scaricabile da sito CNIL
- **Per quanto tempo vale?** Fino al variare degli elementi considerati e almeno nel caso in cui insorgano variazioni del rischio



Consultazione preventiva



La Consultazione preventiva

- **Quando?** Se il trattamento sottoposto a DPIA continua a mostrare un rischio elevato si può richiedere un parere al Garante che si esprime entro 8+6 settimane
- **Cosa comunicare?** Ambiti responsabilità, finalità e mezzi del trattamento, misure di garanzia previste, dati DPO, la Valutazione di impatto, ogni altra informazione richiesta dal Garante
- **Che succede se il Garante non risponde nei termini previsti?**



Data Breach

Il Data Breach:

- Informare la «gerarchia»
- Notificare la violazione al Garante mediante apposito modulo *on-line* indicando: *a)* natura della violazione, *b)* contatti DPO; *c)* possibili conseguenze; *d)* misure adottate)
- Informare l'interessato se vi sono rischi particolari (indicando *b)* *c)* e *d)*) a meno che i dati siano cifrati, o siano state assunte successive misure di riduzione rischio, o la comunicazione richieda sforzi eccessivi



L'esercizio dei diritti

Informativa

- «Potenziamento»: specifica dati di contatto e del DPO, base giuridica, eventuale trasferimento in paesi III e su quale base; periodo di conservazione dei dati; presenza di eventuali processi decisionali automatizzati (compresa la profilazione) e la relativa logica
- Fornita prima della raccolta dei dati o, se questi sono raccolti presso terzi, al max entro un mese
- Forma concisa, trasparente, facilmente accessibile, chiara e semplice



L'esercizio dei diritti



Dare corso all'esercizio dei diritti degli interessati

L'interessato ha il diritto di

- Accedere ai propri dati, conoscerne l'origine, le finalità del trattamento, i destinatari o le categorie di destinatari, il periodo di conservazione o i relativi criteri.
- Egli ha altresì il diritto di chiedere la rettifica, la cancellazione, la limitazione del trattamento e di conoscere l'eventuale esistenza di un processo automatizzato e la sua logica, nonché il trasferimento verso Paesi extra UE,
- Diritto di proporre reclamo



L'esercizio dei diritti



Novità

- modifica della tempistica: 1 mese (max 3 in caso di complessità) per rispondere;
- possibilità di contributo per richieste onerose o ripetitive
- possibilità di ricevere una «copia» dei dati ove possibile

Modalità del riscontro

- riscontro in forma scritta anche attraverso strumenti elettronici (in forma orale solo se richiesto dall'int.);

Obblighi per il titolare

- adottare misure tecniche e organizzative per favorire l'esercizio dei diritti e il riscontro in forma semplice e chiara



3. Contenzioso, accertamenti e responsabilità

1. Reclami e segnalazioni

- diritti dell'interessato
- reclami e segnalazioni

2. I procedimenti innanzi al Garante

- regolamenti interni, tempi e tipi di provvedimento
- ispezioni e sanzioni

3. Le procedure di cooperazione e il ricorso all'a.g.

- meccanismi di cooperazione e coerenza
- ricorso alla giurisdizione ordinaria

4. Focus sui soggetti pubblici

- il regime particolare
- esercitazione pratica



I diritti dell'interessato



Dare corso all'esercizio dei diritti degli interessati

L'interessato ha il diritto di

- Accedere ai propri dati, conoscerne l'origine, le finalità del trattamento, i destinatari o le categorie di destinatari, il periodo di conservazione o i relativi criteri.
- Egli ha altresì il diritto di chiedere la rettifica, la cancellazione, la limitazione del trattamento e di conoscere l'eventuale esistenza di un processo automatizzato e la sua logica, nonché il trasferimento verso Paesi extra UE,
- Diritto di proporre reclamo



I diritti dell'interessato



Attenzione ai «nuovi» diritti

- **Estensione del diritto alla cancellazione: il diritto all'oblio (art. 17)** un diritto alla cancellazione in forma rafforzata; diritto ad essere dimenticato o meglio, a non essere ulteriormente ricordato per fatti che un tempo sono stati oggetto di cronaca; il titolare che li ha resi pubblici pubblicandoli su un sito web ha l'obbligo comunicare la richiesta di cancellazione a chiunque li stia trattando nei limiti di quanto tecnicamente possibile (limiti: *esercizio libertà espressione; diritto alla difesa, tutela salute pubblica, dati resi anonimi e necessari per ricerca storica statistica e scientifica*)
- **Limitazione del trattamento (art. 18):** più esteso rispetto al blocco, in quanto prevede che il dato (ad es. in attesa di rettifica) sia contrassegnato e in quanto tale non possa essere oggetto di trattamento (ad eccezione della conservazione). Può essere contestata l'esattezza o la liceità e l'interessato chiede un utilizzo limitato



I diritti dell'interessato



❑ Il diritto alla portabilità

- solo per trattamenti automatizzati - Linee guida WP Art.29
- sono portabili solo i dati trattati sulla base del consenso o di un contratto (non quelli il cui trattamento sia basato sull'interesse pubblico o sul legittimo interesse del titolare)
- possono essere oggetto di una richiesta di portabilità esclusivamente i dati forniti consapevolmente e attivamente dall'interessato (nome, cognome, indirizzo) ma anche quelli «forniti» attraverso la fruizione di un servizio o l'utilizzo di un dispositivo
- non si applica al «*trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare*»



L'esercizio dei diritti

Novità

- modifica della tempistica: 1 mese (max 3 in caso di complessità) per rispondere;
- possibilità di contributo per richieste onerose o ripetitive
- possibilità di ricevere una «copia» dei dati ove possibile

Modalità del riscontro

- riscontro in forma scritta anche attraverso strumenti elettronici (in forma orale solo se richiesto dall'int.);

Obblighi per il titolare

- adottare misure tecniche e organizzative per favorire l'esercizio dei diritti e il riscontro in forma semplice e chiara



Il reclamo al Garante



Il reclamo al Garante (art. 77):

- *l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo alla APD dello stato membro in cui risiede, lavora o in cui si è verificata la violazione*
- *il Garante entro 3 mesi deve aver deciso il reclamo o comunicato all'interessato lo stato della procedura*



Mezzi di ricorso – il ricorso all'A.G.



- Contro ogni decisione del Garante che lo riguardi (o in caso di sua inerzia) l'interessato può adire l'autorità giudiziaria del Paese in cui risiede l'APD (art. 78)
- In ogni caso, in via alternativa, per violazioni del t.d.p. l'interessato (art. 79) può rivolgersi all'A.G.
 - a) dello stato membro in cui il tit. si trovi o abbia uno stabilimento;
 - b) dello stato membro in cui risieda abitualmente l'interessato (a meno che il tit. o il resp. sia una pubblica autorità nell'esercizio dei suoi poteri);



Conflitti fra «giurisdizioni»



- L'A.G. di uno stato membro che venga a conoscenza di azioni riguardanti lo stesso oggetto e lo stesso titolare (o resp.) pendenti c/o un'A.G. di altro Stato membro prende contatto con essa e, laddove ciò sia confermato, qualunque A.G. successivamente adita può sospendere le azioni presentate innanzi ad essa
- Se un reclamo è presentato contro un Titolare stabilito in più Stati membri è competente l'APD capofila, a meno che riguardi unicamente lo stabilimento o gli interessati in altro Stato; in tal caso l'APD di quello stato adita informa la Capofila che decide sui seguiti



Richieste di informazioni e ispezioni

Richieste di informazioni e ispezioni del Garante

- Come sono formulate le richieste
- Come avvengono le ispezioni
- La programmazione
- Le attività di accertamento
- Obbligo di cooperazione con il Garante



Responsabilità e sanzioni



- Il quadro complessivo delineato dal GDPR
- Responsabilità amministrative
- Responsabilità civili
- Responsabilità penali
- Le sanzioni amministrative
- Il procedimento innanzi al Garante
- Le sanzioni penali



Responsabilità e risarcimento (art. 82)

- Chiunque subisca un danno materiale o immateriale a causa della violazione del GDPR ha diritto a ottenere un risarcimento a meno che il Tit (o il Resp.) dimostri che questo non è a lui in alcun modo imputabile.
- In caso di più Tit. o Resp. ognuno è responsabile in solido per l'intero ammontare del danno, salvo rimborso da parte degli altri anche con azione di rivalsa innanzi l'a.g.



Sanzioni amministrative (art. 83)

- Ogni APD provvede affinché le sanzioni amministrative pecuniarie per violazioni del GDPR siano effettive, proporzionate e dissuasive tenendo conto di:
 - a) natura, gravità e durata della violazione;
 - b) carattere doloso o colposo;
 - c) misure adottate per attenuare il danno;
 - d) grado e responsabilità del Tit. in ragione delle misure tecniche e organizzative messe in atto;
 - e) eventuali precedenti
 - f) grado di cooperazione con APD per rimediare



Sanzioni amministrative (*segue*)

- g) categorie di dati coinvolte
- h) modalità di avvenuta conoscenza da parte APD
- i) rispetto di eventuali provvedimenti prescrittivi già disposti da APD
- j) adesione a codici di condotta o a meccanismi di certificazione
- k) eventuali altri fattori aggravanti o attenuanti (es. benefici conseguiti o perdite evitate)



Sanzioni amministrative (*segue*)

- Se, in relazione allo stesso trattamento o a più trattamenti collegati, un Tit. viola con dolo o colpa più disposizioni del GDPR l'importo della sanzione non può superare quello previsto per la violazione più grave
- La sanzione può arrivare a 10 milioni € o a 2% fatturato mondiale tot. annuo in caso di violazione di:
 - a) obblighi del Tit
 - b) obblighi dell'organismo di certificazione
 - c) obblighi dell'organismo di controllo



Sanzioni amministrative (*segue*)

- La sanzione può arrivare a 20 milioni € o a 4% fatturato mondiale tot. annuo in caso di violazione di:
 - a) principi del trattamento, compreso consenso
 - b) diritti dell'interessato
 - c) trasferimenti in Paesi terzi
 - d) obblighi degli Stati membri ex Capo IX GDPR
 - e) Inosservanza ordini APD

Applicabili i principi del giusto procedimento e del ricorso giurisdizionale



Altre sanzioni (art. 84)



- Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del GDPR non soggette a sanzioni amm.ve ex art.83.
- Tali sanzioni devono essere effettive, proporzionate e dissuasive
- Notifica alla Commissione di tali ulteriori sanzioni



Qualche domandina...

Il Decreto n. 196/2003 è stato abrogato?

- a) Sì
- b) No: è stato sostituito dal d.lgs. 101/2018
- c) No: è stato integrato e modificato dal d.lgs n. 101/2018

Quanto tempo ha il titolare per rispondere, in via ordinaria, ad una richiesta di accesso?

- a) 15 gg
- b) 30 gg
- c) 90 gg



Qualche domandina...

Quando posso fare ricorso al Garante?

- a) Ogni volta che ritengo ci sia una violazione del Reg.
- b) Solo quando sono violati diritti dell'interessato
- c) Mai

Che tipo di responsabilità prevede il Reg.?

- a) Amministrativa e penale
- b) Civile, penale, amministrativa
- c) Civile e penale



Qualche domandina...

Quali tipi di ispezione del Garante ai soggetti pubblici?

- a) Solo in base a specifiche lagnanze
- b) Solo di iniziativa ed a campione
- c) Di iniziativa o in base a specifiche lagnanze

Quali regole devono seguire i soggetti pubblici per comunicare dati particolari a soggetti privati?

- a) Norma di legge
- b) Norma di legge o di regolamento
- c) Norma di legge o di regolamento o autoriz. Garante



Come tenersi aggiornati



- Comunicati stampa
- Newsletter
- Sito web Garante

www.garanteprivacy.it