Il Regolamento Europeo sulla protezione dei dati

Regolamento Ue 679/2016

› bluenext ‹

Dalla 675/96 al regolamento Ue

- L.675/96
- D.Lgs.196/2003 in vigore sino al 25 maggio 2018
- Regolamento UE 679/2016 in vigore dal maggio 2016

  Obbligatorio dal 25 maggio 2018

I numeri del Garante nel 2016

- Riscontro a 4.633 reclami e segnalazioni
- Decisi 277 ricorsi
- 53 Violazioni segnalate all'Autorità Giudiziaria per mancata adozione delle misure di sicurezza
- Contestate 2.339 Sanzioni
- Riscosse sanzioni amministrative per circa 3 milioni e 300 mila euro

(Relazione annuale Garante Privacy 2016)

Adempimenti privacy D.Lgs.196/2003

Oggetto della tutela

Garanzia che i trattamenti dei dati personali rispettino i diritti e le libertà fondamentali e la dignità dell'interessato (riservatezza, identità personale, diritto alla protezione dei dati)

Cosa intendiamo per dato personale?

Qualsiasi informazione riguardante un persona fisica, identificata o identificabile

Quali elementi rendono identificabile una persona fisica?

- Nome
- Un numero di identificazione
- Dati relativi all'ubicazione
- Identificativo on line
- Uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

Le categorie di dati personali

- Dati comuni
- Dati sensibili
- Dati giudiziari

D.Lgs.196/2003

- Dati particolari:
  origine razziale ed etnica, opinioni politiche, convinzioni filosofiche o religiose, appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale
- Dati relativi a condanne penali
- Dati Comuni

Regolamento Ue 679/2016

l Regolamento Ue vieta il trattamento dei dati particolari a meno che…

- L'interessato ha prestato il proprio consenso
- Il trattamento sia necessario per assolvere obblighi in materia di diritto del lavoro o sicurezza sociale e protezione sociale
- Il trattamento è effettuato da un'associazione o fondazione e i dati non siano comunicati all'esterno
- Il trattamento riguardi dati resi manifestamente pubblici dall'interessato
- Il trattamento è necessario per finalità di medicina preventiva, del lavoro o valutazione della capacità lavorativa

Ambito soggettivo del trattamento

Titolare del trattamento

- Persona fisica, giuridica ente o associazione che determina modalità e finalità del trattamento ed i profili della sicurezza

Responsabile del trattamento

- Soggetto cui il Titolare affida il trattamento dei dati

Incaricato del trattamento

- Soggetto autorizzato a svolgere operazioni di trattamento che opera sotto il controllo e l'autorità del Titolare

Informativa

Ex art. 13 D. Lgs.196/2003

Ex art. 13 Regolamento Ue 679/2016

› bluenext ‹

D.Lgs.196/2003 (vigente sino al 25 maggio 2018)	Regolamento Ue 679/2016 (dal 25 maggio 2018)
Finalità e modalità di trattamento	Finalità del trattamento
Natura obbligatoria o facoltativa del conferimento dei dati	
	Base giuridica del trattamento
	Se il trattamento si basa sull'art.6, §1 lettera f) , i legittimi interessi perseguiti dal titolare del trattamento o di Terzi
Le conseguenze di un eventuale rifiuto a rispondere	
Soggetti o le categorie di soggetti dei i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, ambito di diffusione dei dati medesimi	Eventuali destinatari o le eventuali categorie di destinatari dei dati personali
Diritti di cui all'art.7	
	Ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.
Estremi identificativi del titolare e, se designato del rappresentate nel Territorio dello stato e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco dei responsabili.	Identità e dati di contatto del titolare del trattamento
	I dati di contatto del RPD (DPO) ove applicabile

Accountability

Obblighi del titolare

› bluenext ‹

Il Titolare del trattamento può affidare dati

- Unicamente a responsabili del trattamento che presentino garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento UE 679/2016 e garantisca la tutela dell'interessato

Il Responsabile del trattamento

Art.28 Regolamento UE 679/2016

› bluenext ‹

Il Responsabile del trattamento

- Non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento.

Nomina del Responsabile

- Disciplinata **da un contratto o da altro atto giuridico** a norma del diritto dell'unione o degli altri Stati membri che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli 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, gli obblighi e i diritti del titolare del trattamento.

Il contratto prevede in particolare che il responsabile del trattamento..

- Tratti i dati soltanto su istruzione documentata del titolare
- Garantisca che le persone autorizzate al trattamento si siano impegnate alla riservatezza o abbiano un obbligo legale di riservatezza
- Adotti tutte le misure ai sensi dell'art. 32
- Rispetti le condizioni per ricorrere ad altro responsabile
- Assista il titolare nel rispetto degli obblighi del regolamento
- Su scelta del titolare cancelli o restituisca tutti i dati al termine della prestazione
- Metta a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi del presente articolo e consenta l'attività di revisione ed ispezione del titolare

Art.32 Misure di sicurezza adeguate che comprendono :

- Pseudoanonimizzazione
- Riservatezza,
- integrità e disponibilità dei dati su base permanente, resilenza dei sistemi e dei servizi
- Capacità di ripristino dei dati
- Procedure per testare il ripristino dei dati

L. LEGGE 20 novembre 2017, n.167
Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017. (17G00180) (GU Serie Generale n.277 del 27-11-2017)

Modifiche al codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196

› bluenext ‹

Modifica art. 29 D.Lgs.196/2003

2. I titolari stipulano con i predetti responsabili atti giuridici in forma scritta, che specificano la **finalita' perseguita**, la **tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalita' di trattamento;** i predetti atti sono adottati in conformita' a schemi tipo predisposti dal Garante»;

Entrata in vigore della L. 167

12 Dicembre 2017

Gli incaricati del trattamento

Incaricati del trattamento

Chiunque agisca sotto l'autorità del titolare del trattamento o del responsabile o abbia accesso ai dati personali **NON** può trattare tali dati se non è istruito in tal senso dal titolare del trattamento.

- Sono nominati per iscritto
- La designazione individua puntualmente l'ambito di trattamento consentito
- Devono essere istruiti al trattamento

LA SICUREZZA DEI DATI

Dal D.LGS.196/2003 AL REG.UE 679/2016

› bluenext ‹

Codice Privacy

Misure Idonee

- Art.31

Misure Minime

- Art.33-34-35

ACCOUNTABILITY

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 presente regolamento.

Dette misure sono riesaminate e aggiornate qualora necessario

Procedura per adeguamento Privacy

Le misure devono Garantire

- Pseudo anonimizzazione e cifratura
- Capacità di assicurare : riservatezza, integrità, disponibilità e resilienza dei sistemi
- Procedura di verifica e valutazione misure di sicurezza
- Analisi dei rischi
- Adesione a Codici di Condotta

PRIVACY BY DESIGN

Art. 25 Regolamento Ue

› bluenext ‹

Il titolare del trattamento mette in atto misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati necessari per ogni specifica attività di trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento , il periodo di conservazione, e l'accessibilità.

REGISTRI DELLE ATTIVITA' DI TRATTAMENTO

Art.30 Regolamento Ue

› bluenext ‹

Soggetti obbligati alla tenuta

Titolari del trattamento

Responsabili del trattamento

- più di 250 dipendenti
- trattamenti che presentino un rischio per i diritti e le libertà dell'interessato
- categorie particolari di dati (art.9)
- dati giudiziari art. 10

Contenuto del registro

- Titolare e contitolare eventuale
- Finalità del trattamento
- Categorie di interessati
- Categorie di destinatari
- Trasferimenti verso paesi terzi
- Tempi per la cancellazione dati
- Misure di sicurezza adottate

Il Garante Italiano sul Registro dei trattamenti

RACCOMANDAZIONI

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì ***parte integrante di un sistema di corretta gestione dei dati personali****. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta. I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.*

Notificazione violazione dati

Art. 33 Regolamento UE

› bluenext ‹

IL TITOLARE:

- NOTIFICA ALL'AUTORITA' DI CONTROLLO
  - Ove possibile entro 72 ore dal momento in cui il titolare ne è venuto a conoscenza
  - Se fatta oltre le 72 ore deve contenere motivi del ritardo

- DOCUMENTA la violazione, le circostanze ad essa relative, le conseguenze ed i provvedimenti adottati

Contenuto della notifica:

- Natura della violazione
- Ove possibile, categorie e numero di interessati e di registrazioni di dati personali coinvolti
- Nome e dati di contatto del responsabile della protezione dei dati o altro soggetto di riferimento
- Descrizione probabili conseguenze della violazione
- Descrizione misure adottate o da adottare per porre rimedio alla violazione e attenuarne effetti negativi

QUANDO LA VIOLAZIONE DEI DATI PERSONALI E' SUSCETTIBILE DI PRESENTARE UN **RISCHIO ELEVATO** PER I DIRITTI E LE LIBERTA' DELLE PERSONE FISICHE

OBBLIGO DI COMUNICAZIONE DELLA VIOLAZIONE DEI DATI PERSONALI AGLI INTERESSATI

Fatta senza ritardo

Descrive in modo semplice e chiaro la natura della violazione, le possibili conseguenze, le misure adottate dal titolare

L’obbligo di comunicazione all’interessato della violazione viene meno se:

- Erano state applicate ai dati oggetto della violazione misure di sicurezza adeguate, in particolare quelle idonee a renderli incomprensibili (es, la cifratura)
- Il titolare del trattamento ha adottato in seguito alla violazione misure idonee ad evitare il sopraggiungere di un rischio elevato per i diritti e le libertà personali
- Tale comunicazione richiederebbe sforzi sproporzionati. In tal caso si dovrà fare una comunicazione pubblica

Valutazione di impatto sulla protezione dei dati

Art.35 Regolamento UE

› bluenext ‹

Obbligatoria se

- Il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche

Richiesta in particolare se …

- Valutazione sistematica e globale di aspetti personali relative a persone fisiche (*profilazione*)
- Trattamento su larga scala di dati personali particolari (art. 9 e art.10)
- Sorveglianza sistematica su larga scala di una zona accessibile al pubblico

La consultazione preventiva

Art.36 Regolamento UE

› bluenext ‹

Quando?

- Prima di procedere al trattamento

- Se la valutazione d'impatto indica che il trattamento presenta un **rischio elevato** ed il Titolare deve quindi adottare misure idonee ad attenuare tale rischio

Contenuto della comunicazione all'Autorità di Controllo:

- Le responsabilità del titolare del trattamento, dei contitolari, dei responsabili.
- Le finalità ed i mezzi del trattamento
- Le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati
- I dati di contatto del titolare
- La valutazione d'impatto sulla protezione dei dati

procedimento:

- L'Autorità di Controllo valuta se il trattamento descritto è conforme al Regolamento e se il titolare ha identificato ed attenuato il rischio in maniera sufficiente

- In caso di esito negativo della valutazione, l'Autorità fornisce al titolare del trattamento una consulenza per iscritto

Responsabile della protezione dei dati (DPO)

Art. 37 Regolamento UE

› bluenext ‹

E’ designato in funzione:

- Delle qualità professionali
- Della capacità di assolvere ai compiti indicati dall’art. 39

Può essere:

- Un dipendente del titolare o del responsabile
- Può svolgere i suoi compiti sulla base di un contratto di servizi

Quando è obbligatoria la designazione

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

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

oppure

c) se 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 .

Compiti del DPO

- Consulenza sugli obblighi derivanti dal regolamento
- Sorvegliare l'osservanza del Regolamento
- Fornire pareri sulla PIA e sorvegliare lo svolgimento
- Fungere da contatto con l'autorità di controllo

Le sanzioni

Gli stati membri

- Stabiliscono le **norme relative alle sanzioni** per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'art. 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione.
- Tali sanzioni devono essere effettive, proporzionate e dissuasive

Sanzioni pecuniarie sino a 20.000.000,00 di euro euro o, per le imprese fino al 4% del fatturato mondiale annuo

- Violazione dei principi del trattamento, comprese le condizioni di consenso
- Diritti degli interessati
- Trasferimento verso un paese terzo
- Qualsiasi obbligo ai sensi delle legislazioni degli stati membri

Sanzioni pecuniarie sino a 10.000.000,00 di euro euro o, per le imprese fino al 2% del fatturato mondiale annuo

- Violazione degli obblighi del titolare del trattamento
- Obblighi dell'organismo di certificazione
- Obblighi dell'organismo di controllo

Art. 80 Regolamento UE 679/2016

1. L'interessato ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti di cui agli articoli 77, 78 e 79 nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento di cui all'articolo 82.

Art.82 Regolamento UE 679/2016

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.
2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato
dal suo trattamento che violi il presente regolamento.
Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente
diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento

Qualora più titolari del trattamento o responsabili del trattamento oppure
entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile
in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato

GRAZIE PER L'ATTENZIONE

› bluenext ‹