info@pclex.it

Prof. Avv. Fabio Montalcini - Prof. Avv. Camillo Sacchetto
info@pclex.it

Regolamento UE 2016/679 (Data Protection)

Soggetti
Informativa - Liceità Trattamento
Data Breach

Università di Torino - Dipartimento Informatica

Regolamento (UE) 2016/679 (GDPR) del Parlamento Europeo e del Consiglio del 27 aprile 2016

Soggetti che effettuano il Trattamento

Regolamento (UE) 2016/679 (GDPR) del Parlamento Europeo e del Consiglio del 27 aprile 2016

Soggetti che effettuano il Trattamento

Articolo 4 del Regolamento (UE) 2016/679 - Definizioni
Ai fini del presente regolamento s'intende per:

«***titolare del trattamento***»:

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, ***determina le finalità e i mezzi del trattamento di dati personali***; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Regolamento (UE) 2016/679 (GDPR) del Parlamento Europeo e del Consiglio del 27 aprile 2016

Soggetti che effettuano il Trattamento

Articolo 4 del Regolamento (UE) 2016/679 - Definizioni
Ai fini del presente regolamento s'intende per:

«***responsabile del trattamento***»:

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che ***tratta dati personali per conto del titolare del trattamento***;

Articolo 28, comma 3, del Regolamento (UE) 2016/679

I trattamenti da parte di un responsabile del trattamento sono ***disciplinati da un contratto o da altro atto giuridico*** a norma del diritto dell'Unione o degli Stati membri.

Regolamento (UE) 2016/679 (GDPR) del Parlamento Europeo e del Consiglio del 27 aprile 2016

Soggetti che effettuano il Trattamento

«***Incaricato***»

non più espressamente previsto ma….

Articolo 29 del Regolamento (UE) 2016/679 - Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

Il responsabile del trattamento, o ***chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento***, che abbia accesso a dati personali ***non può trattare tali dati*** se non è ***istruito*** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Regolamento (UE) 2016/679 (GDPR) del Parlamento Europeo e del Consiglio del 27 aprile 2016

Interessato:

la persona fisica identificata o identificabile cui si riferiscono i dati personali

E' il baricentro della normativa che deve essere interpretata sempre a sua tutela

All'**Interessato** si ricollegano principalmente **DIRITTI** previsti dalla normativa
agli altri soggetti si ricollegano principalmente **DOVERI**

«***Considerando n° 1 GDPR***» : La protezione delle **persone fisiche** con riguardo al **trattamento dei dati** di carattere personale è **un diritto fondamentale**.

«***Considerando n° 4 GDPR***» : Il trattamento dei dati personali dovrebbe essere **al servizio dell'uomo**. Il diritto alla protezione dei dati di carattere personale **non è una prerogativa assoluta**, ma va considerato alla luce della sua funzione sociale e **va contemperato con altri diritti fondamentali** […] in particolare […], la libertà di pensiero, […] la libertà di espressione e d'informazione, la libertà d'impresa, […]

Diritti dell'Interessato

a) **conoscitivi**:

- diritto a ricevere l'informativa
- diritto di richiedere ed ottenere informazioni (accesso)
- diritto a ricevere informazioni in caso di violazioni (comunicazione data breach)

b) di **controllo sul trattamento**

- diritto al consenso e autorizzazione del trattamento (art 6 a e 9) di revoca del consenso (art 7) e opposizione (art 21)
- diritto alla limitazione del trattamento (art. 18)

c) di **intervento** sui dati

- portabilità (art 20) rettifica ed integrazione (modifica) (art 16)
- cancellazione ed oblio (eliminazione) (art 17)

d) di non essere **sottoposto a decisione basata unicamente sul trattamento automatizzato, compresa la profilazione** che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona (art 22)

Regolamento (UE) 2016/679 (GDPR) del Parlamento Europeo e del Consiglio del 27 aprile 2016

Responsabile per la protezione dei dati (RPD)

o

Data Processor Officer (DPO)

Responsabile della protezione dei dati (DPO)

E’ OBBLIGATORIO IN 3 CASI

1) autorità pubblica o organismo pubblico

2) controllo regolare e sistematico degli interessati su larga scala

3) trattamento, su larga scala, di categorie particolari di dati

- è una figura di vigilanza, interna o esterna
- un gruppo di imprese può nominare un unico DPO
- è designato in funzione delle qualità professionali
- è coinvolto in tutte le questioni relative al trattamento dati
- non deve ricevere istruzioni e non dev’essere in conflitto d’interessi

Responsabile della protezione dei dati (DPO)

compiti e finalità:

- informare e consigliare;
- sorvegliare
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- cooperare con l’autorità di controllo;
- essere punto di contatto per l'autorità di controllo per questioni connesse al trattamento di dati personali;
- considerare debitamente i rischi inerenti al trattamento, tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del medesimo.

Autorità di Controllo in ambito GDPR Privacy

Ogni Stato Membro dispone di un'Autorità per la Protezione dei Dati
le Autorità sono riunite nel **Comitato Europeo (CEPD o EDPB**)

In Italia: Autorità Garante Protezione dei Dati Personali (o Autorità Garante Privacy)
È una delle **Autorità Amministrative Indipendenti (Authority)**

L'Autorità Garante ha funzioni di **controllo normativo** sulle materie di **competenza nazionale**.

Organo Collegiale (tra cui Presidente e Vicepresidente) composto di **quattro membri eletti dal Parlamento** della **durata di 7 anni**.

L'attuale Collegio è stato eletto dal Parlamento (ai sensi dell'articolo 153, comma 1, del D.Lgs. 196/2003) il 14 luglio 2020, si è insediato il 29 luglio 2020 ed è così composto:

Pasquale Stanzione **(Presidente) -** Ginevra Cerrina Feroni **(Vice Presidente)**
Agostino Ghiglia **-** Guido Scorza **(Componenti)**

Autorità di Controllo in ambito GDPR Privacy

L'Ufficio del Garante si articola in:

- **Segreteria Generale**
- **Dipartimenti**

(Attività Ispettive; Reti telematiche e Marketing; Libertà Manifestazione Pensiero e Cyberbullismo, Sanità e Ricerca, Realtà Pubbliche, ...).

- **Servizi**

(affari legislativi e istituzionali, relazioni internazionali e con l'Unione europea, relazioni con il pubblico, relazioni esterne e media,…)

L'attività ispettiva del Garante è svolta, oltre che dai **Funzionari**, dalla **Guardia di Finanza Nucleo Privacy** mediante Protocollo d'Intesa.

Sono presenti anche Protocolli di Intesa con Polizia di Stato e Corecom Piemonte in materia di prevenzione e contrasto del fenomeno del cyberbullismo.

Regolamento (UE) 2016/679 (GDPR) del Parlamento Europeo e del Consiglio del 27 aprile 2016

Informativa all'Interessato

Liceità del Trattamento

Regolamento (UE) 2016/679 (GDPR) del Parlamento Europeo e del Consiglio del 27 aprile 2016

Informativa all'Interessato

Art. 12 del Regolamento (UE) 2016/679
(Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato)

1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni [..] relative al trattamento in forma ***concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro***, in particolare nel caso di informazioni destinate specificamente ai minori.
Le informazioni sono fornite ***per iscritto*** o con altri mezzi, anche, se del caso, con mezzi elettronici.
Se richiesto dall'interessato, le informazioni **possono essere fornite oralmente, purché sia comprovata con altri mezzi** l'identità dell'interessato.

Regolamento (UE) 2016/679 (GDPR) del Parlamento Europeo e del Consiglio del 27 aprile 2016

Informativa all'Interessato

Art. 13 del Regolamento (UE) 2016/679
(Informazioni da fornire qualora i dati personali siano **raccolti presso l'interessato**)

1. In caso di raccolta ***presso l'interessato*** di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

- ***l'identità e i dati di contatto del titolare del trattamento*** e, ove applicabile, del suo rappresentante;

- i ***dati di contatto*** del responsabile della protezione dei dati (***DPO***), ove applicabile;

- le ***finalità del trattamento*** cui sono destinati i dati personali nonché la ***base giuridica del trattamento***;

[...]

- gli eventuali ***destinatari o le eventuali categorie di destinatari*** dei dati personali;

- 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, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili;

- il ***periodo di conservazione*** dei dati personali oppure, se non è possibile, i ***criteri utilizzati*** per determinare tale periodo;

- l'esistenza del ***diritto dell'interessato*** di chiedere al titolare del trattamento ***l'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***;

- qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del ***diritto di revocare il consenso in qualsiasi momento*** senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

[...]

- ***l'esistenza di un processo decisionale automatizzato***, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, ***informazioni significative sulla logica utilizzata***, nonché ***l'importanza e le conseguenze*** previste di tale trattamento per l'interessato.

Regolamento (UE) 2016/679 (GDPR) del Parlamento Europeo e del Consiglio del 27 aprile 2016

Liceità del trattamento

Art. 6 del Regolamento (UE) 2016/679 (Liceità del trattamento)

Il ***trattamento è lecito*** solo se e nella misura in cui ricorre ***almeno una delle seguenti condizioni***:

a) l'interessato ha espresso il ***consenso*** al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario ***all'esecuzione di un contratto*** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per ***adempiere un obbligo legale*** al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la ***salvaguardia degli interessi vitali*** dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per ***l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*** di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il ***perseguimento del legittimo interesse del titolare del trattamento o di terzi***, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Regolamento (UE) 2016/679 (GDPR) del Parlamento Europeo e del Consiglio del 27 aprile 2016

Consenso dell'Interessato

Considerando 32 del Regolamento (UE) 2016/679

- Il consenso espresso mediante un ***atto positivo inequivocabile*** con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano (***NO : silenzio, l'inattività o la preselezione di caselle***).

- Se il trattamento ha ***più finalità***, il consenso deve essere ***prestato per ognuna di queste***.

Regolamento (UE) 2016/679 (GDPR) del Parlamento Europeo e del Consiglio del 27 aprile 2016

Consenso dell'Interessato

Art. 7 del Regolamento (UE) 2016/679 - Condizioni per il consenso

1. 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. (***onere della prova a carico del titolare***)

2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, ***la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro***. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.

Regolamento (UE) 2016/679 (GDPR) del Parlamento Europeo e del Consiglio del 27 aprile 2016

Consenso dell'Interessato

Art. 7 del Regolamento (UE) 2016/679 - Condizioni per il consenso

3. L'interessato ha il ***diritto di revocare il proprio consenso in qualsiasi momento***. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

4.Nel ***valutare se il consenso sia stato liberamente prestato***, si tiene nella massima considerazione l'eventualità, tra le altre, che ***l'esecuzione di un contratto***, compresa la prestazione di un servizio, sia ***condizionata alla prestazione del consenso*** al trattamento di dati personali ***non necessario all'esecuzione di tale contratto***.

Violazione di sicurezza dei dati

(«Data Breach»)

Data Breach

Il WP29 ha ricordato che il *Data Breach* consiste in una 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.

Il Gruppo di lavoro ex art. 29 ("WP29") ha adottato il 6 febbraio 2018 la versione definitiva delle linee guida sulla notifica delle violazioni dei dati personali (cd. "*Data Breach*") ai sensi del Regolamento UE n. 679/2016 (cd. "GDPR").

Data Breach

Il WP29, riprendendo la distinzione già operata nel suo precedente parere 03/2014, suddivide la violazione dei dati personali in tre categorie:

– "***Confidentiality breach***": in caso di divulgazione o accesso non autorizzato o accidentale a dati personali;

– "***Availability breach***": in caso di cancellazione / distruzione non autorizzata o accidentale di dati personali;

– "***Integrity breach***": in caso di modifica non autorizzata o accidentale di dati personali.

Notifica di una violazione di dati (*Data Breach*)

- Il titolare del trattamento notifica la violazione **all'autorità di controllo competente** […] senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, a meno che sia **improbabile** che la violazione dei dati personali presenti un **rischio per i diritti e le libertà delle persone fisiche.**

- Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Notifica di una violazione di dati (*Data Breach*)

- Il WP29 ha illustrato, inoltre, uno scenario in cui il titolare del trattamento, venendo a conoscenza di una prima violazione, si ritrovi, prima della notifica, a rilevare altre **violazioni simili, ma con cause diverse**.

- In tal caso, a seconda delle circostanze, il WP29 ha chiarito che il titolare, invece di notificare ogni singolo *Data Breach*, potrà provvedere **con un'unica notifica contenente le diverse violazioni**, qualora tali violazioni riguardino le **stesse categorie di dati** e si siano verificate **tramite le stesse modalità**, in un arco temporale ristretto.

- Qualora, invece, le violazioni riguardino categorie diverse di dati personali e si siano verificate **tramite differenti modalità**, il titolare dovrà effettuare una **notifica specifica per ciascuna violazione riscontrata**, in conformità all'articolo 33 del GDPR.

Comunicazione di una violazione di dati

Quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

La comunicazione all'interessato <u>non è richiesta</u> se il titolare:

a) ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati.

info@pclex.it