info@pclex.it

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

Regolamento UE 2016/679 (Data Protection)

Principi Generali e Definizioni
Soggetti

Università di Torino - Dipartimento Informatica

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

Normativa

Regolamento (UE) 2016/679	→	**In vigore dal 25 maggio 2018**
D.Lgs. 196/2003	→	Nuovo D.Lgs. 101/2018 – ***Abrogazione selettiva***
Direttiva 2002/58 (trattamento dati comunicazioni elettroniche)	→	**Codice Europeo Comunicazioni Elettroniche** Direttiva 2018/1972 - D.Lgs. 207/2021
Provvedimenti Garante Privacy	→	NON Decadono fino a quando non verranno modificati, sostituiti o abrogati
Accordi Internazionali su trasferimento dati	→	NON Decadono fino a quando non verranno modificati, sostituiti o abrogati

L’approccio innovativo basato sull’accountability del Titolare (art. 24 GDPR)

Il TITOLARE è responsabile per la *compliance* ai principi privacy

e deve essere in grado di DIMOSTRARLA (art. 5, co.2)

Tenuto conto di NATURA, AMBITO, CONTESTO, FINALITA’, RISCHI

↓

mette in atto

Misure TECNICHE ed ORGANIZZATIVE ADEGUATE per garantire, ed **essere in grado di dimostrare**, che il trattamento è effettuato conformemente al GDPR. Dette misure sono riesaminate ed aggiornate qualora necessario.

Ciò implica l’adozione di un **SISTEMA DI GESTIONE DELLA DATA PROTECTION che consenta di gestire nel tempo** la *compliance.*

L'approccio innovativo basato sull'accountability del Titolare e le principali novità del Regolamento

- Le definizioni e di principi generali previsti dal Codice Privacy restano sostanzialmente invariati, ma **cambia la filosofia**

- **Nuovo approccio metodologico**, risk-based, basato sulla **protezione dei dati dell'utente** e sull'**effettivo rischio** per ogni azienda

- Da un sistema di tipo formalistico ad un sistema di Governance dei Dati Personali basato su un'alta responsabilizzazione sostanziale («***accountability***») del Titolare, a cui è richiesto **proattività**, cioè di **prevenire** e non correggere, nonché di **dimostrare**, tramite l'elaborazione di un **idoneo sistema documentale** di gestione della privacy e di appropriate policies interne, **da esibire** in caso di richiesta da parte dell'Autorità, la conformità al GDPR e **l'adeguatezza delle proprie scelte/valutazioni**.

Protezione sin dalla progettazione
(*by design e by default*)

Le misure a protezione di dati devono essere **adottate già al momento della progettazione di un prodotto o software (*design*)**.

Il titolare del trattamento deve mettere in atto misure tecniche e organizzative **adeguate** per garantire in ogni caso che siano trattati **solo i dati necessari per ogni specifica finalità (*default*)**.

Accountability - Obblighi Documentali

Registro Trattamenti

DPIA

Lettere Incarico / Nomina Responsabile / ….

Policy Organizzativa e Misure (Tecniche) di Sicurezza

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

Applicabilità GDPR alle sole persone fisiche

Definizione di trattamento e dato personale

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

Applicabilità GDPR alle sole persone fisiche + Def. Dato Personale

Articolo 4 Definizioni
Ai fini del presente regolamento s'intende per:

1) ***«dato personale»***: qualsiasi informazione riguardante una ***persona fisica identificata o identificabile («interessato»)***; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

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

Definizione di trattamento

Articolo 4 Definizioni
Ai fini del presente regolamento s'intende per:

2) ***«trattamento»***: ***qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali***, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

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

Trattamento di categorie particolari di dati personali

Articolo 9, comma 1 (***ex Dati Sensibili***)

Dati personali che rivelino **l'origine razziale o etnica**, le **opinioni politiche**, le convinzioni **religiose o filosofiche**, o **l'appartenenza sindacale**, nonché trattare **dati genetici**, **dati biometrici** intesi a identificare in modo univoco una persona fisica, dati relativi alla **salute** o alla **vita sessuale** o **all'orientamento sessuale** della persona

Articolo 10 (***ex Dati Giudiziari***)

dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza

CASO 1 - E-mail del dipendente

L’e-mail di lavoro di un dipendente è un dato personale?

CASO 1 - E-mail del dipendente

L'e-mail di lavoro di un dipendente è un dato personale? Dipende.

1. Nel caso in cui l'e-mail sia formulata in termini generici, facendo riferimento alla **funzione** della società di appartenenza (es. HRoffice@companyname.com) questa **non sarà un dato personale**, ma rientrerà in ogni caso nella nozione di "*contraente*" rispetto ai servizi di comunicazione elettronica;

2. Nel caso in cui invece l'indirizzo sia **associato a uno specifico individuo** (es. m.bianco@companyname.com), anche l'indirizzo e-mail lavorativo dovrà essere **considerato dato personale**.

CASO 2 - Persone decedute e nascituri

La definizione di dato personale fa espresso riferimento alla nozione giuridica di "*persona fisica*", ossia secondo le norme civilistiche, ogni essere umano nato vivo, che in quanto tale **diventa centro di imputazione di situazioni giuridiche**.

Quindi le Persone decedute e i Nascituri ?

CASO 2 - Persone decedute e nascituri

1. Persone decedute: il GDPR **esclude** dal proprio ambito di applicazione i "**dati personali delle persone decedute**". Tuttavia, il GDPR continua ad applicarsi nel caso in cui:

- **non si possa accertare** la morte della persona;

- il dato del defunto è **indirettamente riferibile anche a una persona in vita** (es. il **dato sanitario di una malattia genetica** del defunto potrebbe rilevare la medesima patologia nel figlio);

Inoltre, anche a seguito del decesso della persona, **l'art. 2-terdecies del Codice Privacy (D.Lgs. 196/2003 e successive modifiche)** attribuisce **agli eredi o altri soggetti legati al defunto la facoltà di esercitare i diritti di cui agli artt. 15-22 GDPR** con riferimento ai dati del defunto nel caso in cui abbiano un **interesse proprio o agiscano a tutela dell'interessato** (a meno che lo stesso **interessato non avesse vietato tale esercizio quando ancora in vita**).

In ogni caso, anche in assenza della copertura fornita dalla normativa sul trattamento dei dati personali, le informazioni potrebbero essere soggette a un **diverso regime di protezione derivante alla luce di altra normativa nazionale (es. obblighi di confidenzialità del medico)**.

2. Nascituri: né il GDPR, né il Codice Privacy prevedono nulla espressamente. Tuttavia, alla luce degli interventi giurisprudenziali sulla **soggettività giuridica del nascituro** e sulla **sua titolarità di specifici diritti**, nel nostro Paese non sarebbe ingiustificata **un'estensione della tutela in materia di protezione dei dati personali anche nei confronti del concepito**.

CASO 3 - L’Indirizzo IP (*Internet Protocol Address*) è un dato personale?

CASO 3 - L'Indirizzo IP (*Internet Protocol Address*) è un dato personale?

Nonostante l'indirizzo IP non contenga di per sé ulteriori informazioni, può essere utilizzato per elaborare o dedurre ulteriori informazioni sul proprio utente. Proprio per tale motivo, l'indirizzo IP ha sempre rappresentato un **tema abbastanza controverso dal punto di vista della privacy**, specialmente se teniamo inconsiderazione la possibilità che l'IP sia id tipo dinamico (ovvero un indirizzo che cambia ogniqualvolta un utente si connetta ad una determinata rete).

Il GDPR ha definitivamente sciolto ogni dubbio, affermando che **l'indirizzo IP debba essere considerato come un dato personale in quanto ricadrebbe nell'ambito degli identificativi online (*online identifiers*)** come peraltro i cookies.

La ratio di tale scelta è piuttosto evidente: gli indirizzi IP sono registrati dagli internet service providers i quali sono a conoscenza degli utenti ai quali gli indirizzo sono assegnati. Il gestore di una pagina internet registra gli indirizzi IP che accedono ad una determinata pagina. **Se le due informazioni venissero combinate potrebbero permettere l'identificazione di un utente associato ad un determinato indirizzo IP**.

Altri dati che l'indirizzo IP consente di identificare sono la geo-localizzazione e un determinato fornitore di servizi internet.

CASO 4 – I Location data sono dati personali?

CASO 4 – I Location data sono dati personali?

Il GDPR non è stato invece chiaro nel disciplinare più in generale i cosiddetti “Location data”, le informazioni circa l’esatta collocazione geografica di un individuo o di un oggetto. Infatti il **GDPR non ne fornisce una definizione né indicazioni circa la loro gestione**.

Le informazioni sulla esatta localizzazione di un individuo giocano un ruolo estremamente importante nella nostra società e specialmente nella sharing economy (pensiamo ad esempio alle piattaforme di mobilità).

I **dati sulla posizione geografica di un individuo sono sempre dati personali? No, non necessariamente**. Un’attenta valutazione deve essere fatta caso e per caso e molto dipende dal contesto.

CASO 4 – I Location data sono dati personali?

Facciamo alcuni esempi:

- i dati che identificano gli **autoveicoli di una flotta *non* sono dati personali**;

- i dati che individuano la **posizione di un individuo al momento di un pagamento in un centro commerciale *costituiscono* dati personali**;

- i dati che localizzano un **individuo all'interno di un ospedale, o le frequenti visite in un luogo di culto o ad un sindacato** non solo sono **dati personali ma potrebbero rientrare anche nella categoria dei dati sensibili in quanto identificherebbero dati relativi allo stato di salute, orientamento religioso e/o politico di un individuo**.

Famoso è il caso avvenuto agli inizi del 2018 quando una **famosa App (Strava)** che opera come una sorta di social network dei ciclisti e degli sportivi, attraverso la propria heatmap aveva rivelato la **localizzazione di basi militari situate in regioni piuttosto remote**. L'App, che mostra sentieri, piste di allenamento di atleti in tutto il mondo (inclusi i soldati) aveva finito per **rendere le basi militari americane chiaramente identificabili da chiunque**. Impostazione privacy nell'app si è resa fondamentale.

info@pclex.it