Regolamento generale sulla protezione dei dati (GDPR)

REGOLAMENTO (UE) 2016/679
DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 27 aprile 2016
G.U. 04/05/2016 n. L119

In vigore dal 25/05/2016

==========
==========
==========

CAPO VIII - Mezzi di ricorso, responsabilità e sanzioni

CAPO IX - Disposizioni relative a specifiche situazioni di trattamento
---

CAPO X - Atti delegati e atti di esecuzione

CAPO XI - Disposizioni finali

==========
==========
==========

DEFINIZIONI

Dato Personale:
qualsiasi informazione riguardante una persona fisica identificata o identificabile
(direttamente o indirettamente)

Trattamento:
qualsiasi operazione con o senza processi automatizzati (raccolta, registrazione,
organizzazione, strutturazione, conservazione, adattamento, modifica, estrazione,
consultazione, uso, comunicazione, trasmissione, diffusione, messa a disposizione,
raffronto, interconnessione, limitazione, cancellazione, distruzione)

Interessato:
Persona fisica che fornisce i propri dati personali a un Titolare
per le finalità specificate nell'informativa. Proprietario dei dati personali.

Titolare del Trattamento:
La persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente,
associazione od organismo cui competono, anche unitamente ad altro titolare,
le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali
ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Autorizzato al Trattamento:
Persona fisica autorizzata, dal Titolare o dal Responsabile, a compiere le operazioni
di trattamento dei dati, attenendosi alle istruzioni impartite

Responsabile Esterno:
Persona fisica o giuridica che esegue trattamenti per conto del Titolare,
sulla base di un contratto o altro atto giuridico.
Può designare sub-responsabili, ma soltanto previa autorizzazione scritta e specifica.

Responsabile della Protezione dei Dati RPD/DPO (Data Protection Officer):
Designato dal Titolare del trattamento, è obbligatoria per alcune tipologie di soggetti,
tra i quali la Pubblica Amministrazione, i soggetti che trattano dati particolari quali
quelli sanitari, o quelli su larga scala.
La nomina del DPO deve essere comunicata all'Autorità di Controllo (Garante).

Compiti del DPO:
- consulenza sugli obblighi del Regolamento
- sorveglianza sul rispetto del Regolamento
- pareri sulle DPIA
- essere un riferimento per il pubblico e un raccordo con l'Autorità di Controllo

---

In Insubria:

Il Titolare del Trattamento è l'Università degli Studi dell'Insubria, nella persona
del Magnifico Rettore, con sede legale a Varese (VA) in Via Ravasi, 2.

Il Responsabile del trattamento per la fornitura dei servizi del sistema Portale di Ateneo
è il consorzio CINECA con sede legale in Via ..., ... Casalecchio di Reno (BO).

L'Ateneo ha nominato il Responsabile della protezione dei dati (RPD/DPO),
Avv. Valerio Edoardo Vertua, indirizzo e-mail privacy@uninsubria.it

Il Rettore ha autorizzato i Direttori di Dipartimento, il Presidente della Scuola
di Medicina, il Direttore Generale, i Dirigenti alla sottoscrizione in propria vece,
per quanto di rispettiva competenza, delle nomine ad Autorizzato al Trattamento
e a Responsabile Esterno in tutti i casi necessari.

Categorie di Dati Personali:

Dati Identificativi
Tutte le informazioni identificative, dai dati anagrafici alle immagini che ritraggono
la persona, compresi numeri identificativi univoci (es. matricola, CF) o nomi utente

Dati relativi alle comunicazioni elettroniche
Via telefono o internet come, per esempio, un indirizzo IP

Dati di Geolocalizzazione
che consentono di geolocalizzare una persona e da cui è possibile capire dove è andata,
quando e a volte anche con chi

Dati particolari (ex sensibili)
Possono rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni
religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici,
dati relativi alla salute o alla vita sessuale o all'orientamento sessuale.

Dati genetici
Caratteristiche genetiche ed ereditarie o acquisite, informazioni sulla fisiologia
o sulla salute, dall'analisi di un campione biologico.

Dati biometrici
Ottenuti da un trattamento tecnico specifico relativo alle caratteristiche fisiche,
fisiologiche o comportamentali, consentono o confermano l'identificazione univoca
(es. immagine facciale o dati dattiloscopici).

Dati relativi alla salute
Attinenti alla salute fisica o mentale, compresa la prestazione di servizi di assistenza
sanitaria che rilevano informazioni relative allo stato di salute.

Dati relativi a condanne penali e reati (ex giudiziari)
Riguardanti provvedimenti giudiziari, condanne penali e reati e/o misure di sicurezza
ad essi connesse.

I dati possono essere:

1. Provided, cioè forniti consapevolmente dall’utente (es. registrazione)
2. Observed, cioè desumibili dalla navigazione dell’utente
3. Derived, cioè derivati da una precedente raccolta (es. profilazione)
4. Inferred, cioè aggregati su cui vengono fatte previsioni statistiche

---
Consenso

Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile
con la quale l'interessato manifesta il proprio assenso,
mediante dichiarazione o azione positiva inequivocabile,
che i dati personali che lo riguardano siano oggetto di trattamento.

Il consenso dei minori è valido a partire dai 16 anni, prima è necessario quello
dei genitori o di chi ne fa le veci.
Il consenso non è obbligatorio e può essere revocato in ogni momento.
Il Titolare del trattamento è tenuto a di dimostrare i consensi acquisiti.

Informativa - dovrà contenere:
 - identità e contatti del Titolare e del DPO
 - finalità del trattamento ed eventuali destinatari
 - eventuale trasferimento ad un paese terzo
 - periodo di conservazione
 - diritti dell'interessato
 - esistenza di un eventuale processo decisionale automatizzato, compresa la profilazione

---
Diritti degli interessati:
1. Accesso
2. Rettifica
3. Cancellazione (cd. Oblio)
4. Limitazione
5. Portabilità
6. Opposizione
7. Revoca (del Consenso)

Principi GDPR del Trattamento:
- Liceità (base giuridica e consenso)
- Accountability (Responsabilizzazione)
- Minimizzazione (solo i dati necessari)
- Limitazione (solo per la finalità descritta)
- Sicurezza (applicazione di misure e standard)
- Correttezza (veridicità ed aggirnamento dei dati)
- Integrità (minimizzazione degli errori di gestione)

Liceità del trattamento (almeno una):
1. l'interessato ha espresso il consenso
2. esecuzione di un contratto di cui l'interessato è parte
3. adempiere un obbligo legale
4. salvaguardia degli interessi vitali
5. esecuzione di un compito di interesse pubblico o esercizio di pubblici poteri
6. perseguimento del legittimo interesse del titolare

Accountability (Responsabilizzazione) e Approccio basato sul Rischio:

Il Titolare deve attuare le disposizioni del Regolamento ed essere in grado di comprovare
la conformità dei trattamenti. Deve adottare un approccio basato sul rischio,
ovvero deve considerare i rischi che potrebbero configurarsi per i diritti e le libertà
degli interessati in relazione alle attività di trattamento:
a. Data Protection by Design e by Default
b. Valutazione d'impatto sulla protezione dei dati personali (DPIA)
c. Registro delle attività di trattamento
d. Sicurezza del trattamento
e. Notifica dei Data Breach

a. Data Protection by Design e by Default

1. Le misure tecniche e organizzative adottate dal titolare del trattamento devono essere, fin dall'inizio, coerenti con i vincoli normativi e con le finalità del trattamento nonché adeguate rispetto ai rischi per i diritti e le libertà degli interessati.

2. Per impostazione predefinita, siano trattati solo dati personali necessari per ogni specifica finalità

b. Valutazione di impatto sulla protezione dei dati personali (DPIA)

In certe situazioni il titolare deve compiere una valutazione di impatto sulla protezione dei dati personali (Data Protection Impact Assessment, DPIA). É lo strumento necessario a valutare i rischi per i diritti e le libertà degli interessati connessi all'attività di trattamento. Sulla base di tale analisi dei rischi è possibile determinare probabilità, minacce, impatti e misure di sicurezza in grado di mitigare il rischio rilevato.

Obbligatoria per:
- trattamento automatizzato
- profilazione
- trattamento su larga scala
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico

Deve contenere:
- descrizione dei trattamenti previsti e delle finalità
- valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità
- valutazione dei rischi per i diritti e le libertà degli interessati
- misure previste per mitigare i rischi

I risultati della valutazione dovranno essere la base per la progettazione delle misure di sicurezza adeguate ai rischi rilevati.

c. Registro delle attività di trattamento

Il Registro delle attività di trattamento è un importante strumento che consente al Titolare di disporre un quadro sempre aggiornato dei trattamenti all'interno dell'organizzazione ai fini della corretta gestione dei dati personali.
In particolare, per ciascuna attività di trattamento, devono essere riportate in tale registro le tipologie di dati, le misure tecniche e organizzative adottate, le categorie di interessati, le finalità del trattamento e le basi giuridiche.

d. Sicurezza del trattamento

L'Accountability e l'approccio basato sul rischio impongono che ci sia da parte del titolare l'adozione di adeguate misure di sicurezza, tecniche e organizzative, per la protezione dei dati personali, tenuto conto dei costi di attuazione e dei rischi per i diritti e le libertà degli interessati.
A titolo esemplificativo: la cifratura e la pseudonimizzazione; la capacità di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di ripristinare la disponibilità e l'accesso dei dati personali in caso di incidente; una procedura per testare e verificare l'efficacia delle misure tecniche e organizzative.

e. Notifica dei data breach

La violazione dei dati personali comporta, qualora la stessa presenti un rischio per i diritti e le libertà dell'interessato, l'obbligo in capo al Titolare di notifica all'Autorità entro delle tempistiche prestabilite (72 ore dal momento in cui ne viene a conoscenza). Inoltre, in alcuni casi di particolare gravità la comunicazione deve essere fatta anche nei confronti dell'Interessato in modo tale da permettere a quest'ultimo di proteggersi da eventuali conseguenze negative della violazione.

DATA BREACH

Violazione di sicurezza che comporta, accidentalmente o in modo illecito:
 - distruzione
 - perdita
 - modifica
 - divulgazione non autorizzata
 - accesso ai dati personali trasmessi, conservati e trattati

Possibili Cause:
 - Errore umano (es. smarrimento dispositivo, cancellazione/modifica accidentale)
 - Attività infedele (modifica/rivelazione non autorizzata, furto)
 - Accesso abusivo (attraverso i sistemi informatici da parte di soggetti esterni)

Misure di sicurezza da adottare, di tipo:
 - organizzativo
 - fisico
 - logico
adeguate a minimizzare i rischi.

Classificazione delle violazioni:
 - riservatezza: accesso/divulgazione
 - integrità: alterazione
 - disponibilità: perdita (definitiva o temporanea)
in ogni caso non autorizzati o accidentali

Esempi:
 - invio email a destinatari errati (riservatezza)
 - modifica di un DB per scopi/vantaggi personali (integrità)
 - impossibilità di accedere ai dati per attacchi informatici (disponibilità)

Procedure:
- adottare una specifica policy l'utilizzo delle risorse informatiche aziendali
- organizzare apposite sessioni formative per il personale
- adottare una procedura interna per la gestione delle violazioni
- individuare con chiarezza le figure che devono essere avvisate e coinvolte
- predisporre un registro delle violazioni in cui documentare tutti i databreach
  a prescindere dalla notifica all'autorità o dalla comunicazione agli interessati:
  il Titolare deve documentare le relazioni in un apposito registro al fine di consentire
  eventuali controlli dell'autorità sul rispetto della normativa.
- il DPO deve essere coinvolto nella valutazione del rischio e nella scelta delle misure
  di sicurezza tecniche e organizzative. In caso di data breach per la valutazione circa
  la necessità della notifica all'autorità di controllo e della comunicazione agli
  interessati.
