GDPR

nuove regole, strumenti operativi per la privacy

Obiettivi

Il documento ha l'obiettivo di:
dare una sintetica panoramica dei requisiti del Regolamento, integrata con la normativa italiana, concentrare l'attenzione sulle disposizioni applicabili alle associazioni e fornire una lista ragionata di 'cose da fare' per approcciare la conformità

Cosa è il **GDPR - UE 2016/679**

Il GDPR è un Regolamento direttamente applicabile e vincolante per tutti gli Stati membri.
È in vigore dal 2016 e diventato definitivamente applicabile in via diretta in tutti gli Stati membri dal 25 maggio 2018.
Si applica integralmente a tutte le organizzazioni, pubbliche e private, situate nel territorio dell'Unione Europea ed alle imprese situate fuori dall'Unione europea che offrono servizi e prodotti a persone che si trovano nel territorio dell'Unione stessa.

Dove si applica?

Cosa è il **GDPR - UE 679/2016?**

Il **G**eneral **D**ata **P**rotection **R**egulation
uniforma i diritti delle persone su tutto il territorio dell'Unione
uniforma le definizioni delle responsabilità e l'applicabilità
delle regole
uniforma gli obblighi per i titolari di trattamento sul territorio dell'Unione
al fine di garantire la protezione e la libera circolazione
dei dati personali
Il GDPR si occupa di tutelare i diritti e le libertà delle persone fisiche

Com’era regolamentata la privacy prima del **GDPR?**

- direttiva CE n°46/1995 (da cui è scaturita in Italia la legge 675/1996)
- codice in materia di protezione dei dati personali d.lgs. 196/2003

GDPR chi tutela?

il GDPR si occupa di tutelare i diritti e le libertà delle

persone fisiche

Cosa sono i **dati personali**?

- nomi
- foto
- indirizzi mail
- dettagli bancari
- interventi sui siti web
- social network
- informazioni mediche
- indirizzi ip

Cosa sono i dati personali **particolari**?

dati

- genetici
- biometrici
- relativi alla salute

dati personali che rivelino

- l'origine razziale o etnica,
- le opinioni politiche,
- le convinzioni religiose o filosofiche,
- l'appartenenza sindacale, l'orientamento sessuale
- condanne penali

Quali sono gli **imperativi** nel trattamento dei dati personali?

1. **MINIMIZZAZIONE**: tratta meno dati possibile e solo quelli essenziali
2. Distribuisci le responsabilità
3. Favorisci l'**ANONIMIZZAZIONE** e la **PSEUDONIMIZZAZIONE**
4. **ACCOUNTABILITY**

Accountability cosa vuol dire?

- archivi protetti
- antivirus, backup
- scrivanie pulite, scrivania con faldoni crociati
- fabbrica sotto bolla

Accountability cosa vuol dire?

TRASPARENZA & RESPONSIVITA’
(capacità di rendere conto)

Accountability cosa vuol dire?

La protezione dei dati deve essere messa in atto **by design**:
il Titolare del trattamento deve progettare e adottare misure tecniche e organizzative adeguate a rispettare i principi e le disposizioni del Regolamento e deve saper dimostrare questo requisito (documentare la progettazione del trattamento).

La protezione dei dati deve essere garantita **by default**:
il Titolare del trattamento deve garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (quantità, portata, periodo di conservazione e accessibilità).

Come deve essere l'**informativa**?

Deve essere sempre resa, anche non per iscritto.
Deve essere precisa, intellegibile, semplice e chiara.
Deve contenere almeno:

- Identità e contatti del titolare del trattamento (e del DPO)
- Finalità del trattamento e fondamento di liceità del trattamento
- Eventuali destinatari
- Eventuali trasferimenti fuori UE
- Periodo di conservazione
- Diritti dell'interessato
- Eventuale esistenza di un processo decisionale automatizzato

Quali sono i **diritti** dell'interessato?

- ACCESSO Conferma del trattamento, accesso ai dati e diritto ad una copia
- RETTIFICA Correzione o integrazione dei dati personali inesatti, parziale cancellazione
- OBLIO Diritto di decidere che siano cancellati e non sottoposti ulteriormente a trattamento i dati personali non più necessari per le finalità per le quali sono stati raccolti
- LIMITAZIONE DEL TRATTAMENTO Limitazione del trattamento alla sola conservazione
- RECLAMO Reclamo all'autorità di controllo per ogni presunta violazione del Regolamento
- REVOCA DEL CONSENSO Il consenso può essere sempre revocato
- PORTABILITÀ Ricezione dei dati personali in un formato strutturato, di uso comune, leggibile da dispositivo automatico e liberamente trasferibile ad altro titolare senza impedimenti
- OPPOSIZIONE Il diritto all'opposizione si riferisce invece sempre alle specifiche modalità di trattamento da parte del titolare o di terzi. L'interessato ha il diritto di opporsi in qualsiasi momento al trattamento automatizzato dei dati personali che lo riguardano, oppure che abbia finalità di profilazione, di marketing diretto, di ricerca scientifica, storica o statistica. In quest'ultimo caso il diritto dell'interessato può essere limitato per interessi pubblici superiori

Quando il trattamento è **lecito**?

Il trattamento di dati personali è lecito soltanto se basato su uno dei seguenti fondamenti:

- il consenso
- l'esecuzione di un contratto
- gli obblighi legali del titolare
- la salvaguardia degli interessi vitali di un terzo
- l'interesse pubblico rilevante
- l'interesse legittimo del titolare del trattamento

Come chiedere il **consenso**?

- linguaggio semplice, chiaro
- specificare le finalità
- modalità comprensibile, accessibile
- liberamente prestato
- dimostrabile

E i **minori**?

Il trattamento dei dati personali dei minori di anni 18 necessita dell’autorizzazione dei genitori

E i minori?

Per quanto riguarda l'offerta diretta di servizi delle società dell'informazione ai minori (es. Facebook, Instagram, Google), il trattamento di dati personali è lecito ove l'interessato, con almeno 16 anni d'età, abbia prestato il suo consenso.

Se il minore ha meno di 16 anni, tale trattamento è lecito soltanto se il consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

Gli Stati membri possono stabilire per legge un'età inferiore, ma la soglia minima è 13 anni.

Nel decreto italiano la soglia minima è di 14 anni.

Chi è il **titolare** del trattamento?

La persona fisica, giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o congiuntamente, determina le finalità e i mezzi del trattamento.Il titolare del trattamento mette in atto, riesamina e aggiorna le misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR.

Cos’è il **trattamento**?

Trattamento è 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.

Ad esempio: la raccolta, la registrazione, la conservazione, l'organizzazione, la consultazione, l’elaborazione, la modificazione, la selezione, l’estrazione, il raffronto, l’utilizzo, il blocco, la comunicazione, la diffusione e la cancellazione di dati personali.

Chi è il **responsabile** del trattamento?

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare e non può trattare dati personali se non è istruito dal titolare del trattamento.
In particolare, il soggetto identificato come responsabile deve:

- presentare garanzie sufficienti ad attuare misure adeguate di protezione
- trattare i dati sulla base di un chiaro rapporto contrattuale (natura, finalità, durata del trattamento, tipi di dati, categorie di interessati, obblighi e diritti)
- garantire l'impegno o il vincolo alla riservatezza degli incaricati
- mettere a disposizione tutte le informazioni per comprovare la conformità
- impegnarsi a cancellare i dati al termine della prestazione di servizi

Se un responsabile viola il regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento

Chi materialmente tratta i dati?

Il titolare o il responsabile del trattamento individua le modalità più opportune per autorizzare alla raccolta e al trattamento dei dati personali i collaboratori che operano sotto la propria autorità diretta.

L’autorizzazione deve essere formalizzata.

Gli autorizzati devono essere opportunamente formati.

Quando la nomina del **DPO** (Data Protection Officer) è **obbligatoria**?

in ambito privato sono tenuti alla designazione del responsabile della protezione dei dati personali i soggetti le cui principali attività consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala di categorie particolari di dati personali o di dati relative a condanne penali e a reati

Ricorrendo i suddetti presupposti, sono tenuti alla nomina, a titolo esemplificativo e non esaustivo:

istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; caf e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento.

Cosa fa il **DPO** (Data Protection Officer)?

Le funzioni del DPO riguardano principalmente la consulenza al titolare e al responsabile del trattamento sul rispetto degli obblighi derivanti dal GDPR e dalla normativa nazionale, oltre a verificarne l'osservanza.

Al DPO si chiede inoltre di collaborare con il Garante e di esserne il punto di riferimento per facilitare l'accesso a documenti e informazioni riguardanti l'azienda o l'ente.

Collaborare con titolare e responsabile, se richiesto, alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento.Al DPO si chiede di comunicare al Garante eventuali violazioni dei dati personali

DPO **interno** od **esterno** all'organizzazione ?

Il DPO può essere un dipendente oppure un soggetto esterno all'organizzazione, assunto in base a un contratto di servizi, i cui dati di contatto sono pubblicati e comunicati all'autorità Garante nazionale.

Particolare attenzione va posta nel caso di nomina di un dipendente, in quanto il ruolo che ricopre nell'organizzazione deve escludere ogni forma di conflitto di interesse ed essere compatibile con l'esercizio autonomo ed indipendente delle sue funzioni.

Cos'è il **registro dei trattamenti**?

Le note del Garante Italiano:
«La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì integrante di un sistema di corretta gestione dei dati personali. Il Garante invita tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro (compiere un'accurata ricognizione dei trattamenti rispettive caratteristiche)»
Il registro contiene almeno:

1. Il nome e i dati di contatto del titolare del trattamento e, se nominati, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati (DPO)
2. Finalità di ogni trattamento
3. Descrizione delle categorie di interessati e di dati
4. Categorie (eventuali) di destinatari
5. Trasferimenti (eventuali) verso paesi terzi
6. Termini per la cancellazione delle diverse categorie di dati
7. Descrizione generale delle misure tecniche e organizzative

Quando è **obbligatorio?**

In particolare, in ambito privato, i soggetti obbligati sono così individuabili:

- imprese o organizzazioni con almeno 250 dipendenti;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che possano presentare un rischio – anche non elevato – per i diritti e le libertà dell'interessato;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti non occasionali;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle **categorie particolari** di dati o di dati personali relativi a **condanne penali e a reati**.

Chi è il **Garante?**

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

www.garanteprivacy.it

Chi è il **Garante?**

Autorità amministrativa **indipendente**
Istituita nel 1996

www.garanteprivacy.it

Quali poteri ha il **Garante?**

Potere di controllo:

- ammonire il titolare del trattamento o il responsabile del trattamento
- ingiungere di conformare i trattamenti alle disposizioni del Regolamento
- imporre una limitazione provvisoria o definitiva del trattamento, incluso il divieto di trattamento
- ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento
- imporre sanzioni pecuniarie

Chi supporta il **Garante** nell'attività di controllo?

La Guardia di Finanza

www.gdf.gov.it

Come?

attraverso l’attività ispettiva e di verifica

Cosa fa il **Garante?**

- cura l'informazione e sviluppa la consapevolezza del pubblico e dei titolari del trattamento in materia di protezione dei dati personali;
- segnala al Parlamento e altri organismi e istituzioni l'esigenza di adottare atti normativi e amministrativi relativi alle questioni riguardanti la protezione dei dati personali;
- formula pareri su proposte di atti normativi e amministrativi;
- partecipa alla discussione su iniziative normative con audizioni presso il Parlamento;
- predispone una relazione annuale sull'attività svolta e sullo stato di attuazione della normativa sulla privacy da trasmettere al Parlamento e al Governo;
- partecipa alle attività dell'Unione europea ed internazionali di settore, anche in funzione di controllo e assistenza relativamente ai sistemi di informazione Europol, Schengen, VIS, e altri;

www.garanteprivacy.it

Associazioni Sportive e GDPR

Le associazioni sportive trattano sempre dati personali e rientrano pertanto nella normativa GDPR: elenco associati

Il conferimento dei dati avviene al momento dell'iscrizione/tesseramento

CUS e **GDPR**

Il CUS di Bergamo nel rispetto della nuova normativa:

- ha aggiornato la propria modulistica (informativa e richiesta del consenso in sede di iscrizione) e le procedure interne
- ha espressamente autorizzato gli incaricati al trattamento
- si è dotata di registro elettronico
- ha una rete informatica con i più elevati standard di sicurezza

CUS e **INFORMATIVA**

La nuova informativa del CUS spiega

- chi è il titolare del trattamento
- quali sono le finalità del trattamento e come esso verrà effettuato
- chi sono i destinatari dei dati personali e per quanto tempo verranno conservati

La nuova informativa del CUS elenca i diritti dell'interessato

- accesso
- modifica
- rettifica
- oblio
- etc...

CUS e **INFORMATIVA**

La nuova informativa del CUS specifica
chi è il responsabile della protezione dei dati al quale l'utente può sempre rivolgersi

privacy@cusbergamo.it

CUS e **INFORMATIVA**

L’informativa PRECEDE la richiesta del consenso al trattamento

Ai fini dell’accesso agli impianti e servizi il CUS chiede il consenso per l’acquisizione e la conversione in un codice numerico dell’impronta digitale, secondo modalità che rispettano la normativa sulla privacy

Cosa fare in caso di **RECLAMO?**

Ricordare all'utente il contenuto dell'informativa e del consenso sottoscritto

In caso di ulteriori dubbi invitare l'utente a rivolgersi al responsabile della protezione dei dati scrivendo a

privacy@cusbergamo.it

CUS e **personale autorizzato**

All’interno del CUS solo il personale espressamente autorizzato ed opportunamente formato può trattare i dati personali

Che cos'è il **data breach**?

Il data breach è una violazione di sicurezza dei dati.

Ad esempio:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati
- il furto o la perdita di dispositivi informatici contenenti i dati
- l'alterazione dei dati personali
- l'impossibilità di accedere ai dati per attacchi esterni accidentali quali virus, malware
- la perdita o la distruzione dei dati a causa di incidenti, incendi o altre calamità
- la divulgazione non autorizzata

Cosa fare in caso di **data breach**?

Il personale autorizzato del Centro Universitario Sportivo di Bergamo che rilevi una violazione dei dati personali dovrà immediatamente comunicarlo al titolare e al responsabile della protezione dei dati all'indirizzo mail:

privacy@cusbergamo.it

grazie per l'attenzione

avv. Brancato Samanta