

General
Data
Protection
Regulation

Protezione
Riservatezza
Integrità
Vera
Assoluta
Completa
Yang o No



Quando la
Parrocchia si
occupa della
povertà
digitale
e dei doveri
digitali

Di cosa parliamo

La privacy come protezione delle persone.

Cosa significa parlare di Privacy, GDPR e protezione delle persone.

Internet e dati: risorsa a pericolo.



Di cosa parliamo



Di cosa parliamo

Cos'è la privacy:

- Le capacità della rete rendono difficile spiegarlo
- Anche le parrocchie (ed i gruppi parrocchiali) devono essere **competenti** e **prudenti**

Privacy o GDPR?

- Sono sinonimi
- GDPR significa:
 - **G**enerale **D**ata **P**rotection **R**esource
 - Riservatezza delle Informazioni

Privacy o GDPR?



- Un esempio della *logica* GDPR



- ***** , congregazione *****
- Laureato in ***** *****
- Informatico per lavoro (****)
- Certificato **** *****
- Ex ****, partecipante *****
- Attualmente *** *****

- Stefano Bortolato, congregazione Don Orione
- Laureato in Scienze Della Comunicazione Sociale
- Informatico per lavoro (RHCS)
- Certificato ITIL foundation
- Ex ISC², partecipante CLUSIT
- Attualmente Don dell'Oratorio

Cos'è il GDPR

Iniziamo scoprendo il GDPR.



Cos'è il GDPR

- **Regolamento EU 2016/679** del 27 aprile 2016
- Regolamento: legge da applicare subito
- Nasce dal bisogno di proteggere le persone di fronte alle nuove tecnologie

Cf. attacco all'Ospedale "San Giovanni" di Roma del 2021

Cos'è il GDPR

- Testo del regolamento

http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ITA&toc=OJ:L:2016:119:TOC

- Un'ottima guida introduttiva (scaricare il PDF)

<http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali>

Cos'è il GDPR

- Il regolamento è fatto da:
 - 173 note di premessa
 - 99 articoli
- L'articolo 91 riguarda le chiese e le associazioni:

Cos'è il GDPR

1. Qualora in uno Stato membro chiese e associazioni o comunità religiose applichino, al momento dell'entrata in vigore del presente regolamento, corpus completi di norme a tutela delle persone fisiche con riguardo al trattamento, tali corpus possono continuare ad applicarsi purché siano resi conformi al presente regolamento.
2. Le chiese e le associazioni religiose che applicano i corpus completi di norme di cui al paragrafo 1 del presente articolo sono soggette al controllo di un'autorità di controllo indipendente che può essere specifica, purché soddisfi le condizioni di cui al capo VI del presente regolamento.

Inquadramento Generale

I principali assi del GDPR.



Inquadramento Generale

- È un framework normativo
- Filosofia: prescrive il fine, non l'agire (approccio anglosassone)
- Rango: regolamento UE = legge esecutiva (non serve né recipimento, né norme attuative)
- Consenso: è richiesto, deve essere esplicito, inequivocabile e dimostrabile. È valido dai 16 anni

Inquadramento Generale

- Ricade su tutte le relazioni commerciali ed aziendali
- Non serve autorizzazione per le aziende pubbliche (es. anagrafe comunale) e per i dati necessari ai contratti
- Dati sensibili sono: origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, dati penali, dati *militari*.

GDPR: pene

- Massimale fissato a fino a €20.000.000 o al 4% del fatturato totale mondiale dell'impresa-Diocesi-Congregazione

GDPR: attenzione!

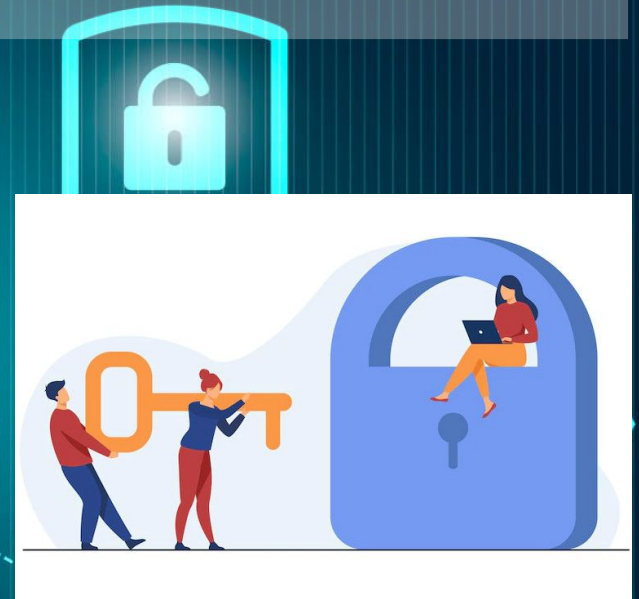
- Il consenso:
 - Deve essere espresso (mai sottinteso o predefinito)
 - Deve essere esplicito
 - Deve essere inequivocabile
 - Deve essere dimostrabile
 - Nelle dichiarazioni scritte deve essere chiaramente distinguibile
 - Deve essere (facilmente) comprensibile
 - Deve essere chiara la finalità della raccolta dati e le modalità di conservazione

Concetti Chiave

Le terminologie specifiche del GDPR.

Le persone *chiave*.

Le autorizzazioni necessarie.



GDPR: concetti chiave

- **Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);
- **Trattamento:** qualsiasi operazione compiuta con o senza l'ausilio di processi automatizzati;
- **Profilazione:** qualsiasi forma di trattamento per valutare determinati aspetti personali;

GDPR: concetti chiave

- **Pseudonimizzazione:** tecnica con cui i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive;
- **Archivio:** qualsiasi insieme strutturato di dati personali;
- **Interessato:** persona fisica che dà i dati e/o il consenso;

GDPR: concetti chiave

- **Titolare del trattamento:** chi ha i dati e li tratta;
- **Responsabile del trattamento:** chi gestisce il trattamento dei dati per il titolare del trattamento;
- **Consenso dell'interessato:** la manifestazione dell'assenso libero, specifico, informato e inequivocabile dell'interessato;
- **Violazione dei dati personali:** distruzione, perdita, modifica, divulgazione o l'accesso ai dati personali sia accidentalmente, sia illecita.

GDPR: responsabile

- Sempre il Parroco (persona giuridica)
- Sempre il Presidente (di un gruppo/associazione; cf. norme terzo settore)
- Il Parroco o il Presidente “nomina” (non delega) i sotto-responsabili
- Il Parroco o il Presidente può avvalersi di un “Responsabile della Protezione Dati” (=DPO o RPD)

GDPR: !! ATTENZIONE !!

Nessuno può accedere ai dati personali se non è **nominato** o non ha preso un **impegno di riservatezza**.
I dati personali e sensibili **non devono essere accessibili**.

GDPR: !! ATTENZIONE !!

- Tutto il Regolamento si basa su 2 idee base:
 - **By design**: gli strumenti sono sicuri (criptazioni, armadi securizzati, ecc...)
 - **By Default**: l'organizzazione è sicura (persone formate, operatori nominati-autorizzati, ecc...)

Aspetti Esecutivi

Le principali cose da fare.

I principali diritti da rispettare.



GDPR: diritti degli interessati

- Accesso ai dati
- Rettifica dei dati
- Diritto all'oblio
- Diritto di limitazione del trattamento

Responsabile Protezione dei Dati

- RPD o DPO: acronimi
 - **R**esponsabile **P**rotezione **D**ati
 - **D**ata **P**rotection **O**fficer
- Non è obbligatorio
- È un dipendente interno o esterno (~Consulente)
- È un tecnico specialista nel GDPR e nel dominio di lavoro (sanità, chiesa, scuola, ecc...)

Hardware e Device

- Sistemi Cartacei: basta che siano custoditi
- Sistemi elettronici (device):
 - È (molto) complicato
 - Solo sistemi della Parrocchia o autorizzati
 - Solo sistemi criptati
 - Attenersi almeno alla sicurezza base obbligatoria

Data Breach

La violazione dei dati e la fuga di dati



Data Breach

- **Data Brach** = Violazione dei dati personali;
- **Violazione** = distruzione, perdita, modifica, divulgazione o accesso non autorizzato anche accidentale;

Data Breach

In caso di data breach:

- Il Titolare lo notifica all'Autorità entro 72 ore
- Il Titolare documenta la violazione
- Il Titolare lo notifica all'Interessato
- Il Titolare adotta misure correttive

Domande?



Promemoria

**Prossimo incontro: Lunedì 16 Gennaio
2023, ore 20:45-22:45**

Tesseramento: ANSPI

Copie testi su richiesta:

- **Stampati Diapositive (€0,50)**
- **Testo del GDPR (€2,00)**

General
Data
Protection
Regulation

Protezione
Riservatezza
Integrità
Vera
Assoluta
Completa
Yang o No



Quando la
Parrocchia si
occupa della
povertà
digitale
e dei doveri
digitali