lunedì 6 agosto 2018

# APF - GDPR

https://www.gpdp.it/home/doveri

# GENERAL DATA PROTECTION REGULATION REGOLAMENTO UE 679/2016

## “Il principio del buonsenso”

## Raccogliere i dati in modo strutturato,

creare un archivio che contenga / protegga i dati personali dei soci e collaboratori, ad oggi la nostra associazione conserva i dati personali che gestisce, online sulle piattaforme Google drive e Dropbox quindi non al sicuro dal furto. La nuova legge espone l’associazione a controlli discrezionali da parte del Garante per la privacy e della Guardia di finanza, che possono evidenziare mancanza di attenzione e protezione.

## Limitazione dei dati, valutazione e blocco dei dati:

i dati devono essere utilizzati con uno scopo specifico e con tempistiche precise, indicate al proprietari prima del consenso.

I dati dovranno essere contrassegnati e cancellati nel momento in cui non servono più, per esempio i dati raccolti per un evento dovranno essere eliminati al termine dello stesso. I dati dei soci avranno valenza annuale come l’adesione. È importante che il proprietario dei dati sia messo al corrente prima del consenso all’uso, che i suoi dati personali saranno eliminati con delle tempistiche precise.

## PROFILAZIONE

= trattamento automatizzato di dati con lo scopo di analizzare e registrare profili, gusti, aspetti della persona. La nostra associazione non fa profilazione.

## NUOVA INFORMATIVA? (ART. 13)

comunicazione che deve essere fornita all’interessato prima di raccogliere i suoi dati e può essere fornita con le modalità ritenute più idonee

- deve indicare CHI effettua il trattamento,
- COME è effettuato il trattamento,
- DOVE circoleranno i dati raccolti (in particolare va specificato se i dati vengano trasferiti all'estero e /o in paese terzo),
- PER QUANTO i dati raccolti saranno conservati e i DIRITTI DEL PROPRIETARIO. Quindi il GDPR impone che nell'informativa sia individuata esattamente la "vita" dei dati dal momento in cui vengono raccolti al momento in cui verranno cancellati.
- Si attende dal Garante un modello di informativa ai sensi del GDPR.
- Ovviamente le informative saranno più d'una (volontari, dipendenti, commercialista, fornitori, ecc.

# INFORMAZIONI IN PIÙ DA INSERIRE IN INFORMATIVA

- UNA "MAPPA" DEL DATO: dove va il dato e quali sono i destinatari (con particolare riguardo al caso del trasferimento di dati personali a un paese terzo o a un'organizzazione internazionale);
- il PERIODO DI CONSERVAZIONE dei dati raccolti o, laddove ciò non sia possibile, i criteri utilizzati per determinare tale periodo di conservazione: la ratio di tale obbligo sta nella volontà del GDPR di imporre che, ad un certo punto, i dati siano cancellati
- Il diritto di presentare un RECLAMO all'autorità di controllo.
- Quindi: verificare tutti gli aspetti in cui i dati raccolti potrebbero servire (ad es. procedimenti giudiziari, obblighi di conservazione di legge o regolamentari) e stabilire che all'esaurimento degli stessi, i dati vengano cancellati.
- criterio generale: esaurimento delle finalità per le quali si è effettuato il trattamento (es. organizzazione di evento e dati dei partecipanti).

non contestabili le informative già fornite, tutto il pregresso e i relativi adempimenti restano tali. L'obbligo sorge dal 25.5.2018 in avanti.

•Quindi, ad oggi e in attesa dei decreti attuativi per la disciplina di altri aspetti, prima del 25 maggio bisogna:

RINNOVARE LE INFORMATIVE ALLA LUCE DEL NUOVO ART.13 GDPR con l'inserimento della descrizione della "vita" dei dati raccolti (dalla loro raccolta alla loro cancellazione) e del periodo di conservazione dei dati raccolti/dei criteri di conservazione

# I **FONDAMENTI DI LICEITÀ** del trattamento

ogni trattamento deve trovare fondamento in un'idonea base giuridica

sono indicati all'art. 6 del regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice privacy:

- consenso
- adempimento obblighi contrattuali
- interessi vitali della persona interessata o di terzi
- obblighi di legge cui è soggetto il titolare
- interesse pubblico o esercizio di pubblici poteri
- interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati (es. videosorveglianza)

# CONSENSO

- deve essere libero, specifico, informato
- deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile" (NO consenso tacito o presunto - no a caselle pre-spuntate su un modulo)
- NON necessariamente "documentato per iscritto", né con "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili)
- inoltre, il titolare (art. 7.1) deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento

# VALE IL VECCHIO CONSENSO?

- Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche del Regolamento. Sennò va raccolto di nuovo. In particolare, occorre

verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2)

# TRATTAMENTO DATI SENSIBILI

1. È **vietato** trattare dati personali **che rivelino**
   - **l'origine razziale o etnica,**
   - **le opinioni politiche,**
   - **le convinzioni religiose o filosofiche,**
   - **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.
2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:
   a) l'interessato ha prestato il proprio **consenso ESPLICITO** al trattamento di tali dati personali **per una o più finalità specifiche**, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1
   b) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, **da una fondazione, associazione o altro organismo senza scopo di lucro** che persegua finalità **politiche, filosofiche, religiose o sindacali,** a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato.

# DATA PROTECTION OFFICER **(DPO)** RESPONSABILE DELLA PROTEZIONE DEI DATI **(RPD)**

**Sono obbligati alla nomina:**

- gli ENTI PUBBLICI

- i soggetti la cui attività principale consiste in trattamenti che richiedono il "monitoraggio regolare e sistematico" degli interessati "su larga scala"
- i soggetti la cui attività principale consiste nel trattamento SU LARGA SCALA di dati sensibili (o meglio dati cd. particolari) e dati giudiziari (relativi, ad oggi, a condanne penali; reati e misure di sicurezza).

**Quindi la certezza sull'obbligo di nomina del DPO, al momento, riguarda: settore pubblico; banche e assicurazioni e multinazionali.**

Si attende un elenco dei soggetti tenuti alla nomina del DPO elaborato dal Garante.

il GDPR non definisce cosa costituisca **larga scala**, ma il WP29 suggerisce i seguenti fattori:

1. numero di persone interessate, come numero specifico o come percentuale della popolazione di riferimento
2. volume dei dati e / o la gamma di diversi elementi di dati in corso di elaborazione
3. la durata o la permanenza dell'attività di elaborazione dati;
4. l'estensione geografica delle attività di elaborazione

# REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

registro in forma cartacea (Buffetti) o in formato elettronico (software *ad hoc*) che deve essere esibito al Garante qualora lo richieda nell'ambito di un controllo

- può essere assimilato al vecchio "documento programmatico sulla sicurezza" – DPS
- però (!) se ne deve tenere **uno per ogni tipo di trattamento dei dati che si effettua** (es. in base all'interessato: dati dei volontari, dati dei dipendenti, dati raccolti per finalità pubblicitarie o di fundraising, ecc; in base alle attività dell'associazione o alla gravità del dato trattato.

# ART. 30 GDPR

- La tenuta di un registro del trattamento è **obbligatoria** solo per le imprese od organizzazioni **con più di 250 dipendenti** (anche VOLONTARI???)

- Le imprese od organizzazioni con **meno di 250 dipendenti**, invece, sono obbligate alla tenuta del Registro del trattamento solo nel caso in cui effettuino un trattamento in grado di presentare un **rischio per i diritti e le libertà dell'interessato** e, alternativamente:

**non occasionale**

ovvero **relativo a categorie particolari di dati personali** ai sensi dell'art. 9.1 del Regolamento (origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, 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)

ovvero **relativo a condanne penali**, a reati o a connesse misure di sicurezza

# SI CONSIGLIA DI FARE I REGISTRI

# CONTENUTO DEL REGISTRO DEI TRATTAMENTI

2. estremi completi del Titolare del trattamento, P.Iva, Recapiti, etc
3. estremi di contatto del Rappresentante Legale
4. estremi di contatto del Responsabile Privacy
5. elenco ed estremi di contatto di tutti i Responsabili Esterni ex art. 2 GDPR
6. elenco dettagliato dei trattamenti
7. misure Tecniche ed Organizzative a protezione dei dati

https://www.gpdp.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili#registro

# DATA BREACH

fuoriuscita di dati indipendentemente dalla volontà anche perdere una chiavetta USB contenente dati o subire il furto del computer o di un archivio dati

**obbligo di denuncia entro 72 ore dall'evento al Garante**

La denuncia deve essere fatta anche agli interessati i cui dati sono fuoriusciti, ma solo laddove sia possibile che da tale fuoriuscita essi possano subire un danno ai loro diritti *(cfr. modello di comunicazione sul sito del Garante)*

ATTENZIONE

Consiglieri, volontari e dipendenti vanno tutti responsabilizzati sui rischi di data breach e devono essere in grado di gestirli, nel senso di essere consapevoli su quello che debba essere fatto in caso di fuoriuscita di dati.

# ACCOUNTABILITY (ART. 24)
# Un approccio responsabile al trattamento:

il titolare del trattamento è responsabile dell'adozione di misure idonee e proporzionali ai rischi riscontrati per i dati oggetto di trattamento

Il titolare del trattamento deve poter dimostrare l'accountability, e per far questo:

- predispone una vera e propria POLICY aziendale/associativa (=trasfondere le previsioni del GDPR senza riferimenti agli articoli)
- effettua una MAPPATURA delle operazioni di trattamento;
- ripartisce i RUOLI e forma in modo personalizzato i volontari/dipendenti.
- adotta le MISURE DI SICUREZZA IDONEE facendo riferimento (art.
- 32) allo stato dell'arte del settore di appartenenza e dei costi sostenibili, alla natura, oggetto, contesto, finalità del trattamento e dei rischi per i diritti degli interessati

# RESPONSABILE DEL TRATTAMENTO

La nomina di tale soggetto è facoltativa, il GDPR non prevede la possibilità di nominare un responsabile interno *(confrontando l'art. 28 GDPR con l'art. 29 del Codice Privacy si evince una esternalizzazione della figura)*.

Ad oggi non è chiaro si possa continuare a nominare un responsabile interno

**L'art. 28, al 3°comma, specifica che i trattamenti da parte di un responsabile del trattamento debbano essere disciplinati da un contratto o da un altro atto giuridico equivalente e indica le previsioni che deve contenere (sono già presenti modelli).**

https://www.gpdp.it/regolamentoue/titolare-responsabile-incaricato-del-trattamento

# INCARICATO DEL TRATTAMENTO

- figura presente nel solo sistema italiano, non è prevista espressamente nel GDPR
- tuttavia all'art. 29 si fa riferimento a "soggetti istruiti" dal titolare del trattamento.

# PRIVACY IMPACT ASSESSMENT P.I.A.

È una valutazione d'impatto da fare quando un certo tipo di trattamento presenta un elevato rischio per i diritti e le libertà delle persone fisiche interessate

L'art. 35 individua 3 casi in cui tale valutazione è richiesta:

- valutazione sistematica e globale di aspetti personali relativi a persone fisiche basata su un trattamento automatizzato, compresa la profilazione e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo e significativamente sulle persone fisiche;
- trattamento su larga scala di categorie particolari di dati personali di cui all'art. 9 paragrafo 1 (ovvero i dati sensibili: dati che rivelano origine razziale/etnica; opinioni politiche, convinzioni religiose o filosofiche o appartenenza sindacale; dati genetici e biometrici; dati relativi alla salute e alla vita o orientamento sessuale) o di dati relativi a condanne penali e a reati di cui all'art. 10;
- sorveglianza sistematica su larga scala di zona accessibile al pubblico.

## COSA FARE ORA?

- MAPPATURA aggiornata dei dati e dei trattamenti
- inventario delle proprie INFORMATIVE e verificare come potrebbero cambiare in funzione delle nuove regole
- analizzare i processi di gestione delle istanze degli INTERESSATI e verificare come gestire questi processi

*Mappatura dei principali trattamenti che si svolgono, per avere chiaro il tipo di dati che si trattano, le finalità perseguite e le informazioni che devono essere fornite all'interessato (con particolare riguardo agli aspetti introdotti dal GDPR, ovvero indicazioni sui tempi di conservazione dei dati e finalità indicate in modo specifico).*

La nostra associazione raccoglie i dati dei soci ordinari, soci volontari, gruppo AMA, Sala musicale, soci sostenitori, soci onorari.

Nome Cognome, indirizzo, telefono, mail, codice fiscale, professione, data iscrizione, pagamento.

APF raccoglie i dati di chi opera presso la Casa Famiglia Pollicino, personale che riceve stipendio o rimborso, dati che comunichiamo al commercialista, in questo caso acquisiamo anche l'IBAN del conto corrente per il versamento dello stipendio

Valutazione: sono tutti necessari? Possiamo eliminarne alcuni?

- Soci ordinari / volontari / sostenitori sostengono le nostre attività, con contributi di vario tipo, economico, tempo, donazione di materiale, donazione del proprio lavoro / professionalità
  i dai sono raccolti per compilare la scheda di adesione, per fare informazione sulle attività dell'associazione
- Affidatari gruppo AMA
  i dati sono raccolti per fare rete sui bisogni di informazioni e di condivisione, organizzare gli incontri periodici.
- Sala Musicale Noi
  i dati sono raccolti per fare informazione sulle attività specifiche della sala musicale.
- Soci onorari
  i dati sono raccolti per redigere il documento di attestazione, fare informazione sulle attività dell'associazione
- Donazioni: acquisiamo dati per registrare ed emettere ricevuta delle donazioni fatte all'associazione; dati che riceviamo da terzi (Gruppo Dallerba)

## Presenza dell'APF sulla rete

www.casapollicino.it - il nostro blog -

social: Facebook - YouTube

il sito non contiene elementi che analizzano e raccolgono dati sui visitatori

Contiene un link che porta ad un modulo Google da compilare e inviare che deve essere ancora aggiornato con un testo conforme al GDPR

Per il blog la piattaforma Blogger ha provveduto a inserire una nota per i nuovi visitatori:

*(Il diritto dell'Unione Europea ti impone di informare i visitatori provenienti dall'UE sui cookie utilizzati e i dati raccolti sul tuo blog. In molti casi, le normative ti impongono anche di ottenerne il consenso.*

*A titolo di cortesia, abbiamo aggiunto una nota al tuo blog per spiegare l'uso da parte di Google di determinati cookie di Blogger e Google, compresi i cookie Google Analytics e AdSense e altri dati raccolti da Google.*

*Spetta a te confermare che questa nota sia effettivamente visualizzata sul tuo blog ed efficace. Se utilizzi altri cookie, ad esempio tramite l'aggiunta di funzioni di terze parti, questa nota potrebbe non essere sufficiente per te. Se includi funzionalità di altri provider, è possibile che vengano raccolti ulteriori dati sull'utente.*

*Scopri di più su questa notifica e sulle tue responsabilità.)*

## COSA È MEGLIO FARE

- trattare meno dati che si può
- distribuire le responsabilità e documentare i trattamenti
- favorire l'anonimizzazione e la pseudonimizzazione
- rispettare sempre le FINALITÀ del trattamento
- rispettare il principio di PROPORZIONALITÀ del trattamento (art. 1): rispetto al fine e al tempo

## MISURE PRINCIPALI

(anche da valutare con gli esperti informatici)

- PSEUDONIMIZZAZIONE e CIFRATURA dei dati personali;
- capacità di assicurare su base permanente RISERVATEZZA, INTEGRITÀ (cioè non modificabilità), DISPONIBILITÀ e RESILIENZA (resistenza ad attacchi esterni) dei sistemi di trattamento;
- capacità di RIPRISTINARE tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- procedura per TESTARE e valutare periodicamente l'efficacia delle misure adottate (es. penetration testing)

- Tenuta REGISTRI del TRATTAMENTO / Adesione a CODICI DI CONDOTTA / meccanismi di CERTIFICAZIONE

## Data breach

Alcuni esempi:

• Un disco che si rompe e non è disponibile un backup per il ripristino

• Accesso ai dati (interno o esterno) non autorizzato

• Furto di dati (basta la copia)

• Furto d'identità (social engineering)

• Intrusione in un archivio o in una rete a scopo di sabotaggio

• Virus, malware e altre tipologie di minacce informatiche (cybersecurity)

• Un data breach che si presume possa arrecare danno agli Interessati va notificato al garante entro 72 ore da quando se ne viene a conoscenza (art. 33)

• Un data breach suscettibile di rischio elevato per la libertà e i diritti degli Interessati va notificata a questi ultimi nel più breve tempo possibile (art. 34)