Pane e internet

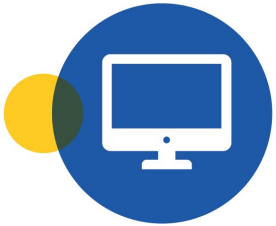
Cittadini 100% digitali

Privacy e Associazioni: come si possono utilizzare i dati degli Associati?

Avv. Maria Livia Rizzo

RegioneEmiliaRomagna
AgendaDigitale ER
Emilia-Romagna facciamo la differenza.
per la cultura e i saperi

Il progetto Pane e Internet



È un progetto finanziato dalla Regione Emilia-Romagna, nell'ambito dell'Agenda Digitale Regionale
Ha l'obiettivo di favorire lo sviluppo delle competenze digitali dei cittadini al fine di garantire una piena cittadinanza digitale.
Il "cittadino digitale" è un cittadino che, a tutte le età, usa le tecnologie per accedere alle informazioni, per fruire di servizi sempre più avanzati e per cogliere le opportunità che il digitale offre nel suo territorio.
Si snoda nel territorio attraverso la rete di Punti Pane e Internet e collabora costantemente con biblioteche, scuole e associazioni, ecc.

Il GDPR

REGOLAMENTO (UE) 2016/679
DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 27 aprile 2016

relativo alla protezione delle persone fisiche
con riguardo al trattamento dei dati personali,
nonché alla libera circolazione di tali dati

e che abroga la direttiva 95/46/CE

(regolamento generale sulla protezione dei dati)

Costituzione
DELLA REPUBBLICA
ITALIANA

Il GDPR

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali,

nonché alla libera circolazione di tali dati

e che abroga la direttiva 95/46/CE

(regolamento generale sulla protezione dei dati)

COMMISSIONE EUROPEA

Bruxelles, 6.5.2015
COM(2015) 192 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI

Strategia per il mercato unico digitale in Europa

{SWD(2015) 100 final}

Cos'è il DATO PERSONALE?

Art. 4 GDPR

Qualsiasi informazione riguardante una **persona fisica**

IDENTIFICATA

IDENTIFICABILE attraverso:

- Un identificativo
- Uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

QUANDO VENGONO TRATTATI DATI PERSONALI?

COSA VUOL DIRE TRATTARE I DATI PERSONALI?

Art. 4 GDPR

Il **TRATTAMENTO DI DATI PERSONALI** è qualsiasi operazione o insieme di operazioni 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.

A QUALI TRATTAMENTI SI APPLICA IL GDPR?

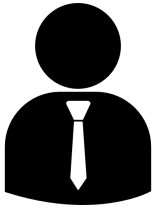
Art. 2 GDPR

COSA VUOL DIRE TRATTARE I DATI PERSONALI?

1. Trattamenti **automatizzati**, anche parzialmente
2. Trattamenti **non automatizzati** solo se i dati sono contenuti in un archivio, o sono destinati a essere inseriti in un archivio

Non si applica alle attività svolte «a titolo domestico»

CHI DECIDE IL TRATTAMENTO DEI DATI?



Art. 4 GDPR

TITOLARE DEL TRATTAMENTO

È la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento** di dati personali.

Può accadere che due o più titolari determinino congiuntamente le finalità e i mezzi del trattamento: in tal caso sono **CONTITOLARI** del trattamento (art. 26, GDPR) e il loro rapporto deve essere formalizzato tramite **contratto**.

Il Sistema di Gestione dei dati Personali

APPROCCIO BASATO SUL RISCHIO

Fornendo **dimostrazione** della adeguatezza al caso concreto delle misure tecniche e organizzative

SCELTE DEL TITOLARE

Accountability

Sanzioni amministrative fino 20 mln di euro o al 4% del fatturato mondiale annuo; responsabilità civili; sanzioni penali

Prima del GDPR: adempimento di obblighi formali e **misure minime** di sicurezza disciplinati precisamente dalla normativa

Dopo il GDPR: adozione di **misure adeguate** in base ad una valutazione del rischio del proprio trattamento e dell'impatto sugli interessati

Quali principi rispettare?

		Principi art. 5 GDPR
Posso trattare dati?		LICEITÀ
Per quale scopo posso trattare i dati?		LIMITAZIONE DELLA FINALITÀ
Quali/quanti dati posso trattare?		MINIMIZZAZIONE
Per quanto tempo posso conservare i dati?		LIMITAZIONE DELLA CONSERVAZIONE
Come devo trattare i dati?		ESATTEZZA INTEGRITÀ E RISERVATEZZA

Parametri RID

ART. 32 GDPR

Riservatezza

i dati devono essere trattati solo dai **soggetti autorizzati**

Integrità

i dati non devono subire **modifiche** non autorizzate

Disponibilità

i dati devono sempre essere **disponibili** per i soggetti autorizzati

Data breach – violazione di dati personali

Si verifica una violazione di dati quando:

I dati vengono PERSI	I dati vengono MODIFICATI per sbaglio o illegittimamente	Ai dati ACCEDE qualcuno che non è legittimato a farlo
I dati non sono più disponibili	I dati non sono più integri	I dati non sono più riservati

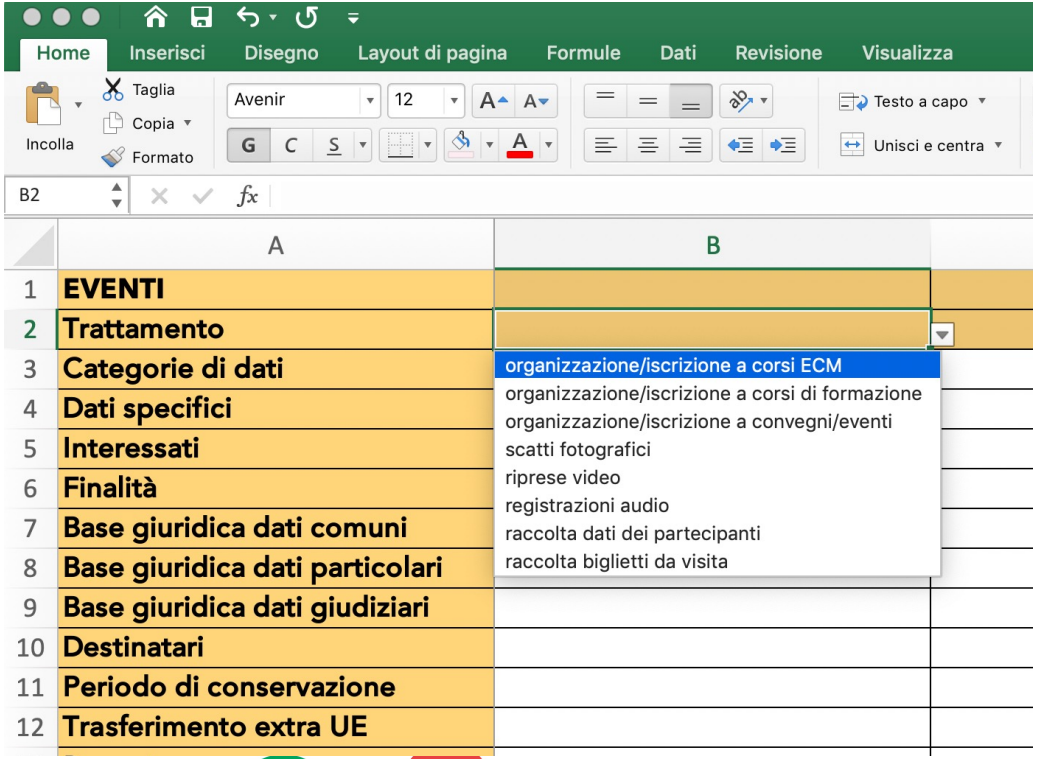
LE CAUSE?

Art. 33 GDPR

- Falla o **vulnerabilità** di sicurezza
- **Incidente** o **calamità** (incendio, terremoto, ecc.)
- **Errore** (di invio, di battitura, di manipolazione, ecc.)
- **Malevolenza** (furto di materiali, frode interna o esterna, accesso fraudolento, ecc.)




Il Registro dei trattamenti



Art. 30 GDPR

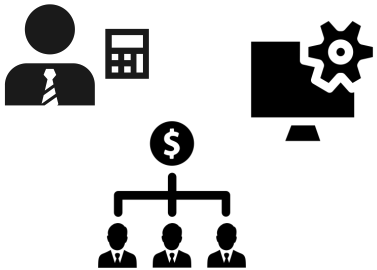
Come scegliere i fornitori?

OPERATORI <u>ESTERNI</u> ALLA ASSOCIAZIONE CHE TRATTANO DATI PER SUO CONTO

Il fornitore deve assicurare GARANZIE SUFFICIENTI di rispetto della normativa privacy

Atto scritto

Art. 28 GDPR



NOMINA A RESPONSABILE ESTERNO:
Contratto o **altro atto giuridico** che vincola il responsabile al titolare e parallelo al contratto di fornitura del prodotto/servizio

Scegliere solo fornitori GDPR *compliant*

Il personale deve essere autorizzato a trattare i dati

Art. 29 GDPR

DIPENDENTI/ COLLABORATORI/ VOLONTARI <u>INTERNI</u> ALL'ASSOCIAZIONE

Devono essere istruiti a trattare dati sotto l'autorità della Associazione

NOMINA AD AUTORIZZATO:
Attribuzione di specifici compiti e funzioni, e indicazione di istruzioni per comprendere la portata dell'autorizzazione.

OBBLIGO DI FORMAZIONE:
Anche tramite appositi corsi privacy per aumentare la consapevolezza del personale e minimizzare i rischi.

L’informativa privacy

Informative differenziate per i diversi interessati:

- ASSOCIATI/ADERENTI
- BENEFICIARI
- DIPENDENTI
- COLLABORATORI/STAGISTI/VOLONTARI
- CLIENTI/FORNITORI
- UTENTI DEL SITO WEB
- VISITATORI (VIDEOSORVEGLIANZA)
- PARTECIPANTI AGLI EVENTI
- RELATORI AGLI EVENTI

Contenuto ⇒ Art. 13 GDPR

Come fornirla?

…e devo richiedere il consenso al trattamento dei dati?

«CATEGORIE PARTICOLARI DI DATI PERSONALI»

Art. 9 GDPR

«Dati personali che rivelino:

l'origine razziale o etnica, 

le opinioni politiche, 

le convinzioni religiose o filosofiche, 

l'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.» 

È obbligatorio chiedere il consenso al trattamento dei dati per l'iscrizione all'Associazione?

Il trattamento di <u>dati comuni</u> è lecito quando ricorre una di queste condizioni (art. 6):

CONSENSO DELL'INTERESSATO

<u>TRATTAMENTO PREVISTO DA UN CONTRATTO</u>

ADEMPIMENTO DI UN OBBLIGO LEGALE

SALVAGUARDIA DI INTERESSI VITALI

COMPITO DI INTERESSE PUBBLICO

LEGITTIMO INTERESSE DEL TITOLARE

Art. 6 GDPR

Se l’Associazione tratta dati particolari?

Non serve richiedere il consenso se:

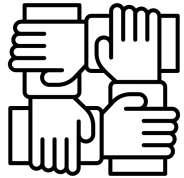
Art. 9 GDPR

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.

Prescrizioni relative al trattamento di particolari categorie di dati (Aut. Gen. n. 3/2016 – Autorità Garante)

SONO AUTORIZZATI A TRATTARE DATI PARTICOLARI:

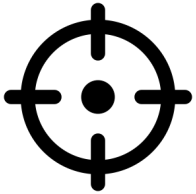
a) **associazioni anche non riconosciute**, **partiti e movimenti politici**, **associazioni e organizzazioni sindacali**, **patronati, associazioni di categoria**, **casse di previdenza**, organizzazioni assistenziali o di **volontariato** e del **terzo settore**, **federazioni e confederazioni**
b) **fondazioni**, **comitati ente, consorzio od organismo senza scopo di lucro** (**Onlus**);
c) **cooperative sociali** e **società di mutuo soccorso;**
d) **istituti scolastici**, limitatamente al trattamento dei dati che rivelino le convinzioni religiose;
e) **chiese, associazioni o comunità religiose**.



Prescrizioni relative al trattamento di particolari categorie di dati (Aut. Gen. n. 3/2016 – Autorità Garante)

GLI ETS POSSONO TRATTARE DATI PARTICOLARI PER LE SEGUENTI FINALITÀ:

perseguimento di **scopi determinati e legittimi individuati dalla legge, dall'atto costitutivo, dallo statuto** o dal **contratto collettivo**, ove esistenti, e in particolare per il perseguimento di finalità culturali, religiose, politiche, sindacali, sportive o agonistiche di tipo non professionistico, di istruzione anche con riguardo alla libertà di scelta dell'insegnamento religioso, di formazione, di patrocinio, di tutela dell'ambiente e delle opere d'interesse artistico e storico, di salvaguardia dei diritti civili, di beneficenza, assistenza sociale o socio-sanitaria.



Prescrizioni relative al trattamento di particolari categorie di dati (Aut. Gen. n. 3/2016 – Autorità Garante)

ETS POSSONO COMUNICARE DATI PARTICOLARI A SOGGETTI TERZI CON SCOPO DI LUCRO O A LIBERI PROFESSIONISTI:

- per svolgere le loro **attività** finalizzate a perseguire le finalità indicate o per la tenuta dei registri e scritture contabili o per la gestione amministrativa o per l'adempimento di obblighi fiscali o la diffusione di riviste, bollettini e simili o per ottenere beni o servizi,
- solo i dati **strettamente indispensabili** allo svolgimento delle attività indicate (generalità degli interessati/indirizzari)
- redigendo previamente un "**atto scritto** che individui con precisione le informazioni comunicate, le modalità del successivo utilizzo e le particolari misure di sicurezza adottate"
- indicando nell'**informativa** ex art. 13 GDPR resa agli interessati (soci/aderenti, beneficiari, lavoratori, ecc.) l'indicazione dei terzi e delle finalità per le quali utilizzano i loro dati.

Prescrizioni relative al trattamento di particolari categorie di dati (Aut. Gen. n. 3/2016 – Autorità Garante)

ETS POSSONO COMUNICARE DATI PARTICOLARI DI UN ASSOCIATO/ADERENTE A UN ALTRO ASSOCIATO/ADERENTE:

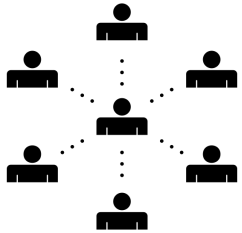
- **senza il consenso** se:
  - la comunicazione sia prevista dall'atto costitutivo o dallo statuto per il perseguimento di scopi determinati e legittimi
  - le modalità di utilizzo dei dati siano rese note agli associati/aderenti in sede di rilascio dell'informativa
- laddove vengano in considerazione **profili esclusivamente personali** riferiti agli associati/aderenti, devono essere utilizzate forme di consultazione individualizzata con gli stessi, adottando ogni misura opportuna volta a prevenire un'indebita comunicazione di dati personali a soggetti diversi dal destinatario

Prescrizioni relative al trattamento di particolari categorie di dati (Aut. Gen. n. 3/2016 – Autorità Garante)

ETS POSSONO COMUNICARE DATI PARTICOLARI DI UN ASSOCIATO/ADERENTE ALL'ESTERNO O DIFFONDERLI:

- **solo con il consenso**
- solo se la comunicazione è strettamente **pertinente** rispetto alle finalità dell'ETS
- solo se nell'**informativa** sono state precisate le tipologie di destinatari e le finalità della comunicazione/diffusione dei dati

Le comunicazioni ai Soci



Possono essere inviate senza consenso?

Invio di comunicazioni relative all'attività dell'Associazione
Invio di materiale pubblicitario
Pubblicazione dei dati sul sito web dell'Associazione

L’invio di comunicazioni ai cittadini per attività «promozionali»/sensibilizzazione/fund raising

È lecito l’invio senza consenso?

Invio di newsletter	
Invio di e-mail a indirizzi e-mail personali raccolti da: • **social network** • **pubblici elenchi o albi** **Invio di e-mail a indirizzi mail di aziende (info@...)**	
Invio di messaggi agli utenti di social network	

Valutazione di impatto privacy (DPIA) nelle Associazioni

Art. 35 GDPR

Se trattamento prevede l'uso di **nuove tecnologie** e può presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**:

Es. trattamenti su larga scala di dati particolari relativi a persone vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)

Individuazione delle **minacce** e relative **vulnerabilità**.

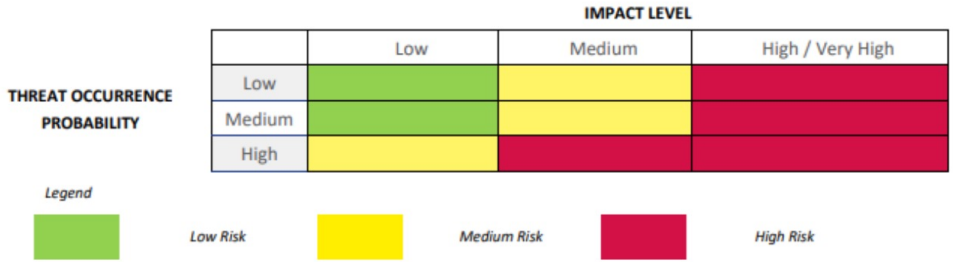
Individuazione di tutti i **rischi** derivanti dal trattamento e dei correlati **livelli di gravità e probabilità**.

Valutazione dell'efficacia delle **misure** adottate per ridurre il rischio.

Definizione del **rischio potenziale** che ne deriva.

Valutazione del **rischio residuo** e sua accettabilità.

Se rischio residuo non è accettabile: **CONSULTAZIONE PREVENTIVA** con il Garante



Il Data Protection Officer (DPO)

Art. 39 GDPR

Fornisce **consulenze e pareri** sulla normativa privacy a chi tratta dati personali	
Sorveglia l'osservanza della normativa privacy	
Coopera con Autorità di controllo	GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

CONTROLLORE O CONSULENTE?

Per l'Associazione è obbligatorio nominare il DPO?

Art. 37 GDPR

La nomina di un DPO è obbligatoria in tre casi specifici:

a) se il trattamento è svolto da un'**autorità pubblica** o da un **organismo pubblico**;

b) se le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che richiedono il **monitoraggio regolare e sistematico di interessati su larga scala**;

c) se le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel **trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati**.

Cosa fare se l'interessato vuole esercitare i propri diritti?

Artt. 15-22 GDPR

RETTIFICA

PORTABILITÀ

ACCESSO

CANCELLAZIONE – OPPOSIZIONE – LIMITAZIONE

INVALIDITÀ EFFETTI GIURIDICI TRATTAMENTI AUTOMATIZZATI

paneeinternet.it