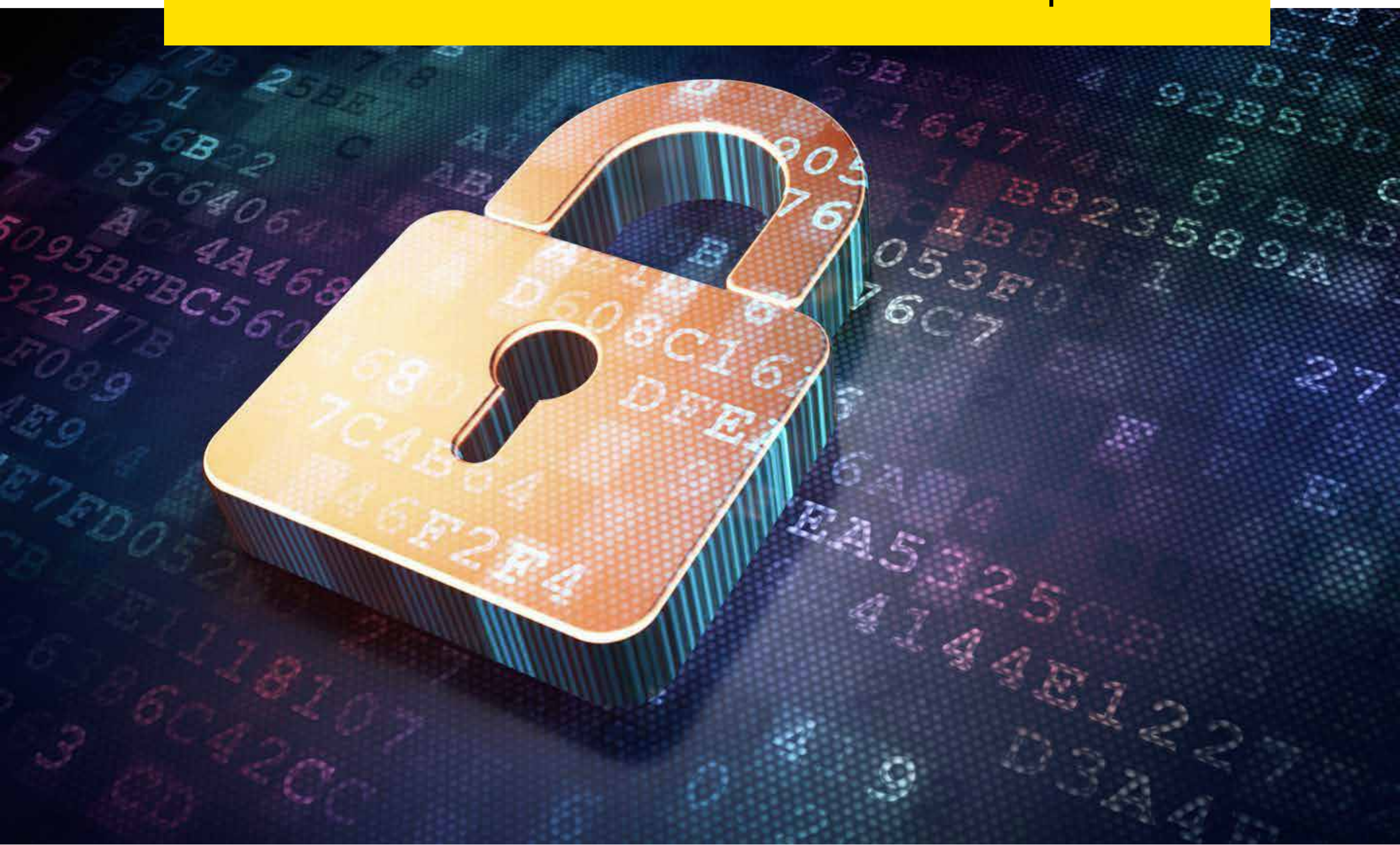
AssoFacile

GDPR

Tutto ciò che le Associazioni
Non-Profit
devono sapere
sulla nuova normativa europea



25 MAGGIO

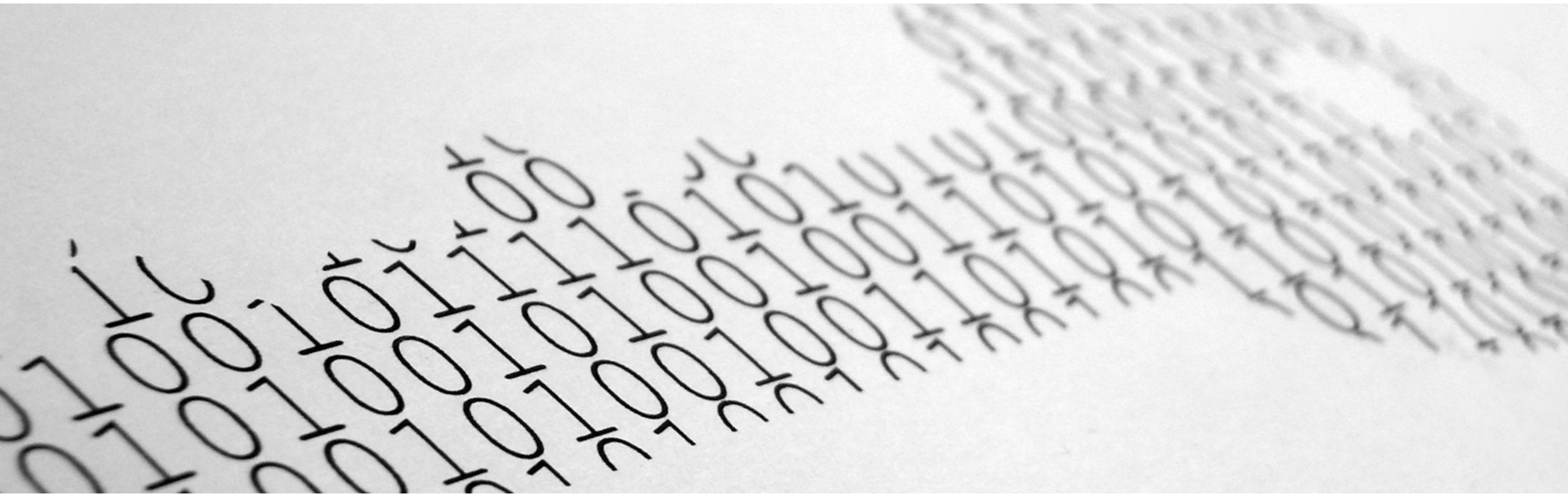
Il 25 maggio **sarà efficace** il Regolamento europeo 2016/679 sulla protezione dei dati personali (G D P R - General Data Protection Regulation).

La nuova normativa **si estende a tutte le organizzazioni, comprese quelle del terzo settore,** imponendo oneri e richiedendo attenzione ai loro dirigenti.

La normativa richiama al concetto di **«accountability» «responsabilità»** cioè l'associazione responsabile del trattamento dei dati dei suoi associati deve decidere se e quali attività sono sottoposte e sono coerenti con la normativa del GDPR.

I dati dovranno essere raccolti per **finalità esplicite e legittime**, trattati in modo coerente con le finalità dichiarate nelle informative, adeguati pertinenti e non eccedenti rispetto a quanto è necessario al trattamento, in ogni momento corretti ed aggiornati, conservati e trattati per garantire un'adeguata sicurezza e protezione.

AssoFacile



Data protection By default and By Design

La protezione dei dati deve essere predefinita e progettata.

• L’obiettivo di ogni progetto nel quale si trattano dati personali deve essere la protezione degli stessi da effettuare attraverso una procedura (documentata) di raccolta e utilizzo. Ogni modifica nella procedura di raccolta e trattamento dei dati, o una modifica della finalità nell’utilizzo, prevedrà un riesame documentato di tutta la procedura precedentemente definita.

Titolare e Responsabile del trattamento

Il Titolare del trattamento è l'organizzazione che ha bisogno del processo di trattamento dei dati. Colui il quale, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento .

Il Responsabile del trattamento è chi lo mette in atto, può essere il titolare stesso o un fornitore cioè chi tratta i dati personali per conto del titolare del trattamento (es. Webmaster o agenzia di marketing) .

Se titolare e il fornitore non coincidono, deve essere molto chiaro e documentato il loro rapporto.

AssoFacile

Vediamo in pochi passi come un’associazione deve procedere

Adeguamento al GDPR

Sarebbe opportuno che il direttivo si riunisse per discutere del disegno del progetto di adeguamento alla normativa europea e che lo certifichi attraverso un verbale inviato a tutti i partecipanti.

AssoFacile

Verifica dei dati in possesso

Ogni associazione dovrebbe chiedersi di quali dati disponga (**cosa ho raccolto in tutti questi anni, dove sono conservati , chi ha accesso a questi dati?**) e quindi crearsi un **Registro dei dati** (LIBRO MASTRO)
Verificare i consensi raccolti prima del GDPR e , se necessario, integrarli aggiornando le informative e raccogliendo dei nuovi consensi.

Per ogni tipologia di dati è fondamentale ***indicare come sono stati utilizzati*** , dividerli per categorie a seconda dell'uso e stabilirne l'utilizzo che ne verrà fatto in futuro.

Non conserviamo MAI dati che non intendiamo utilizzare!

AssoFacile

Come porsi davanti ad un dato ?

Per entrare nella logica del GDPR ci poniamo , per ogni dato in possesso, una serie di domande :

1. Ho necessità di questo dato, so a cosa mi servirà?

2. La persona che mi ha fornito questo dato è a conoscenza dell'uso che io intendo farne?

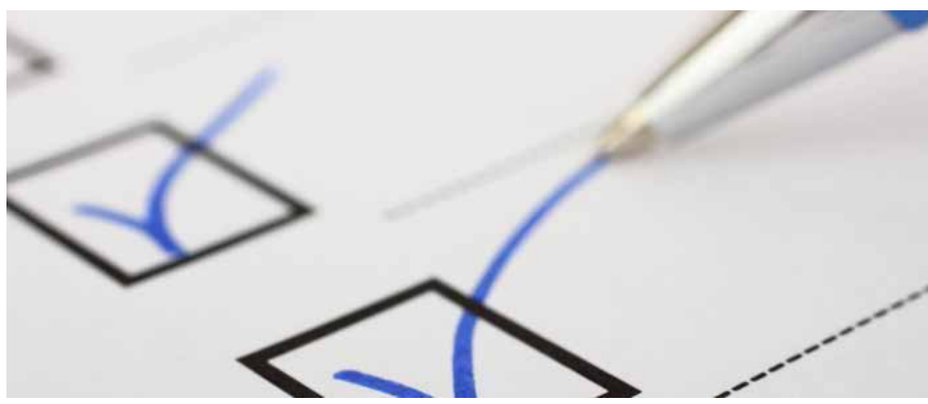
3. Ho adottato la soluzione più sicura, adottata da me o da terzi, per la protezione di questo dato?

4. Chi può accedere a questo dato?

5. Chi ha accesso a questo dato è stato adeguatamente formato in modo da adempiere alla normativa del GDPR?

Definire le basi legali

Ogni associazione deve definire quale base legale/normativa gli da diritto di raccogliere e trattare i dati personali, **redigere un documento** nel quale i responsabili dell'organizzazione esplicitano su quali basi operano.



Predisporre un'informativa aggiornata

Secondo il GDPR l'informativa deve essere :

- **CONCISA** = breve e chiara in tutte le sue parti.
- **TRASPARENTE** = non deve contenere parti non perfettamente comprensibili o ambiguità .
- **INTELLEGIBILE** = scritta in italiano semplice senza tecnicismi .

L'informativa raccoglierà il CONSENSO

Secondo il GDPR per essere valido il consenso deve essere:

- **ESPLICITO** = non valgono i consensi impliciti non espressi.
- **INFORMATO** = preceduto da lettera informativa.
- **CHIARO** = linguaggio semplice e comprensibile.
- **SPECIFICO** = deve essere chiaramente riferito alle finalità per cui è richiesto .
- **DISTINTO** = la richiesta di consenso non è mai unita con altre dichiarazioni.
- **REVOCABILE** = il consenso deve poter essere sempre revocato in maniera semplice dal titolare dei dati.

AssoFacile

Definire i RESPONSABILI del trattamento

All’interno dell’associazione una persona o un dipartimento (che andranno adeguatamente formati secondo il GDPR) devono assumersi la responsabilità del trattamento dei dati.

E’ anche possibile nominare un DPO (Data Protection Officer – responsabile della protezione dei dati)

Contratti con i fornitori

• Se L’associazione utilizza fornitori esterni che tratteranno i dati raccolti (webmaster, agenzie di marketing) dovete scrivere i contratti in modo che sia chiaro il tipo di utilizzo dei dati .

Garanzia di protezione dei dati

• L’associazione deve dimostrare in maniera documentata di aver predisposto tutte le misure opportune anti- intrusione.

• E che sta utilizzando tutti i mezzi possibili per poter evitare i rischi di diffusione, alterazione , cancellazione dei dati raccolti.

Accesso per modifica o cancellazione dei dati

• I titolari dei dati possono chiedere la modifica o la cancellazione degli stessi, è quindi opportuno predisporre le procedure e i tempi minimi necessari in caso di richieste di accesso/modifica o cancellazione.

AssoFacile

IMPORTANTE!!!...

lo scopo del GDPR non è la detenzione dei dati personali ma il trattamento degli stessi, perché solo nel trattamento dei dati si possono determinare gravi danni alla privacy.

Molto semplicemente secondo il nuovo regolamento europeo utilizzo i dati ESCLUSIVAMENTE per la finalità per cui sono stati raccolti e per la quale è stato prestato il consenso , non raccolgo e conservo ciò che non mi serve e non li utilizzo per scopi estranei al servizio richiesto e per i quali non ho ricevuto il consenso.

Es. E' lecito che un'associazione di volontariato chieda l'indirizzo del soggetto a cui presta il servizio , non è lecito utilizzare l'indirizzo per inviare pubblicità a casa via posta.

Per non incorrere in una SANZIONE, il nostro gestionale web potrà tutelarti con l'apposita area dedicata al GDPR.

Se ancora non conosci AssoFacile ti invitiamo a provare la demo gratuitamente per 7 giorni. ***Clicca in basso per accedere***

AssoFacile

Il Software per la tua Associazione

ACCEDI ALLA DEMO

www.assofacile.it