<Comunità Energetica
Rinnovabile Dinamo E.T.S.

Via Palmaroli n. 25
63066 – Grottammare (AP)
Cod. Fisc. 91053630447
Tel. 0735 588207
e-mail: info@dinamocer.org
PEC: dinamocer@pec.it

Modello Organizzativo GDPR

Data revisione:

Maggio 2024

MODELLO ORGANIZZATIVO SULLA PROTEZIONE DEI DATI PERSONALI

Sommario

1. PREMESSA 2

2. DEFINIZIONI 2

3. OBIETTIVO E STRUTTURA DEL MODELLO ORGANIZZATIVO 3

4. TITOLARI, RESPONSABILI E DESIGNATI 3

A) Titolare del Trattamento 3

B) Responsabile del Trattamento 3

C) Designati al trattamento 4

5. POLICY DELL'ORGANIZZAZIONE 4

5.1 Responsabilità dei Designati al trattamento 5

5.2 Procedure di sicurezza 6

5.2.1 Controllo degli accessi agli archivi elettronici e protezione degli stessi 6

5.2.2 Controllo degli accessi agli uffici e protezione dei locali dove vengono custoditi gli archivi 6

5.2.3 Gestione dei fascicoli cartacei 6

5.2.4 Siti web e social network 6

6. RISK ASSESSMENT 7

7. GESTIONE DEL DATA BREACH 7

Created in Master PDF Editor

1. PREMESSA

Il presente Modello Organizzativo sulla Protezione dei Dati Personali (di seguito per brevità semplicemente "MODELLO") raccoglie le misure tecniche ed organizzative che la Comunità Energetica Rinnovabile Dinamo E.T.S. (di seguito anche semplicemente "ORGANIZZAZIONE") attua per garantire la conformità al Regolamento UE 2016/679 (di seguito per brevità semplicemente "GDPR") delle attività di trattamento dei dati personali delle persone fisiche che l'Organizzazione effettua direttamente o che soggetti terzi effettuano per suo conto.

2. DEFINIZIONI

Ai fini del GDPR ed in relazione ai concetti specificamente coinvolti dalle attività di trattamento effettuate direttamente ed indirettamente dall'Organizzazione, ai sensi dell'art. 4 del GDPR si intendono per:

1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2) «trattamento»: 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, 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;
3) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati;
4) «titolare del trattamento»: 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;
5) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
6) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali;
7) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
8) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso,

Creato in Master PDF Editor

mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

9) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

3. OBIETTIVO E STRUTTURA DEL MODELLO ORGANIZZATIVO

L'obiettivo del presente Modello è di garantire e dimostrare che il trattamento dei dati personali da parte della Comunità Energetica Rinnovabile Dinamo E.T.S. avviene in modo lecito, corretto e trasparente, da raggiungere attraverso la realizzazione di una gestione interna che promuova la cultura della privacy e della sicurezza dei dati personali, consolidando i principi comportamentali idonei a garantire la trasparenza, la sicurezza e la correttezza dei trattamenti.

Il presente Modello fornisce una panoramica sul sistema complessivo delle misure tecniche e organizzative che, sulla base delle concrete esigenze sistematiche ed operative della Organizzazione e all'esito dell'analisi dei rischi, si ritengono adeguate, contenendo i principi, le regole organizzative e gli strumenti di controllo per garantire il trattamento lecito, corretto e trasparente dei dati personali.

4. TITOLARI, RESPONSABILI E DESIGNATI

La Comunità Energetica Rinnovabile Dinamo E.T.S. ha ritenuto di non nominare un Data Protection Officer ai sensi dell'art. 37 GDPR, non ritenendosi detta figura necessaria in ragione della natura dei dati trattati e dei rischi per i diritti e le libertà fondamentali degli interessati. Pertanto, le figure e le funzioni coinvolte dall'Organizzazione nelle attività di protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale sono:

A) Titolare del Trattamento

È la stessa Comunità Energetica Rinnovabile Dinamo E.T.S. che riveste tale funzione e sulla quale, conseguentemente, incombono tutti gli obblighi e le responsabilità che la legge, italiana ed europea, le impone. Primo fra tutti, l'obbligo di mettere in atto, riesaminare ed aggiornare le misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è da essa effettuato conformemente al GDPR.

B) Responsabile del Trattamento

Il GDPR definisce all'art. 28 il Responsabile del trattamento come il soggetto che effettua trattamenti di dati personali per conto del Titolare, presentando garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che i trattamenti stessi soddisfino i requisiti del GDPR e garantiscano la tutela dei diritti dell'interessato.

È opinione diffusa tra gli interpreti che la figura or ora delineata sia riferita al Responsabile del trattamento "esterno" rispetto alla struttura aziendale del Titolare del trattamento e che, pertanto, non sia espressamente disciplinata la figura del Responsabile del trattamento "interno".

Created in Master PDF Editor

La Comunità Energetica Rinnovabile Dinamo E.T.S. si può avvalere di Responsabili del Trattamento attraverso specifici atti di designazione o attraverso contratti di servizio.

Quanto al regime di responsabilità, i Responsabili del trattamento rispondono per il danno causato dal trattamento solo se non hanno adempiuto gli obblighi del GDPR specificatamente loro diretti o se hanno agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare del trattamento.

C) Designati al trattamento

La figura del Designato al trattamento è definibile come la persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile.

Anche se nella traduzione italiana del GDPR non compare mai il termine "designato al trattamento" e pur non essendo espressamente prevista dal GDPR questa figura come funzione giuridicamente autonoma, il Garante italiano, nella guida all'applicazione del Regolamento, giustifica e considera non incompatibile con il regolamento la figura del Designato. Anzi, tale modalità operativa è considerata una buona prassi volta a poter ulteriormente comprovare la *compliance* al GDPR.

I Designati del trattamento della Comunità Energetica Rinnovabile Dinamo E.T.S. sono coloro i quali provvedono materialmente al trattamento dei dati personali sotto la supervisione del Titolare del trattamento.

La Comunità Energetica Rinnovabile Dinamo E.T.S. cura l'aggiornamento dei propri Designati.

5. POLICY DELL'ORGANIZZAZIONE

La Comunità Energetica Rinnovabile Dinamo E.T.S ha per oggetto la costituzione e la gestione di una comunità di energia rinnovabile. Per lo svolgimento della suddetta attività la CER DINAMO gestisce le seguenti tipologie di dati personali:

1. Dati anagrafici degli associati compresa copia del documento di identità;
2. Dati anagrafici dei beneficiari dei servizi e di soggetti esterni;
3. Dati anagrafici dei fornitori;
4. Dati anagrafici degli utenti immessi sul sito web per la presentazione delle domande di adesione on line inviati via email e accodati nel database del sito;
5. Dati fiscali (codice fiscale, partita IVA);
6. Recapiti telefonici e di posta elettronica;
7. Codici POD (Point Of Delivery –Punto di fornitura) e IBAN (International Bank Account Number);
8. Dati relativi agli utenti del sito web che non presentano domanda di adesione.

Le basi giuridiche del trattamento di tali dati da parte della Comunità Energetica Rinnovabile Dinamo E.T.S. sono indicate nelle rispettive informative rilasciate agli interessati e possono di seguito riepilogarsi:

- esecuzione di contratti o di accordi precontrattuali;
- consenso dell'interessato;
- obblighi di legge.

I dati suddetti possono essere trattati attraverso strumenti cartacei ed elettronici, sia presso la sede operativa, che attraverso la Rete Internet.

Nel trattamento dei dati personali, l'Organizzazione osserva le regole che seguono.

5.1 Responsabilità dei Designati al trattamento

Le autorizzazioni ai designati al trattamento (di seguito semplicemente "Designati") sono concesse dal Titolare del Trattamento mediante nomina scritta nella quale si individua ambito e profilo di autorizzazione.

Il Designato deve attenersi scrupolosamente alle procedure operative indicate dal Titolare del Trattamento.

I Designati hanno l'obbligo di segnalare immediatamente al Titolare del Trattamento qualsiasi evento o situazione di rischio della sicurezza dei sistemi informatici o delle informazioni al fine di tutelare i diritti e le libertà degli interessati e il patrimonio informativo dell'Organizzazione oltre che garantire la necessaria continuità operativa.

Ciascun Designato deve:

- rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR) e della normativa nazionale in vigore, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti dell'Organizzazione;
- rispettare le misure di sicurezza idonee adottate dall'Organizzazione, atte a salvaguardare la riservatezza e l'integrità dei dati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del Titolare;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il Titolare in caso di incidente di sicurezza che coinvolga i dati;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli dell'Organizzazione e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;

Created in Master PDF Editor

- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

5.2 Procedure di sicurezza

5.2.1 Controllo degli accessi agli archivi elettronici e protezione degli stessi

Al fine di proteggere i dati personali contenuti negli archivi elettronici dell'Organizzazione, sono state adottate le seguenti misure:

1) l'accesso agli archivi elettronici dei dati è consentito solo al Titolare del trattamento;
2) quotidianamente viene effettuato il backup automatico di tutti gli archivi elettronici da parte dell'Azienda di hosting di riferimento.

5.2.2 Controllo degli accessi agli uffici e protezione dei locali dove vengono custoditi gli archivi

Il locale ove sono custoditi i dati personali è soggetto a controllo e a verifica da parte del Titolare, al fine di evitare che i dati suddetti possano essere conosciuti o accessibili da parte di soggetti non autorizzati.

5.2.3 Gestione dei fascicoli cartacei

1) È tassativamente vietato ai Designati accedere ai fascicoli cartacei per finalità diverse da quelle necessarie per la lavorazione della pratica;
2) i Designati autorizzati ad accedere ai fascicoli cartacei sono obbligati a riporre ciascun fascicolo all'interno del relativo archivio;
3) è tassativamente vietato a chiunque portare fuori dall'ufficio i fascicoli cartacei;
4) l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni;
5) ogni Designato è obbligato a verificare che i dati trattati non siano accessibili a terzi non autorizzati;
6) è fatto divieto di lasciare incustoditi e accessibili a terzi gli strumenti elettronici con i quali il Designato effettua il trattamento dei dati;
7) gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati dai Designati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di collaborazione;
8) distruzione delle copie cartacee: si deve procedere alla distruzione del supporto qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli.

5.2.4 Siti web e social network

La Comunità Energetica Rinnovabile Dinamo E.T.S. si avvale di un proprio sito web ufficiale, www.dinamocer.org nell'ambito del quale i dati comunicati dall'utenza o comunque raccolti nel corso della navigazione non sono accompagnati da alcuna informazione personale aggiuntiva rispetto agli usuali dati la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet (quali ad esempio nomi di dominio, indirizzi IP, sistema operativo utilizzato, tipo di device e di browser utilizzati per la connessione) e vengono trattati per gestire esigenze di controllo delle modalità di utilizzo dello stesso, accertare responsabilità in caso di ipotetici reati informatici e ricavare informazioni statistiche anonime sull'uso del sito. La base giuridica che legittima il trattamento di tali dati è la necessità di rendere utilizzabili le funzionalità del sito a seguito dell'accesso dell'utente.

Creato in Master PDF Editor

Nel caso di invio da parte dell'utenza del sito informatico di domande di adesione all'Associazione, i dati personali aggiuntivi sono raccolti e trattati esclusivamente per la suddetta finalità di adesione ed in tal caso la base giuridica che legittima il trattamento è il consenso dell'interessato.

La Comunità Energetica Rinnovabile Dinamo E.T.S. può avvalersi anche di social network per scopi divulgativi e informativi.

Qualora sia necessario o strumentale per l'esecuzione delle specifiche finalità, i dati personali, sono comunicati a destinatari nominati ai sensi dell'art. 28 del GDPR, che li trattano in qualità di Responsabili del Trattamento al fine di ottemperare ad obblighi di legge, a contratti o alle finalità connesse. Precisamente, i dati potrebbero essere comunicati a destinatari appartenenti alle seguenti categorie:

- commercialista;
- Istituti di Credito;
- Compagnie Assicurative;
- Manutentore sistema informatico.

In nessun caso i dati raccolti dall'Organizzazione saranno oggetto di diffusione.

Nel rispetto di quanto previsto dall'art. 5, comma 1, lett. e) del GDPR, i dati personali vengono conservati in una forma che consenta l'identificazione dell'Interessato per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati stessi sono trattati o in base alle scadenze previste dalle norme di legge. La verifica sulla obsolescenza dei dati conservati in relazione alle finalità per cui sono stati raccolti viene effettuata periodicamente.

6. RISK ASSESSMENT

Al fine di implementare le azioni volte all'adeguamento al GDPR, è stata effettuata una ricognizione dell'attuale organizzazione e della documentazione vigente in materia di privacy e delle misure tecniche utilizzate.

In particolare, si è proceduto ad un'analisi dei rischi inerenti il trattamento dei dati, che si allega al presente Modello (**All. n. 1**).

All'esito di detta analisi dei rischi è stato individuato sia il livello di impatto del trattamento dei dati sui diritti e le libertà degli interessati, sia il livello di rischio e sono state individuate le misure tecniche e organizzative idonee a mitigare i rischi inerenti.

7. GESTIONE DEL DATA BREACH

L'art. 33 GDPR impone al Titolare del Trattamento di notificare all'autorità di controllo l'eventuale violazione di dati personali entro 72 ore dal momento in cui ne viene a conoscenza.

Creato in Master PDF Editor

L'obbligo di notifica scatta se la violazione comporta un rischio per i diritti e le libertà delle persone fisiche; qualora, poi, il rischio sia elevato, oltre alla notifica il Titolare è tenuto a darne comunicazione all'Interessato.

Nel caso in cui l'Incaricato e/o un Responsabile del Trattamento, ove nominato, abbiano notizia di una o più delle violazioni sottoindicate, gli stessi avranno l'obbligo di darne immediata comunicazione al Titolare del Trattamento inviandogli un'e-mail all'indirizzo di posta elettronica info@dinamocer.org:

1. violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
2. violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
3. violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità o distruzione, accidentale o non autorizzata, di dati personali.

La comunicazione di violazione dovrà contenere tutti i dettagli della violazione, compresa la descrizione dell'accaduto, la quantità e la tipologia di dati personali coinvolti.

L'obbligo di notifica e quello aggiuntivo di comunicazione verranno valutati caso per caso dal Titolare del Trattamento in relazione alla tipologia di violazione e al suo impatto sui diritti e libertà degli Interessati. Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell'entità dei rischi:

- **Rischio assente:** la notifica al Garante non è obbligatoria
- **Rischio presente:** è necessaria la notifica al Garante
- **Rischio elevato:** In presenza di rischi "elevati", è necessaria la comunicazione agli interessati.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari).

Per la notifica della violazione e la comunicazione al Garante occorre compilare gli appositi moduli messi a disposizione dal Garante stesso e reperibili su www.garanteprivacy.it

Di seguito gli schemi da seguire per la compilazione della notifica ai sensi dell'art. 33 terzo comma GDPR e della comunicazione ai sensi dell'art. 34 secondo comma GDPR:

Notifica	Comunicazione
a) Descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione. b) Comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni. c) Descrivere le probabili conseguenze della violazione	a) Descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali. b) Comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni. c) Descrivere le probabili conseguenze della violazione dei dati personali. d) Descrivere le misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio

dei dati personali. d) Descrivere le misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.	alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

Il Titolare del Trattamento, ove necessario in funzione della gravità della violazione, metterà in atto le misure tecniche e organizzative più adeguate per scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati, tenendone traccia scritta, tra le quali:

a) contenimento della violazione e ripristino dei dati;
b) valutazione del *data breach* e adozione delle misure atte a scongiurare il ripetersi in futuro della violazione.

* * *

Il presente Modello Organizzativo è soggetto a verifica periodica, almeno annuale, ed eventuale aggiornamento.

Grottammare, Maggio 2024	Il Titolare del Trattamento

Allegati:

1) Documento di analisi dei rischi;
2) Organigramma privacy;
3) Registro dei trattamenti.

Created in Master

Analisi dei rischi connessi al trattamento dei dati personali

COMUNITÀ ENERGETICA RINNOVABILE DINAMO E.T.S.

PASSAGGI METODOLOGICI

La presente valutazione dei rischi, che riprende le linee guida dell'ENISA (European Network and Information Security Agency) per le PMI, adotta un approccio alla valutazione del rischio che si basa su quattro fasi, come segue:

1. Definizione dell'operazione di trattamento e del suo contesto;
2. Comprensione e valutazione dell'impatto;
3. Definizione di possibili minacce e valutazione della loro probabilità (probabilità di occorrenza della minaccia);
4. Valutazione del rischio (combinando la probabilità di accadimento della minaccia e l'impatto).

A seguito della valutazione del rischio, è possibile adottare misure di sicurezza tecniche e organizzative che sono appropriate al livello di rischio.

DEFINIZIONE DELL'OPERAZIONE DI TRATTAMENTO E DEL SUO CONTESTO

Questo è il primo passo della valutazione di impatto del rischio ed è fondamentale per il Titolare del trattamento al fine di tracciare i confini del sistema del trattamento dei dati personali (in corso di valutazione) e il relativo contesto.
La COMUNITÀ ENERGETICA RINNOVABILE DINAMO E.T.S. (di seguito CER DINAMO) ha per oggetto la costituzione e la gestione di una comunità di energia rinnovabile. Per lo svolgimento della suddetta attività la CER DINAMO gestisce le seguenti tipologie di dati personali:

1. Dati anagrafici degli associati compresa copia del documento di identità;
2. Dati anagrafici dei beneficiari dei servizi e di soggetti esterni;
3. Dati anagrafici dei fornitori;
4. Dati anagrafici degli utenti immessi sul sito web per la presentazione delle domande di adesione on line, inviati via email e accodati nel database del sito;
5. Dati fiscali (codice fiscale, partita IVA);
6. Recapiti telefonici e di posta elettronica;
7. Codici POD (Point Of Delivery –Punto di fornitura) e IBAN (International Bank Account Number);
8. Dati relativi agli utenti del sito web che non presentano domanda di adesione.

Le attività svolte sono le seguenti:

1. Raccolta delle domande di adesione all'Associazione presentate in formato analogico o digitale;
2. Valutazione delle domande;
3. Accoglimento o rigetto delle domande;
4. Iscrizione nel libro degli associati;
5. Partecipazione alle attività associative;
6. Organizzazione di configurazioni per la condivisione dell'energia rinnovabile;
7. Riparto delle entrate derivanti dalla condivisione dell'energia elettrica rinnovabile prodotta dagli impianti nella disponibilità della comunità energetica;
8. Gestione del sito web.

FASE 1: CAPIRE E VALUTARE IL LIVELLO DI IMPATTO DEL TRATTAMENTO

A questo punto il Titolare del trattamento deve valutare l'impatto sui diritti fondamentali e le liberà degli individui che può derivare dalla possibile perdita di dati personali. Vengono presi in considerazione 4 livelli di impatto (basso, medio, alto, molto alto), secondo la tabella che segue.

Creato con Master PDF Editor

Tabella 1: Descrizione dei livelli di impatto del trattamento

Livello di impatto	Descrizione
BASSO	Gli interessati possono andare incontro a pochi e minori inconvenienti che supereranno senza alcun problema (tempo speso a fornire nuovamente le informazioni, fastidi, irritazioni, ecc…)
MEDIO	Gli interessati possono andare incontro a significativi inconvenienti che saranno in grado di superare nonostante piccole difficoltà (costi extra, diniego di accesso ai servizi per gli affari, paura, incomprensioni, stress, piccoli disturbi fisici, ecc…)
ALTO	Gli interessati possono andare incontro a inconvenienti significativi, che potrebbero essere in grado di superare, sebbene con serie difficoltà (appropriazioni indebite di capitali, inserimento nella lista nera di istituzioni finanziarie, danni alla proprietà, perdita del lavoro, citazione in giudizio, peggioramento della salute, ecc…)

La valutazione di impatto è un processo qualitativo e debbono essere considerati diversi fattori dal Titolare del trattamento, come ad esempio la tipologia dei dati personali, le criticità delle operazioni di trattamento, il volume dei dati personali raccolti.
Al fine di aiutare il Titolare in questo procedimento, può essere utilizzata la Tabella che segue per valutare in modo separato l'impatto derivante dalla perdita di riservatezza, di integrità e disponibilità dei dati.
Dopo tale valutazione, saranno ottenuti tre livelli di impatto (per la perdita di riservatezza, integrità, disponibilità).
Il più alto di questi livelli viene considerato come il risultato finale della valutazione d'impatto, relativamente al trattamento complessivo dei dati.

Tabella 2: valutazione dei tre livelli di impatto

No.	Domanda	Valutazione
I.1	Per cortesia rifletta sull'impatto che una rivelazione non autorizzata (perdita di riservatezza) – nel contesto dove si svolge la sua attività – può avere sull'interessato ed esprima una valutazione	☒ Basso ☐ Medio ☐ Alto
I.2	Per cortesia rifletta sull'impatto che un'alterazione non autorizzata (perdita di integrità) dei dati personali - nel contesto dove si svolge la sua attività – può avere sull'interessato ed esprima una valutazione	☒ Basso ☐ Medio ☐ Alto
I.3	Per cortesia rifletta sull'impatto che una distruzione o una perdita non autorizzate (perdita di disponibilità) dei dati personali - nel contesto dove si svolge la sua attività – può avere sull'interessato ed esprima una valutazione	☒ Basso ☐ Medio ☐ Alto

FASE 2: DEFINIZIONE DELLE POSSIBILI MINACCE E VALUTAZIONE DELLA LORO PROBABILITÀ

Creato in Master PDF Editor

La tabella sottostante riassume le domande correlate alla valutazione delle probabilità di avveramento delle minacce.

Tabella 3: valutazione delle probabilità di avveramento delle minacce

A. RISORSE TECNICHE E NETWORK		
1	Una parte del trattamento dei dati viene realizzata attraverso internet?	**SI**
2	È possibile fornire l'accesso a un sistema di trattamento interno di dati personali tramite Internet?	Il sistema informatico inteso come sito web dell'Associazione è gestibile da remoto solo da personale autorizzato.
3	Il sistema di trattamento dei dati personali è interconnesso con un altro servizio IT, esterno o interno?	NO
4	Persone non autorizzate al trattamento possono avere accesso facilmente al trattamento dei dati?	**NO**
5	Il processo del trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le più importanti "*best practice*"?	NO
B. PROCESSI/PROCEDURE CORRELATE AL TRATTAMENTO DEI DATI		
6	I ruoli e le responsabilità rispetto al trattamento dei dati personali sono vaghi o non chiaramente definiti?	**NO**
7	L'uso della rete, dei sistemi e delle risorse fisiche nell'Azienda non è accettabile o non chiaramente definito?	**NO**
8	I dipendenti hanno il permesso di usare i loro device per connettersi al sistema del trattamento dei dati?	Non vi sono dipendenti
9	I dipendenti hanno il permesso di trasferire, immagazzinare o altro il procedimento di trattamento dei dati personali fuori dall'Azienda?	Non vi sono dipendenti
10	Il procedimento del trattamento dei dati personali può essere effettuato senza aver prima creato i file di log?	**SI**

Created in Master PDF Editor

C. PERSONE E PARTI DIFFERENTI COINVOLTE NEL TRATTAMENTO		
11	Il procedimento del trattamento è effettuato da un numero non definito di impiegati?	**NO**
12	Parti del trattamento sono svolte da terze parti (responsabili del trattamento esterni)?	**SI**
13	Gli obblighi degli incaricati al trattamento sono ambigui o non chiaramente statuiti?	**NO**
14	Il personale coinvolto nel trattamento è all'oscuro della materia della sicurezza delle informazioni?	**NO**
15	Il personale coinvolto nel trattamento trascura di immagazzinare in modo sicuro e/o distruggere i dati personali?	**NO**
D. SETTORE DI BUSINESS E PESO DEL TRATTAMENTO		
16	Considera il suo settore di business incline ad essere oggetto di cyber attacchi?	**NO**
17	Ha la sua Azienda sofferto di cyber attacchi o di altri tipi di attacchi negli ultimi due anni?	**NO**
18	Ha ricevuto mai alcuna notificazione e/o citazione riguardante la sicurezza del sistema di informazione usato per il trattamento dei dati personali negli ultimi due anni?	**NO**
19	I trattamenti dei dati personali riguardano un grande volume di interessati e/o di dati personali?	**NO**
20	Esistono specifiche "best practice" per il suo settore di affari che non sono state adeguatamente seguite?	**NO**

Seguendo questo approccio, il livello di probabilità di occorrenza della minaccia può essere definito per ciascuna delle aree di valutazione, come segue:

- Basso: è improbabile che la minaccia si materializzi.
- Medio: c'è una ragionevole possibilità che la minaccia si materializzi.
- Alto: la minaccia potrebbe materializzarsi.

Created in Master PDF Editor

Le tabelle 4 e 5 sono utilizzate per documentare la probabilità di occorrenza delle minacce per ciascuna area di valutazione e di conseguenza calcolare il suo valore finale.

Tabella 4: Valutazione della probabilità di occorrenza delle minacce per area

AREA DI VALUTAZIONE	PROBABILITÀ	
	LIVELLO	**PUNTEGGIO**
RISORSE TECNICHE E NETWORK	☒ Basso	1
	☐ Medio	2
	☐ Alto	3
PROCESSI/PROCEDURE CORRELATE AL TRATTAMENTO DEI DATI	☒ Basso	1
	☐ Medio	2
	☐ Alto	3
PERSONE E PARTI DIFFERENTI COINVOLTE NEL TRATTAMENTO	☒ Basso	1
	☐ Medio	2
	☐ Alto	3
SETTORE DI BUSINESS E PESO DEL TRATTAMENTO	☒ Basso	1
	☐ Medio	2
	☐ Alto	3

Tabella 5: Valutazione della probabilità di occorrenza di una minaccia

SOMMA TOTALE PROBABILITA' DI VERIFICAZIONE DELLA MINACCIA	LIVELLO DI PROBABILITA' VERIFICAZIONE DELLA MINACCIA
4 -5	Basso

FASE 3: VALUTAZIONE DEL RISCHIO

Dopo aver valutato l'impatto del trattamento dei dati personali e la probabilità di verificazione della minaccia, è possibile effettuare la valutazione del rischio.

	LIVELLO DI IMPATTO		
	BASSO	**MEDIO**	**ALTO**
BASSO			
MEDIO			

Created in Master PDF Editor

ALTO			

PROBABILITA' DI VERIFICAZIONE DELLA MINACCIA

Legenda:		
Rischio basso	Rischio medio	Rischio alto

MISURE DI SICUREZZA

A seguito della valutazione del livello di rischio, l'Associazione può procedere con la selezione delle misure di sicurezza appropriate per la protezione dei dati personali.

A.1 Misure di sicurezza tecniche e organizzative da adottarsi in caso di rischi alla sicurezza qualificati come di valore BASSO.

	CATEGORIA DI APPARTENENZA DELLA MISURA DI SICUREZZA	DESCRIZIONE DELLA MISURA DI SICUREZZA
1	Politica di sicurezza e procedure per la protezione dei dati personali	L'organizzazione dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.
2	Politica di sicurezza e procedure per la protezione dei dati personali	La politica di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale.
3	Ruoli e responsabilità	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con le politiche di sicurezza.
4	Ruoli e responsabilità	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo, l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.
5	Responsabili del trattamento	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.
6	Responsabili del trattamento	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.
7	Responsabili del trattamento	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.

Create PDF Editor

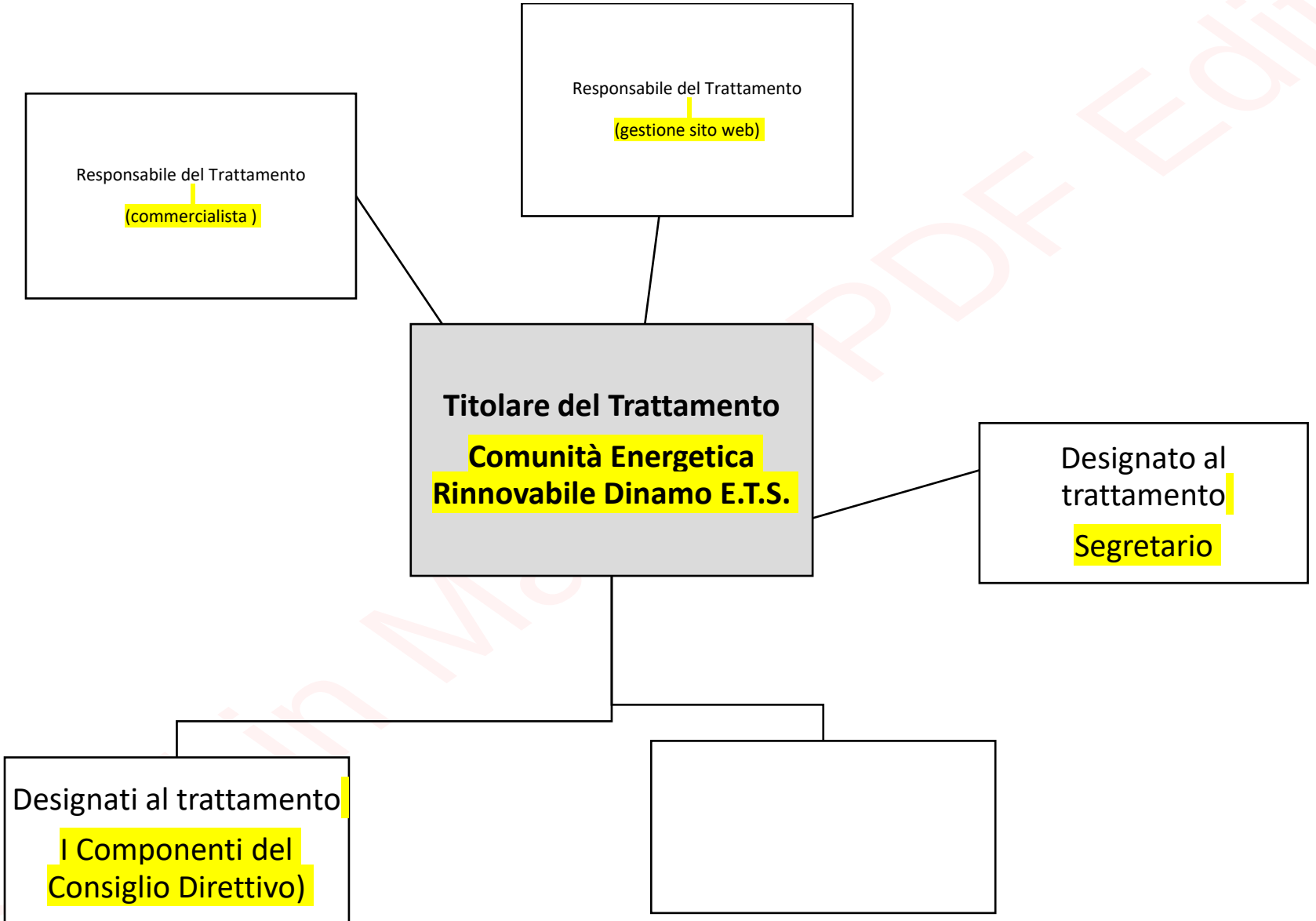
8	Gestione degli incidenti / Violazione dei dati personali (Personal data breaches)	Le violazioni dei dati personali (come definite dall'art. 4 del GDPR) devono essere segnalate immediatamente al Management competente secondo l'organizzazione interna. Dovrebbero essere in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi degli art. 33 e 34 GDPR.
9	Business continuity	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali). **NON APPLICABILE**
10	Obblighi di riservatezza imposti al personale	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di preassunzione e / o assunzione.
11	Formazione	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica.
12	Controllo degli accessi e autenticazione	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente. **NON APPLICABILE**
13	Controllo degli accessi e autenticazione	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità. **NON APPLICABILE**
14	Controllo degli accessi e autenticazione	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità. **NON APPLICABILE**
15	Controllo degli accessi e autenticazione	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile). **NON APPLICABILE**
16	Sicurezza delle Postazioni di lavoro	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza**. NON APPLICABILE**
17	Sicurezza delle Postazioni di lavoro	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base settimanale**. NON APPLICABILE**
18	Sicurezza delle Postazioni di lavoro	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate**. NON APPLICABILE**

Created with WPS Editor

19	Sicurezza delle Postazioni di lavoro	Il sistema dovrebbe attivare il time-out di sessione quando l'utente non è stato attivo per un certo periodo di tempo. **NON APPLICABILE**
20	Sicurezza delle Postazioni di lavoro	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente. **NON APPLICABILE**
21	Sicurezza della Rete e delle Infrastrutture di comunicazione Elettronica	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL). **NON APPLICABILE**
22	Back-up	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità**. Non necessario in quanto la pagina web e i database risiedono nei server dell'Azienda di hosting di riferimento (SiteGround)**
23	Back-up	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine. **Come sopra**
24	Back-up	L'esecuzione dei backup deve essere monitorata per garantirne la completezza. **Come sopra**
25	Back-up	I backup completi devono essere eseguiti regolarmente. **Come sopra**
26	Dispositivi mobili / portatili	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo. **NON APPLICABILE**
27	Dispositivi mobili / portatili	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere preregistrati e preautorizzati. **NON APPLICABILE**
28	Dispositivi mobili / portatili	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali. **NON APPLICABILE**
29	Sicurezza del ciclo di vita delle applicazioni	Dovrebbero essere seguiti standard e pratiche di codifica sicure. **NON APPLICABILE**
30	Cancellazione / eliminazione dei dati	La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica.
31	Cancellazione / eliminazione dei dati	È necessario eseguire la triturazione della carta e dei supporti portatili utilizzati per memorizzare i dati personali.
32	Sicurezza fisica	Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile da personale non autorizzato. **NON APPLICABILE**

Created with Free Editor

ORGANIGRAMMA PRIVACY



Creato in Master PDF Editor

TRATTAMENTI EFFETTUATI IN QUALITA' DI TITOLARE DEL TRATTAMENTO (art. 30 secondo comma GDPR)

	TRATTAMENTO			DATI PERSONALI			INTERESSATI		DESTINATARI		TRASFERIMENTI	SICUREZZA
	Descrizione	Finalità	Contitolare	Categoria	Dati Particolari (ex sensibili) SI/NO	Termine Ultimo Cancellazione	Categoria	Consenso (SI/NO)	Categoria	Paesi terzi, org.ni int.li (eventuale) SI/NO	Paesi terzi, org.ni int.li (eventuale) SI/NO	Misure Tecniche ed organizzative adottate (e rimandi ad eventuali allegati di dettaglio)
1	**SOCI E ASPIRANTI SOCI**	Gestione del rapporto associativo (es. invio della corrispondenza, convocazione alle sedute degli organi, procedure amministrative interne); organizzazione ed esecuzione del servizio, adempimento obblighi di legge (es. fiscali, ecc.) riferiti ai soci dell'Associazione; invio (tramite posta, posta elettronica, newsletter o cellulare o altri mezzi informatici) di comunicazioni legate all'attività e alle iniziative dell'Associazione; organizzazione di configurazioni per la condivisione dell'energia rinnovabile; riparto entrate derivanti dalla condivisione dell'energia.	NO	Dati personali comuni (es. dati anagrafici, C.F., riferimenti telefonici, e-mail, pec, residenza, codici POD e IBAN); immagini fotografiche.	NO	In caso di mancata iscrizione all'Organizzazione, i dati sono conservati (limitatamente a nome e cognome ed esito della valutazione di idoneità) ai soli fini storici e statistici e al fine di conservare traccia della richiesta di adesione; i dati dei soci sono conservati anche successivamente alla cessazione del rapporto associativo per finalità di archivio, obblighi legali o contabili o fiscali o per esigenze di tutela dell'Organizzazione, con esclusione di comunicazioni a terzi e diffusione	Chiunque presenti domanda di adesione, soci /aspiranti soci	SI	I dati dei soci possono essere trasmessi: agli altri soci ai sensi di statuto, per l'organizzazione ed esecuzione del servizio; ai soggetti deputati allo svolgimento di attività a cui l'Organizzazione è tenuta in base ad obbligo di legge (commercialista, ecc.); a tutte le persone fisiche e/o giuridiche, pubbliche e/o private quando la comunicazione risulti necessaria o funzionale allo svolgimento dell'attività istituzionale. Previo consenso del socio, vengono diffuse mediante il sito dell'Associazione, i social network dell'Associazione, la newsletter o materiale cartaceo, immagini/video raffiguranti i soci in occasioni ed eventi istituzionali.	NO	NO	Misure indicate nel documento di Analisi dei Rischi.
2	**FORNITORI**	Gestione del rapporto di fornitura di beni o servizi.	NO	Dati personali comuni (es. dati anagrafici, C.F.,Partita IVA, riferimenti telefonici, e-mail, PEC, residenza,IBAN)	NO	Per tutta la durata del rapporto di fornitura e fino a 15 anni dal termine del medesimo, salvo termini più lunghi previsti dalla normativa, anche fiscale, applicabile al rapporto in questione.	Fornitori di beni e servizi	NO	I dati possono essere comunicati a consulenti e commercialisti o altri professionisti che eroghino prestazioni funzionali alle finalità indicate; ad istituti bancari e assicurativi che eroghino prestazioni funzionali alle finalità indicate; a soggetti che elaborano i dati in esecuzione di specifici obblighi di legge; a pubbliche amministrazioni per l'adempimento degli obblighi di legge.	NO	NO	Misure indicate nel documento di Analisi dei Rischi.
3	**UTENTI SITO WEB**	Evasione di richieste da parte di utenti del sito web.	**NO**	Dati personali comuni (es. dati anagrafici, C.F., riferimenti telefonici, e-mail, pec, residenza, codici POD); immagini fotografiche.	NO	I dati personali trattati per l'assistenza o richiesta di informazioni saranno conservati per il tempo necessario la gestione della richiesta. Decorsi i periodi di conservazione suindicati i dati personali saranno cancellati o anonimizzati in modo permanente. Con riferimento alle domande di adesione all'Associazione, In caso di mancata iscrizione all'Organizzazione, i dati sono conservati (limitatamente a nome e cognome ed esito della valutazione di idoneità) ai soli fini storici e statistici e al fine di conservare traccia della richiesta di adesione; i dati dei soci sono conservati anche successivamente alla cessazione del rapporto associativo per finalità di archivio, obblighi legali o contabili o fiscali o per esigenze di tutela dell'Organizzazione, con esclusione di comunicazioni a terzi e diffusione	Utenti sito web	SI	I dati possono essere conosciuti dai soggetti che sono incaricati della manutenzione degli strumenti informatrici dell'Organizzazione.	NO	NO	Misure indicate nel documento di Analisi dei Rischi.

Creation Editor