MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

ASHTANGA YOGA GENOVA ASD

Sommario

1 IL REGOLAMENTO UE 2016/679 (GDPR) 3
1.1 L'adeguamento della normativa nazionale 3
1.2 I principi generali e le nuove regole per il trattamento dei dati personali 3
1.3 Responsabilità 4
1.4 Sanzioni 5
1.5 Esimente della responsabilità 7
2 Il modello organizzativo privacy dell'associazione Ashtanga Yoga Genova ASD 8
2.1 Finalità del modello organizzativo privacy 8
2.2 Destinatari 8
2.3 Elementi fondamentali del modello organizzativo privacy 8
2.4 Riferimenti normativi 9
2.5 Termini e Definizioni 9
2.6 Percorso metodologico di definizione del modello organizzativo privacy: valutazione del contesto e risk &privacy assessment 10
2.6.1 L'ASSESSMENT: ANALISI E VALUTAZIONE DEL CONTESTO 10
2.6.2 L'ASSESSMENT: ANALISI DEL RISCHIO Con l'introduzione del GDPR la privacy diventa risk based. 13
2.6.3 LA REMEDIATION: PRINCIPI E MISURE ADOTTATE 13
2.6.4 LA REMEDIATION: LE POLITICHE 14
2.6.5 LA REMEDIATION: LE INFORMATIVE, I CONSENSI 14
2.6.6 LA REMEDIATION: LE NOMINE E LE ISTRUZIONI 14
2.6.7 LA REMEDIATION: IL REGISTRO DEI TRATTAMENTI 15
2.6.8 LA REMEDIATION: I DIRITTI DEGLI INTERESSATI 15
2.6.9 LA REMEDIATION: IL SISTEMA DI CONTROLLO INTERNO DELL'ASSOCIAZIONE 15
3 ORGANI E FUNZIONI COINVOLTI NELLA DATA PROTECTION 16
3.1 ORGANIGRAMMA PRIVACY 16
3.2 DESIGNAZIONE DEL DATA PROTECTION OFFICER 16
3.3 LE FUNZIONI DI GOVERNANCE DEL MODELLO ORGANIZZATIVO PRIVACY 16
3.4 MONITORAGGIO, VALUTAZIONI E MIGLIORAMENTO CONTINUO 16
3.5 AUTORI DEL MONITORAGGIO, VALUTAZIONI E MIGLIORAMENTO CONTINUO 17
3.6 SEGNALAZIONI 17
4 OSSERVAZIONI, DISPOSIZIONI SANZIONATORIE, DIFFUSIONE DEL DOCUMENTO 18
4.1 OSSERVANZA E DISPOSIZIONI SANZIONATORIE 18
4.2 DIFFUSIONE DEL MODELLO ORGANIZZATIVO 18

1 IL REGOLAMENTO UE 2016/679 (GDPR)

1.1 L'adeguamento della normativa nazionale

Il Regolamento UE 2016/679 (GDPR) è una normativa europea che unifica e rafforza la protezione dei dati personali nell'Unione Europea. Introduce obblighi per garantire un trattamento lecito e corretto dei dati da parte di Titolari e Responsabili del trattamento.
In Italia, l'adeguamento al GDPR è stato recepito con il Decreto Legislativo 10 agosto 2018, n. 101, che ha modificato il Codice Privacy (D.lgs. 196/2003).
Il GDPR tutela i dati personali, ovvero qualsiasi informazione che identifica direttamente o indirettamente una persona fisica o giuridica, inclusi dati sensibili come quelli sulla salute o opinioni politiche. Il Titolare del trattamento determina finalità e modalità del trattamento, mentre Responsabili e Autorizzati agiscono per suo conto.
La normativa si applica sia a enti UE sia a organizzazioni extra UE che trattano dati di residenti nell'Unione o offrono loro servizi.
L'adeguamento al GDPR richiede, tra l'altro, l'adozione di un Modello Organizzativo Privacy che consenta di:

- prevenire e valutare i rischi legati al trattamento dei dati personali;
- gestire tempestivamente eventuali criticità;
- dimostrare l'efficacia del sistema di controllo per evitare responsabilità e sanzioni.

1.2 I principi generali e le nuove regole per il trattamento dei dati personali

Il trattamento dei dati personali deve rispettare i seguenti principi fondamentali:

- Diritto alla protezione dei dati personali: ogni individuo ha il diritto che i suoi dati siano trattati con elevata tutela, nel rispetto dei diritti, della libertà, della riservatezza e della dignità.
- Liceità, correttezza e trasparenza: il trattamento deve essere conforme alla legge, trasparente per l'interessato, vietando pratiche ingannevoli; dati trattati illecitamente non possono essere utilizzati.
- Finalità: i dati devono essere raccolti per scopi legittimi, specifici e non incompatibili con l'uso previsto.
- Necessità e minimizzazione: si devono trattare solo i dati strettamente necessari per le finalità dichiarate, evitando raccolte eccessive.
- Proporzionalità: ogni operazione di trattamento deve essere pertinente e non eccedere rispetto agli scopi.
- Integrità e riservatezza: i dati devono essere custoditi con misure tecniche e organizzative adeguate per prevenire perdita, distruzione, accessi non autorizzati o trattamenti illeciti.
- Accountability (responsabilizzazione): il Titolare deve dimostrare di aver agito in

conformità al GDPR adottando un approccio proattivo basato sulla valutazione del rischio.

- Privacy by Design: la protezione dei dati deve essere integrata fin dalla progettazione di sistemi e processi.
- Privacy by Default: il trattamento deve limitarsi ai dati necessari e prevedere la conservazione per il tempo strettamente necessario.
- Consenso: il consenso deve essere libero, specifico, informato e revocabile; per i minori è richiesta la verifica dell'età e, se necessario, il consenso dei genitori.
- Data Breach: in caso di violazioni dei dati, il Titolare deve notificare l'Autorità di controllo entro 72 ore e, se necessario, informare gli interessati.
- Diritti degli interessati: includono accesso, cancellazione (diritto all'oblio), limitazione, rettifica e portabilità dei dati.
- Trasferimento dati extra UE: è consentito solo se garantite adeguate misure di protezione, come clausole contrattuali, decisioni di adeguatezza o altri strumenti previsti dal GDPR.
- Data Protection Officer (DPO): figura incaricata di garantire la conformità al GDPR, supportare il Titolare e fungere da punto di contatto con l'Autorità di controllo.
- Misure tecniche e organizzative: l'organizzazione deve adottare procedure, formazione e controlli interni per assicurare la conformità e prevenire trattamenti illeciti.

1.3 Responsabilità

Responsabilità derivante dalla violazione della normativa sul trattamento dei dati personali
La violazione della normativa in materia di protezione dei dati personali può comportare responsabilità di natura civile, penale e/o amministrativa, anche cumulabili qualora derivino da un unico fatto.

Responsabilità civile

In ambito civile, la persona fisica o giuridica che, mediante il trattamento illecito di dati personali, cagioni un danno a terzi è tenuta al risarcimento ai sensi dell'art. 2050 del Codice Civile. Tale norma disciplina la responsabilità per l'esercizio di attività pericolose, includendo tra queste anche il trattamento dei dati personali. Secondo tale disposizione, chi causa un danno nello svolgimento di un'attività pericolosa è obbligato a risarcirlo, salvo che provi di aver adottato tutte le misure idonee ad evitarlo.

La responsabilità civile prescinde dalla colpa o dal dolo dell'autore del trattamento illecito: si configura infatti un'inversione dell'onere della prova, in base alla quale spetta al presunto responsabile dimostrare di aver adottato ogni cautela necessaria per prevenire il danno. Alla parte danneggiata compete invece l'onere di provare il danno subito e il nesso causale tra l'attività svolta e il pregiudizio patito.

I danni risarcibili possono essere sia **patrimoniali** (es. perdita economica) che **non patrimoniali**, comprendenti le sofferenze fisiche e/o morali, il cui ammontare è stabilito dal giudice in via equitativa.

Responsabilità penale

Sotto il profilo penale, assumono particolare rilevanza le seguenti fattispecie:

- **Accesso abusivo a un sistema informatico o telematico** (art. 615-ter c.p.);
- **Detenzione e diffusione abusiva di codici di accesso** a sistemi informatici o telematici (art. 615-quater c.p.);

- Reati previsti dal **Codice in materia di protezione dei dati personali** (D.lgs. 196/2003, come modificato dal D.lgs. 101/2018), tra cui:
  - *Art. 167*: Trattamento illecito di dati;
  - *Art. 167-bis*: Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala;
  - *Art. 167-ter*: Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala;
  - *Art. 168*: Falsità nelle dichiarazioni e notificazioni al Garante; interruzione dell'attività o dei poteri del Garante;
  - *Art. 170*: Inosservanza dei provvedimenti del Garante;
  - *Art. 171*: Violazioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori.

Responsabilità amministrativa

Il **Regolamento (UE) 2016/679 (GDPR)** prevede l'applicazione di sanzioni amministrative pecuniarie, che vengono determinate caso per caso sulla base di criteri specifici, tra cui:

- La natura, gravità e durata della violazione;
- Il numero di interessati coinvolti e l'entità del danno subito;
- Il carattere doloso o colposo della violazione;
- Le misure adottate per mitigare il danno;
- Il grado di responsabilità del Titolare o del Responsabile del trattamento, anche in relazione alle misure tecniche e organizzative attuate;
- L'eventuale presenza di precedenti violazioni;
- Il livello di cooperazione con l'Autorità di controllo;
- Le categorie di dati coinvolti;
- Le modalità con cui la violazione è stata rilevata (es. notifica spontanea o su segnalazione);
- Il rispetto degli eventuali provvedimenti del Garante;
- L'adesione a codici di condotta o a meccanismi di certificazione;
- Altri fattori aggravanti o attenuanti, come vantaggi economici ottenuti o perdite evitate a seguito della violazione.

Soggetti responsabili

Sono soggetti a responsabilità sia il **Titolare del trattamento**, che il **Responsabile del trattamento**.

- Il **Titolare** è tenuto a risarcire qualsiasi danno derivante dalla violazione del Regolamento, qualora il danno sia a lui imputabile.
- Il **Responsabile** risponde se ha agito in violazione delle istruzioni ricevute o non ha adempiuto agli obblighi che gli spettano specificamente.

1.4 Sanzioni

L'articolo 82 del Regolamento (UE) 2016/679 (GDPR) disciplina il diritto al risarcimento, stabilendo che chiunque subisca un danno, materiale o immateriale, a causa di una violazione del Regolamento ha diritto a ottenere il risarcimento dal Titolare del trattamento o dal Responsabile del trattamento.

Il sistema sanzionatorio previsto dal GDPR si articola in sanzioni amministrative pecuniarie proporzionate alla gravità della violazione e alle circostanze del caso concreto. In particolare:

- Fino a 10 milioni di euro, o fino al 2% del fatturato annuo globale dell'esercizio precedente (se superiore), nei casi previsti dall'art. 83, par. 4. Tali ipotesi includono, a titolo esemplificativo, la mancata adozione di misure relative a: protezione dei minori, dati

pseudonimizzati, privacy by design e by default, accordi tra contitolari, tenuta dei registri delle attività di trattamento, valutazioni d'impatto sulla protezione dei dati, istruzioni agli autorizzati, sicurezza dei dati, e nomina del Data Protection Officer (DPO).

- Fino a 20 milioni di euro, o fino al 4% del fatturato annuo globale dell'esercizio precedente (se superiore), nei casi previsti dall'art. 83, par. 5 e 6. Rientrano in questa categoria le violazioni dei principi fondamentali del trattamento, dei diritti degli interessati, delle norme sui trasferimenti internazionali di dati, tra gli altri.

Il Regolamento riconosce alle Autorità di controllo un margine di discrezionalità nell'infliggere sanzioni e nel determinare l'importo delle stesse. Tale discrezionalità, tuttavia, non equivale a una libertà assoluta, poiché è vincolata al rispetto dei criteri fissati all'art. 83, par. 2, tra cui:

- natura, gravità e durata della violazione;
- intenzionalità o negligenza del comportamento;
- misure adottate per attenuare i danni;
- grado di responsabilità del Titolare o del Responsabile;
- eventuali violazioni precedenti;
- grado di cooperazione con l'Autorità di controllo;
- categorie di dati coinvolti;
- modalità con cui l'Autorità è venuta a conoscenza della violazione;
- adesione a codici di condotta o meccanismi di certificazione.

Il D.lgs. 196/2003 (Codice Privacy), come modificato dal D.lgs. 101/2018, all'art. 166, ha integrato tali criteri, specificando ulteriormente le modalità di applicazione delle sanzioni amministrative e del procedimento sanzionatorio.

Il Considerando 148 del GDPR prevede inoltre che, in caso di violazioni minori o qualora la sanzione pecuniaria rappresenti un onere sproporzionato per una persona fisica, l'Autorità di controllo possa optare per un ammonimento in luogo della sanzione pecuniaria.

Oltre alle sanzioni amministrative, il GDPR consente agli Stati membri di prevedere sanzioni penali. In Italia, il Codice Privacy – come modificato – contempla specifici reati, tra cui quelli disciplinati dagli articoli 167, 167-bis, 167-ter, 168, 170 e 171, in attuazione del Considerando 149 e dell'art. 84 del Regolamento.

Infine, l'articolo 58 del GDPR attribuisce alle Autorità di controllo poteri correttivi, tra cui la possibilità di limitare o vietare un trattamento di dati. L'esercizio di tali poteri può comportare conseguenze rilevanti per l'organizzazione, come l'interruzione di servizi o attività aziendali.

1.5 Esimente della responsabilità

L'adozione di un Modello Organizzativo Privacy (MOP) rappresenta per imprese, enti e organizzazioni uno strumento idoneo a escludere la responsabilità derivante da eventuali violazioni della normativa in materia di protezione dei dati personali. Tuttavia, per beneficiare dell'esimente, è necessario dimostrare di aver **effettivamente adottato, attuato e applicato** il MOP in modo conforme alle disposizioni del Regolamento (UE) 2016/679 (GDPR).

Affinché il Modello sia ritenuto efficace, il GDPR impone l'adozione di un approccio **basato sul rischio** (*risk-based approach*), in base al quale il Titolare del trattamento è tenuto a:

- **analizzare i trattamenti effettuati**, attraverso uno o più assessment, per identificare e valutare i rischi potenziali per i diritti e le libertà fondamentali degli interessati (valutazione dei rischi e degli impatti – *Risk & Privacy Impact Assessment*);
- **definire e attuare interventi correttivi** (*remediation*) e attività di implementazione, tramite un piano di adeguamento strutturato secondo priorità, volto a garantire la conformità al Regolamento;
- **introdurre procedure specifiche** per attuare e monitorare il piano di adeguamento, anche in riferimento alla formazione del personale e all'adozione di decisioni che assicurino l'operatività in linea con il GDPR;
- **valutare e pianificare le risorse finanziarie necessarie** alla realizzazione del piano di adeguamento;
- **istituire obblighi informativi** nei confronti dell'organismo di vigilanza interno incaricato del controllo sull'attuazione e sull'osservanza del MOP;
- **istituire un sistema disciplinare** idoneo a sanzionare le violazioni delle disposizioni contenute nel Modello Organizzativo Privacy.

Per assicurare la concreta applicazione del MOP, è inoltre necessario prevedere:

- **una verifica periodica** dell'efficacia del Modello, con conseguente aggiornamento in caso di violazioni significative, cambiamenti organizzativi o operativi, o modifiche normative;
- **l'applicazione di sanzioni interne** in caso di inosservanza delle prescrizioni contenute nel MOP.

2 Il modello organizzativo privacy dell'associazione Ashtanga Yoga Genova ASD

2 . 1 Finalità del modello organizzativo privacy

Il presente documento costituisce il Modello Organizzativo Privacy di Ashtanga Yoga Genova asd (di seguito "Associazione"), che effettua trattamenti di dati personali, nella sua qualità di Titolare e/o di Responsabile.

Tale documento descrive le attività poste in essere dall'Associazione per assicurare la conformità al GDPR e il relativo approccio metodologico utilizzato, oltre agli aspetti di governance, risk management e compliance applicabili alla protezione dei dati personali con la finalità di definire:

- i meccanismi organizzativi e gestionali, inclusi ruoli, responsabilità in materia di protezione dei dati personali ("governance");
- le modalità di gestione dei rischi in materia di protezione dei dati personali ("risk management");
- un sistema strutturato di procedure a presidio dei rischi che sono stati rilevati, nonché una costante azione di monitoraggio sulla corretta attuazione di tale sistema in conformità ai requisiti normativi applicabili in materia di protezione dei dati personali ("compliance").

ASHTANGA YOGA GENOVA, consapevole dell'importanza di adottare ed efficacemente attuare un Modello Organizzativo Privacy, ha predisposto questo documento, che costituisce un valido strumento di sensibilizzazione dei destinatari (come definiti al paragrafo 1.2) per assumere comportamenti conformi ai requisiti del GDPR.

2.2 De st i n a t ar i

Le disposizioni del presente Modello Organizzativo Privacy sono vincolanti per i dipendenti (ivi inclusi i dirigenti) dell'Associazione, per i collaboratori sottoposti a direzione o vigilanza dei dipendenti dell'Associazione e per tutti coloro che, pur non appartenendo all'Associazione, operano a vario titolo gestendo attività che implicano il trattamento di dati personali (di seguito i "Destinatari").

2.3 Elementi fondamentali del modello organizzativo privacy

Gli elementi fondamentali del Modello Organizzativo Privacy, sviluppati dall'Associazione nell'ambito delle attività di adeguamento al GDPR, possono essere così riassunti:

- la predisposizione e prossima adozione di una Procedura per la gestione del Data Breach;
- la Procedura per la gestione della Data Retention è inclusa nell'Informativa Dati Personali GDPR (identificazione, finalità e politica di conservazione;
- la adozione di un documento di Approccio metodologico al Privacy Impact Assessment; DPIA è stata ritenuta <u>non necessaria</u> dato che il trattamento svolto non presenta un rischio elevato per i diritti e le libertà delle persone;
- l'aggiornamento della documentazione privacy rilevante (es. informative, consensi, nomine interne ed esterne);
- la programmazione di attività di informazione e formazione sui contenuti e i cambiamenti introdotti dal GDPR e volte alla diffusione del presente Modello Organizzativo Privacy;

2.4 Riferimenti normativi

Il presente documento fa riferimento e si ispira alle seguenti norme:

- "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";
- Decreto Legislativo 10 agosto 2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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)";
- Standard UNI EN ISO / IEC 27001:2013 "Tecnologia per l'Informazione – Tecniche per la Sicurezza – Sistemi di Gestione per la Sicurezza delle Informazioni – Requisiti";
- Linee Guida e Provvedimenti specifici dell'Autorità Garante per la Protezione dei Dati Personali;
- ARTICLE 29 DATA PROTECTION WORKING PARTY: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

2 . 5 Termini e Definizioni

Nel presente documento si riportano le definizioni e gli acronimi utilizzati, al fine di garantire un'interpretazione univoca dei termini:

- **GDPR**: General Data Protection Regulation, Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati.
- **Dato Personale**: Qualsiasi informazione riguardante una persona fisica identificata o identificabile (c.d. "interessato"). Si considera identificabile una persona che può essere riconosciuta, direttamente o indirettamente, mediante un identificativo come il nome, un numero identificativo, dati relativi all'ubicazione, un identificativo online, oppure uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- **Trattamento**: Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di strumenti automatizzati, applicate a dati personali, come la raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, diffusione, raffronto, interconnessione, limitazione, cancellazione o distruzione.
- **Titolare del Trattamento**: Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o congiuntamente ad altri, determina le finalità e i mezzi del trattamento di dati personali. Qualora tali finalità e mezzi siano stabiliti dal diritto dell'Unione o degli Stati membri, il Titolare può essere designato in base a tale normativa.
- **Responsabile del Trattamento**: Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.
- **Rischio**: Possibilità che si verifichi un evento che incida negativamente sulla sicurezza dei dati personali e sui diritti e le libertà fondamentali dell'interessato. Il livello di rischio viene determinato considerando la natura, la portata, il contesto e le finalità del trattamento, mediante una valutazione oggettiva.
- **Impatto**: Conseguenze che un rischio può produrre sui diritti e le libertà degli interessati. L'impatto tiene conto del tipo di trattamento, del numero di interessati coinvolti, della sensibilità dei dati trattati e delle misure di sicurezza adottate per mitigare i rischi.

- **Analisi e Valutazione del Rischio**: Processo strutturato finalizzato a comprendere la natura dei rischi, valutarne la probabilità e le possibili conseguenze, e determinare il livello di rischio residuo rispetto alla protezione dei dati personali e alla sicurezza delle informazioni.
- **Identificazione del Rischio**: Attività di analisi, individuazione e descrizione dei rischi potenziali associati al trattamento dei dati.
- **Fonte del Rischio**: Fattore, interno o esterno, che da solo o in combinazione con altri elementi può generare un rischio.
- **Vulnerabilità**: Debolezza di un sistema, processo o controllo che può essere sfruttata da una minaccia per compromettere la sicurezza dei dati o dei trattamenti.
- **Minaccia**: Evento o condizione potenzialmente in grado di causare un incidente con impatti negativi sui dati personali, sui trattamenti o sui sistemi informativi.
- **Conseguenza**: Effetto diretto o indiretto di un evento che influisce sul raggiungimento degli obiettivi.
- **Livello del Rischio**: Valutazione complessiva del rischio, espressa come combinazione della probabilità di accadimento di un evento e delle sue conseguenze.
- **Ponderazione del Rischio**: Confronto tra i risultati dell'analisi del rischio e i criteri di accettabilità definiti, al fine di determinare se il rischio sia accettabile, tollerabile o richieda interventi correttivi.
- **Criterio di Rischio**: Parametri utilizzati per stabilire la significatività del rischio e determinare le soglie di accettabilità.
- **Trattamento del Rischio**: Insieme di azioni volte a modificare il rischio, riducendone la probabilità o l'impatto mediante misure correttive, preventive o compensative.
- **Controllo**: Misura tecnica e/o organizzativa implementata per ridurre un rischio o per garantire la conformità normativa.
- **Rischio Residuo**: Rischio che permane dopo l'attuazione delle misure di trattamento.

2 . 6 Percorso metodologico di definizione del modello organizzativo privacy: valutazione del contesto e risk &privacy assessment

Con riguardo a tutte le attività di adeguamento al GDPR che sono state svolte, ASHTANGA YOGA GENOVA ha adottato un approccio metodologico in linea con i requisiti del GDPR, gli standard e le best practice in materia di protezione di dati personali.

2.6.1 L'ASSESSMENT: ANALISI E VALUTAZIONE DEL CONTESTO

I dati personali trattati sono influenzati da fattori inerenti il contesto di riferimento esterno ed interno. Tali fattori costituiscono anche la fonte dei rischi per la protezione dei dati personali e sono stati valutati nel contesto degli assessment sopra esposti.

Contesto esterno

La valutazione del contesto esterno deve prendere in considerazione i seguenti fattori:

- contesto settoriale: valutazione degli aspetti inerenti fornitori, terze parti, visitatori del settore in cui l'Associazione opera;
- contesto normativo: valutazione dell'applicabilità del GDPR e di normative, incluse specifiche normative di settore, all'Associazione in materia di protezione dei dati personali;
- contesto tecnologico: valutazione dell'andamento di minacce e vulnerabilità inerenti l'utilizzo dei sistemi informatici per il trattamento dei dati personali;
- contesto socio-economico: valutazione del valore intrinseco dei dati personali trattati dall'Associazione e potenziali minacce;
- contesto territoriale: valutazione delle caratteristiche del contesto territoriale esterno all'Associazione e del relativo impatto sulla protezione dei dati personali.

Contesto interno

La valutazione del contesto interno deve prendere in considerazione i seguenti fattori:

- contesto legale: valutazione della natura giuridica e della responsabilità dell'Associazione in base a cui è effettuato il trattamento dei dati personali;
- contesto organizzativo e delle risorse umane: valutazione del modello organizzativo e delle risorse umane mediante cui è effettuato il trattamento dei dati personali;
- contesto IT: valutazione dei servizi IT, della relativa infrastruttura IT, dei sistemi mediante cui è effettuato il trattamento dei dati personali e relative misure di sicurezza.;
- contesto fisico e ambientale: valutazione dei siti fisici e delle caratteristiche ambientali mediante cui è effettuato il trattamento dei dati personali.

1.6.3 L'ASSESSMENT: ANALISI DELLE PARTI COINVOLTE NELLA PROTEZIONE DI DATI PERSONALI

Le principali parti coinvolte nella protezione di dati personali individuate dall'Associazione nel corso dell'assessment sono le seguenti.

Parte Interessata	Coinvolgimento	Esigenze e Aspettative
Titolare del trattamento	Assicura la conformità ai requisiti della normativa applicabile	- Garantire il rispetto del GDPR e delle normative applicabili - Valutare e gestire i rischi connessi al trattamento dei dati - Definire e attribuire ruoli e responsabilità, sia internamente che verso soggetti esterni - Essere responsabile dell'adozione di misure tecniche e organizzative adeguate
Responsabile del trattamento	Tratta dati personali per conto del Titolare	- Essere formalmente nominato dal Titolare ai sensi dell'art. 28 GDPR - Ricevere istruzioni chiare, documentate e tracciabili - Agire nel rispetto delle istruzioni ricevute - Essere strumento di accountability e controllo per conto del Titolare
Referente interno del trattamento	Soggetto interno che tratta dati personali	- Ricevere istruzioni chiare dal Titolare - Trasmettere tali istruzioni agli Autorizzati interni - Ricevere formazione adeguata sui requisiti normativi e sulle procedure aziendali - Assicurare la corretta applicazione delle misure tecniche e organizzative stabilite
Interessati al trattamento	Soggetti di cui sono trattati i dati personali	- Essere informati in modo chiaro e trasparente sui trattamenti effettuati - Ottenere garanzie di conformità rispetto ai principi del GDPR - Poter esercitare i propri diritti (accesso, rettifica, cancellazione, opposizione, portabilità, limitazione) - Esprimere il proprio consenso, ove richiesto - Avere a disposizione un punto di contatto facilmente accessibile - Ricevere tempestive comunicazioni in caso di violazioni o incidenti
Autorità Garante Privacy	Vigila sulla corretta applicazione delle normative	- Ricevere tempestive segnalazioni di data breach - Ottenere collaborazione trasparente da parte del Titolare - Vigilare sull'adeguatezza delle misure adottate dall'organizzazione - Intervenire in caso di violazioni o reclami

2.6.2 L'ASSESSMENT: ANALISI DEL RISCHIO Con l'introduzione del GDPR la privacy diventa risk based.

L'Associazione, nell'ambito delle attività di adeguamento al GDPR, ha esaminato e gestito (o intende gestire) il rischio secondo il seguente ciclo di attività:

- identificazione dell'architettura, delle parti coinvolte dei ruoli e delle responsabilità per la gestione dei rischi;
- attuazione della gestione del rischio, attraverso le attività di analisi e valutazione del rischio (risk assessment), di trattamento dei rischi - cioè di individuazione, attuazione delle misure organizzative e tecniche a mitigazione dei rischi, nonché di attribuzione di una priorità alle stesse (remediation e implementation);
- monitoraggio e riesame del modello (monitoring for continuous improving) volto a realizzare un miglioramento continuo del sistema di gestione dei rischi di data protection.

La protezione dei dati personali viene effettuata dall'Associazione nell'ottica del perseguimento dei seguenti obiettivi strategici:

- confidenzialità dei dati personali trattati;
- disponibilità dei dati personali trattati, anche a seguito di incidenti che potrebbero comportare la perdita di continuità operativa nel trattamento di tali dati e dei correlati obiettivi di resilienza;
- integrità dei dati personali trattati.

La mappatura dei trattamenti, unitamente all'analisi delle misure, nonché la valutazione dei rischi connessi a ciascun trattamento, sono documentate all'interno del Registro delle Attività di trattamento, che illustra anche la metodologia adottata.

2.6.3 LA REMEDIATION: PRINCIPI E MISURE ADOTTATE

A seguito dell'assessment condotto, l'Associazione ha ritenuto necessario implementare un insieme di **misure correttive e preventive** finalizzate ad assicurare la piena conformità alla normativa in materia di protezione dei dati personali. Le principali misure adottate sono:

- **Informative privacy e consensi**
  Redazione e aggiornamento delle informative privacy in conformità agli articoli 12-14 del GDPR. Predisposizione dei relativi moduli di acquisizione del consenso, ove richiesto.
- **Procedure privacy**
  Definizione e adozione di procedure operative specifiche in ambito privacy, tra cui gestione delle richieste degli interessati, data breach, conservazione dei dati e gestione dei consensi.
- **Nomine dei soggetti interni**
  Formale designazione dei soggetti interni come:
  - Incaricati del trattamento
  - Responsabili interni del trattamento
  - Amministratori di sistema
    Le nomine includono la definizione dell'ambito dei trattamenti consentiti, con attribuzione di profili di autorizzazione differenziati in base al tipo di attività svolta, al fine di garantire il principio di minimizzazione dell'accesso.
- **Amministratori di sistema**
  Aggiornamento e formalizzazione delle nomine degli amministratori di sistema, in linea con le indicazioni del Garante Privacy.

- **Modello Organizzativo Privacy (MOP)**
  Adozione del presente Modello Organizzativo Privacy, quale strumento di governance e accountability interna.
- **Misure di sicurezza**
  Adozione e/o rafforzamento delle misure di sicurezza tecniche e organizzative, inclusi processi formalizzati per la gestione della sicurezza informatica, accessi ai dati e protezione dei sistemi informativi.
- **Formazione del personale**
  Pianificazione e realizzazione di attività formative periodiche rivolte a dipendenti e collaboratori, con focus sugli obblighi e responsabilità derivanti dal GDPR.
- **Registro dei trattamenti**
  Istituzione e aggiornamento del Registro dei trattamenti, in conformità all'art. 30 del GDPR, come strumento di tracciabilità e trasparenza.
- **Mantenimento e controllo della conformità**
  Adozione di un processo di verifica periodica dell'effettiva conformità al GDPR e di aggiornamento continuo delle misure adottate, anche in base all'evoluzione normativa o organizzativa.

2.6.4 LA REMEDIATION: LE POLITICHE

Politiche per la protezione dei dati personali

L'Associazione ha ritenuto necessario impegnarsi ad assicurare che tutti i trattamenti di dati personali svolti avvengano nel rispetto dei requisiti cogenti applicabili, con particolare riferimento ai principi e alle regole da osservare.

L'Associazione, nell'ambito del presente Modello Organizzativo Privacy e delle procedure adottate e divulgate internamente all'Associazione, formalizza le linee guida in merito ai principi comportamentali e alle nuove regole, sensibilizzando attraverso adeguate attività di informazione e formazione tutto il personale, compresi coloro che collaborano con l'Associazione, in merito alla sistematica e puntuale osservanza degli stessi principi e regole.

In particolare, sono state adottate e/o sono in corso di adozione, ad esempio le seguenti procedure:

- Data Retention (incluso nell' Informativa Dati Personali GDPR che descrive quali dati sono trattati dall'Associazione, quali sono i tempi di trattamento necessario e quindi di conservazione;

- Data Breach, che descrive il processo di notifica all'Autorità e all'Interessato, ove ritenuto necessario, delle violazioni di dati personali;

2.6.5 LA REMEDIATION: LE INFORMATIVE, I CONSENSI

L'Associazione ha ritenuto necessario impegnarsi ad assicurare che tutti i soggetti di cui si trattano dati personali vengano adeguatamente informati.
Per questo, ASHTANGA YOGA GENOVA ha pianificato l'aggiornamento di tutte le informative agli interessati e dei relativi consensi, e sta pianificando attività di sensibilizzazione per i dipendenti e i collaboratori.

2.6.6 LA REMEDIATION: LE NOMINE E LE ISTRUZIONI

L'Associazione ha ritenuto necessario impegnarsi ad assicurare che tutti i soggetti che trattano dati personali vengano adeguatamente informati ed istruiti. Per questo ha nominato Responsabile interni ed eventuali Incaricati del trattamento.

1.6.10 LA REMEDIATION: LA FORMAZIONE – LA CONSAPEVOLEZZA

L'Associazione ha ritenuto necessario impegnarsi ad assicurare che tutti i soggetti che trattano dati personali vengano adeguatamente formati.
Per questo, L'Associazione sta pianificando una formazione adeguata sia agli Incaricati del trattamento che ai Responsabili interni del trattamento, relativamente ai contenuti del GDPR e alle procedure adottate dall'Associazione.

2.6.7 LA REMEDIATION: IL REGISTRO DEI TRATTAMENTI

A seguito delle attività di assessment condotte, è emerso che l'Associazione tratta dati classificabili come dati personali ai sensi del GDPR. L'Associazione ha ritenuto necessario predisporre l'elenco descrittivo di detti trattamenti contenuto nel Registro dei trattamenti.
Il Registro dei trattamenti comprende le attività di trattamento svolte sotto la responsabilità del Titolare del trattamento.

2.6.8 LA REMEDIATION: I DIRITTI DEGLI INTERESSATI

L'Associazione ha ritenuto necessario impegnarsi ad assicurare che gli interessati possano adeguatamente esercitare i propri diritti e che gli Incaricati ne siano a conoscenza. A tal riguardo, sono state predisposte informative adeguate.

2.6.9 LA REMEDIATION: IL SISTEMA DI CONTROLLO INTERNO DELL'ASSOCIAZIONE

L'Associazione riconosce l'importanza di garantire un costante impegno nell'adozione di strumenti adeguati di **controllo**, **monitoraggio**, **audit** e **riesame** in materia di protezione dei dati personali.
A tal fine, ha definito e adottato il presente **Modello Organizzativo Privacy (MOP)**, che integra il sistema di controllo interno già in essere, con l'obiettivo di valutare **l'idoneità, l'efficacia e l'effettiva attuazione dei controlli specifici** posti a presidio dei rischi di non conformità (compliance) identificati.
Il sistema di controllo interno dell'Associazione si fonda, oltre che sulle regole comportamentali previste nel MOP, sui seguenti elementi già adottati o in corso di adozione:

- **Modello di Organizzazione, Gestione e Controllo** adottato ai sensi del D.lgs. 231/2001, nonché sul **Codice di comportamento** e di **condotta scientifica**;
- **Codice Etico**, quale riferimento per i valori e i principi condivisi dall'Associazione;
- **Sistema di procedure interne**, volte a regolamentare i processi e garantire la coerenza operativa;
- **Struttura organizzativa e gerarchico-funzionale**, comprensiva dell'organigramma, dei soggetti coinvolti nella protezione dei dati personali (interni ed esterni, Responsabili e Incaricati del trattamento);
- **Sistema di deleghe e procure**, volto ad assicurare una chiara attribuzione delle responsabilità e dei poteri decisionali;
- **Sistemi informativi**, progettati secondo i principi di segregazione delle funzioni e di protezione delle informazioni trattate;
- **Tracciabilità delle operazioni**, in base alla quale ogni attività deve, ove possibile, essere adeguatamente documentata e i processi decisionali, autorizzativi ed esecutivi devono risultare verificabili anche a posteriori, attraverso idonea documentazione;
- **Verifiche periodiche** sull'effettiva applicazione e sull'efficacia dei controlli, condotte dal **Consiglio di Sorveglianza**.

Questo approccio strutturato consente all'Associazione di mantenere un elevato livello di conformità al Regolamento (UE) 2016/679 (GDPR) e di rafforzare il proprio impegno verso la tutela dei diritti e delle libertà fondamentali delle persone fisiche in materia di protezione dei dati personali.

3 ORGANI E FUNZIONI COINVOLTI NELLA DATA PROTECTION

3.1 ORGANIGRAMMA PRIVACY

Ashtanga Yoga Genova asd ha strutturato il proprio organigramma privacy come segue:

Titolare: l'Associazione
Responsabile: DPO nominato dal Consiglio Direttivo

3.2 DESIGNAZIONE DEL DATA PROTECTION OFFICER

Nell'ambito del programma di adeguamento al GDPR il Consiglio Direttivo dell'Associazione, procederà alla designazione della figura del Data Protection Officer (DPO) ai sensi dell'art. 37 del GDPR.

3.3 LE FUNZIONI DI GOVERNANCE DEL MODELLO ORGANIZZATIVO PRIVACY

All'interno dell'Associazione, la gestione degli aspetti connessi alla protezione dei dati personali è affidata principalmente al **Consiglio Direttivo**, il quale esercita un ruolo di indirizzo, coordinamento e supervisione. In particolare, il Consiglio svolge le seguenti attività:

- **Informazione e consulenza**: fornisce supporto informativo e consulenziale al Titolare o al Responsabile del trattamento, nonché ai dipendenti coinvolti nelle attività di trattamento, in merito agli obblighi previsti dal GDPR e dalle normative nazionali e sovranazionali in materia di protezione dei dati;
- **Vigilanza sulla conformità**: monitora l'osservanza delle disposizioni normative da parte del Titolare o del Responsabile del trattamento, assicurando un'efficace attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale autorizzato, nonché il rispetto delle procedure interne;
- **Relazioni con il Garante**: cura la gestione delle comunicazioni e delle eventuali segnalazioni all'Autorità Garante per la protezione dei dati personali;
- **Registro dei trattamenti**: assiste il Titolare nella predisposizione, gestione e aggiornamento del Registro delle attività di trattamento, conformemente alle indicazioni ricevute. Monitora l'efficacia delle procedure adottate e del Modello Organizzativo Privacy, proponendone l'aggiornamento periodico, se necessario;
- **Aggiornamento del framework documentale**: si occupa del costante aggiornamento e della revisione della documentazione privacy (es. informative, nomine a Responsabili esterni, autorizzazioni al trattamento, nomine degli Amministratori di Sistema);
- **Procedure interne**: provvede alla redazione, manutenzione e aggiornamento delle procedure organizzative per la gestione degli adempimenti privacy, quali ad esempio la procedura per la gestione dei data breach, la policy di conservazione dei dati (data retention), e le istruzioni operative per la gestione della documentazione;
- **Formazione**: pianifica e realizza attività formative periodiche in materia di protezione dei dati personali, rivolte al personale autorizzato al trattamento;
- **Sicurezza informatica**: supervisiona e, ove necessario, promuove l'implementazione di misure tecniche e organizzative adeguate a garantire la sicurezza dei sistemi informatici e la protezione dei dati trattati.

3.4 MONITORAGGIO, VALUTAZIONI E MIGLIORAMENTO CONTINUO

ASHTANGA YOGA GENOVA, in qualità di Titolare, ed i Referenti interni del trattamento devono monitorare in modo sistematico l'adeguatezza, l'efficacia e l'effettiva operatività del Modello Organizzativo Privacy in materia di protezione dei dati personali.

Con riguardo all'adeguatezza, all'efficacia e all'effettiva operatività, la valutazione del Modello Organizzativo Privacy (assessment) deve essere effettuata, a titolo esemplificativo e non esaustivo, a fronte di:

- modifiche o evoluzioni del contesto esterno di riferimento, incluse variazioni dei requisiti normativi in materia di protezione di dati personali;
- modifiche o evoluzioni contesto interno di riferimento, incluse evoluzioni che comportano nuovi o mutati trattamenti, finalità di trattamento, scenari di rischio, ecc.;
- modifiche ai sistemi informativi utilizzati per il trattamento dei dati personali;
- esiti degli audit interni che evidenziano non conformità dei trattamenti rispetto ai requisiti applicabili, inclusi i requisiti definiti dallo stesso Titolare del trattamento;
- riesame, su base annuale o comunque periodica; riesame su base occasionale in caso di:
    - gravi o ripetute non conformità, incluse violazioni dei requisiti normativi o dei requisiti definiti dallo stesso Titolare del trattamento;
    - incidenti in materia di protezione dei dati personali (cd. "Data breach"); o significative variazioni del contesto di riferimento esterno, incluse variazioni del quadro normativo;
    - significative variazioni del contesto di riferimento interno.

ASHTANGA YOGA GENOVA, inoltre,consapevole dell'importanza di adottare ed attuare efficacemente un Modello Organizzativo Privacy, idoneo a prevenire i rischi e i danni derivanti dall'attuazione di illeciti trattamenti degli stessi, promuove il riesame e l'adeguamento continuo del MOP in funzione delle opportunità di miglioramento rilevate in sede di valutazione dei rischi, di monitoraggio, di audit e di analisi di incidenti e non conformità.

3 . 5 AUTORI DEL MONITORAGGIO, VALUTAZIONI E MIGLIORAMENTO CONTINUO

Il monitoraggio è effettuato dal Consiglio Direttivo

3.6 SEGNALAZIONI

Al fine di promuovere l'osservanza del GDPR, ASHTANGA YOGA GENOVA invita a segnalare ogni informazione, azione, operazione e, più in generale, qualsiasi attività posta in violazione delle prescrizioni del GDPR stesso, nonché gli specifici incidenti in relazione ai dati personali.

ASHTANGA YOGA GENOVA vieta atteggiamenti discriminazione o penalizzazione nei confronti del segnalante.

4 OSSERVAZIONI, DISPOSIZIONI SANZIONATORIE, DIFFUSIONE DEL DOCUMENTO

4.1 OSSERVANZA E DISPOSIZIONI SANZIONATORIE

In caso di violazione delle disposizioni contenute nel presente Modello Organizzativo Privacy da parte di dipendenti o collaboratori dell'Associazione, quest'ultima applicherà sanzioni disciplinari proporzionate alla gravità delle infrazioni, garantendo coerenza, imparzialità e uniformità. Tali sanzioni saranno sempre conformi alle disposizioni di legge e alle previsioni del Contratto Collettivo Nazionale applicabile.
L'osservanza delle norme previste dal Modello Organizzativo Privacy costituisce parte integrante e fondamentale delle obbligazioni contrattuali dei dipendenti dell'Associazione, ai sensi e per gli effetti degli articoli 2104 e seguenti del Codice civile.
La violazione delle disposizioni del Modello potrà configurare inadempimento contrattuale e/o illecito disciplinare, secondo le procedure stabilite dall'articolo 7 dello Statuto dei Lavoratori, con tutte le conseguenze di legge, comprese quelle relative alla conservazione del rapporto di lavoro e all'eventuale risarcimento dei danni. Analogamente, il rispetto dei principi del Modello Organizzativo Privacy rappresenta un obbligo contrattuale essenziale anche per i collaboratori esterni.
In caso di violazione da parte di terzi, tali comportamenti potranno costituire inadempimento degli obblighi contrattuali assunti, con conseguenze legali che includono la facoltà dell'Associazione di risolvere il contratto e di richiedere il risarcimento dei danni.

4.2 DIFFUSIONE DEL MODELLO ORGANIZZATIVO

ASHTANGA YOGA GENOVA, consapevole dell'importanza che gli aspetti formativi e informativi assumono in una prospettiva di prevenzione, per assicurare che il trattamento dei dati personali avvenga nel rispetto dei requisiti normativi applicabili, definirà un programma di comunicazione e formazione volto a garantire la diffusione delle competenze e conoscenze necessarie per applicare in modo corretto e sistematico le disposizioni in materia di protezione dei dati personali, incluso il presente Modello Organizzativo Privacy.

L'attività di informazione e formazione deve coinvolgere tutti i dipendenti e i collaboratori, nonché tutte le risorse che in futuro saranno inserite nell'organizzazione ASHTANGA YOGA GENOVA. A tale proposito, le relative attività formative dovranno essere previste e concretamente effettuate mansioni, sia al momento dell'assunzione, sia in occasione di eventuali mutamenti di nonché a seguito di aggiornamenti e/o modifiche del Modello Organizzativo Privacy.

Con riguardo alla diffusione del Modello Organizzativo Privacy, l'Associazione si impegna a:

- inviare una comunicazione a tutto il personale, informandolo dell'adozione del presente Modello Organizzativo Privacy;
- pubblicare il Modello Organizzativo Privacy sul sito web e/o renderlo accessibile tramite altri canali ritenuti idonei;
- organizzare attività formative finalizzate a diffondere la conoscenza e accrescere la consapevolezza sull'importanza di perseguire i seguenti obiettivi:
    - garantire il trattamento dei dati personali nel rispetto dei principi e dei requisiti previsti dalla normativa vigente in materia di protezione dei dati personali;
    - gestire i dati personali in modo da minimizzare i rischi connessi, consapevoli delle conseguenze derivanti dalla mancata osservanza della normativa, delle procedure interne e dei controlli operativi stabiliti dall'Associazione.