Data Protection Impact Assessment by **“UNI OSTIA APS - Università di Promozione Culturale e Solidale”**

Author:PhD Davide Venditti
Date: 24/10/2025

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
APS associazione di promozione sociale

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

UNI OSTIA APS segreteriauniostia@uniostia.it

Codice Fiscale: 97877730586 -

UNI OSTIA, Università di Promozione Culturale e Solidale, è una associazione di volontariato iscritta nel Registro del Terzo Settore. L’Associazione ha come scopo primario la promozione sociale nella accezione più ampia del termine, perseguendo tale finalità, con particolare attenzione al X° Municipio di Roma, con la attivazione di definiti programmi didattici rivolti a tutti i cittadini dai 18 anni in poi, la realizzazione di attività culturali, turistiche, ricreative, nonché a tutela dell’ambiente ed in difesa della legalità.

Table of Contents

1. Panoramica

Descrizione dei trattamenti

In relazione all'attività di UNI OSTIA APS - Università di Promozione Culturale e Solidale, che è un'Associazione di

Promozione Sociale (APS) che promuove corsi a scopo culturale e sociale, la gestione dei trattamenti dei dati personali si basa sull'applicazione del Regolamento Generale sulla Protezione dei Dati (GDPR - Regolamento UE 2016/679), come indicato anche nell'informativa privacy dell'Associazione.
Il trattamento principale dei dati personali è legato alla **gestione del rapporto associativo** e alla fornitura dei servizi culturali e formativi promossi dall'Associazione

Gli standard principali applicabili al trattamento dei dati sono quelli imposti dalla normativa europea, senza che risultino immediatamente applicabili specifici codici di condotta o certificazioni di protezione dati per questa specifica APS.

Standard Rilevanti

- Regolamento (UE) 2016/679 (GDPR): È lo standard normativo fondamentale. L'Associazione è tenuta al rispetto di tutti i suoi principi e articoli, inclusi:
    - Principio di Liceità, Correttezza e Trasparenza (trattare i dati in modo lecito e informare gli interessati).
    - Principio di Limitazione delle Finalità (trattare i dati solo per gli scopi dichiarati).
    - Principio di Minimizzazione dei Dati (trattare solo i dati strettamente necessari).
    - Misure di Sicurezza (adottare adeguate misure tecniche e organizzative per proteggere i dati).
    - Diritti degli Interessati (garantire i diritti di accesso, rettifica, cancellazione, ecc.).
- D.Lgs. 196/2003 (Codice Privacy) e successive modifiche (adeguamento al GDPR): Rappresenta la normativa nazionale che integra e specifica il GDPR.
- Normativa sul Terzo Settore: Essendo una APS, l'Associazione deve conformarsi anche agli obblighi previsti dal Decreto Legislativo n. 117/2017 (Codice del Terzo Settore), che possono prevedere specifici obblighi statutari o di trasparenza, indirettamente collegati al trattamento dei dati dei soci.

Codici di Condotta e Certificazioni

- Codici di Condotta (Art. 40 GDPR): Non risultano codici di condotta specifici approvati per le Associazioni di Promozione Sociale a livello nazionale o settoriale che siano stati adottati dall'UNI OSTIA APS. Tali codici sono volontari e servono a dettagliare l'applicazione del GDPR in specifici settori.
- Certificazioni di Protezione Dati (Art. 42 GDPR): Non risultano certificazioni di protezione dati (es. ISO 27001 o certificazioni GDPR specifiche) applicabili o ottenute dall'Associazione. L'ottenimento di tali certificazioni è generalmente volontario e tipico di organizzazioni più grandi o che trattano dati particolarmente sensibili.

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

Breve sunto del trattamento

Aspetto	Descrizione
Nome	Gestione Soci e Attività Associative
Scopo	Mantenimento e adempimento del rapporto associativo (iscrizione, convocazioni, quota associativa, adempimenti legali e assicurativi).
Finalità	1. **Gestione del rapporto:** Corrispondenza e rintracciabilità dei soci, convocazione alle assemblee, gestione del pagamento della quota associativa. 2. **Adempimenti legali:** Assolvimento degli obblighi di legge e assicurativi. 3. **Comunicazione:** Invio newsletter, comunicazioni dell'Associazione, campagne interne di informazione e sensibilizzazione. 4. **Fornitura dei servizi:** Gestione della partecipazione ai corsi e alle iniziative culturali.
Dati trattati	Dati personali comuni (es. nome, data di nascita, indirizzo, telefono, e-mail).
Base giuridica	**Esecuzione di un contratto** (il rapporto associativo e l'erogazione dei servizi richiesti) e **adempimento di obblighi legali** (art. 6, par. 1, lett. b e c, GDPR). Il consenso può essere richiesto per finalità specifiche come l'invio di newsletter non strettamente legate al rapporto associativo.
Contesto d'uso	Ambito associativo (APS) e della promozione culturale/sociale, attraverso la segreteria (fisica e online) e sistemi informatici di gestione.
Modalità	I trattamenti vengono svolti e i dati conservati da incaricati autorizzati, in forma **cartacea** e **informatica**.
Comunicazione/ Diffusione	I dati **non sono comunicati a terzi né diffusi**, salvo che per gli adempimenti di legge e assicurativi.

Introduzione

Questo documento è una valutazione dell'impatto sulla protezione dei dati (DPIA) che valuta il trattamentoi per nome dell'Associazione Uniostia. La DPIA è un'analisi delle attività di trattamento previste relative alle valutazioni e copre i dettagli dell'attività di elaborazione stessa e una valutazione dei rischi associati alle attività di trattamento, comprese eventuali misure che devono essere adottate per mitigare tali rischi. Contiene anche la decisione sull'avvio di una consultazione preliminare con il DPO competente.

La presente DPIA viene eseguita in ottemperanza, ai sensi dell'articolo 35 del GDPR, laddove il trattamento rischia di comportare un rischio elevato per i diritti e le libertà delle persone fisiche, il responsabile del trattamento effettua una valutazione dell'impatto dell'elaborazione prevista.

Le valutazioni hanno valore per i soggetti, le organizzazioni e la società, cui è indirizzata. La presente DPIA valuta i rischi per la privacy personale del processo di valutazione e identifica le misure, le salvaguardie e i meccanismi esistenti per mitigare tali rischi e identifica ove ci sia necessità di trattare i dati personali il corretto bilanciamento tra i diritti alla privacy e quelli di raccolta ed elaborazione dei dati.

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

Contesto

Il trattamento dei dati personali da parte di **UNI OSTIA APS** è descritto in linea con gli obblighi del GDPR, sebbene i dettagli specifici su tempi di conservazione esatti e architettura IT interna non siano generalmente resi pubblici in un'informativa standard.
I dati trattati dall'Associazione sono principalmente dati personali comuni, raccolti al momento dell'iscrizione (online o

Categoria di Dati	Dati Specifici Rilevati	Durata dell'Archiviazione (Conservazione)	Destinatari	Persone con Accesso (Incaricati)
Dati Identificativi e di Contatto	Nome, Data di Nascita (necessari), Indirizzo, Telefono, Indirizzo E-mail.	**Durata del rapporto associativo**, più il periodo di tempo richiesto dagli obblighi di legge (es. 10 anni per finalità fiscali, contabili e amministrative) o per la tutela dei diritti dell'Associazione.	**Nessuna comunicazione a terzi**, salvo che per gli **obblighi di legge e assicurativi** (es. agenzie assicurative convenzionate, commercialista/ consulente fiscale).	**Incaricati autorizzati** al trattamento (es. membri del Consiglio Direttivo, personale di Segreteria, gestori del sito web per la parte tecnica).
Dati Associativi e Amministrativi	Quota associativa versata, data di iscrizione/rinnovo, storico della partecipazione ai corsi e alle assemblee.	Vedi "Durata del rapporto associativo" sopra.	Vedi sopra.	Vedi sopra.
Dati di Comunicazione	Corrispondenza e rintracciabilità dei soci, dati di iscrizione alle newsletter.	Fino alla revoca del consenso (per le newsletter) o per la durata del rapporto associativo. La corrispondenza è conservata in base alle necessità amministrative.	Vedi sopra.	Vedi sopra.

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

in segreteria) e durante lo svolgimento del rapporto associativo.
Elenco dei dati, archiviazione, destinatari e accessi
I trattamenti operati dall'organizzazione:

- Trattamento associati: dati identificativi di contatto, didattici, anagrafici necessari all'inclusione dell'associazione
- Trattamento docent: dati identificativi di contatto, didattici, anagrafici necessari all'inclusione dell'associazione

- Trattamento Corso x: dati identificativi di contatto, didattici, anagrafici necessari all'inclusione dell'associazione
- Trattamento Corso y: dati identificativi di contatto, didattici, anagrafici necessari all'inclusione dell'associazione

Il ciclo di vita del trattamento dei dati segue le fasi standard previste dal GDPR, dalla raccolta alla distruzione, in funzione degli scopi associativi

Descrizione dei processi effettuati

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

Fase	Descrizione del Processo
1. Raccolta (Collection)	**Modalità:** I dati sono raccolti principalmente attraverso la **modulistica di iscrizione** (cartacea o online tramite il sito web) al momento dell'associazione Vengono acquisiti anche attraverso contatti successivi (e-mail, telefono, WhatsApp) per richieste di informazioni o comunicazioni. **Luogo:** Segreteria fisica o piattaforma web/caselle di posta elettronica dedicate alle iscrizioni.
2. Registrazione e Organizzazione	I dati raccolti dal modulo vengono inseriti e strutturati. **Formato:** In forma **cartacea** (archivi fisici della segreteria) e in forma **informatica** (database o fogli di calcolo su supporti digitali). L'organizzazione include la catalogazione per finalità (es. lista soci, lista newsletter, registri contabili).
3. Utilizzo (Processing)	I dati sono utilizzati per le finalità stabilite: - **Gestione contrattuale:** Invio della tessera associativa, convocazione alle assemblee. - **Adempimenti:** Gestione contabile della quota sociale, adempimenti fiscali e assicurativi. - **Comunicazione:** Invio di newsletter e comunicazioni relative alle attività, ai corsi e alle iniziative culturali. - **Fornitura dei servizi:** Gestione della presenza e della partecipazione ai corsi.
4. Conservazione e Protezione (Storage)	I dati sono conservati in archivi protetti, sia fisici che informatici. Le misure di sicurezza (tecniche e organizzative) sono volte a prevenire l'accesso non autorizzato, la perdita o la distruzione. La conservazione avviene: - Su **supporti digitali** (es. server o cloud, gestiti internamente o da terzi Responsabili del Trattamento). - Su **archivi cartacei** (Segreteria).
5. Comunicazione (Eventuale)	I dati **non vengono diffusi**, ma possono essere **comunicati** a soggetti terzi solo se strettamente necessario per l'adempimento di un obbligo legale o per l'esecuzione di servizi richiesti (es. comunicazione al consulente fiscale, all'ente assicurativo).
6. Distruzione (Destruction)	Al termine del rapporto associativo e scaduti i termini di legge per la conservazione obbligatoria (es. 10 anni fiscali), i dati devono essere cancellati o resi anonimi in modo irreversibile. Ciò include la cancellazione dai sistemi informatici e la distruzione sicura dei documenti cartacei.

Le risorse di supporto (inclusi sistemi, applicazioni e protocolli) che ospitano e gestiscono i dati dell'Associazione rientrano tipicamente nell'infrastruttura IT di un'organizzazione di piccole-medie dimensioni che opera sia fisicamente che online.

Elenco delle risorse che ospitano i dati

Tipologia di Risorsa	Esempi di Sistemi e Applicazioni (Ipotizzati su base di prassi comune)
Infrastruttura Hardware/Sistema Operativo	- **Workstation e PC** della Segreteria (Windows o MacOS) per l'elaborazione quotidiana. - **Dispositivi mobili** (smartphone/tablet) utilizzati dagli incaricati per la comunicazione (es. WhatsApp Business/e-mail).
Applicazioni d'Ufficio e Amministrative	- **Pacchetti Office:** Software per la creazione e gestione di fogli di calcolo (es. Excel/Google Sheets) per le liste soci e registri contabili. - **Software di Contabilità/Fiscale:** Applicativi utilizzati per gli adempimenti fiscali e la gestione delle quote associative (spesso gestiti dal commercialista).
Gestione delle Comunicazioni	- **Servizio E-mail:** Caselle di posta elettronica (es. `info@uniostia.it`, `segreteriauniostia@uniostia.it`) per la corrispondenza e la raccolta delle iscrizioni. - **Piattaforme Newsletter:** Servizi di terze parti (se utilizzati) per l'invio massivo di comunicazioni.
Gestione Web e Archiviazione Digitale	- **Sito Web e Hosting:** Server e Database Management System (DBMS, es. MySQL/PostgreSQL) che ospitano il sito (`www.uniostia.it`) e la funzionalità di iscrizione online. - **Archiviazione Cloud:** Servizi di archiviazione (es. Google Drive, Dropbox, OneDrive) per la conservazione sicura di documenti digitali e backup.
Protocolli e Sicurezza (Configurazioni)	- **Protocolli Internet:** Protocolli di rete sicuri (es. HTTPS sul sito web) per la trasmissione crittografata dei dati. - **Configurazioni di Sicurezza:** Firewall, software antivirus sulle workstation, policy di accesso con password per l'accesso ai dati digitali.
Archivi Fisici	- **Armadi e Classificatori:** Locali o mobili chiusi a chiave presso la Segreteria per la conservazione dei moduli di iscrizione cartacei e della documentazione amministrativa originale.

Trattamento

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

Tavola di riferimento con le informazioni chiave:

Informazioni Chiave		
(a)	Titolare del trattamento	Augusto Rosati Presidente
(b)	Responsabile del trattamento	Santino Pudda Vice Presidente

		Maddalena Venditti Segretario Renata Nardi Tesoriere Lucia Carletti Consigliere Tiziana Marchetti Consigliere Pasqualina Morella Consigliere Sandro Favi Consigliere Annamaria Bafaro Consigliere Sandro Favi Consigliere Responsabili esterni nominati
(c)	Descrizione del Trattamento	Trattamento associati Trattamento docenti Trattamento corso X Trattamento corso Y UNIOSTIA UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE C.F. 97877730586
(d)	Scopo del Trattamento	Somministrazioni di corsi Certificazioni(?) Organizzazioni di eventi pubblici Comunicazioni commerciali
(e)	Contesto, ambito e background	Il progetto si inserisce nell'ambito della gestione delle risorse umane e delle attività didattiche interne. I dati trattati servono per pianificare corsi, assegnare incarichi, monitorare la preparazione dei docenti e dei volontari, e assicurare che le attività svolte rispecchino gli standard qualitativi dell'associazione. Il trattamento ha dunque una portata interna ed è limitato ai soggetti che partecipano attivamente alle attività associative.
	Soggetti e relative mansioni, coinvolti nel trattamento	Valutazioni e i trattamenti descritti riguardano le seguenti categorie di interessati: • **Soci Docenti** Partecipano all'organizzazione ed erogazione delle attività formative e culturali dell'associazione. I dati trattati riguardano la loro preparazione, la qualità dell'insegnamento e gli eventuali risultati delle valutazioni interne. • **Soci Volontari** Collaborano nelle attività logistiche, organizzative, di supporto ai corsi e agli eventi. I dati trattati riguardano le competenze, le attività svolte e gli esiti delle valutazioni interne utili alla gestione dell'organizzazione. Tutti i soggetti svolgono ruoli formalmente riconosciuti all'interno dell'associazione e partecipano alle attività nel rispetto dello statuto e dei regolamenti interni.

(f)	Tipologia di dati personali	L'associazione acquisisce e tratta principalmente le seguenti categorie di dati personali: **Dati identificativi** • Nome e cognome • Indirizzo e-mail • Numero di telefono (se fornito) **Eventuali ulteriori dati** • Dati tecnici relativi alla fruizione di piattaforme interne • Dati relativi alla presenza, partecipazione ai corsi e attività svolte Non vengono trattati dati appartenenti a categorie particolari (dati sensibili) salvo specifici e separati casi documentati e solo previo consenso o base giuridica adeguata.
(g)	Categorie speciali di dati	Assenti
(h)	Destinatari dei dati personali: chi sarà in grado di vedere e avere accesso ai risultati della DPIA	I seguenti ruoli avranno accesso ai risultati della valutazione: • Augusto Rosati Presidente • Santino Pudda Vice Presidente • Maddalena Venditti Segretario • Renata Nardi Tesoriere • Lucia Carletti Consigliere • Tiziana Marchetti Consigliere • Pasqualina Morella Consigliere • Annamaria Bafaro Consigliere • Sandro Favi Consigliere

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

Il trattamento dei dati personali da parte di UNI OSTIA APS, in qualità di Associazione di Promozione Sociale (APS), deve aderire ai principi cardine del GDPR per essere considerato legittimo.
Gli scopi del trattamento sono specifici, espliciti e legittimi

Sì, le finalità del trattamento dei dati da parte di UNI OSTIA APS sono considerate specifiche, esplicite e legittime ai sensi dell'Art. 5, par. 1, lett. b del GDPR.

Spiegazione delle finalità

- Specifiche ed Esplicite: Le finalità sono chiaramente definite nell'informativa privacy e nello Statuto dell'Associazione. Non sono generiche, ma mirano espressamente a:
  - Gestire l'adesione associativa (es. registrazione e rintracciabilità dei soci).
  - Garantire la partecipazione alla vita associativa (es. convocazione alle assemblee).
  - Erogare i servizi culturali e formativi (es. iscrizione ai corsi).
  - Assolvere agli obblighi amministrativi, fiscali e assicurativi legati all'attività di APS.
- Legittime: Le finalità sono lecite perché si basano su:
  - L'adempimento di obblighi legali (es. normative fiscali per le APS, obblighi assicurativi).
  - L'esecuzione di un contratto o di misure precontrattuali (il rapporto associativo stesso è un accordo vincolante tra socio e associazione).

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

Quali sono le basi legali che rendono il trattamento legittimo

Le principali basi giuridiche che rendono il trattamento dei dati legittimo, in conformità all'Art. 6 del GDPR, sono:

Base Giuridica	Art. 6, par. 1, lett.	Descrizione e Contesto di UNI OSTIA APS
Esecuzione di un Contratto	b)	Essenziale per la **gestione del rapporto associativo**, che è la base contrattuale tra il socio e l'APS. Copre l'iscrizione, la gestione della quota sociale, la fornitura dei corsi e le comunicazioni connesse.
Obbligo Legale	c)	Necessaria per adempiere agli **obblighi imposti dalla legge** all'APS, in particolare in ambito fiscale, contabile e assicurativo, come previsto dal Codice del Terzo Settore e da altre normative nazionali.
Consenso dell'Interessato	a)	Potrebbe essere la base legale per trattamenti non strettamente necessari al rapporto associativo, come l'**invio di newsletter o comunicazioni promozionali** non essenziali, qualora l'interessato abbia dato esplicito permesso.

I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario (minimizzazione dei dati)

Sì, i dati raccolti (nome, data di nascita, indirizzo, telefono, e-mail, quota associativa) sono generalmente considerati adeguati, rilevanti e limitati alle finalità del trattamento (Art. 5, par. 1, lett. c del GDPR).

Spiegazione della Necessità di ogni dato

Dato Raccolto	Perché è Necessario (Minimizzazione)
Nome e Data di Nascita	**Identificazione univoca** e verifica dei requisiti di età per l'iscrizione. Necessario per la tenuta del Libro Soci e per gli adempimenti assicurativi.
Indirizzo di Residenza	Obbligatorio per gli **adempimenti fiscali e amministrativi** delle APS e per l'invio di comunicazioni formali (es. convocazioni assembleari cartacee, ove previste).
Telefono ed E-mail	**Rintracciabilità e comunicazione** essenziale con il socio (es. variazioni di corso, urgenze, invio di newsletter e comunicazioni). Sono i principali canali di interazione.
Quota Associativa	Necessario per la **gestione contabile e fiscale** dell'Associazione, comprovando il pagamento e lo stato di socio attivo.

, mentre il conferimento degli altri dati è facoltativo, rispettando così il principio di minimizzazione.

Il trattamento dei dati personali da parte di UNI OSTIA APS, in qualità di Associazione di Promozione Sociale (APS), deve aderire ai principi cardine del GDPR per essere considerato legittimo.

Le finalità del trattamento dei dati da parte di UNI OSTIA APS sono considerate **specifiche, esplicite e legittime** ai sensi dell'Art. 5, par. 1, lett. b del GDPR.

Spiegazione delle finalità

- **Specifiche ed Esplicite:** Le finalità sono chiaramente definite nell'informativa privacy e nello Statuto dell'Associazione. Non sono generiche, ma mirano espressamente a:
  - Gestire l'**adesione associativa** (es. registrazione e rintracciabilità dei soci).
  - Garantire la **partecipazione alla vita associativa** (es. convocazione alle assemblee).
  - Erogare i **servizi culturali e formativi** (es. iscrizione ai corsi).
  - Assolvere agli **obblighi amministrativi, fiscali e assicurativi** legati all'attività di APS.
- **Legittime:** Le finalità sono lecite perché si basano su:
  - L'**adempimento di obblighi legali** (es. normative fiscali per le APS, obblighi assicurativi).
  - L'**esecuzione di un contratto** o di misure precontrattuali (il rapporto associativo stesso è un accordo vincolante tra socio e associazione).

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

Basi legali che rendono il trattamento legittimo

Le principali basi giuridiche che rendono il trattamento dei dati legittimo, in conformità all'Art. 6 del GDPR, sono:

Base Giuridica Art. 6, par. 1, lett.Descrizione e Contesto di UNI OSTIA APS

- **Esecuzione di un Contratto** b) Essenziale per la **gestione del rapporto associativo**, che è la base contrattuale tra il socio e l'APS. Copre l'iscrizione, la gestione della quota sociale, la fornitura dei corsi e le comunicazioni connesse.
- **Obbligo Legale** c) Necessaria per adempiere agli **obblighi imposti dalla legge** all'APS, in particolare in ambito fiscale, contabile e assicurativo, come previsto dal Codice del Terzo Settore e da altre normative nazionali.

- **Consenso dell'Interessato** a) Potrebbe essere la base legale per trattamenti non strettamente necessari al rapporto associativo, come l'**invio di newsletter o comunicazioni promozionali** non essenziali, qualora l'interessato abbia dato esplicito permesso.

I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario (minimizzazione dei dati)

Sì, i dati raccolti (nome, data di nascita, indirizzo, telefono, e-mail, quota associativa) sono generalmente considerati **adeguati, rilevanti e limitati** alle finalità del trattamento (Art. 5, par. 1, lett. c del GDPR).

Spiegazione della Necessità di ogni dato

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

Dato Raccolto	Perché è Necessario (Minimizzazione)
Nome e Data di Nascita	**Identificazione univoca** e verifica dei requisiti di età per l'iscrizione. Neces… la tenuta del Libro Soci e per gli adempimenti assicurativi.
Indirizzo di Residenza	Obbligatorio per gli **adempimenti fiscali e amministrativi** delle APS e per l'invi… comunicazioni formali (es. convocazioni assembleari cartacee, ove previste).
Telefono ed E-mail	**Rintracciabilità e comunicazione** essenziale con il socio (es. variazioni di cors… urgenze, invio di newsletter e comunicazioni). Sono i principali canali di interazio…
Quota Associativa	Necessario per la **gestione contabile e fiscale** dell'Associazione, comprovandc… pagamento e lo stato di socio attivo.

L'informativa conferma che l'indicazione di nome, data di nascita, indirizzo, telefono ed e-mail è **necessaria per la gestione del rapporto associativo e per l'adempimento degli obblighi di legge**, mentre il conferimento degli altri dati è facoltativo, rispettando così il principio di minimizzazione.

I dati sono accurati e mantenuti aggiornati

L'Associazione ha l'obbligo, ai sensi del GDPR (Art. 5, par. 1, lett. d), di garantire che i dati siano accurati e, se necessario, aggiornati, adottando misure ragionevoli per cancellare o rettificare i dati inesatti.

1. **Verifica in fase di Iscrizione:** Il processo di iscrizione (online o in segreteria) richiede al socio di inserire i dati in modo accurato. La segreteria può effettuare un controllo visivo o formale sui dati forniti.
2. **Richiesta di Aggiornamento Annuale (Iscrizione/Rinnovo):** Ad ogni rinnovo annuale (Anno Accademico), al socio viene implicitamente o esplicitamente richiesto di confermare o aggiornare i propri dati di contatto e residenza.
3. **Gestione su Segnalazione del Socio:** Il socio ha il diritto di **rettifica** (Art. 16 GDPR). L'Associazione deve disporre di un canale (es. e-mail della segreteria) per ricevere e processare tempestivamente le richieste di modifica o correzione dei dati da parte degli interessati.
4. **Pulizia Periodica dei Dati (Data Cleansing):** Vengono probabilmente intraprese attività interne, ad esempio prima dell'invio massivo di comunicazioni, per verificare la validità degli indirizzi e-mail e dei recapiti telefonici (es. eliminando indirizzi e-mail che generano "hard bounces").

Qual è la durata della conservazione dei dati

La durata della conservazione dei dati deve essere **limitata** a quanto è necessario per il conseguimento delle finalità per cui sono trattati (Art. 5, par. 1, lett. e del GDPR), e tale limitazione è giustificata da requisiti legali e necessità di trattamento.

La durata tipica di conservazione per un'APS si articola in due periodi principali:

1. **Durante il Rapporto Associativo:** I dati sono conservati per tutta la durata in cui il soggetto è socio attivo, in quanto essenziali per l'esecuzione del contratto associativo e la fruizione dei servizi.
2. **Post-Rapporto Associativo (Conservazione Giustificata):** Una volta che il socio recede o non rinnova l'iscrizione, i dati non vengono immediatamente distrutti, ma sono conservati per un periodo specifico per:
    - **Requisiti Legali e Fiscali:** I dati relativi alle transazioni economiche (pagamento della quota) e alla documentazione contabile/fiscale devono essere conservati per un periodo di **10 anni** (come previsto dal Codice Civile e dalle norme tributarie italiane) dalla data dell'ultima registrazione.
    - **Tutela Legale:** I dati possono essere conservati per il periodo necessario a far valere o difendere un diritto in sede giudiziaria (prescrizione ordinaria di 10 anni).
    - **Storicità Associativa:** I dati minimi (es. nome e periodo di associazione) potrebbero essere conservati a fini storici e statistici, purché resi anonimi o pseudonimizzati ove possibile.

In sintesi, i dati vengono conservati per il tempo necessario alla gestione del rapporto associativo, **più un periodo aggiuntivo (tipicamente 10 anni)** per assolvere agli obblighi di legge e per finalità di difesa in giudizio.

MISURE, REGOLE, PROCEDURE, NORME E NORME PER GARANTIRE I LIVELLI DI SICU ZZA RICHIESTI IN QUESTO DOCUMENTO

IDENTIFICAZIONE E AUTENTICAZIONE

Misure e standard per l'identificazione e l'autenticazione del personale autorizzato

L'Associazione Culturale **UNIOSTIA APS** adotta misure tecniche e organizzative idonee a garantire che solo il personale espressamente autorizzato (ai sensi dell'art. 29 GDPR) possa accedere ai dati personali trattati nell'ambito delle attività associative. Le procedure di identificazione e autenticazione sono progettate per assicurare la tracciabilità delle operazioni e la protezione contro accessi non autorizzati.

1. Identificazione Unica degli Utenti

• Ogni utente autorizzato dispone di **credenziali univoche e personali**, non condivise con altri membri dell'associazione.
• È tassativamente vietata la condivisione delle credenziali o l'utilizzo di account generici o condivisi.
• L'accesso ai sistemi è consentito solo previa verifica dell'autorizzazione formale registrata nel "Registro del Personale Autorizzato al Trattamento".

2. Modalità di Autenticazione

L'autenticazione avviene principalmente tramite:

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

A. Password personale

Le password sono definite secondo criteri di sicurezza che assicurano:
• lunghezza minima di **8 caratteri**,
• presenza di lettere maiuscole, minuscole, numeri e preferibilmente caratteri speciali,
• assenza di riferimenti personali facilmente intuibili (nomi, date di nascita, ecc.).

B. Sistemi aggiuntivi (se presenti)

Qualora l'associazione utilizzi piattaforme esterne (ad es. Google Workspace, piattaforme e-learning, gestionali), vengono rispettate anche le loro policy di sicurezza.

3. Procedura di Allocazione e Distribuzione delle Password

Passaggio 1 – Creazione password

• La password iniziale è generata dall'**Amministratore di Sistema**, secondo i criteri definiti.

Passaggio 2 – Consegna password

– comunicazione separata e protetta (es. telefono + e-mail distinta).

• L'utente è informato dell'obbligo di modificarla al primo accesso.

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

Passaggio 3 – Modifica al primo accesso

• L'utente deve sostituire la password iniziale con una nota solo a lui/lei.

4. Regole di Archiviazione e Protezione delle Password

• Le password **non sono conservate in chiaro** in nessun archivio dell'associazione.
• L'Amministratore di Sistema non conserva copie delle password personali dopo la loro consegna.
• Eventuali documenti con password iniziali vengono distrutti dopo la prima modifica.
• Non è ammesso annotare le password su fogli, post-it o supporti non sicuri.

5. Periodicità della Modifica delle Password

• Le password devono essere modificate **almeno una volta ogni 12 mesi**, come previsto dalle buone pratiche GDPR.
• La modifica può essere richiesta anche con maggiore frequenza nei seguenti casi:
– sospetta violazione di sicurezza;
– smarrimento o compromissione della password;
– cambio di ruolo o incarico che comporta nuovi livelli di accesso.

6. Revoca delle Credenziali

In caso di cessazione dell'incarico o revoca dell'autorizzazione:
• l'**Amministratore di Sistema** disattiva immediatamente l'account;
• l'operazione è registrata nel "Registro Revoche Autorizzazioni";
• eventuali dispositivi o accessi remoti vengono bloccati entro 24 ore.

7. Monitoraggio e Tracciamento degli Accessi

• I sistemi utilizzati, quando tecnicamente possibile, registrano i tentativi di accesso e le operazioni rilevanti (log).
• I log sono consultabili solo dall'Amministratore di Sistema e dal Referente Privacy.
• Eventuali anomalie vengono segnalate al Presidente per valutazione di eventuali incidenti di sicurezza.

CONTROLLO ACCESSI

Il personale può accedere solo ai dati e alle risorse necessari allo svolgimento delle proprie funzioni. L'Associazione applica meccanismi per impedire qualsiasi accesso non autorizzato.

1. Meccanismi di controllo degli accessi

• Ogni utente dispone di credenziali uniche e personali.
• I sistemi prevedono livelli di accesso differenziati (lettura, modifica, amministrazione)..
• Le password rispettano criteri di sicurezza e sono rinnovate almeno annualmente.
• Sono registrati i log degli accessi (quando tecnicamente possibile).

2. Responsabile degli accessi

Solo AUGUSTO ROSATI è autorizzato a concedere, modificare o revocare l'accesso a dati e risorse, secondo i criteri definiti dal Responsabile del file.

3. Procedura sintetica per autorizzazione, modifica e revoca

A. Nuova autorizzazione

1. L'interessato presenta richiesta (modulo o e-mail).
2. Il Responsabile del file verifica la necessità.
3. **AUGUSTO ROSATI** approva.
4. L'Amministratore IT configura tecnicamente l'accesso.
5. Il Responsabile del file aggiorna l'Allegato I.

B. Modifica

Stessa procedura: richiesta → verifica → approvazione di Augusto Rosati → aggiornamento tecnico → aggiornamento registro.

C. Revoca

Segnalazione → approvazione di Augusto Rosati → disattivazione immediata → aggiornamento Allegato I.
Revoca entro **24 ore** dalla richiesta.

4. Controlli sui sistemi informativi

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

- Accessi basati sui privilegi minimi necessari.
- Blocco accesso dopo tentativi falliti ripetuti.
- Nessun account condiviso.
- Monitoraggio periodico dei profili autorizzati.

5. Aggiornamento Allegato I

- Il Responsabile del file aggiorna l'elenco degli utenti autorizzati (Allegato I) dopo ogni cambiamento.
- Revisione generale almeno **una volta l'anno**.

GESTIONE DEI SUPPORTI E DOCUMENTI CARTACEI

I supporti e i media contenenti dati personali sono identificati, inventariati e conservati in un **luogo ad accesso limitato** presso accessibile solo al personale autorizzato.

---

1. Luogo di conservazione e personale autorizzato

Luogo di conservazione:

- Archivio riservato situato in **Segreteria associazione Via mar dei Caraibi**, dotato di chiusura fisica e accesso controllato.

Personale autorizzato:

- Responsabile del file
- Augusto Rosati
- Soci collaboratori espressamente autorizzati

Procedura per abilitare o revocare accesso:

- Autorizzazione concessa o revocata esclusivamente da **Augusto Rosati**, con registrazione nell'Allegato II.
- Accesso revocato immediatamente alla cessazione dell'incarico.

Accesso in casi d'urgenza:

- Il personale non autorizzato può accedere solo in caso di emergenza (incendio, allagamento, rischio per la sicurezza) e sempre sotto supervisione della persona responsabile del file.

2. Identificazione ed etichettatura dei supporti

Sistema di etichettatura (non riconoscibile a terzi):

- Indicazioni generiche come "Documentazione riservata" senza riferimenti personali
- Registro corrispondente conservato separatamente e accessibile solo agli autorizzati

3. Inventario e standard di conservazione

Standard di conservazione:

- Supporti cartacei: archiviati in raccoglitori sigillati o buste chiuse, conservati nell'archivio.
- Supporti digitali (USB, HDD, backup): conservati in contenitori protetti e non accessibili al pubblico.

Procedura di inventario:

- Ogni supporto è annotato in un inventario custodito dal Responsabile del file (Allegato III).
- L'inventario può essere digitale o cartaceo; se digitale, è protetto da password e accessibile solo ai soggetti autorizzati.

4. Uscita o trasferimento dei media dal locale protetto

L'uscita di documenti o supporti contenenti dati personali dai locali è consentita solo quando necessario.

Autorizzazione:

- Deve essere concessa dalla persona responsabile del file o da **Augusto Rosati**.

• L'autorizzazione è registrata in Allegato III.

Dispositivi mobili:

• Laptop, tablet o chiavette USB contenenti dati personali possono uscire dai locali solo se cifrati e protetti da password.

5. Distruzione o cancellazione dei supporti

Prima dello smaltimento, i supporti devono essere resi irrecuperabili.

Procedure di distruzione:

• Cartaceo: triturazione con distruggidocumenti a norma (taglio incrociato).
• Supporti digitali: formattazione sicura, sovrascrittura multipla o distruzione fisica del supporto.
• Registrazione dell'avvenuta distruzione nell'inventario.

6. Trasferimento della documentazione

Durante il trasferimento interno o esterno di media contenenti dati personali l'associazione adotta le seguenti misure:

• Trasporto in buste chiuse o contenitori sigillati.
• Registrazione dell'uscita e del rientro del supporto.
• Divieto di lasciare incustoditi documenti o dispositivi in luoghi pubblici.
• Per invii elettronici, uso di allegati protetti da password o sistemi cifrati.

2. Descrizione delle operazioni delle operazioni di trattamento previste

Trattamenti previsti

Questa sezione del DPIA fornisce una descrizione sistematica delle operazioni di elaborazione previste per il trattamento.

Segue una descrizione funzionale del processo. Le operazioni di elaborazione previste possono essere suddivise in sei fasi, come illustrato di seguito:

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

1. **Planning assessment/ Pianificazione della Valutazione**

Prima di creare domande o una valutazione, un processo di progettazione definisce gli obiettivi della valutazione. Parte di questo processo definisce gli argomenti all'interno griglia in cui vengono poste le domande. Un processo di redazione viene quindi così definito, con i ruoli assegnati ai ruoli di Staff per consentire loro di [illegible] vedere [illegible] valutazioni.

2. **Authoring questions/ Implementazione dei dati**
I consulenti sono responsabili della scrittura di domande (chiamate anche voci) che sono inserite e memorizzate nella DPIA. A seconda degli scopi della valutazione, le domande vengono esaminate all'interno dello staff e le interviste contengono la cronologia delle domande, inclusi i dettagli di revisione e le modifiche apportate.

3. **Construct and finalize assessment/costruzione e redazione della DPIA**
Ogni Consulente quindi costruisce una valutazione utilizzando le domande create nel passaggio precedente e garantendo che la valutazione soddisfi le esigenze normative. In molti casi, c'è anche una fase pilota e di revisione da parte nostra per garantire questo. Parte del processo consiste nell'impostare una revisione per le vulnerabilità o tagliare il punteggio. La valutazione viene quindi pubblicata.

4. **Deliver to participants/revisione di gruppo**

5. **Reports available/ redazione di report gestionali**
Una volta che un Consulente termina una valutazione, nella DPIA si calcolano i punteggi utilizzando i criteri definiti. Abbiamo un processo di revisione per garantire che i punteggi siano calcolati correttamente e un processo di ricorso in caso di preoccupazione dei partecipanti.

6. **Results shared/Condivisione dei risultati**
Ultimata la valutazione, i risultati e i ruoli identificati nei dettagli chiave del progetto, possono essere rilasciati. I risultati possono essere resi disponibili sia in formato cartaceo o esportando report inclusi in formato PDF. Tali rapporti contengono in genere dati personali.

Risorse coinvolte nel processo di trattamento dei dati

Questa sezione della DPIA contiene un elenco delle risorse attraverso le quali avviene l'elaborazione dei dati personali, sia interni che esterni alla Società/Ente.

1. **1. Internal IT (Sistemi Interni)**

I dati personali sono trattati tramite computer e sistemi informatici interni di UniOstia APS.
Misure: accesso con password, antivirus aggiornati, backup periodici, utilizzo della rete protetta e formazione base sulla sicurezza.

2. Strutture di UniOstia APS

I trattamenti avvengono anche nei locali dell'associazione (ufficio, archivi, spazi di iscrizione).
Misure: archivi cartacei custoditi in armadi chiusi, accesso limitato al personale autorizzato.

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

3. External IT (Servizi Esterni)

Alcuni dati sono gestiti tramite servizi cloud e hosting esterni (email, sito web, archiviazione).
Misure: utilizzo di fornitori conformi al GDPR, connessioni cifrate, accesso limitato ai soli autorizzati.

4. Not IT Assessment (Supporti Non Digitali)

Sono trattati anche documenti cartacei (modulistica, registri, certificazioni).
Misure: conservazione in archivi protetti, distruzione sicura dei documenti non necessari, controllo dei trasferimenti fisici.

FORMAZIONE E OBBLIGHI DEL PERSONALE

Garantire che tutti soci consiglieri conoscano:

- norme di sicurezza e protezione dei dati personali;
- regole operative interne;
- conseguenze della non conformità.

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

Aggiornamenti periodici

- **Frequenza:** almeno una volta all'anno o a seguito di modifiche normative/procedure.
- **Modalità:** comunicazioni interne.
- **Responsabile invio:** Referente Privacy, approvato dal Presidente.
- **Registrazione conferma:** obbligo per tutti i destinatari di confermare ricezione e lettura.

Conseguenze della non conformità

- Accesso revocato temporaneamente o permanentemente ai sistemi e archivi.
- Segnalazione al Presidente per eventuali sanzioni associative.
- Obbligo di partecipare nuovamente alla formazione.

Funzioni e obblighi del personale

Tutto il personale che accede ai dati personali di **UniOstia APS** è tenuto a:

- Conoscere e rispettare le misure, le regole, le procedure e gli standard di sicurezza previsti dall'associazione;
- Informare immediatamente i **Responsabili del file** o i **Responsabili della sicurezza**, secondo quanto previsto nelle procedure di notifica, gestione e risposta agli incidenti, di ogni incidente di sicurezza o violazione di dati personali di cui vengono a conoscenza;
- Mantenere la **massima riservatezza** sui dati personali trattati nello svolgimento delle proprie funzioni.

Funzioni e obblighi dei profili principali

Profilo	Obblighi principali	Persona/Posizione di riferimento	Deleghe in caso di assenza
Amministratore di sistema	Gestione account utenti, configurazione sistemi, manutenzione sicurezza IT	[AUGUSTO ROSATI, SANTINO PUDDA]	Deleghe temporanee a altro amministratore designato dal Presidente
Responsabile IT / Sistemi	Supervisione infrastruttura IT, gestione backup, aggiornamenti software	[AUGUSTO ROSATI, SANTINO PUDDA]	Deleghe temporanee ad altro membro qualificato
Responsabile del file	Autorizzazione accessi, gestione registro utenti, verifica conformità GDPR	Augusto Rosati	Deleghe temporanee approvate dal Presidente
		Augusto Rosati,	

Responsabile sicurezza fisica	Controllo accesso ai locali e archivi fisici, sorveglianza degli armadi riservati	Santino Pudda, Renata Nardi, Maddalena Venditti, Tiziana Marchetti, Pasqualina Morella, Annamaria Bafaro, Sandro Favi	Deleghe temporanee definite dal Presidente
Personale operativo / soci volontari	Trattamento dati limitato alle attività assegnate, rispetto procedure di sicurezza e riservatezza		UNIOSTIA UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE C.F. 97877730586

Personale non coinvolto nel trattamento dati

- Accede solo in misura necessaria a supportare attività che **non richiedono trattamento dei dati personali**;
- L'accesso a supporti fisici o sistemi è **strettamente limitato**.

Personale di terze parti

- I contratti di fornitura prevedono espressamente:
  • divieto di accesso ai dati personali;
  • obbligo di segretezza sulle informazioni eventualmente conosciute durante l'esecuzione del servizio.

Autorizzazioni delegate

- Le seguenti autorizzazioni possono essere delegate dal **Responsabile del file (Augusto Rosati)** a utenti o profili specifici:
  • gestione password di primo livello per soci volontari;
  • accesso limitato ai dati non sensibili dei partecipanti ai corsi;
  • gestione documentazione cartacea sotto supervisione.

Tutte le deleghe sono registrate nel **registro autorizzazioni interne** e sono revocabili in qualsiasi momento.

Conseguenze per violazioni

Il mancato rispetto, da parte del personale o dei collaboratori, delle misure, procedure e obblighi di sicurezza previsti in questo documento comporta l'applicazione delle seguenti misure sanzionatorie:

1. **Avvertenza formale** – per violazioni minori o involontarie, comunicata per iscritto dal **Presidente** o dal **Responsabile del file**.
2. **Richiamo scritto** – in caso di reiterazione o violazioni più gravi.
3. **Revoca temporanea o permanente delle autorizzazioni di accesso ai dati** – a seconda della gravità dell'infrazione, decisa dal **Responsabile del file (Augusto Rosati)**.

4. **Sospensione dalle attività associative** – nei casi di violazioni gravi o deliberate, fino a valutazione da parte del **Consiglio Direttivo**.
5. **Segnalazione alle autorità competenti** – se la violazione comporta rischi legali o illeciti ai sensi della normativa vigente (GDPR art. 83).

Riferimenti normativi interni:

- Statuto associativo di UniOstia APS, articoli relativi a obblighi e responsabilità dei soci e volontari;

Tutte le azioni sanzionatorie sono documentate e conservate nel registro interno delle violazioni.

Acquisizione dati personali

UNIOSTIA UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

Questa sezione descrive in dettaglio i tipi di informazioni personali acquisite dagli interessati.
Le seguenti informazioni generali possono essere acquisite dagli interessati:

-UniOstia APS acquisisce e tratta le seguenti informazioni personali dei soci, volontari, docenti e partecipanti alle attività associative:

1. Informazioni identificative e di contatto

- **Nome e cognome**
- **Indirizzo e-mail**
- Numero di telefono (se previsto per comunicazioni interne o emergenze)
- Gruppo, categoria o ufficio all'interno dell'associazione a cui l'interessato appartiene (es. volontario, socio docente, collaboratore)

2. Informazioni di accesso e log

- Data e ora di creazione dell'account o registrazione nel sistema
- Data e ora dell'ultimo accesso ai sistemi o piattaforme gestionali dell'associazione
- Tutti i dati sono trattati nel rispetto dei principi di **minimizzazione e pertinenza** ai fini delle attività associative.
- I dati di accesso e log sono utilizzati esclusivamente per finalità di sicurezza e gestione interna degli account.

I soggetti interessati come sono informati del trattamento?

Informativa scritta al momento della registrazione o iscrizione alle attività associative;
Comunicazioni via e-mail o messaggi interni, contenenti finalità del trattamento, base giuridica, destinatari dei dati e durata della conservazione;
Pagine informative sul sito web dell'associazione, accessibili a tutti i soggetti interessati.

Come si ottiene il consenso dei soggetti interessati?

Il consenso è richiesto in modo **esplicito e documentato**, ad esempio tramite:
• Moduli cartacei firmati,
• Moduli online con checkbox di accettazione,
•I controlli includono la registrazione della data e dell'oggetto del consenso nell'archivio interno dell'associazione, verificabile in caso di richiesta.

I soggetti interessati come esercitano i loro diritti di acceso alla portabilità dei dati?

Gli interessati possono richiedere l'accesso ai loro dati tramite e-mail o modulo interno.Il personale autorizzato fornisce:

•**Copia dei dati personali** in formato leggibile,

• Possibilità di ricevere i dati in un formato portabile (CSV, PDF, ecc.), pronto per il trasferimento a terzi se richiesto.

- Tutte le richieste sono registrate nel registro delle richieste degli interessati.

Come i soggetti interessati esercitano i loro diritti alla rettifica e alla cancellazione?

- Gli interessati possono richiedere la modifica o cancellazione dei loro dati tramite modulo o e-mail.
- Il personale incaricato verifica la richiesta, aggiorna o elimina i dati e conferma l'avvenuta operazione all'interessato.
- La procedura garantisce che non rimangano copie non autorizzate dei dati eliminati.

i soggetti interessati come esercitano il loro diritto di restrizione e obiezione?

- Gli interessati possono chiedere di limitare o obiettare il trattamento dei loro dati.
- Le richieste sono valutate dal **Responsabile del file (Augusto Rosati)** e attuate nei sistemi digitali e archivi fisici secondo quanto previsto dal GDPR.
- Gli interessati ricevono conferma scritta dell'esito della richiesta.

Gli obblighi dei responsabili del trattamento sono chiaramente identificati e governati da un contratto?

Ogni responsabile del trattamento esterno (es. hosting, cloud, servizi IT):

• ha **contratto scritto** che definisce responsabilità, durata, scopo e istruzioni documentate;

• è vincolato al rispetto del GDPR e delle procedure interne;

• deve fornire eventuali certificazioni, codici di condotta o attestazioni di conformità.

- I contratti sono conservati in archivio e verificabili in caso di audit.

Nel caso di trasferimento di dati fuori dall'Unione Europea, i dati sono adeguatamente protetti?

- I dati personali non vengono trasferiti al di fuori dell'UE, salvo che i fornitori esterni siano conformi a standard di sicurezza equivalenti.
- Per eventuali trasferimenti necessari, l'associazione adotta:
  - • contratti con clausole tipo GDPR (Standard Contractual Clauses),
  - • verifica della protezione dei dati nel Paese destinatario,
  - • cifratura dei dati trasferiti.

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

3. Necessità e proporzionalità del trattamento

Contesto generale che giustifica il trattamento e la valutazione d'Impatto

La Valutazione d'Impatto sulla Protezione dei Dati (Data Protection Impact Assessment - DPIA) è un processo previsto dall'Art. 35 del GDPR, obbligatorio quando un trattamento di dati personali "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche". Nel contesto dell'UniOstia APS non è necessario ma viene utilizzata per cristallizzare le modalità di trattamento definire gli elementi del registro ed avere una base essenziale per la tutela dei

diritti e delle libertà individuali degli interessati coinvolti

Interessi legittimi

UNIOSTIA APS fornisce valutazioni come descritto nelle informazioni chiave all'inizio di questo DPIA. È una parte necessaria del processo di valutazione che le informazioni vengono raccolte dai partecipanti in modo che siano in grado di dimostrare competenza ed è necessario che l'integrità del processo di valutazione per queste informazioni sia conservata come prova e giustificazione dei risultati della valutazione. Abbiamo un legittimo interesse a valutare come segue:

- UniOstia APS raccoglie informazioni dai partecipanti come parte integrante dei processi di valutazione descritti nel presente DPIA.
- La raccolta delle informazioni è necessaria affinché i partecipanti possano **dimostrare ampliamento delle consocenze**
- L'integrità del processo di valutazione deve essere preservata, garantendo che i dati raccolti siano **conservati come prova e giustificazione dei risultati**.
- UniOstia APS ha un **legittimo interesse** a valutare competenze e conoscenze, a garantire la qualità e l'affidabilità dei processi di valutazione.

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

UniOstia APS raccoglie informazioni dai partecipanti come parte integrante dei processi di valutazione descritti nel presente DPIA.

- La raccolta dei dati è necessaria affinché i partecipanti possano **dimostrare competenza e conoscenze acquisite e ampliamento della cultura sul territorio**.
- Le valutazioni permettono all'associazione di **misurare l'efficacia dei programmi di formazione**, identificare aree di miglioramento e garantire l'aggiornamento continuo dei corsi.
- L'integrità del processo di valutazione è preservata, garantendo che i dati raccolti siano **conservati come prova e giustificazione dei risultati**.
- Le valutazioni contribuiscono a **rafforzare la fiducia delle parti interessate.** n
- UniOstia APS ha un **legittimo interesse** a condurre valutazioni affidabili per assicurare qualità, trasparenza e conformità alle normative vigenti, supportando sia lo sviluppo professionale dei partecipanti sia la reputazione dell'associazione.

4. Rischi e Correttivi

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

Metodologia di valutazione del rischio

Questa sezione considera il rischio per le persone fisiche, in questo caso i partecipanti al processo di valutazione. Altri rischi che si applicano all'organizzazione, ma che non incidono sulla privacy, sono fuori portata. Ciò che è nel campo di applicazione sono i rischi che potrebbero comportare danni fisici, materiali o immateriali alla persona interessata, comprese eventuali discriminazioni, danni alla reputazione, perdita di riservatezza dei dati protetti dal segreto professionale o qualsiasi altro significativo svantaggio economico o sociale.

Nella nostra analisi, tutti i rischi sono anche associati a una probabilità:

-Probabile. Forte (alta) possibilità che lo scenario documentato possa verificarsi. Di tanto in tanto si verificano rischi elevati, ad esempio guasti alle apparecchiature in una situazione in cui non è prevista alcuna ridondanza.
- Possibile. Possibilità media (neutra) che lo scenario documentato possa verificarsi. Tra il basso e l'alto.
- Difficilmente. Lo scenario è improbabile - non dovrebbe accadere più spesso di una volta in un decennio o più raro.

I rischi sono anche associati a una gravità.

- Critico. Vi è un danno significativo e reale a un gran numero di soggetti dei dati, ad esempio una violazione dei dati su larga scala.
- Grave. Vi è un danno significativo e reale a uno o un numero limitato di soggetti dei dati o un danno minore a un gran numero di soggetti dei dati.
- Moderato. Problema minore o procedurale che non comporta danni significativi.

Minacce ai dati personali

Prima di analizzare i rischi in dettaglio, dobbiamo considerare le probabili minacce. Dal punto di vista dell'interessato, ecco le probabili minacce alla privacy:

1. **Divulgazione di dati personali.** Un interessato considererà le informazioni fornite dal fornitore di valutazioni come confidenziali e potrebbero essere in difficoltà o subire danni alla reputazione se fossero trapelate impropriamente. Ad esempio, un interessato non si aspetterebbe che le informazioni che lui / lei ha risposto a una domanda facile o importante in modo errato per essere divulgate pubblicamente, e sarebbe preoccupato per i risultati della valutazione condivisa in modo inappropriato.
2. **Integrità dei dati personali.** Una persona interessata sarebbe preoccupata se i dati di valutazione su di essi fossero imprecisi, ad esempio fossero danneggiati durante il trasporto o classificati in modo errato con dati su un'altra persona o modificati in modo errato.
3. **Perdita di dati personali.** Se un partecipante prende un esame e i risultati sono persi, allora lui o lei ha perso importanti prove di competenza. Una persona interessata sarebbe preoccupata che i risultati della valutazione siano archiviati in modo sicuro per tutto il tempo necessario.
4. **Qualcuno fallisce una valutazione ingiustamente**. Una seria preoccupazione per un interessato è che non dovrebbero fallire la valutazione se hanno la competenza per superarla. Ad esempio, se il sistema dovesse mescolare i risultati di una persona con un'altra, o avere un errore nel punteggio, o se la valutazione non è

corretta, valida e affidabile, allora l'interessato che dovrebbe passare potrebbe non essere riuscito. E questo potrebbe avere conseguenze per l'interessato.

Passare una valutazione quando qualcuno dovrebbe fallire è una preoccupazione meno seria per l'interessato, ma è una preoccupazione per la società, l'organizzazione e per altri soggetti interessati, poiché svaluta i risultati della valutazione per le altre persone. Ed è un interesse legittimo della nostra organizzazione che tali errate classificazioni non dovrebbero accadere.

5. **Mancanza di capacità di esercitare i diritti previsti dalla legge sulla protezione dei dati.** Una persona interessata ha molti diritti secondo la legge sulla protezione dei dati e potrebbe essere preoccupata per esempio di non essere in grado di ottenere copie dei propri dati personali o dati elaborati in modo inappropriato.

Le seguenti sezioni trattano i rischi relativi a queste minacce, considerando separatamente:

- Violazione di minacce di riservatezza o integrità (1 e 2 sopra)
- Minacce alla perdita o disponibilità di dati personali (3 sopra)
- Minacce di classificazione errata (4 sopra)
- Mancanza di diritti secondo la legge sulla protezione dei dati (5 sopra)

UNIOSTIA UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

Rischi connessi alla violazione della riservatezza o dell'integrità dei dati

La tabella seguente mostra i rischi rappresentativi relativi alla violazione della riservatezza o dell'integrità dei dati.

ID	Natura del rischio	Probabilità	Gravità	Correttivi e adeguamenti possibili
1	Accesso fisico ai dati in trattamento memorizzati nei server	Improbabile	critico	
2	La vulnerabilità del software, la mancata patch o il malware nel sistema consentono l'accesso di un utente malintenzionato e causano una violazione dei dati	Improbabile	critico	
3	La password dell'amministratore o degli incaricati per il sistema di trattamento viene indovinata o trovata o ottenuta tramite attacco di phishing per consentire l'accesso ai risultati o ad altri dati nel sistema o nei sistemi organizzativi	Improbabile	Grave	

Rischi connessi alla perdita di dati personali

La tabella seguente mostra i rischi rappresentativi relativi alla perdita di dati o alla cancellazione dei dati. Si noti che molti dei rischi sopra riferiti alla riservatezza potrebbero anche comportare la cancellazione dei dati.

Rischi connessi ad un trattamento non conforme alle finalità della raccolta

ID	Natura del rischio	Probabilità	Gravità	Correttivi e adeguamenti possibili
4	Indisponibilità delle risorse informatiche in assenza di backup o di sistemi di disaster recovery	Probabile	Moderato	
5	Infezione da Ransomware, perdita delle chiavi d'accesso, criptazione	Probabile	Moderato	

	irreversibile			
6	Sottrazione fisica delle risorse informatiche e/o cartacei, furto	Probabile	Critico	
7	Distruzione accidentale degli archivi per agenti catastrofici	Possibile	Critico	

Rischi connessi all'esercizio dei diritti in materia di dati nella legge sulla protezione dei dati

ID	Natura del rischio	Probabilità	Gravità	Correttivi e adeguamenti possibili
8	Gli interessati non possono avere accesso ai loro dati personali	Improbabile	Moderato	Risponderemo ai requisiti legali a qualsiasi interessato che richieda informazioni. Siamo in grado di fornire informazioni complete sui tentativi di valutazione e sui risultati utilizzando reports periodici.
9	Rischio che i dati vengano elaborati da un processore che non soddisfa i requisiti di protezione dei dati	Improbabile	Moderato	Il nostro contratto con gestore di cloud e altri sub-processori è conforme al GDPR o sarà il 25 maggio 2018.

Misure relative alla sicurezza, controlli esistenti o pianificati

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

			Si	*No*
	Crittografia			x
	Anonimizzazione	DB del CRM su drive, con chiavi	x	
	Partizionamento dei dati	I dati degli associati si trovano su drive del CRM	x	
	Controllo degli accessi	Gli accessi fisici sono controllati, gli accessi logici con Pass e Login Assegnate dal gestore CRM	x	
	Tracciabilità	Log registrati dal Drive del gestore CRM	x	
	Archiviazione	Archiviazione fisica, solo negli archivi chiusi presenti in sede, archiviazione logica su drive	x	
	Sicurezza dei documenti cartacei	Archivi armadio chiusi presenti nella sede	x	
	Minimizzare la quantità di dati personali	I dati sono minimizzati by default	x	
	Vulnerabilità	Assessment e valutazione delle vulnerabilità	x	
	Lotta contro il malware	Antimalware standard aggiornato	x	
	Gestione postazioni	Postazione unica	x	
	Sicurezza dei siti web	Sito vetrina		x
	Backup	Back up su drive, responsabilità di terzi	x	
	Manutenzione			x
	Contratti di trattamento			x
	Sicurezza della rete			x
	Controllo degli accessi fisici	Sede chiusa con politica di gestione chiavi d'accesso	x	
	Monitoraggio dell'attività della rete			x
	Sicurezza dell'hardware			x
	Evitare le fonti di rischio			x
	Protezione contro fonti di rischio non umane			x
	Organizzazione	Organigramma privacy	x	

	Politiche			**x**
	Gestione dei rischi sulla privacy	Politica dell'organizzazione	**x**	
	Integrare la protezione della privacy nei progetti			**x**
	Gestire le violazioni dei dati personali	Lettere d'incarico	**x**	
	Gestione del personale	Formazione	**x**	
	Relazioni con terze parti			**x**
	Supervisione			**x**
	Pseudonimizzazione			**x**

5. Informazioni di supporto

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586

Codici di condotta

L'articolo 35, paragrafo 8, del GDPR stabilisce che una DPIA può prendere in considerazione la conformità con i codici di condotta approvati. Poiché al momento non sono disponibili codici di condotta pertinenti, non abbiamo tenuto conto di tali codici di condotta, tuttavia abbiamo tenuto conto del fatto che il processore e il fornitore del sistema è certificato ISO 27001.

Richieste degli interessati

L'articolo 35, paragrafo 9, del GDPR stabilisce che, se del caso, il responsabile del trattamento deve chiedere il parere degli interessati o dei loro rappresentanti in merito al trattamento previsto.

- **Consultazione diretta:** Non è stata effettuata una consultazione diretta degli interessati o dei loro rappresentanti, in quanto:
  • I trattamenti riguardano dati personali strettamente pertinenti alle finalità associative
  • Le informazioni trattate sono **minime, necessarie e proporzionate**;
  • Sono state adottate **misure tecniche e organizzative adeguate** per garantire la sicurezza e la riservatezza dei dati.

- **Giustificazione per la mancata consultazione:**
  La consultazione non è stata ritenuta necessaria perché:
  • I soggetti interessati (soci, volontari) **sono già informati delle finalità e dei trattamenti** tramite informativa GDPR;
  • Le operazioni di trattamento sono a basso rischio per i diritti e le libertà degli interessati, e le misure di sicurezza adottate riducono al minimo qualsiasi rischio residuo.

- **Garanzie aggiuntive:**
  • I partecipanti possono esercitare i propri diritti di accesso, rettifica, cancellazione, limitazione, opposizione e portabilità;
  • Le procedure interne garantiscono che eventuali preoccupazioni o richieste degli interessati siano **gestite tempestivamente** dal Responsabile del file.

6. Conclusioni

Valutazione finale

Nelle parti precedenti di questo DPIA, abbiamo

- Descritto il progetto e fornito una panoramica funzionale
- Descritto i dati personali che sono stati catturati
- Identificato lo scopo del trattamento e gli interessi legittimi nel condurre tale elaborazione
- Identificati i rischi per la privacy delle persone interessate e le attenuazioni in atto per loro

Ora dobbiamo valutare se permane il rischio residuo elevato e se sia necessario consultare l'autorità di controllo.

Rischio residuale

Ai sensi del GDPR, è necessario consultare l'autorità di vigilanza prima dell'elaborazione in cui una DPIA indica che il trattamento comporterebbe un rischio elevato in assenza di misure adottate dal responsabile del trattamento per mitigare il rischio. In sostanza, se il rischio residuo dopo le attenuazioni adottate rimane elevato, l'autorità di vigilanza deve essere consultata.

Gli orientamenti del gruppo di lavoro articolo 29 sui DPIA forniscono esempi di rischio residuo elevato inaccettabile:

a) casi in cui le persone interessate possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (ad esempio un accesso illegittimo ai dati che porta a una minaccia sulla vita degli interessati, una cassa integrazione, un rischio finanziario)

b) quando sembra ovvio che si verificherà il rischio (ad es .: non essendo in grado di ridurre il numero di persone che accedono ai dati a causa delle modalità di condivisione, uso o distribuzione, o quando una vulnerabilità ben nota non è patchata).

Non ci sono rischi all'interno dei nostri processi di valutazione in cui sembra ovvio che il rischio si verificherà. La nostra organizzazione gestisce il suo programma di valutazione in modo professionale e attenua i rischi in larga misura. Il punto elenco (b) non sembra applicarsi a noi. Esistono due aree in cui è stato considerato possibile applicare il primo punto (a).

1. Violazione dei dati/ Data breach. C'è un piccolo rischio di violazione dei dati, nel caso, ad esempio, di un attacco di cibersicurezza di successo. Le conseguenze sugli interessati potrebbero essere significative e irreversibili a seconda dei dati coinvolti nella violazione, tuttavia esistono una serie considerevole di attenuazioni contro una violazione dei dati, in linea con e probabilmente in eccesso rispetto agli standard del settore, e nonostante le informazioni sulla valutazione i risultati sono altamente riservati, non sono così gravi come la divulgazione di altri tipi di informazioni, ad esempio informazioni finanziarie che potrebbero portare a un furto di identità. Non sembra che il rischio residuo in quest'area sia alto.

2. Mis-classificazione. Se una persona interessata ha fallito una valutazione ingiustamente, ad esempio perché le domande erano ambigue o, più in generale, la valutazione non era valida o affidabile, l'interessato potrebbe subire una conseguenza significativa. Tuttavia, questo rischio è mitigato da:

- misure sostanziali in atto comprese quelle sopra descritte per garantire l'affidabilità e la validità della valutazione;

- La possibilità per l'interessato di riprendere la valutazione;

- Una procedura di ricorso in cui l'interessato può chiedere la revisione del risultato della valutazione.

Luogo e data Roma 28.07.2026

Il titolare del trattamento

AUGUSTO
ROSATI
28.07.2026
18:25:10
GMT+02:00

UNIOSTIA
UNIVERSITÀ DI PROMOZIONE CULTURALE E SOLIDALE
C.F. 97877730586