



UNIVERSITA' PER LA TERZA ETA' APS di TEMPIO PAUSANIA)

Regolamento per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali ("GDPR") e del D.lgs. 196/2003 così come modificato dal d.lgs 101/2018 ("Codice Privacy")

Art. 1 – Oggetto

Art. 2 - Titolare del trattamento

Art. 3 - Finalità del trattamento

Art. 4 - Responsabile del trattamento

Art. 5 - Responsabile della protezione dati

Art. 6 - Sicurezza del trattamento

Art. 7 - Registro delle attività di trattamento e delle categorie di attività trattate

Art. 8 - Valutazione d'impatto sulla protezione dei dati

Art. 9 - Violazione dei dati personali

Art. 10 – Rinvio

Art. 1 Oggetto

1. L'**UNIVERSITA' PER LA TERZA ETA' DI TEMPIO PAUSANIA** "Associazione di promozione sociale APS si dota del presente regolamento ("**Regolamento**") che ha per oggetto misure procedurali e regole di dettaglio finalizzate alla migliore funzionalità ed efficacia dell'attuazione, del Regolamento europeo (Regolamento Generale Protezione Dati del 27 aprile 2016 n. 679 del Parlamento Europeo e del Consiglio, di seguito indicato con "G.D. P. R.", "General Data Protection Regulation"), relativo alla protezione delle persone fisiche con riguardo al trattamento ed alla libera circolazione dei dati personali, nonché nel rispetto del D.lgs 196/2003 così come modificato dal d.lgs 101/2018 ("**Codice Privacy**").
2. Si rimanda all'**allegato A)** per un'agevole sintesi ai principi e alle definizioni contenute nel Codice, nonché un richiamo alle modalità di trattamento di particolari categorie di dati personali.

Art. 2 Titolare del trattamento

1. L'Associazione, rappresentata ai fini previsti dal GDPR dal Presidente *pro tempore*, è il Titolare del trattamento (di seguito indicato con "Titolare") dei dati personali, raccolti o meno in archivi, automatizzati o cartacei, come definiti dall'art. 4, paragrafo 1, n. 6 GDPR. Il Presidente può assegnare le proprie funzioni organizzative in materia di *privacy*, autorizzandone il relativo trattamento, ai membri dell'Assemblea e del Consiglio Direttivo e al personale che intrattiene rapporti di collaborazione/dipendenza con l'Associazione, in possesso di adeguate competenze.
2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
3. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al GDPR (art. 24 GDPR). Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio. Gli interventi necessari per l'attuazione delle misure sono considerati previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
4. Il Titolare adotta misure appropriate per fornire all'interessato, ovverosia la persona fisica identificata o identificabile, le seguenti informazioni:
 - a le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;
 - b le informazioni indicate dall'art. 14 GDPR, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.
5. Nel caso in cui un tipo di trattamento, specie se prevede l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA", "*Data Protection Impact Assessment*"), ai sensi dell'art. 35 GDPR, considerando la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.
6. Il Titolare, inoltre, provvede a:
 - a Designare le persone autorizzate al trattamento dei dati con deleghe speciali, individuandoli nei soggetti che sono preposti al trattamento dei dati contenuti negli archivi esistenti nell'Associazione o nei siti web, social e in tutti i canali informativi digitali comunque gestiti dall'Associazione. Per il trattamento di dati, il Titolare può avvalersi anche di soggetti pubblici o privati;
 - b Nominare, quale Responsabile del trattamento, la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo affidatari di attività e servizi per conto dell'Associazione, relativamente alle banche dati gestite da soggetti esterni alla stessa, in virtù di convenzioni, di contratti, o di incarichi professionali, o di altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali.

- c Se lo ritiene necessario, nominare fra i componenti del consiglio direttivo un soggetto che garantisca l'omogeneità dell'applicazione delle norme in materia di privacy, sovrintendendo allo svolgimento delle funzioni dei designati/nominati e coordinandone l'attività in materia.

Art. 3 Finalità del trattamento

1. I trattamenti sono leciti ai sensi dell'art. 6 GDPR e sono compiuti dall'Associazione, per le seguenti finalità:
- L'esecuzione dei compiti di cui all'articolo 2 dello statuto Associativo per i quali l'interessato abbia espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità
 - L'esecuzione di un contratto con soggetti interessati.
 - il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento
 - Specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art. 4 Responsabile del trattamento (esterno all'Ente)

1. Il Titolare può avvalersi, per il trattamento di dati, anche particolari ai sensi dell'art. 9 GDPR, di persone fisiche o giuridiche, autorità pubbliche, servizi o altri organismi, che, in qualità di Responsabili del trattamento (art. 28 GDPR), forniscano garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche organizzative di cui all'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.
2. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, paragrafo 3, GDPR; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali, oppure dalla Commissione europea.
3. È consentita, ex art. 28, paragrafi 2 e 4 GDPR, la nomina di sub-responsabili da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali, ex art. 28, paragrafo 3 GDPR, che legano il Titolare ed il Responsabile primario, previa autorizzazione scritta, specifica o generale del Titolare stesso.
4. Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato adeguatamente sull'operato del sub-responsabile.
5. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza (art. 29 GDPR).
6. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:
 - alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare (art. 30, paragrafo 2, GDPR);

- all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti (art. 32 GDPR);
- all'istruzione e alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo (art. 29 GDPR);
- alla designazione del Responsabile per la Protezione dei Dati (DPO), qualora sia necessario ai sensi dell'art. 37 GDPR;
- ad assistere il Titolare nella "DPIA", fornendo allo stesso ogni informazione di cui è in possesso (artt. 35-36 GDPR);
- ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "*data breach*"), per la successiva notifica della violazione al Garante Privacy, nel caso in cui il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati (art. 33 GDPR).

Art. 5 Responsabile della protezione dati (DPO)

1. Tenuto conto delle finalità associative e dei dati personali necessari per il perseguimento delle stesse, non si applica l'articolo 37 GDPR e pertanto **non** si prevede la figura del Responsabile della protezione dei dati ("*DPO*" *Data Protection Officer*)

Art. 6 Sicurezza del trattamento

1. **L'UNIVERSITA' PER LA TERZA ETA' DI TEMPIO PAUSANIA "Associazione di promozione sociale APS** mette in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza commisurato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono ai sensi dell'art. 32 GDPR: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
3. Costituiscono misure tecniche ed organizzative che possono essere adottate:
 - sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
 - misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.
4. Restano salve le disposizioni di cui al Codice Privacy per quanto applicabili.

Art. 7 Registro delle attività di trattamento e delle categorie di attività trattate

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca, ai sensi dell'art. 30 GDPR, almeno le seguenti informazioni:
 - a) il nome ed i dati di contatto dell'Associazione, eventualmente del Contitolare del trattamento;
 - b) le finalità del trattamento;
 - c) le categorie di trattamenti effettuati: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;
 - d) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
 - e) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
 - f) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione
 - g) internazionale;
 - h) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
 - i) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.
2. Il Registro è tenuto dal Titolare, ovvero dal soggetto dallo stesso delegato ai sensi del precedente art. 2 del Regolamento in forma telematica/cartacea.

Art. 8 Valutazioni d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, specie se prevede l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo (DPIA) ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.
2. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, paragrafo 3, GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato sono, secondo le Linee Guida in materia dell'ex WP 29 (Gruppo di Lavoro ex articolo 29), i seguenti:
 - a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
 - b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

- c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
 - d) le categorie di dati personali particolari e giudiziari di cui agli artt. 9 e 10 GDPR, qualora siano trattate su larga scala, tenendo conto: del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
 - e) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
 - f) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti/collaboratori dell'Associazione, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
 - g) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
 - h) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.
3. Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati, occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.
4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno all'Associazione.
5. La DPIA non è necessaria nei casi seguenti:
- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, paragrafo 1, GDPR;
 - se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA; in questo caso, si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
 - se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
 - se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.
 - se taluni trattamenti siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o di un DPO e continuino ad essere condotti con le stesse modalità oggetto di tale verifica; a questo proposito, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.
6. La DPIA è condotta, prima di dar luogo al trattamento, attraverso i seguenti processi:
- a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento, dei dati personali oggetto del trattamento, dei destinatari e del periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; descrizione degli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei); b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:
 - delle finalità specifiche, esplicite e legittime;

- della liceità del trattamento;
 - dei dati adeguati, pertinenti e limitati a quanto necessario;
 - del periodo limitato di conservazione;
 - delle informazioni fornite agli interessati;
 - del diritto di accesso e portabilità dei dati;
 - del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
 - dei rapporti con i responsabili del trattamento;
 - delle garanzie per i trasferimenti internazionali di dati;
 - della consultazione preventiva del Garante privacy;
- b) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;
- c) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il GDPR e con il Codice Privacy, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
7. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.
8. Il Titolare, ai sensi dell'art. 36 GDPR, deve consultare il Garante Privacy prima di procedere al trattamento, se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari, tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Art. 9 Violazione dei dati personali

1. Per violazione dei dati personali (in seguito "*data breach*"), conformemente all'art. 33 GDPR, si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Comune.
2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire senza ingiustificato e, ove possibile, entro 72 ore dal momento dell'avvenuta conoscenza.
3. Il Responsabile esterno del trattamento e il designato interno al trattamento sono obbligati ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuti a conoscenza della violazione.
4. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del GDPR, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
 - perdita del controllo dei dati personali;
 - limitazione dei diritti, discriminazione;
 - furto o usurpazione d'identità;
 - perdite finanziarie, danno economico o sociale.
 - decifratura non autorizzata della pseudonomizzazione;
 - pregiudizio alla reputazione;
 - perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).
5. Se il Titolare ritiene elevato il rischio per i diritti e le libertà degli interessati derivato dalla violazione, deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro, al fine consentire loro la comprensione della natura della violazione dei dati personali verificatasi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo esemplificativo:
- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
 - riguardare categorie particolari di dati personali;
 - comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio, dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
 - comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio, rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).
6. La notifica deve avere il contenuto minimo previsto dall'art. 33 GDPR; la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33 GDPR, come richiamato dall'art. 34, paragrafo 2, GDPR.
7. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza, al fine di essere esibita al Garante Privacy, qualora la richieda per verificare il rispetto delle disposizioni del GDPR e del Codice Privacy.

Art. 10 Rinvio

1. Per tutto quanto non espressamente disciplinato con il presente Regolamento , si applicano le disposizioni del GDPR e tutte le sue norme attuative emanate ed emanande, nonché del Codice Privacy.