Pontificia
Università
della
SANTA
CROCE

# REGOLAMENTO PRIVACY

ROMA 2019

Pontificia
Università
della
SANTA
CROCE

# REGOLAMENTO PRIVACY

Roma

26 Novembre 2019

*Pontificia Università della Santa Croce*

*Il Rettore Magnifico*

RM 170/19

Il Rettore Magnifico, allo scopo di adeguare i processi organizzativi della Pontificia Università della Santa Croce alla necessaria protezione dei dati personali e di assicurare adeguate garanzie al loro trattamento, a salvaguardia *"dell'eminente dignità della persona umana, superiore a tutte le cose e i cui diritti e doveri sono universali e inviolabili"* (cfr. *Gaudium et Spes* art. 26),

Tenuto conto degli Statuti e di quanto previsto sul tema dal Codice di Comportamento, dalla disciplina canonistica e civile generale in materia e dai Regolamenti europei,

Sentito il suo Consiglio e accogliendo infine il parere espresso dagli avvocati della Pontificia Università della Santa Croce e dai suoi consulenti in materia di protezione dei dati personali,

**emana il**

**il Regolamento sulla Privacy**

**della Pontificia Università della Santa Croce**

Roma, 26 novembre 2019

Rev. Prof. Luis Navarro

# SOMMARIO

# 1.
# PREMESSA

La Pontificia Università della Santa Croce gode di personalità giuridica con carattere universale quale ente eretto dalla Santa Sede, beneficiando delle prerogative per gli Enti Centrali della Chiesa previste dal Trattato del Laterano del 1929 tra la Santa Sede e lo Stato Italiano.

Il presente Regolamento è emanato dal Rettore, sentito il suo Consiglio, in applicazione di quanto previsto sul tema "privacy" dal Codice di Comportamento e tenuto conto degli Statuti della Pontificia Università della Santa Croce, della disciplina canonistica e civile generale in materia e dei Regolamenti europei.

La Pontificia Università della Santa Croce adotta un Modello Organizzativo per la protezione dei dati personali per tutte le attività gestite dall'Ente, allo scopo di rispettare i principi previsti dalla costituzione Pastorale sulla Chiesa nel mondo contemporaneo *Gaudium et Spes*:

> «Pertanto ogni gruppo deve tener conto dei bisogni e delle legittime aspirazioni degli altri gruppi, anzi del bene comune dell'intera famiglia umana. Contemporaneamente cresce la coscienza dell'eminente dignità della persona umana, superiore a tutte le cose e i cui diritti e doveri sono universali e inviolabili. Occorre perciò che sia reso accessibile all'uomo tutto ciò di cui ha bisogno per condurre una vita veramente umana, come il vitto, il vestito, l'abitazione, il diritto a scegliersi liberamente lo stato di vita e a fondare una famiglia, il diritto all'educazione, al lavoro, alla reputazione, al rispetto, alla necessaria informazione, alla possibilità di agire secondo il retto dettato della sua coscienza, alla

> salvaguardia della vita privata e alla giusta libertà anche in campo religioso[1]».

Altresì la protezione dei dati personali è prevista dal Codice di Diritto Canonico[2] che salvaguarda il pieno rispetto della vita privata e dell'immagine pubblica.

Il Codice di Comportamento della Pontificia Università della Santa Croce prevede espressamente che «La Pontificia Università della Santa Croce tutela la riservatezza dei dati dei propri membri, a tal fine adottando adeguate misure di sicurezza[3]».

Nel corpus normativo dell'Università è vigente il Regolamento degli studenti, il quale, relativamente agli studenti, riconosce «il diritto a ricevere una informazione tempestiva, trasparente ed esaustiva riguardo alla propria situazione di studente e al percorso formativo intrapreso».

In tal senso la finalità che si propone il modello organizzativo della Pontificia Università della Santa Croce (d'ora in avanti anche Santa Croce) attraverso il presente Regolamento è quella di assicurare adeguate garanzie al trattamento dei dati personali disciplinando le modalità organizzative e di salvaguardia della protezione dei dati personali. Nella definizione del Modello si è altresì tenuto conto dell'impostazione generale di tutti i sistemi di gestione contenuta nella Norma Uni En Iso 9001:2015 nonché delle raccomandazioni dell'Agenzia della Santa Sede per la Valutazione e la Promozione della Qualità delle Università e Facoltà Ecclesiastiche (AVEPRO)[4].

---

1 Costituzione apostolica *Gaudium et Spes*, n. 26.

2 CDC, 220: «Non è lecito ad alcuno ledere illegittimamente la buona fama di cui uno gode, o violare il diritto di ogni persona a difendere la propria intimità».

3 Cfr Codice di comportamento della Pontificia Università della Santa Croce, *IX. Riservatezza e protezione delle informazioni*, 31.

4 www.avepro.va (AVEPRO guidelines)

# 2.
# DEFINIZIONI

Il presente Regolamento utilizza le seguenti definizioni per la protezione dei dati personali, con particolare riferimento ai concetti qui riportati:

1. "Trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, la strutturazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
2. "Dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
3. "Categorie particolari di dati": i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filo-

sofiche, l'appartenenza sindacale, i dati genetici, dati biometrici atti a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale, dati sul rendimento accademico;

4. "Limitazione di trattamento": il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
5. "Titolare del trattamento": la Pontificia Università della Santa Croce, che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
6. "Responsabile Protezione Dati" (RPD): figura specializzata nel supporto al Titolare del trattamento;
7. "Responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
8. "Interessato al trattamento": la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
9. "Consenso dell'interessato": qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
10. "Destinatario": la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazioni di dati personali, che si tratti o meno di terzi. Sono da considerare come "Destinatari" anche tutti i soggetti, di diritto civile, canonico ed ecclesiastico, che – in forza di un legittimo interesse, come successivamente qualificato – supportano positivamente l'interessato nel perseguimento

dei suoi fini, come portatore degli stessi interessi legittimi. Sono da considerare "destinatari" a titolo di esempio: una Diocesi o circoscrizione ecclesiastica nonché il suo Ordinario, una Congregazione religiosa o ente assimilato nonché il suo Superiore, chiunque detenga una autorità legittima verso chierici, religiosi e candidati al sacerdozio (ad es. Rettori di Seminari e Collegi sacerdotali);

11. "Terzo": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali;
12. "Profilazione": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica;
13. "Registro attività di trattamento": elenco dei trattamenti di dati in forma cartacea o telematica effettuati dal Titolare e dal Responsabile per la Protezione Dati secondo le rispettive competenze;
14. "Archivio": qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
15. "Violazione dei dati personali": la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
16. "Pseudonimizzazione": è il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a con-

dizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

# 3.
# POLITICA PER LA PROTEZIONE DEI DATI PERSONALI

La Pontificia Università della Santa Croce effettua il trattamento di dati personali per lo svolgimento delle sue legittime attività, e il conseguimento delle sue finalità di ricerca e di formazione nelle diverse scienze ecclesiastiche così come definite nei suoi Statuti[5], al servizio della Chiesa universale[6]. Il trattamento dei dati personali avviene assicurando adeguate garanzie per la protezione dei dati personali per i membri della comunità accademica, gli ex membri e per le persone che hanno contatti con l'Università.

Conformemente a quanto previsto dal Codice di Comportamento – «divieto di comunicare e diffondere i dati personali senza previo consenso dell'interessato»[7] –, l'Università trasferisce i dati personali a soggetti esterni non collegati istituzionalmente, solo previo consenso dell'interessato.

Uniche due deroghe al predetto divieto di trasferimento dei dati personali sono:

1. le ipotesi previste dalla legge, sia civile che canonica;
2. il caso di legittimo interesse del Titolare.

---

[5] Statuti della Pontificia Università della Santa Croce, art. 3 c. 1: «Mediante la ricerca, lo studio e l'insegnamento delle scienze ecclesiastiche, a livello universitario, l'Università intende servire la Chiesa in piena e fedele unione con il suo Magistero, cooperando in tal modo con il Romano Pontefice nella sua sollecitudine per tutte le Chiese».

[6] Cfr anche Statuti, *Proemio*.

[7] Cfr Codice di comportamento della Pontificia Università della Santa Croce, *IX. Riservatezza e protezione delle informazioni*, 32.

In tal senso, l'Università tratterà i dati necessari al perseguimento delle attività istituzionali e di gestione amministrativa comunicandoli a soggetti, anche terzi, verso cui sussista un obbligo così come qualificato dal principio di liceità del trattamento come fissato al paragrafo 4 del presente Regolamento.

Pertanto, a garanzia della dignità degli interessati, la Santa Croce adotta una politica di protezione dei dati personali che prevede che essi siano:

- raccolti in modo lecito, corretto e trasparente nei confronti dell'interessato (principi di liceità, correttezza e trasparenza);
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo compatibile con tali finalità (principio di limitazione della finalità);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di minimizzazione dei dati);
- esatti e, se necessario, aggiornati, adottando a tal fine determinati criteri per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per i quali sono trattati (principio di esattezza);
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (principio di limitazione della conservazione);
- trattati, mediante misure tecniche e organizzative adeguate, in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale (principio di integrità e riservatezza);
- infine, il Titolare del trattamento è competente per il rispetto dei sopra citati principi e deve essere in grado di comprovarlo (principio di responsabilizzazione).

# 4.
# LICEITÀ DEL TRATTAMENTO

La Pontificia Università della Santa Croce s'impegna ad osservare i seguenti comportamenti in materia di protezione dei dati personali:

1. Individuare al proprio interno le figure coinvolte nel trattamento dei dati e fornire loro adeguata formazione;
2. Nominare un Responsabile Protezione Dati competente e indipendente, con il compito di assistere l'Università nell'applicazione della normativa sulla Protezione dei dati personali;
3. Trattare tutti i dati personali in modo lecito, corretto e trasparente nei confronti dell'interessato;
4. Trattare i dati personali solo in presenza di una delle seguenti condizioni di liceità come di seguito elencate:
   a) *consenso dell'interessato* che deve essere libero, specifico, informato ed inequivocabile;
   b) *adempimento di obblighi contrattuali,* ossia il trattamento è lecito se è necessario all'esecuzione di un'obbligazione di cui l'interessato è parte od all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
   c) *obblighi legali* al quale è soggetto il Titolare del trattamento;
   d) *interessi vitali della persona interessata o di terzi:* ossia se è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

*e) interesse pubblico o esercizio di pubblici poteri*, ovvero necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;

*f) legittimo interesse*, quando il trattamento è necessario per il perseguimento dei fini leciti del Titolare del trattamento o di terzi, a condizione di valutare e bilanciare i diritti dell'interessato e la relativa protezione dei dati personali, e tenuto conto delle ragionevoli attese che l'interessato nutre circa il trattamento stesso.

5. Trattare i dati in possesso della Santa Croce in modo compatibile con le finalità per le quali sono raccolti, senza alcun Trattamento eccedente rispetto ad esse;
6. Applicare il principio della minimizzazione dei dati, in base al quale il Trattamento dei dati viene limitato allo stretto indispensabile in relazione alle finalità per le quali i dati sono raccolti;
7. Raccogliere i dati in modo esatto, correggere tempestivamente i dati non esatti ed aggiornarli ogni volta che sia necessario;
8. Conservare i dati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
9. Trattare i dati personali secondo i principi di integrità e riservatezza, quindi in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;

10. Svolgere periodicamente audit interni sul sistema della protezione dati, attraverso il Responsabile Protezione Dati o altri soggetti competenti ed indipendenti;
11. Informare gli interessati dei trattamenti effettuati;
12. Conservare, con l'ausilio del Responsabile Protezione Dati, un Registro di tutti i trattamenti effettuati, comprensivo della valutazione del rischio per ciascun Trattamento;
13. Adottare adeguati provvedimenti disciplinari nei confronti degli addetti dell'Università che non osservano il presente modello organizzativo sulla Privacy;
14. Garantire agli interessati i diritti di accesso, rettifica, revoca del consenso e cancellazione (o oblio) dei dati che lo riguardano.

# 5.
# ORGANIGRAMMA PER LA PROTEZIONE DEI DATI PERSONALI

L'adozione di un modello organizzativo per la protezione dei dati personali comporta, in particolare, la definizione di ruoli, compiti e responsabilità del Titolare e del Responsabile del trattamento dei dati personali, in relazione ai nuovi principi e strumenti necessari per assicurare una corretta applicazione della protezione dei dati personali. L'organigramma è definito considerando anche le previsioni contenute nel Codice di Comportamento della Pontificia Università della Santa Croce par. IX, il quale espressamente fissa che ciascuno deve assicurarsi che le eventuali diffusione e comunicazione dei dati avvenga nella totale osservanza delle procedure interne, in presenza di specifiche autorizzazioni dei vertici ed in conformità alle vigenti normative. Inoltre, lo stesso Codice di Comportamento vieta la diffusione di notizie relative a informazioni e dati riservati appresi in ragione della propria funzione lavorativa, se non previa autorizzazione del superiore gerarchico.

La tabella disegna l'organigramma Privacy che l'Università intende adottare per la protezione dei dati personali che è composto dalle seguenti funzioni:

| RUOLO | CARATTERISTICHE | CHI RICOPRE IL RUOLO |
|---|---|---|
| Titolare del Trattamento | Soggetto con l'autorità ed i poteri per definire le finalità e i mezzi del Trattamento nonché definire le misure tecniche e organizzative.<br>Spetta al Titolare:<br>1. adottare gli interventi necessari, per la protezione dei dati personali;<br>2. designare il Responsabile della Protezione dei Dati;<br>3. designare i soggetti ai quali è affidata l'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;<br>4. effettuare, a mezzo della struttura competente, apposite verifiche sulla osservanza delle misure adottate per la protezione dati, ivi compreso i profili relativi alla sicurezza informatica, in collaborazione con il Responsabile Protezione Dati;<br>5. assicurare l'adeguata istruzione dei soggetti designati e autorizzati al trattamento dei dati personali. | La Pontificia Università della Santa Croce rappresentata dal Legale Rappresentante |
| Soggetto Designato | Persona fisica che effettua un Trattamento per conto del Titolare definendo, sotto il controllo del Titolare, mezzi e modalità del Trattamento.<br>Il soggetto designato deve essere in grado di offrire garanzie sufficienti in termini di conoscenza, esperienza, capacità ed affidabilità, per mettere in atto, sulla base delle istruzioni fornite dal Titolare, le idonee misure tecniche e organizzative adeguate, rivolte a garantire che i trattamenti siano effettuati in conformità al modello organizzativo adottato.<br>Il Soggetto Designato è tenuto a comunicare al Titolare e al Responsabile Protezione Dati eventuali nuovi trattamenti, la cessazione di trattamenti in corso, l'acquisizione di nuove tecnologie che prevedano il trattamento dei dati personali e comunicare tempestivamente al Responsabile Protezione Dati eventuali casi di violazione dei diritti della libertà delle persone fisiche | I Soggetti Designati (detti anche *owner* di processo nel trattamento dei dati personali) sono le figure apicali individuate rispetto ad ogni singolo ufficio/struttura relativamente ai dati dell'utenza che sono raccolti nell'ambito delle rispettive funzioni di competenza.<br>I dati relativi al personale sono trattati a livello centralizzato dal Responsabile del personale in qualità di Soggetto Designato per il trattamento di tale categoria di dati personali. |

| | | |
|---|---|---|
| Autorizzato del Trattamento | Figura che esegue singole operazioni rispetto ai dati personali senza alcuna autonomia decisionale, nel rispetto delle istruzioni di Titolare e Soggetti designati. Soggetto che in base al Codice di comportamento deve essere specificatamente autorizzato al trattamento.<br>Gli Autorizzati devono trattare i dati personali, ai quali hanno accesso, attenendosi alle istruzioni del Titolare e del RPD, avendo cura della natura e finalità dei trattamenti svolti, delle tipologie di dati personali oggetto di trattamento e delle misure tecnico-organizzative attuate per la corretta protezione dei dati personali. Gli Autorizzati al trattamento, che di norma sono i soggetti afferenti alla struttura di riferimento di ogni Soggetto Designato, sono adeguatamente formati e ricevono al momento dell'incarico specifiche istruzioni dal soggetto designato. Nello specifico, l'Autorizzato è tenuto:<br>a) a mantenere il segreto e il massimo riserbo sull'attività prestata e su tutte le informazioni di cui sia venuto a conoscenza durante la stessa;<br>b) a non comunicare senza legittima autorizzazione a terzi o comunque diffondere, con o senza l'ausilio di strumenti elettronici, notizie, informazioni o dati appresi, relativi a fatti e circostanze di cui sia venuto a conoscenza nella propria qualità di soggetto Autorizzato. | Gli Autorizzati al trattamento dei dati all'interno della Santa Croce sono tutti coloro che quotidianamente gestiscono i dati, su supporto sia cartaceo sia informatico (personale tecnico amministrativo, docenti, ricercatori, assegnisti, borsisti etc). |
| Commissione di Vigilanza | L'esercizio dei diritti in materia di protezione dei dati personali ricade tra le competenze che il Codice di Comportamento riconosce alla Commissione di vigilanza par. IV 14. La Commissione di Vigilanza svolge una funzione autonoma di garanzia a tutela delle richieste degli interessati, contribuendo all'applicazione del presente regolamento. | Commissione di Vigilanza |
| Responsabile Protezione Dati (RPD) | È compito del Responsabile Protezione Dati:<br>a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché agli altri addetti della Santa Croce in merito agli obblighi normativi in materia di Privacy;<br>b) sorvegliare l'osservanza del Regolamento Privacy dell'Università;<br>c) fungere da punto di contatto con la stessa per le richieste in materia di protezione dati personali. | Persona fisica e/o giuridica individuata dal Titolare del trattamento che lo nomina con Decreto del Rettore |

| | | |
|---|---|---|
| Amministratore di sistema | Soggetto dedicato alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise Resource Planning) utilizzati nelle organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali. | Nell'organizzazione dell'Università coincide con la figura di Direttore Reti Informatiche. |
| Terzo Destinatario | La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo, che si tratti o meno di terzi, che riceve comunicazioni di dati personali. Sono da considerare come "Terzi Destinatari" anche tutti i soggetti, di diritto civile, canonico ed ecclesiastico, che – in forza di un legittimo interesse – supportano positivamente l'interessato nel perseguimento dei suoi fini, come portatore degli stessi interessi legittimi. | A titolo di esempio: una Diocesi o circoscrizione ecclesiastica nonché il suo Ordinario, una Congregazione religiosa o ente assimilato nonché il suo Superiore, chiunque detenga una autorità legittima verso chierici, religiosi e candidati al sacerdozio (es.: Rettori di Seminari e Collegi sacerdotali). |

# 6.
# GLI STRUMENTI

L'Università tramite la propria organizzazione di protezione dei dati provvede all'adozione ed alla dimostrazione di aver adottato le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza correlato al rischio. Di seguito sono elencati gli strumenti che dovrebbero garantire un'adeguata gestione dei trattamenti dei dati personali all'interno dell'Università.

## 6.1 Misure di sicurezza

Nel quadro della protezione dei dati personali è richiesta al Titolare (nella predisposizione del registro dei trattamenti, vedi punto 6.2) una descrizione generale, dove possibile, delle misure di sicurezza tecniche e organizzative adottate.

Il ricorso ad adeguate misure di sicurezza a cura del Titolare tiene anche conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, 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. La Santa Croce per assicurare un adeguato livello di sicurezza adotta misure tecniche e organizzative che possono comprendere:

1. la pseudonimizzazione e la cifratura dei dati personali;
2. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

3. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
4. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Di seguito un elenco indicativo, che suddivide le misure in "tecniche" e "organizzative":

| MISURE DI SICUREZZA | |
|---|---|
| **Tecniche** | **Organizzative** |
| Antifurto e sistemi di allarme | Accesso controllato (privilegi d'accesso fisico) |
| Antivirus | Accordi di trattamento (DPA) con altri responsabili |
| Armadi chiusi | Adesione a codici di condotta |
| Autenticazione informatica | Adesione a meccanismi di certificazione |
| Autorizzazione (privilegi di accesso logico) | Atti di designazione di responsabili interni e di soggetti designati |
| Backup | Atti di autorizzazione e istruzione al trattamento |
| Business continuity | Audit interni di verifica |
| Cifratura | Contratti di assicurazione contro i danni |
| Data Loss Prevention tools | Formazione |
| Disaster Recovery | Regolamenti e/o policy di utilizzo |
| Firewall | Separazione (fisica) |
| Intrusion Detection | Servizio di vigilanza |
| Log management | |
| Penetration test | |

| | |
|---|---|
| Procedure di modifica credenziali | |
| Pseudonimizzazione | |
| Sistemi di condizionamento | |
| Sistemi antincendio | |
| Videosorveglianza | |

## 6.2 Tipologie dei dati personali e loro trattamento

Le tipologie di dati personali possono essere distinte in due gruppi.

- Dati personali comuni: informazioni generiche riferiti all'identità di una persona e non riconducibili allo stato di salute o a informazioni giudiziarie.
- Dati personali particolari: in sintesi, sono i dati personali che riguardano la sfera più intima della persona e o che a quest'ultima si riferiscono.

Esempi di categorie di dati personali:

| Dati Personali Comuni | Dati Particolari |
|---|---|
| Cognome e nome | Dati relativi alla salute (es. fra tanti, gruppo sanguigno) |
| Matricola / badge | Dati relativi a condanne penali e reati |
| Codice fiscale | Dati su nazionalità e/o cittadinanza |
| Data e luogo di nascita | Dati su origine razziale o etnica |
| Grado di parentela | Dati sugli interessi e/o preferenze personali |

| | |
|---|---|
| Numero di telefono | Dati sugli spostamenti e/o ubicazione |
| Indirizzo e-mail | Dati sui procedimenti giudiziari o disciplinari (non relativi a condanne penali e reati) |
| Indirizzo fisico (residenza e/o domicilio) | Dati relativi ad atti di liberalità |
| Targa di bene mobile registrato | Dati sullo stato civile / sulle relazioni personali |
| Dati relativi a rapporti bancari e/o assicurativi | Dati sulla vita e/o l'orientamento sessuale |
| Dati su istruzione e/o formazione professionale | Dati sul comportamento |
| Dati su riconoscimenti e/o premi | Dati sul rendimento accademico |
| Dati sulla situazione e/o posizione lavorativa | Dati sull'affidabilità (economica, personale, ecc.) |
| | Dati sulla situazione economica ed eventuali benefattori |
| | Dati sulle convinzioni religiose o filosofiche |
| | Dati sulle opinioni politiche |
| | Dati sull'appartenenza sindacale |
| | Dati genetici |
| | Dati biometrici |
| | Impronte digitali |
| | Immagini |
| | Registrazioni vocali |

Le operazioni di trattamento possono essere suddivise in 3 fasi:

## A. Raccolta dei dati

Il trattamento dei dati personali inizia con la raccolta degli stessi mediante sistemi digitali e non. I dati raccolti sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati, che sono determinate, esplicite e legittime.

I dati raccolti sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono stati raccolti e trattati.

Pertanto, prima di iniziare la raccolta dei dati il Titolare verifica che gli stessi siano:

a) pertinenti: i dati raccolti devono essere compatibili con le finalità espresse nell'informativa;
b) completi: per il raggiungimento delle finalità prefissate;
c) non eccedenti le finalità: una volta fissato lo scopo i dati non possono essere estranei allo scopo stesso.

## B. Gestione dei dati

La Pontificia Università della Santa Croce tratta i dati personali in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»). Una volta che i dati sono stati raccolti, gli stessi saranno trattati dal Titolare per raggiungere le finalità specificate nell'informativa. I dati saranno trattati nel rispetto dei diritti e le libertà delle persone fisiche e attuando le misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio valutato in sede di analisi del rischio.

In ogni caso il trattamento dei dati sarà organizzato – per impostazione predefinita (*Privacy by default*) – in modo che sia permesso l'accesso solo ai dati necessari per specifica attività di trattamento.

### C. Conservazione e cancellazione

I dati personali cartacei e digitali sono conservati negli archivi della sede e all'interno dei sistemi informatici specifici.

I dati personali saranno trattati per la durata necessaria per raggiungere la finalità del trattamento e nel rispetto degli obblighi di legge o istituzionali (ad esempio conservazione ai fini di eventuali richieste da parte della Santa Sede).

Al termine del trattamento i dati saranno cancellati o resi anonimi. Se ne prevede un loro uso solo per finalità eventuali di ricerca storica, scientifica e statistica nonché di archiviazione per ragioni di pubblico interesse. Altresì i dati personali non sono oggetto di cancellazione nel caso che occorra accertare l'esercizio o la difesa di un diritto in sede giudiziaria.

## 6.3 Formazione

Il Titolare del Trattamento, con l'assistenza del Responsabile Protezione Dati personali, organizza la formazione e l'aggiornamento periodico di tutto il personale della Santa Croce in materia di Privacy.

Per la formazione sulla Privacy sono previsti i seguenti contenuti minimi:

- formazione iniziale di almeno 4 ore al personale apicale e non apicale per quanto concerne il modello organizzativo adottato dall'Università;
- formazione continua di almeno 4 ore per ogni anno formativo a tutto il personale della Santa Croce sugli aggiornamenti al sistema organizzativo Privacy, e sui risultati dell'attività di audit sulla Privacy nel periodo di riferimento.

## 6.4 Il Registro delle attività di trattamento

Il Regolamento prevede l'adozione di un "Registro delle attività di trattamento", che reca almeno le seguenti informazioni:

- il nome e i dati di contatto del Titolare del trattamento dell'Università, del Soggetto Designato (*owner* di processo) e del Responsabile Protezione Dati;
- le finalità del trattamento;
- la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Il Registro rappresenta l'elemento centrale per la governance del modello di gestione privacy e va tenuto in forma scritta, anche in formato elettronico. Il Registro, redatto sulla base di apposito schema predisposto dal Responsabile Protezione Dati, è unico per tutta l'Università.

Il Responsabile della Protezione Dati coordina le attività di implementazione e aggiornamento sistematico dei dati del registro ad opera dei singoli Soggetti designati, a quali spetta la responsabilità sulla completezza e adeguatezza dei dati e delle misure indicate.

## 6.5 Valutazione di impatto

L'Università, quando un tipo di trattamento può presentare un rischio elevato per i diritti delle persone fisiche, tenuto conto della natura, dell'oggetto, del contesto, delle finalità del trattamento e dell'utilizzo di nuove tecnologie, effettua una valutazione del rischio di impatto dei trattamenti previsti sulla protezione dei dati personali.

La Santa Croce svolge la valutazione d'impatto sulla protezione dei dati con il Responsabile Protezione Dati. La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente sulle persone fisiche;
b) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Il Titolare si consulta con il Responsabile Protezione Dati anche per assumere la decisione di effettuare o meno la valutazione d'impatto; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della valutazione di impatto qualora effettuata.

## 6.6 Comportamenti da adottare in caso di violazione dei dati personali

Nel caso di violazione di dati personali il Titolare del Trattamento predispone un registro degli incidenti che contiene:

- la descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- se ha comunicato agli interessati la violazione dei dati personali e indicato il punto di contatto dove possono ricevere ulteriori informazioni;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del Trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Nel caso di violazione di dati personali la Santa Croce comunicherà agli interessati l'avvenuta violazione. La comunicazione all'interessato riguar-

da la natura della violazione dei dati personali. Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione;
b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati.

# 7.
# ESERCIZIO DEI DIRITTI

L'interessato ha i seguenti diritti in materia di dati personali:

a) diritto di accesso: il diritto di accesso dell'interessato è strettamente connesso alla durata del trattamento dei dati. L'interessato ha sempre il diritto di ottenere dal Titolare del trattamento la conferma che vi sia in corso un trattamento dei propri dati e, in caso positivo, accedere alle informazioni inerenti lo specifico trattamento, ossia sapere per quali fini sono stati adoperati i dati, quali dati sono stati adoperati, a chi sono stati comunicati, il periodo di tempo entro cui i dati saranno conservati o una previsione della durata;
b) diritto di rettifica: l'interessato può esercitare questo diritto ogni qualvolta l'interessato riscontri l'utilizzo di dati personali inesatti;
c) diritto di revoca del consenso: l'interessato ha il diritto di revocare il proprio consenso al trattamento dei dati personali. La revoca non è sottoposta ad alcun vincolo o condizione né di carattere temporale né di natura strutturale. Il diritto di revocare il consenso è, pertanto, esercitabile in qualsiasi momento. Ovviamente il trattamento dei dati avvenuto nell'arco di tempo coperto dal consenso espresso, resta lecito. Del riconoscimento del diritto a revocare il consenso, l'interessato deve averne notizia già nel momento stesso in cui presta il consenso;
d) diritto alla cancellazione (oblio): l'interessato ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo (da considerare quindi in pochi giorni) nei seguenti casi:

1. i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
2. l'interessato revoca il consenso su cui si basa il trattamento, se non esiste alcun altro motivo legittimo per il trattamento;
3. i dati personali sono stati trattati illecitamente.

Il Titolare può continuare ad elaborare i dati se sono comunque necessari per gli scopi per i quali sono stati raccolti, purché continui a disporre di una base giuridica per il trattamento degli stessi.

Pertanto, nei casi in cui il trattamento è necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto cui è soggetto il Titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
c) per motivi di interesse pubblico;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui la cancellazione rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

L'Università adotta misure appropriate per fornire all'interessato tutte le informazioni a garanzia della protezione dei dati personali secondo il presente modello organizzativo nonché per gestire le comunicazioni in

merito all'esercizio dei diritti in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

Le informazioni sono fornite mediante predisposizione di idonea pagina web sul sito istituzionale. Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente della Santa Croce è predisposta apposita informativa.

Una informativa breve è fornita, mediante idonei strumenti:

- attraverso appositi moduli da consegnare agli interessati. Nel modulo sono indicati i soggetti ai quali l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti, anche al fine di consultare l'elenco aggiornato dei soggetti designati;
- in avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture della Santa Croce, nelle sale d'attesa ed in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet del Titolare;
- in apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con l'Università;
- in apposita avvertenza inserita nelle comunicazioni dirette all'Amministrazione;
- in sede di pubblicazione dei bandi, avvisi, ecc.

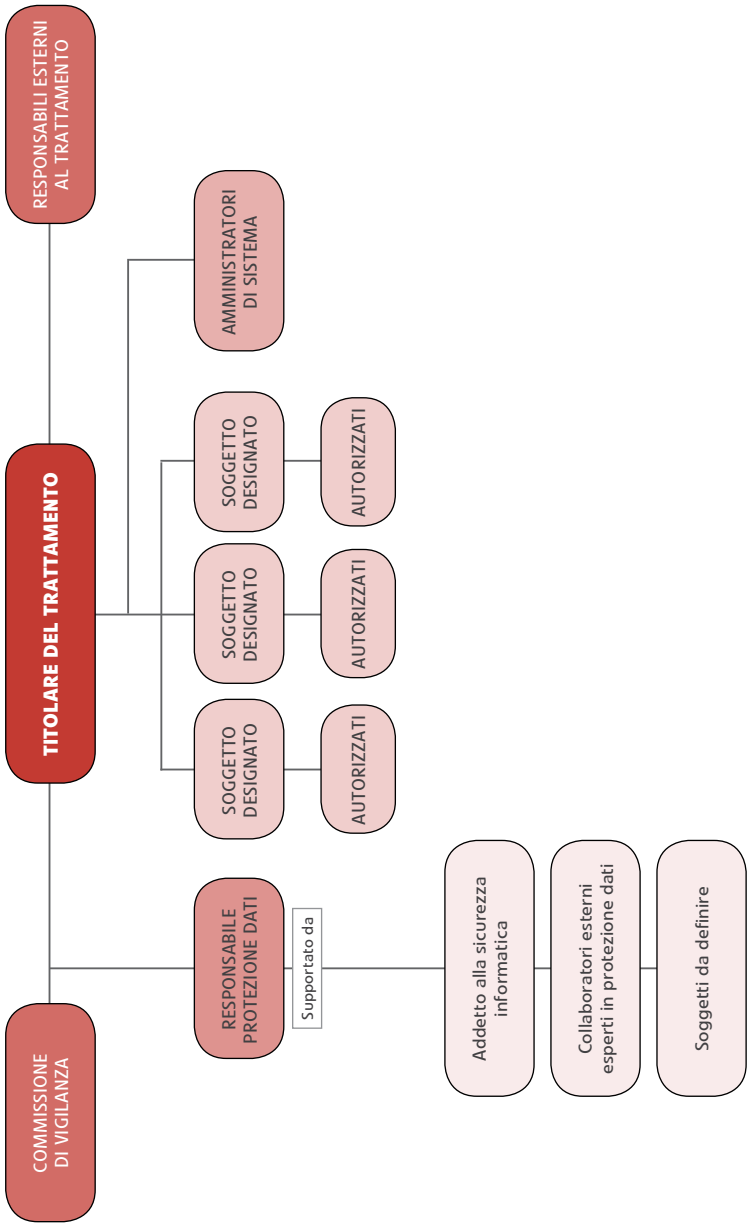
Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

# 8.
# MONITORAGGIO

Il Responsabile Protezione Dati personali, ovvero un auditor per la protezione dati delegato dallo stesso Responsabile Protezione Dati o dal Titolare, effettua periodicamente attività di monitoraggio per verificare la conformità del rispetto all'osservanza della protezione dei dati personali. Le check list di audit sono definite volta per volta sulla base degli elementi che l'auditor intende sottoporre a verifica, anche alla luce delle criticità che si siano eventualmente verificate.

# ALLEGATO

## ORGANIGRAMMA PRIVACY




Pontificia
Università
della
SANTA
CROCE

Piazza di Sant'Apollinare, 49
00186 Roma, Italia
T +39 06 681 641
E-MAIL santacroce@pusc.it
www.pusc.it