Università di Catania

MODELLO ORGANIZZATIVO PRIVACY

(MOP)

ANNO 2024

Sommario

INTRODUZIONE

Il presente documento definisce le misure organizzative che l'Università di Catania adotta per garantire - ed essere in grado di dimostrare - la conformità al REGOLAMENTO (UE) 2016/679 (di seguito indicato "GDPR") e al D. Lgs. n. 2003/196 come novellato dal D. Lgs. n. 2018/101 e ss.mm.ii. (di seguito Codice in materia di protezione dei dati personali).

L'adozione delle misure organizzative adeguate è, infatti, legittimata dagli artt. 24 e ss. del GDPR, ai sensi dei quali le politiche interne e le misure, da attuare per soddisfare i principi della protezione dei dati personali sin dalla progettazione e della protezione dei dati di default, devono tener conto, in concreto, della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento nonché del rischio per i diritti e le libertà delle persone fisiche in un'ottica di responsabilizzazione (*accountability* nell'accezione inglese*)*.

Il principio di *accountability* prevede l'attribuzione in capo al Titolare del potere/dovere di valutare quale sia la migliore organizzazione interna, al fine di assicurare i principi della protezione dei dati rispetto della normativa in materia, ferma restando l'individuazione dei ruoli definiti *ex lege* (es. Responsabile del trattamento, Responsabile della protezione dati RPD o DPO, Contitolare, etc.).

Il Codice in materia di protezione dei dati personali (art. 2-quaterdecies), in questo senso, prevede la possibilità che il Titolare attribuisca compiti e funzioni a persone fisiche che operano sotto la propria autorità e che, a tal fine, dovranno essere espressamente designate.

CONTESTO ORGANIZZATIVO DI RIFERIMENTO

La Struttura amministrativa dell'Università di Catania è definita dallo Statuto, dal Regolamento generale d'Ateneo e dai provvedimenti di macro-organizzazione, assunti dal Consiglio di Amministrazione dell'Ateneo, e dagli atti di micro-organizzazione, assunti dal Direttore generale.

Per l'identificazione della Struttura amministrativa vigente, si rinvia alla specifica sezione del sito istituzionale "Amministrazione trasparente – Organizzazione – Articolazione degli Uffici".

L'assetto delle responsabilità in materia di trattamento e gestione dei dati personali si conforma alla struttura propria dell'Università di Catania, come risultante dal delineato sistema organizzativo interno.

L'Ateneo ha una pluralità di unità organizzative tendenzialmente autonome e a bassa interdipendenza, con processi decisionali anche estremamente articolati; ne consegue la necessità organizzativa di individuare e designare con precisione i soggetti che operano sotto l'autorità del Titolare.

Con il presente Modello Organizzativo Privacy (MOP) è definito il contenuto specifico delle responsabilità in materia di trattamento e gestione dei dati personali ed è delineata, nell'ambito della più generale *governance* dell'Ateneo, un'articolazione "a rete" di funzioni e competenze di gestione e controllo in materia di *privacy compliance*.

Le figure previste dal presente modello organizzativo svolgono compiti attribuiti in materia di trattamento di dati personali nell'esercizio delle ordinarie attività. Le funzioni svolte non comportano alcuna modifica della qualifica professionale e non determinano indennità aggiuntive.

In tale contesto, i processi coordinati a livello centrale dal Titolare del trattamento, coadiuvato dal Responsabile della Protezione dei Dati (RPD), trovano attuazione all'interno della Struttura organizzativa dell'Ateneo attraverso:

1. **Titolare:** persona fisica o giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le scelte sulle finalità e sulle modalità del trattamento dei dati, anche per ciò che riguarda la sicurezza.
2. **Contitolare**: Titolare del trattamento che stabilisce congiuntamente ad un altro Titolare le finalità e i mezzi del trattamento dei dati personali;
3. **Responsabile della protezione dei dati (RPD/DPO):** soggetto interno o esterno all'Ateneo, con funzioni di supporto al Titolare del trattamento e di monitoraggio e controllo del sistema implementato;
4. **Responsabili interni del trattamento:** i responsabili delle strutture nell'ambito delle quali i dati personali sono gestiti per le finalità istituzionali, individuati sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono.
   Ai Responsabili interni del trattamento sono attribuiti specifici compiti e funzioni connessi al trattamento dei dati personali di competenza come di seguito delineati;
5. **Responsabili scientifici – Responsabili interni del trattamento :** Responsabili Scientifici di attività di ricerca svolte nell'ambito dell'attività istituzionale dell'Ateneo, (ad esempio coordinatori di attività di ricerca, referenti scientifici di un progetto di ricerca finanziato, tutor di assegnisti di ricerca, relatori di tesi di laurea o di dottorato, ecc.), ai quali sono attribuiti compiti

di carattere operativo, di collaborazione con il DPO e di supervisione dei ricercatori che collaborano alla predetta attività;

6. **Autorizzati al trattamento:** soggetti che effettuano i trattamenti di dati personali sotto l'autorità diretta e per le finalità stabilite del Titolare e dei Responsabili interni di cui sopra;
7. **Referenti per la protezione dei dati:** figura di supporto al RPD ed al Responsabile interno per agevolare l'attuazione degli adempimenti in materia di protezione dei dati delle persone fisiche, facenti capo alla struttura di competenza;
8. **Amministratori di sistema:** soggetti preposti alla gestione e alla manutenzione di un impianto di elaborazione dati o di sue componenti;
9. **Area dei sistemi informativi:** struttura che collabora con il RPD e a cui sono demandati compiti relativi alla sicurezza informatica dei sistemi e delle Banche dati:
10. **Responsabile della transizione al digitale**: dirigente a cui è affidata "la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità".
11. **Avvocatura d'Ateneo:** struttura a supporto del Responsabile protezione dei dati e dell'ufficio per la protezione dei dati per gli aspetti normativi;
12. **Ufficio protezione dei dati:** ufficio amministrativo, incardinato in Direzione generale, a supporto del RPD e del Titolare.
13. **Responsabili del trattamento (ex art. 4 del GDPR):** soggetti esterni all'Amministrazione (persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo) che trattano dati personali "per conto" del Titolare del trattamento.

ORGANIZZAZIONE FUNZIONALE INTERNA

1. Titolare

Il Titolare del trattamento di dati personali, ai sensi degli artt. 4 paragrafo 7 del GDPR, è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*".

Il Titolare del trattamento è, quindi, il soggetto che decide in merito a determinati elementi chiave del trattamento stesso. La titolarità può essere definita a norma di legge o può derivare da un'analisi degli elementi di fatto o delle circostanze del caso.

L'Università di Catania, nella persona del Rettore pro-tempore, è Titolare di tutti i trattamenti di dati personali svolti nell'ambito delle proprie attività istituzionali.

Il Titolare è responsabile del rispetto dei principi applicabili ai trattamenti stabiliti dall'art.5 del GDPR, ovvero:

- liceità, correttezza e trasparenza
- limitazione della finalità
- minimizzazione dei dati
- esattezza dei dati
- limitazione della conservazione
- integrità e riservatezza

Al Titolare spetta in particolare:

- adottare, nelle forme previste dal proprio ordinamento, le misure tecniche e organizzative necessarie per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento UE 2016/679, anche con riferimento alle disposizioni del Codice per la protezione dei dati personali – D.Lgs. 2003/196 e ss.mm.ii.. Tali misure sono definite sin dalla progettazione del trattamento e messe in atto per applicare in modo efficace i principi di protezione dei dati, per garantire la trasparenza del trattamento e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli da 15 a 22 del GDPR;
- designare il Responsabile della Protezione dei Dati di Ateneo;
- designare i soggetti ai quali è affidata l'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali, ai sensi dell'art. 2-quaterdecies del D.lgs. 2003/196 e ss.mm.ii.;
- nominare i Responsabili del trattamento ai sensi dell'art. 28 del GDPR;

In considerazione della complessità e delle molteplicità delle proprie funzioni istituzionali, il Titolare viene coadiuvato dai Responsabili del trattamento interni ed esterni nonché dagli altri soggetti come di seguito indicati e, pertanto, al fine di assicurare la *compliance* dell'Ateneo al GDPR, ha individuato il presente modello organizzativo. Resta salva la facoltà del Titolare del trattamento di disporre specifiche nomine, singole o per tipologie di Responsabili interni al trattamento, al fine di delimitare specifici e ulteriori ambiti di competenza.

2. Contitolare

Qualora la titolarità, in un trattamento di dati personali, è condivisa tra l'Ateneo e un altro Titolare, tale che la scelta delle finalità e delle modalità impiegate per svolgere un trattamento sia determinata dall'Ateneo in maniera congiunta con altro soggetto pubblico o privato, entrambi i Titolari sono Contitolari del trattamento. Ne deriva una responsabilità congiunta fra (Con)Titolari del trattamento.

L'Ateneo e il Contitolare del trattamento stabiliscono, mediante accordo scritto (Accordo di contitolarità), le rispettive responsabilità, i rispettivi obblighi derivanti dal Regolamento UE e un punto di riferimento e di contatto per gli interessati.

Il contenuto essenziale dell'accordo è messo a disposizione degli interessati da ciascun Contitolare.

3. Responsabile della Protezione dei Dati RPD (o *Data Protection Officer* - DPO)

Il GDPR stabilisce l'obbligo per il Titolare del trattamento, ove questo sia un'amministrazione pubblica, di designare un Responsabile della Protezione dei Dati. Il RPD ha compiti di consulenza nei confronti del Titolare e dei soggetti designati o autorizzati al trattamento e di sorveglianza sull'osservanza del Regolamento.

Il RPD svolge i compiti previsti dalla normativa tra i quali in particolare:

- informare e fornire consulenza al Titolare, ai Responsabili interni, ai Referenti privacy e agli Autorizzati che eseguono il trattamento, in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati;
- vigilare sull'osservanza della normativa in materia di protezione dei dati, nonché delle politiche in materia di protezione dei dati del Titolare, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti, e alle connesse attività di controllo;
- fornire, se richiesto, pareri in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento in Ateneo;
- cooperare e fungere da punto di contatto per il Garante della protezione dei dati in merito alle questioni connesse al trattamento dati.

Il ruolo di RPD non può essere ricoperto da chi determina le finalità o i mezzi del trattamento ossia, tra gli altri, dall'RPCT e dal dirigente dei sistemi informativi e/o da chiunque abbia incarico o funzione che comporti la determinazione di finalità o mezzi del trattamento.

Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare ad una specifica questione attinente alla normativa in materia di protezione dei dati e non può essere rimosso o penalizzato dal Titolare per l'adempimento dei propri compiti.

Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare.

Nel caso in cui il RPD rilevi, direttamente o a seguito di segnalazioni, decisioni o azioni incompatibili con il GDPR e/o con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare e al Responsabile del trattamento.

Il Responsabile protezione dei dati relaziona annualmente sull'attività svolta, al vertice gerarchico dell'Ateneo.

Per lo svolgimento dei propri compiti, il RPD è supportato dall'Ufficio protezione dei dati, dall'Avvocatura di Ateneo, dall'Area Sistemi Informativi e da una rete di Referenti per la protezione dati personali che collaborano con il RPD nell'ambito delle strutture di appartenenza.

Il Titolare assicura che il RPD sia coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Il RPD deve essere consultato immediatamente qualora si verifichi una violazione dei dati o altro incidente che comporti un rischio per i diritti e le libertà degli Interessati.

4. Responsabile interno del trattamento

L'Università di Catania ha individuato i Responsabili interni del trattamento quali soggetti appositamente designati sulla scorta del proprio assetto organizzativo, ai sensi dell'art. 2-quaterdecies del Codice in materia di protezione dei dati (d.lgs.2003/196 e ss.mm.ii.).

Sulla base del vigente assetto organizzativo-direzionale dell'Ateneo, al personale dipendente della Comunità Accademica, che ricopre le funzioni di seguito richiamate, sono affidati tutti gli adempimenti necessari e conseguenti all'attuazione delle norme in materia di protezione dei dati personali:

- Direttore generale
- Dirigenti delle aree
- Direttori di dipartimenti
- Direttori delle strutture didattiche speciali
- Presidente della Scuola Superiore di Catania
- Direttore dell'Azienda agraria sperimentale
- Direttori di centri di Ricerca e Servizi

I provvedimenti di conferimento di incarico o di nomina al ruolo o alla funzione, riporteranno contestualmente la designazione quale Responsabile interno del trattamento.

Possono assumere il ruolo di Responsabili interni del trattamento altre figure interne che, per effetto della carica ricoperta, ai sensi dell'art. 2-quaterdecies, co. 1 del D.Lgs. 196/2003, il Titolare riterrà opportuno designare per il mantenimento delle misure organizzative in Ateneo.

I Responsabili interni, ciascuno per la propria area di competenza, coadiuvano il Titolare nella definizione:

- delle finalità;
- delle modalità di trattamento;
- dei mezzi atti a garantire l'osservanza della normativa europea in tema di protezione dei dati personali.

Al Responsabile interno sono affidati gli adempimenti necessari e conseguenti all'attuazione delle norme in materia di privacy, l'attuazione ed il controllo sulle misure tecniche ed organizzative; egli deve conoscere e rispettare le disposizioni della normativa vigente in

materia di protezione dati e le istruzioni impartite dal Titolare e vigilare sul loro rispetto da parte dei dipendenti e collaboratori afferenti alla propria struttura.

Ai predetti soggetti, in forza dei poteri statutari e regolamentari, nonché delle deleghe gestionali conferite, è assegnata la gestione delle funzioni di seguito descritte:

- garantire che i dati personali oggetto del trattamento siano trattati in modo lecito e secondo correttezza, nel rispetto delle disposizioni contenute nel Regolamento (UE) 2016/679 e nei provvedimenti del Garante della Privacy applicabili, nonché nel rispetto di eventuali istruzioni che saranno fornite dal Titolare;
- adottare le opportune misure di sicurezza per garantire la protezione dei dati personali trattati qualora tali dati dovessero essere raccolti in autonomia dalle strutture al di fuori degli archivi cartacei ed informatizzati o dei server gestiti in maniera centralizzata dall'Ateneo;
- sottoscrivere gli accordi di contitolarità (ex art. 26 GDPR) con enti e istituzioni;
- affidamento incarichi di Responsabile del Trattamento dei dati; definizione e sottoscrizione delle clausole contrattali o atti giuridici analoghi per il conferimento delle relative responsabilità (ex art. 28 GDPR);
- accettazione e sottoscrizione di incarichi di Responsabile del Trattamento dei dati all'Ateneo (art. 4 n. 8 GDPR), conferiti da parte di altri Titolari, laddove sia funzionale all'erogazione dei servizi all'utenza, e regolati da apposito atto (ex art. 28 GDPR);
- implementare e tenere costantemente aggiornato il registro delle attività di trattamento per la struttura di competenza;
- autorizzare i soggetti (di seguito Autorizzati al trattamento) che a vario titolo compiono operazioni di trattamento dei dati personali all'interno della struttura, fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite (sono Autorizzati al trattamento ad esempio: i dipendenti, i collaboratori, studenti part-time, tirocinanti, specializzandi, etc.);
- predisporre le informative relative alle attività di trattamento dei dati personali di competenza, nel rispetto degli articoli 13 e 14 del Regolamento UE 2016/679;
- predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti di cui agli artt. 15-20 del Regolamento UE 2016/679;
- provvedere a dare riscontro alle istanze degli interessati, inerenti all'esercizio dei diritti previsti dalla normativa, mettendone preventivamente a conoscenza il RPD di Ateneo;
- coinvolgere il RPD in tutte le questioni riguardanti la protezione dei dati;
- collaborare con il RPD al fine di consentire a quest'ultimo l'esecuzione dei compiti e delle funzioni assegnate;
- individuare, in base alla complessità della struttura ed all'eterogeneità dei dati trattati, una o più persone di riferimento (Referenti Privacy) che avranno il compito di supporto e raccordo nei rapporti fra il Responsabile della struttura ed il RPD per gli adempimenti previsti dalla normativa vigente;
- designare gli amministratori di sistema in aderenza al Provvedimento del garante del 27 novembre 2008, come modificato dal Provvedimento 25 giugno 2009 recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";
- effettuare eventuale preventiva valutazione d'impatto (DPIA);

- raccogliere le segnalazioni di violazione di dati personali da parte di dipendenti, collaboratori e/o interessati, e comunicarle tempestivamente al RPD e al Titolare, secondo la procedura di segnalazione dei *data breach* adottata dall'Ateneo.

4.1 Il Direttore generale

Il Direttore generale, coerentemente con le competenze statutarie nella qualità di organo di vertice dell'amministrazione, oltre ad esercitare le funzioni assegnate ai responsabili interni, esercita, in materia di protezione dei dati personali, le seguenti funzioni delegate:

- determinare l'organizzazione del sistema privacy all'interno dell'Ateneo;
- revisionare ed aggiornare, con il supporto dell'Ufficio della protezione dei dati e delle strutture nonché la collaborazione del RPD, il Modello organizzativo di Ateneo attribuendo funzioni e compiti, connessi al trattamento dei dati personali, a persone fisiche espressamente designate che operano sotto la responsabilità del Titolare, per dare compiuta attuazione alle disposizioni del Regolamento e del Codice Privacy;
- effettuare, in collaborazione con il Responsabile della Protezione Dati e a mezzo della struttura competente, apposite verifiche sulla corretta applicazione della normativa sulla *data protection* e sulle istruzioni impartite, ivi compresi i profili relativi alla sicurezza informatica;
- predisposizione e approvazione di eventuali documenti operativi (es.: linee guida, procedure, istruzioni operative, etc.) che si rendessero necessari per garantire la più efficace implementazione dei requisiti del GDPR;
- approvazione, sentito il RPD, di percorsi formativi ai soggetti che, agendo sotto l'autorità del Titolare, svolgono trattamenti in Ateneo;
- la collaborazione, per quanto di competenza, con il Responsabile della protezione dei dati dell'Università, nell'esecuzione dei compiti ad esso attribuiti;
- nomina Referenti per la protezione dei dati.

Al Direttore generale è affidata la responsabilità delle attività di trattamento di dati personali svolte dalle Unità operative e/o dagli Uffici a supporto degli organi di vertice (quali ad esempio: Organi collegiali, Nucleo di valutazione, Presidio di qualità) non in possesso di strutture amministrative proprie.

4.2 Il Direttore di Centri di Ricerca e Centri di Servizi

I Centri di ricerca e servizi effettuano attività di trattamento di dati personali al pari delle strutture dipartimentali, in quanto sono strutture autonome finalizzate allo svolgimento di ricerche di rilevante impegno scientifico e finanziario e/o di attività di servizio di interesse comune e dotate di autonomia gestionale. Il Direttore del centro di servizio o di ricerca assume, pertanto, il ruolo di Responsabile interno del trattamento.

Considerato che i Centri di ricerca non hanno personale direttamente incardinato, i compiti di Referente della protezione dei dati e di Autorizzati sono svolti dal personale del Dipartimento di riferimento in cui viene svolta la gestione amministrativa del Centro stesso, sotto la responsabilità dello stesso Direttore; le attività di trattamento dati, svolte in tali strutture, vengono descritte ed analizzate nel Registro delle attività di trattamento del Dipartimento principale cui è affidata la gestione.

5. Il Responsabile Scientifico – Responsabile interno del trattamento

L'Università degli studi di Catania in qualità di "titolare del trattamento" dei dati personali effettuato nell'ambito dell'esecuzione dei propri compiti istituzionali, tra cui l'attività di ricerca scientifica, ha individuato i Responsabili Scientifici – Responsabili interni del trattamento quali soggetti appositamente designati sulla scorta del proprio assetto organizzativo, ai sensi dall'art. 2-quaterdecies del Codice in materia di protezione dei dati (d.lgs.2003/196 e ss.mm.ii.).

Pertanto, ai soggetti che svolgono attività di ricerca di cui l'Università è titolare sono affidati tutti gli adempimenti necessari e conseguenti all'attuazione delle norme in materia di protezione dei dati personali, per i quali dovranno assicurare i necessari standard di sicurezza e protezione dei dati e il rispetto:

- del Regolamento generale sulla protezione dei dati (UE) 2016/679, delle disposizioni normative comunitarie e internazionali relative al trattamento dei dati personali a fini statistici e scientifici;
- delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018. (GU n. 11 del 14 gennaio 2019);
- del Provvedimento del Garante n. 497 del 13 dicembre 2018 – "Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica" (aut. gen. n. 9/2016).

Per quanto previsto nelle suddette Regole deontologiche, l'attività di ricerca dovrà essere preceduta dall'espletamento di alcuni adempimenti atti a documentare che il trattamento dei dati avvenga per effettivi scopi statistici e/o scientifici, tra cui si evidenziano le seguenti:

- la ricerca dovrà essere effettuata sulla base di un progetto redatto conformemente agli standard metodologici del pertinente settore disciplinare;
- il responsabile scientifico (*principal investigator*) deve depositare il progetto presso il Dipartimento di afferenza, il quale ne cura la conservazione, in forma riservata (essendo la consultazione del progetto possibile ai soli fini dell'applicazione della normativa in materia di dati personali), per cinque anni dalla conclusione programmata della ricerca;
- il progetto deve contenere una dichiarazione di impegno a conformarsi alle suddette regole deontologiche. Un'analoga dichiarazione è sottoscritta anche dai soggetti – ricercatori, responsabili e persone autorizzate al trattamento – che fossero coinvolti nel prosieguo della ricerca, e conservata per cinque anni dalla conclusione programmata della ricerca.

Fermo restando quanto stabilito dalle normative vigenti (in particolare quelle su richiamate) e quanto disposto da ulteriori istruzioni fornite dal Titolare, i Responsabili scientifici sono tenuti all'osservanza, delle seguenti prescrizioni generali:

- il trattamento dei dati personali deve avvenire nel rispetto dei principi di liceità, correttezza e trasparenza;
- il trattamento dei dati personali deve essere adeguato, pertinente e limitato a quanto necessario rispetto alle finalità indicate nell'informativa relativa allo specifico progetto (minimizzazione dei dati);

- l'accesso ad eventuali banche dati dedicate al progetto deve essere specificatamente autorizzato dal responsabile del progetto;
- garantire l'applicazione delle misure tecniche ed organizzative atte a garantire il rispetto della normativa in materia di protezione dei dati personali, delle suddette Regole deontologiche;
- svolgere, ove necessario, una "valutazione d'impatto sulla protezione dei dati" per lo specifico progetto di ricerca (ai sensi dell'artt. 35-36 GDPR);
- osservare le procedure disposte dal Titolare del trattamento nel caso di "violazione di dati personali" (data breach) avvenuto nell'ambito del progetto di ricerca;
- trattare, di regola, in forma anonima le particolari categorie di dati di cui all'art. 9 par. 1 e i dati relativi a condanne penali e reati di cui all'art. 10 del GDPR;
- raccogliere il consenso libero ed esplicito dell'interessato sulla base degli elementi previsti per l'informativa, in forma scritta o telematica;
- conservare la documentazione dell'informativa resa all'interessato e dell'acquisizione del relativo consenso per tre anni e renderla disponibile su richiesta del Titolare del trattamento e/o del Responsabile della Protezione dei Dati (RPD).

Qualora il Responsabile scientifico svolga attività di ricerca riguardante, a titolo semplificativo e non esaustivo, un'attività di ricerca individuale (es. GRANT) o un'attività finalizzata alla pubblicazione scientifica, o qualora non depositasse il progetto presso il dipartimento, è considerato Titolare del trattamento in quanto definisce in autonomia finalità, mezzi, misure di sicurezza e trattamento dei dati.

6. Autorizzato al trattamento dei dati personali

Sono Autorizzati al compimento delle operazioni di trattamento dei dati coloro che, in relazione e nei limiti dei compiti assegnati e delle funzioni svolte all'interno della struttura organizzativa cui afferiscono o nell'ambito del progetto di ricerca in cui sono inseriti, eseguono operazioni sui dati personali (docenti, ricercatori, personale tecnico-amministrativo, assegnisti, borsisti, tirocinanti, studenti part-time etc.).

Il personale docente, nell'ambito delle proprie attività istituzionali di didattica, è soggetto autorizzato al trattamento dei dati personali degli studenti.

Sono, comunque, fatte salve eventuali diverse determinazioni volte a definire diversamente il perimetro dei trattamenti leciti e dei soggetti ad essi autorizzati.

Gli Autorizzati sono tenuti a trattare solo i dati personali necessari per ogni specifica finalità del trattamento, conformando le operazioni loro assegnate alla normativa in materia di protezione dei dati personali e alle istruzioni ricevute, anche oralmente, direttamente dal Titolare o per il tramite del Responsabile interno (Responsabile della Struttura/Responsabile del progetto di ricerca).

Le istruzioni possono riguardare anche aspetti di dettaglio da diversificare in relazione alle specificità dei singoli trattamenti.

Qualora il trattamento sia previsto, come incluso nell'attività lavorativa tipica del dipendente, la relativa autorizzazione è insita nell'espletamento della funzione relativa al ruolo rivestito (ad es. Responsabile Servizio Prevenzione e Protezione Rischi, Ufficiale Rogante).

Gli Autorizzati ricevono opportuna formazione/informazione in materia di trattamento dati in relazione ai compiti loro assegnati.

L'Autorizzato è tenuto:

a) a mantenere il segreto e il massimo riserbo sull'attività prestata e su tutte le informazioni di cui sia venuto a conoscenza durante l'attività svolta;
b) a non comunicare a terzi o diffondere, con o senza strumenti elettronici, le notizie, informazioni o dati appresi in relazione a fatti e circostanze di cui sia venuto a conoscenza nella propria qualità di Autorizzato;
c) a segnalare con tempestività al Responsabile interno della propria struttura eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare eventuali procedure di comunicazione delle violazioni di dati al Garante privacy e ai soggetti interessati (istituto del *data breach*);
d) a collaborare, se richiesto, alla tenuta e all'aggiornamento del Registro delle attività di trattamento;
e) a osservare le istruzioni, le politiche e i regolamenti in materia di protezione dei dati adottate dall'Ateneo;
f) qualora svolga le sue funzioni nell'ambito di un progetto di ricerca, a sottoscrivere una dichiarazione di impegno a conformarsi alle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 del Garante per la protezione dei dati.

L'Autorizzato è informato e consapevole che l'accesso e la permanenza nei sistemi informatici per ragioni estranee e comunque diverse rispetto a quelle per le quali è stato abilitato per fini istituzionali e di servizio può configurare il reato di accesso abusivo ai sistemi informativi e può comportare, quindi, sanzioni penali e disciplinari, oltre che esporre l'Amministrazione a danni patrimoniali e reputazionali.

Qualora gli Autorizzati vengano a conoscenza di dati personali per i quali non possiedono l'autorizzazione al trattamento o che non competono alla unità organizzativa cui afferiscono, allorché effettuassero operazioni su tali dati personali, i suddetti autorizzati saranno considerati terzi rispetto all'amministrazione stessa.

7. Referente per la protezione dei dati

Il Responsabile interno individua, all'interno della propria struttura di competenza, uno o più collaboratori a cui assegnare il ruolo di Referente per la protezione dei dati personali. In assenza di individuazione, il ruolo di Referente è individuato nello stesso Responsabile interno.

Il Referente ha il compito di supportare il Responsabile interno in tutte le attività relative al trattamento dei dati personali, di interfacciarsi con il RPD per tutte le attività inerenti alla corretta gestione della tutela dei dati personali e per ogni comunicazione legata all'applicazione della normativa in materia. Per questo motivo sarà coinvolto in tutte le fasi nel flusso dell'attività di trattamento.

I Referenti sono tenuti a seguire gli appositi corsi di formazione e di aggiornamento, erogati dall'Ateneo.

8. Amministratore di Sistema

Sono i soggetti preposti alla gestione e alla manutenzione di un impianto di elaborazione di dati o di sue componenti; gli amministratori di sistema sono nominati e verificati periodicamente dai Responsabili interni.

L'attribuzione delle funzioni di Amministratore di Sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

La nomina quale Amministratore di Sistema deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Il Provvedimento del Garante Privacy del 27 novembre 2008 (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - doc. web n. 1577499), come modificato il 25 giugno 2009 (doc. web n. 1626595) considera tra gli Amministratori di Sistema: gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza, e gli amministratori di sistemi software complessi.

L'Amministratore di sistema svolge i propri compiti sulla base di policy predisposte dall'Area dei sistemi informativi.

L'Amministratore di Sistema supporta i Responsabili interni e gli Autorizzati per gli aspetti di tipo tecnico-informatico nelle normali attività operative.

Gli estremi identificativi delle persone fisiche Amministratori di Sistema, ivi compresi i nominativi degli Amministratori di Sistema relativi ai servizi esternalizzati, devono essere riportati, unitamente all'elenco delle funzioni ad essi attribuite, in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante. Pertanto tali nomine, fino a provvedimento contrario, dovranno essere comunicate all'Ufficio per la protezione dei dati.

Si evidenzia che nel caso specifico di utenti ai quali siano assegnati pc o dispositivi (es. *tablet* e *smartphone*) di servizio forniti dall'Ateneo, dei quali l'utente finale è *de facto* l'unico amministratore (per esempio *personal computer* non gestito centralmente dall'Ateneo), l'atto di consegna del bene implica la contestuale nomina ad Amministratore di Sistema del bene stesso. Quindi, l'utente finale sarà, in relazione a tale bene, responsabile direttamente e personalmente di qualunque violazione del presente regolamento o della normativa vigente.

9. Area Sistemi Informativi

Nell'organigramma del *data protection* di Ateneo, la struttura competente in materia di sistemi informativi ha compiti specifici nella protezione dei dati relativamente ai settori informatici e nelle attività connesse.

Spetta alla suddetta struttura l'adozione di policy in materia di privacy e sicurezza informatica, con particolare riferimento all'utilizzo e alla sicurezza delle risorse informatiche, nonché allo sviluppo delle applicazioni informatiche. Dovrà peraltro assicurare:

- l'aggiornamento periodico delle policy ogni qualvolta l'evoluzione tecnica o normativa lo renda necessario;
- la sorveglianza della corretta applicazione delle policy da parte degli Amministratori di Sistema.

Svolge, altresì, un ruolo di supporto al RPD e all'Ufficio per la protezione dei dati in tema di risorse strumentali e di competenze. La struttura è tenuta a mettere in atto tutte le misure adeguate, tecniche ed organizzative, per garantire la sicurezza informatica nei termini previsti dalle norme in materia, predisponendo, nel rispetto dei principi di accountability, evidenze documentali circa le azioni intraprese, le attività svolte e le caratteristiche dei sistemi, da esibire in caso di eventuali attività ispettive da parte degli organi competenti o di sorveglianza sulla conformità al GDPR da parte del RPD.

Provvede, ogni qualvolta venga avvertito un problema di sicurezza, a:

- attivare la struttura cui sono demandati compiti relativi alla gestione degli incidenti di sicurezza, assicurando la partecipazione del RPD;
- individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del RPD;
- segnalare tempestivamente al RPD le violazioni dei dati personali ai fini della notifica al Garante per la protezione dei dati personali.

Svolge verifiche sulla puntuale osservanza della normativa e delle policy dell'Università degli Studi di Catania in materia di sicurezza delle informazioni e di trattamento di dati personali, prevedendo la partecipazione del RPD e realizza le verifiche specifiche richieste dallo stesso.

Promuove la formazione di tutto il personale dell'Università di Catania in materia di sicurezza informatica, coordinandosi con le azioni promosse dal RPD.

Garantisce fattiva collaborazione con il Responsabile interno e con il RPD nell'esecuzione degli adempimenti previsti nella procedura di *data breach*.

10. Avvocatura di Ateneo

L'avvocatura di Ateneo svolge un ruolo di supporto e di sostegno alle attività del RPD e dell'Ufficio protezione dei dati, in quanto collabora sia per fornire che per ottenere pareri e consulenza in materia di normativa sulla tutela e la protezione dei dati personali, così come per la risoluzione congiunta di casistiche trasversali eventualmente incontrate.

11. Ufficio protezione dei dati

L'Ufficio per la protezione dei dati svolge attività di:

- collaborazione con il RPD per l'espletamento delle attività di controllo e di vigilanza sul trattamento dati in Ateneo e di quanto fissato dal Regolamento UE 2016/679 (GDPR);
- supporto alle strutture dell'Ateneo per il trattamento dei dati di competenza.

12. Responsabile del trattamento (ex art. 4 GDPR)

L'Ateneo si avvale di soggetti esterni all'Amministrazione che sono tenuti, nell'ambito dei servizi di outsourcing a loro volta prestati, ad effettuare trattamenti di dati personali, presentando garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate rispetto ai requisiti definiti dal Regolamento e che, ai sensi dell'art. 28 del GDPR, sono nominati dall'Università "Responsabili del trattamento".

Pertanto, sono "Responsabili del trattamento di dati personali" quei soggetti esterni all'amministrazione che sono tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamento di dati personali per conto dell'Ateneo.

La nomina deve essere effettuata tramite inserimento nei diversi modelli contrattuali di apposite clausole vincolanti in ordine al rispetto delle disposizioni e degli obblighi in materia di protezione dei dati personali.

Il contratto o atto giuridico, che documenta la nomina attiva o passiva a Responsabili del trattamento, è sottoscritto dal Responsabile interno in relazione alle competenze di funzione.

Al Responsabile del trattamento è richiesto di fornire informazioni documentate volte a garantire adeguati livelli di conformità rispetto alla normativa vigente in materia. I Responsabili del trattamento possono nominare dei sub-responsabili, purché autorizzati preventivamente dal Titolare. Il Responsabile risponde nei confronti dell'Università di Catania degli adempimenti o inadempimenti agli obblighi contrattuali del sub-responsabile.

Nei casi in cui l'Università di Catania, sulla base di impegni contrattuali, effettui trattamenti di dati per conto di terzi, sarà nominata dalla controparte "Responsabile del trattamento di dati personali" ex art. 28 del GDPR e dovrà rispondere degli obblighi assunti nei confronti del committente e degli adempimenti normativi in materia di protezione dei dati personali derivanti dalla nomina a Responsabile del trattamento.

GLI STRUMENTI

1. Il Registro delle attività di trattamento

Il registro rappresenta l'elemento centrale per la governance del modello di gestione privacy e viene tenuto in formato elettronico.

La tenuta dei registri in formato elettronico è unica per tutta l'Università degli Studi di Catania ed è affidata al RPD che si avvale dei singoli Responsabili interni, ai quali spetta la responsabilità sulla completezza e adeguatezza dei dati e delle misure indicati.

2. Valutazione di impatto (DPIA)

Qualora un tipo di trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche, tenuto conto della natura, dell'oggetto, del contesto, delle finalità del trattamento e dell'utilizzo di nuove tecnologie, l'Università effettua una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali, fermo restando i casi di DPIA obbligatoria previsti dal Garante per la protezione dei dati nel provvedimento dell'11 ottobre 12018 n. 467.

Una singola valutazione può esaminare un insieme di trattamenti simili che presentano analoghi rischi elevati.

Il Titolare si consulta con il RPD 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.

Il Titolare può, documentandone le motivazioni, adottare condotte difformi da quelle raccomandate dal RPD.

I Responsabili per la protezione dei dati, anche attraverso i Referenti, devono collaborare nella conduzione della valutazione di impatto, fornendo ogni informazione e documentazione necessaria.

Spetta all'Area dei sistemi Informativi fornire supporto ai Responsabili e al RPD per lo svolgimento della valutazione di impatto per i trattamenti informatizzati.

Il Titolare consulta il Garante per la Protezione dei dati personali prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di rischi per i diritti e le libertà dell'interessato.

3. Violazione dei dati o *data breach*

Al fine di tutelare le persone, i dati e le informazioni e documentare i flussi per la gestione delle violazioni dei dati personali trattati o data breach, l'Università, in qualità di Titolare del trattamento, definisce una procedura di gestione delle violazioni di dati personali, definita *Data Breach*.

La violazione dei dati personali si configura nei casi in cui si verifica un incidente di sicurezza che comporti, 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.

Tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del titolare sono tenuti, nel caso di una concreta, potenziale o sospetta violazione dei dati personali, ad informare dell'incidente il responsabile della struttura (responsabile interno della struttura, etc.) il quale si occuperà di informare il Titolare del trattamento mediante la compilazione del Modulo di comunicazione e la procedura di *Data Breach* che sono pubblicate sul sito di Ateneo.

Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Titolare del trattamento o un suo delegato dovrà coinvolgere anche il Responsabile dell'Area dei Sistemi Informativi o, in caso di assenza, un suo delegato.

Ogni qualvolta si verifichi un incidente, il Titolare sarà tenuto a documentarlo. Tale documentazione sarà predisposta con l'ausilio dell'Area dei Sistemi Informativi (qualora la violazione riguardi dati contenuti in sistemi informatici) e del RPD e sarà documentata mediante la tenuta del Registro dei *Data Breach*.

Il Registro dei *Data Breach* deve essere continuamente aggiornato e messo a disposizione del Garante, qualora l'Autorità chieda di accedervi.

La violazione dei dati è gestita attraverso la procedura di *Data breach* allegata al presente MOP 2024.

4. Informazione e formazione

L'obiettivo di garantire un corretto trattamento dei dati, conforme ai requisiti previsti dalla normativa, viene raggiunto dall'Università anche e soprattutto grazie alla particolare attenzione riposta nei confronti della formazione del proprio personale.

Il MOP è divulgato presso il personale già in servizio e, nel caso di nuove risorse umane inserite in organico, fin dal momento del loro ingresso nella compagine dell'ente. Per gli stessi fini di conoscenza, eventuali aggiornamenti sono diffusi con gli strumenti ritenuti di volta in volta più efficaci.

Allo scopo di diffondere le conoscenze relative alla tutela dei dati personali e di fornire adeguate istruzioni a tutto il personale dell'Ateneo, in particolare, sono considerati progetti formativi specifici per:

- Referenti per la protezione dei dati;
- Autorizzati al trattamento;
- Amministratori di sistema.

Inoltre, l'attività di formazione e informazione potrà essere pianificata attraverso ulteriori specifici percorsi o eventi, secondo le modalità ritenute più idonee (seminari, workshop, convention, incontri frontali e altri), nei quali si terrà conto anche delle specifiche esigenze comunicate dai Referenti delle strutture.

Ulteriori attività di formazione/informazione saranno programmate al momento dell'assunzione di nuove risorse, nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento di dati personali.

I dipendenti e collaboratori dell'Ateneo potranno fare riferimento all'Ufficio protezione dei dati o direttamente al RPD per la proposta di quesiti o la richiesta di approfondimenti.

Qualunque componente della Comunità Accademica, compresi gli studenti, ha la possibilità di contattare l'RPD qualora la questione proposta attenga alla tutela dei propri dati personali.

5. Linee guida, modelli, istruzioni operative

L'Ateneo rende disponibili Istruzioni operative generali e predispone specifiche procedure operative interne per gestire i vari adempimenti previsti dalla normativa, al fine di fornire a tutti soggetti che operano in collaborazione con esso, le disposizioni da seguire in ordine alle varie misure organizzative, procedurali, tecniche e logistiche, così da garantire il necessario livello di sicurezza dei trattamenti gestiti in Ateneo. (Vedi Allegati).

6. Privacy Audit

La realizzazione di verifiche e di *Audit*, al fine di verificare l'applicazione della normativa e delle istruzioni impartite, è funzione affidata, nelle fasi di rilevazione dell'esigenza, programmazione e realizzazione, al RPD, coadiuvato dalla struttura di supporto.

Le attività di verifica sono di regola programmate e previamente comunicate ai soggetti coinvolti (salvo esigenze di *Audit* a sorpresa) e sempre condotte alla presenza degli stessi.

Gli esiti delle verifiche verranno formalizzati in forma di *Audit report* del Responsabile della Protezione dei Dati e:

- condivise con i soggetti auditi che possono formalizzare chiarimenti e/o controdeduzioni;
- completate, in caso di rilevazione di Non conformità (NC), dalla proposta di azioni correttive/preventive.

Il RPD informerà il Direttore generale dell'esito dell'*Audit*.

RESPONSABILITA'

Le responsabilità, derivanti dalla non adeguata protezione dei dati, gravano complessivamente su tutti i soggetti che hanno compiti nell'organizzazione e nell'attuazione dell'attività di trattamento dei dati personali nonché di sorveglianza delle misure tecniche ed organizzativa predefinite per il trattamento stesso.

PRECISAZIONI FINALI

- Il presente modello organizzativo è soggetto a revisione periodica da parte dell'Amministrazione, allo scopo di intervenire, anche su proposta e collaborazione del RPD, sull'assetto organizzativo in caso di modifiche normative o necessità di introdurre nuove e più efficaci politiche di gestione dei dati personali. Bisognerà tenere la storicizzazione delle varie versioni per mantenere l'evoluzione del documento nel tempo.
- Il Modello organizzativo (MOP) e gli allegati sono disponibili nel Portale del personale, nella sezione Ufficio per la protezione dei dati, all'interno di "Documenti privacy".

ALLEGATI

1. Organigramma privacy 2023
2. Guida alla lettura delle disposizioni normative in materia di trattamento dei dati personali (2023)
3. Linee guida generali per il trattamento dati personali
4. Linee guida generali per il trattamento dati personali in smart working
5. Format di autorizzazione al trattamento
6. Vademecum per la corretta gestione del trattamento
7. Procedura Violazione dei dati (data breach)
8. Linee guida trasparenza e privacy
9. COME FARE PER……
   a) redigere un'informativa
   b) gestire il trasferimento dati personali all'estero
   c) effettuare una valutazione d'impatto
   d) redigere un atto di nomina di Responsabile del trattamento