POLICY ORGANIZZATIVA DELL'UNIVERSITÀ DEGLI STUDI DI BERGAMO

IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Sommario

PREAMBOLO

VISTO il **Regolamento UE 2016/679** del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (di seguito, RGPD), in vigore dal 24 maggio 2016, e applicato nell'ordinamento interno dal 25 maggio 2018;

VISTO il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), come modificato dal D. Lgs. n. 101 del 10 Agosto 2018 di adeguamento e attuazione, con la normativa dettata dal Regolamento UE 2016/679, al predetto RGPD 2016/679 e l'implementazione, nello specifico, nelle Pubbliche Amministrazioni;

CONSIDERATO CHE l'attuazione del RGPD 2016/679 presuppone il diretto coinvolgimento del vertice delle Pubblica Amministrazione, comportando un profondo cambiamento anche culturale, poiché i cittadini, con le nuove disposizioni, sono al centro del sistema e agli stessi viene riconosciuto un livello elevato e uniforme di tutela dei dati e soprattutto un maggiore controllo sull'utilizzo dei dati stessi;

CONSIDERATO CHE il Regolamento impone una forte responsabilizzazione, poiché la protezione dei dati personali diventa un "asset strategico", che deve essere valutato prima, già nel momento di progettazione di nuove procedure, prodotti o servizi, (principi "data protection by design" e "data protection by default"), richiedendo alle pubbliche amministrazioni di andare oltre le regole e i meri aspetti formali. I dirigenti, i funzionari, tutti i dipendenti dovranno essere attori di tale mutamento culturale, poiché implica un forte impatto organizzativo;

VISTO, ALTRESI' CHE le norme introdotte dal Regolamento UE 2016/679 si traducono, pertanto, in obblighi organizzativi, documentali e tecnici che il Titolare del trattamento dei dati personali deve, fin da subito, considerare e tenere presenti per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di privacy in vigore;

CONSIDERATO che l'Ateneo è rappresentato ai fini previsti dal RGPD 2016/679 dal Rettore *pro tempore*, titolare del trattamento dei dati personali raccolti o meno in banche dati, e che le relative funzioni possono essere delegate ai soggetti che in essa vi operano;

CONSIDERATO che l'amministrazione pubblica, prima di procedere al trattamento, è chiamata ad effettuare una valutazione dell'impatto ("privacy impact assesment") dei trattamenti previsti dal Regolamento quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Tale valutazione di impatto privacy richiede una puntuale e documentata analisi dei rischi per i diritti e le libertà degli interessati;

CONSIDERATO che nella materia del trattamento dei dati vige il generale obbligo di rendicontazione ("principio di accountability") ossia, la stessa è chiamata a:

- dimostrare di avere adottato le misure di sicurezza adeguate ed efficaci per la protezione dei dati e che esse siano costantemente riviste e aggiornate;
- dimostrare che i trattamenti siano conformi ai principi e alle disposizioni del Regolamento europeo, compresa l'efficacia delle misure. Al fine di poter dimostrare la conformità alle disposizioni del Regolamento, viene previsto l'obbligo di tenuta di un registro delle attività di trattamento effettuate sotto la propria responsabilità con relativa descrizione delle misure di sicurezza (art. 30) tecniche e organizzative e che, su richiesta, deve essere messo a disposizione dell'autorità di controllo;
- nominare il "Data Protection Officer" (DPO), che deve sempre essere "coinvolto in tutte le questioni riguardanti la protezione dei dati personali" e svolgere un'opera di sorveglianza sulla corretta applicazione del regolamento europeo, normativa privacy,

formazione, consulenza e rilascio di pareri, in quanto, per legge, tenuto a cooperare con l'Autorità Garante e riferire direttamente.

1. Finalità della policy

Le finalità della policy privacy dell'Università degli studi di Bergamo, in relazione all'applicazione interna del GDPR 2016/679 (d'ora in poi Regolamento) sono riassunte nelle linee guida, adottate con il presente atto di indirizzo, al fine di stabilire modalità organizzative, misure procedimentali e regole di dettaglio, rivolte anche ad omogeneizzare questioni interpretative, che permettano a questo Ateneo di poter agire con adeguata preparazione/formazione, funzionalità ed efficacia nell'attuazione delle disposizioni introdotte dal Regolamento UE 2016 /679 (RGPD), in particolare attraverso:

I. la definizione ed implementazione di un adeguato modello organizzativo conforme alle nuove norme Privacy, mirato ad individuare ruoli, mansioni, eventi, processi, procedure operative, verifiche periodiche, rilevazione e gestione degli eventi di interesse ai fini della sicurezza e della protezione dei dati;
II. l'individuazione dei principali soggetti coinvolti nelle diverse responsabilità dei trattamenti dei dati personali per individuare le modalità di acquisizione dei dati personali, le specifiche categorie, la metodologia, le tecniche e gli strumenti (localizzazione e criteri di rischio) mediante i quali si raggiunge e si mantiene nel tempo l'adeguamento e la conformità alle prescrizioni del RGPD;
III. la definizione di misure organizzative di coordinamento con l'esercizio del diritto di accesso (documentale, accesso civico semplice e generalizzato) e la trasparenza;

2. Definizioni

Il Regolamento definisce come segue:

- "**Dato Personale**": qualsiasi informazione che permetta di identificare o rendere identificabile, anche indirettamente, una persona fisica (c.d. "Interessato"). L'identificazione, diretta o indiretta dell'Interessato, può avvenire in relazione alle sue caratteristiche (per esempio, 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) o le sue abitudini (per esempio, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica).

- "**Trattamento**": qualsiasi operazione, o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, 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.

3. Rinvio a norme e provvedimenti dell'autonomia

Con questo atto si prevede che con successivi provvedimenti, adottati dai diversi soggetti competenti di questo Ateneo, in conformità a quanto stabilito nel Regolamento UE 2016/679, si procederà:

- ✓ alla determinazione dei criteri per l'individuazione all'esterno del Responsabile della Protezione Dati (DPO) e conseguente nomina;
- ✓ alla nomina dei soggetti designati al trattamento;

- ✓ alla nomina da parte del titolare e dei designati degli autorizzati al trattamento;
- ✓ alla nomina dei Responsabili esterni del trattamento, sub-responsabili e incaricati;
- ✓ alla disciplina della contitolarità o titolarità autonoma anche in relazione ai rapporti con altri Atenei, per progetti di ricerca o altre azioni ivi comprese quelle del PNRR, in relazione a specifici rapporti di autonomia economico-contabile-amministrativa anche in rapporto relativo al trattamento dei dati;
- ✓ alla predisposizione di intese, protocolli o accordi con altri Atenei, Enti Agenzie o Associazioni con scopi Statutari conformi alla mission dell'Università degli studi di Bergamo
- ✓ alla regolamentazione uniforme interna di applicazione del Regolamento UE 2016/679 e della normativa nazionale, in tema di riparto dei compiti e responsabilità nel trattamento dei dati;
- ✓ alla predisposizione e tenuta dei registri delle attività di trattamento;
- ✓ nella predisposizione e aggiornamento del Registro dei Data Breach;
- ✓ nella predisposizione, tenuta e popolamento degli affidamenti e degli incarichi ai responsabili esterni dell'Ateneo;
- ✓ regolamentazione e disciplina della videosorveglianza interna ed esterna di sicurezza;
- ✓ nella predisposizione del registro e relativa modulistica per la gestione e riscontro alle istanze degli interessati nei tempi previsti;
- ✓ a mettere in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che i trattamenti dei dati personali vengono effettuati in conformità alla disciplina europea, in ossequio al principio di responsabilizzazione (accountability);
- ✓ ad attivare procedure idonee per l'attuazione delle misure conseguenti ad eventuale violazione dei dati personali;
- ✓ all'aggiornamento della documentazione in essere in Ateneo in relazione ai trattamenti dei dati personali;

4. Tipologie dei dati trattati dall'Università

L'Università effettua trattamenti di dati personali per lo svolgimento delle proprie finalità istituzionali come individuate da disposizioni di legge, statutarie e regolamentari riguardanti, a titolo esemplificativo e non esaustivo:

a) dati relativi al personale docente e ricercatore nonché personale subordinato, parasubordinato o con rapporto di lavoro autonomo, vi compresi i soggetti il cui rapporto di lavoro è cessato o altro personale operante a vario titolo nell'Università, con particolare riferimento a:
   - prove concorsuali/selezioni;
   - gestione del rapporto di lavoro
   - formazione e aggiornamento professionale;
   - gestione di progetti di ricerca;
   - monitoraggio e valutazione della ricerca,
   - attività di trasferimento tecnologico;
   - politiche Welfare e per la fruizione di agevolazioni;
   - salute e sicurezza delle persone nei luoghi di lavoro;
   - erogazione del servizio di telefonia fissa e mobile;
b) dati relativi a studenti intesi nell'accezione più ampia, per tutte le attività e modalità connesse alla qualità di studenti e ai laureati, con particolare riferimento a:
   - attività di orientamento;
   - erogazione del test di ingresso o verifica dei requisiti di accesso;

- erogazione del percorso formativo e gestione della carriera (dall'immatricolazione alla laurea);
- attività di tirocinio;
- attività di job placement;
- attività di fundraising, di comunicazione e informazione istituzionale e sviluppo di community;
- rilevazioni statistiche e valutazione della didattica;
- diffusione dell'elaborato finale o di elementi ad esso connessi;
- servizi di tutorato, assistenza, inclusione sociale;
- servizi e attività per il diritto allo studio;
- procedimenti di natura disciplinare a carico di studenti;

c) dati relativi alle attività gestionali, conto terzi e/o connessi ad attività trasversali, con particolare riferimento a:
   - gestione degli spazi;
   - gestione delle postazioni;
   - gestione degli organi e delle cariche istituzionali:
   - gestione degli infortuni;
   - servizi bibliotecari;
   - servizi di gestione documentale e conservazione;
   - acquisto beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso;
   - servizi di posta elettronica e strumenti di collaboration;
   - erogazione federata di servizi;
   - erogazione del servizio Eduroam;
   - accesso a servizi federati;
   - tracciamento di informazioni non primarie;
d) dati relativi alla didattica, alla ricerca (compresa la ricerca in ambito medico-sanitario) e alla terza missione.

5. Principi applicabili al trattamento dei dati

Ogni trattamento deve avvenire nel rispetto dei principi fissati all'articolo 5 del Regolamento:

a) liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
b) limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
c) minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
d) esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
e) limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
f) integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, l'Università mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento.

In particolare, l'Università adotta misure tecniche ed organizzative:

a) per attuare in modo efficace i principi di protezione dei dati ed integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati (privacy by design);
b) per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento e che i dati personali non siano resi accessibili a un numero indefinito di persone fisiche senza l'intervento della persona fisica (privacy by default).

6. Ruoli e responsabilità

6.1 Ruoli previsti nel Regolamento

Il Regolamento individua diversi ruoli, ciascuno con funzioni e compiti differenti:

a) **Titolare del trattamento**: definito dall'art. 4 del Regolamento come 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;
b) **Contitolare del trattamento** sulla base dell'accordo ex art. 26 del GDPR 2016/679 si ha quando l'Università determina finalità e mezzi del trattamento congiuntamente con un altro Titolare, assumendo in tale ipotesi il ruolo di Contitolare del trattamento. La contitolarità è esercitata sulla base di un accordo trasparente tra di essi Contitolari con determinazione le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento (EU) 2016/79, nonché dalle disposizioni di legge vigenti con riguardo al trattamento dei dati personali. Con l'accordo le Parti stabiliscono, altresì, i rispettivi obblighi in merito all'esercizio dei diritti dell'interessato. Con l'accordo di contitolarità - ai sensi dell'art. 26 del GDPR - saranno determinati i profili di responsabilità per ciascuno dei Contitolari.
c) **Responsabile della protezione dei dati** (di seguito anche Data Protection Officer o DPO): figura prevista dagli artt. 37 e ss. del Regolamento, che ne disciplinano compiti, funzioni e responsabilità;
d) **Designato al trattamento**: chiunque agisca sotto l'autorità diretta del Titolare del Trattamento che operi attenendosi alle istruzioni impartite al fine di realizzare in modo diretto i processi gestionali e di elaborazione del dato personale.
e) **Autorizzato al trattamento**: chiunque effettui operazioni di trattamento in relazione alle attività di propria competenza, e che operano sotto la diretta autorità del titolare o del Designato che lo ha nominato o che dirige la struttura di riferimento e competenza.
f) **Referente:** Referente per la protezione dei dati (Referente privacy)": figura nominata dal Titolare del Trattamento, al fine di svolgere un ruolo di raccordo tra colleghi e collaboratori, secondo le indicazioni e le autorizzazioni concesse all'atto di nomina e riportando gerarchicamente al Titolare del Trattamento;
g) **team di supporto:** gruppo di lavoro svolgere un ruolo di supporto e di raccordo, sulla base di precise istruzioni del RPD;
h) **amministratori di sistema:** figura professionale dedicata alla gestione e alla manutenzione degli impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui Dati Personali;

6.2 Titolare del trattamento

Il Titolare del trattamento di dati personali, ai sensi degli artt. 4 e 24 del Regolamento, è l'Università degli Studi di Bergamo, nella persona del Rettore *pro tempore*, a cui spetta l'adozione di misure tecniche e organizzative adeguate per garantire, ed essere in grado di

dimostrare, che il trattamento è effettuato conformemente al Regolamento. In particolare, l'Università svolge i seguenti compiti:

a) attuare, nelle forme previste dal proprio ordinamento, quanto necessario per rispettare gli obblighi previsti dal Regolamento e dal Codice;
b) designare il responsabile della protezione dei dati (DPO);
c) nomina i designati al trattamento, cioè le persone fisiche a cui attribuire specifici compiti e funzioni connessi al trattamento di dati personali;
d) promuovere la formazione di tutto il personale dell'Università in materia di protezione dei dati personali;
e) effettuare, in collaborazione con il DPO apposite verifiche sull'osservanza delle vigenti disposizioni in materia di protezione di dati personali, ivi compresi i profili relativi alla sicurezza informatica.

6.3Designati al trattamento

Il Titolare individua, con proprio provvedimento, quali Designati al trattamento, le seguenti figure, ciascuno per il proprio ambito di competenza, attribuendo la facoltà di autorizzare all'interno della struttura di competenza il personale di pertinenza e di impiego ai quali attribuire singoli o plurime abilitazioni al trattamento dei dati personali.

a) Direttore Generale;
b) Dirigenti;
c) Direttori di Dipartimento/centro
d) Presidi;
e) Presidenti di Consiglio di corso di studio;
f) Responsabili delle unità organizzative dell'amministrazione centrale;
g) Responsabili delle unità organizzative decentrate;
h) Titolari di progetti di ricerca;

I Designati al trattamento svolgono i seguenti compiti:

a) tenere e aggiornare il registro delle attività di trattamento di dati personali svolte nella struttura di riferimento, ai sensi dell'art. 30 del Regolamento;
b) effettuare una valutazione dei rischi connessi al trattamento dei dati, con il supporto dei Servizi informativi nel caso di trattamenti con mezzi informatici;
c) effettuare una preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, avvalendosi se necessario, del parere del DPO;
d) consultare il Garante, ai sensi dell'art 36 del Regolamento, nei casi in cui la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenta un rischio residuale elevato, avvalendosi, se necessario, del supporto dei Servizi informativi;
e) comunicare ai Servizi informatici, nel momento dell'adozione, i nuovi software e le basi di dati utilizzati per il trattamento di dati personali;
f) predisporre le informative relative al trattamento dei dati personali, nel rispetto degli artt. 13 e 14 del Regolamento;
g) predisporre il consenso, qualora necessario, nel rispetto dell'art 7 del Regolamento;
h) individuare e designare i soggetti autorizzati a compiere operazioni di trattamento (di seguito "autorizzati"), fornendo agli stessi istruzioni per il corretto trattamento dei dati;

i) individuare, negli atti di costituzione di gruppi di lavoro/commissioni comportanti il trattamento di dati personali, i soggetti che effettuano tali trattamenti quali soggetti autorizzati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;
j) valutare la sussistenza di ipotesi di contitolarità del trattamento, nel rispetto dell'art. 26 del Regolamento;
k) adottare, se necessario, specifici disciplinari di settore, anche congiuntamente con altri responsabili interni, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi alla propria area di competenza;
l) segnalare tempestivamente ai Servizi informativi la violazione di dati personali, qualora ne venga a conoscenza;
m) disporre le modifiche necessarie al trattamento dei dati personali perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
n) provvedere, anche con il supporto degli autorizzati, a dare riscontro alle istanze degli interessati inerenti all'esercizio dei diritti previsti dalla normativa;
o) adottare i provvedimenti imposti dal Garante;
p) verificare che i software e le piattaforme acquisite rispettino i principi privacy by design e privacy by default ai sensi dell'art. 25 del Regolamento;
q) verificare la legittimità dei trattamenti effettuati nella struttura di riferimento;
r) vigilare sull'attuazione delle istruzioni impartite ai soggetti autorizzati;
s) collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
t) garantire ai Servizi informatici e al DPO i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza.
u) ogni altra prescrizione attribuita con l'atto di Designazione al trattamento dei dati personali.

6.4 Soggetti autorizzati al trattamento

Sono autorizzate al trattamento dei dati personali tutte le persone strutturate (personale tecnico e amministrativo, personale docente e ricercatore) assegnate agli uffici, dipartimenti, centri, che effettuano operazioni di trattamento in relazione alle attività di propria competenza, e che operano sotto la diretta autorità del Titolare o dei designati.

Sono altresì soggetti autorizzati al trattamento le persone che, a seguito di atto di assegnazione anche temporaneo (collaborazioni coordinate e continuative, contratti a progetto, 150 ore per studenti, stagisti, volontari del servizio civile, dottorandi, borsisti, tutor, assegnisti di ricerca ecc.) afferiscono alle strutture che effettuano operazioni di trattamento in relazione alle attività di propria competenza e che operano sotto la diretta autorità del Titolare o dei designati.

I soggetti autorizzati sono designati:

a) tramite individuazione nominativa delle persone fisiche specificando trattamenti che possono effettuare;
b) tramite assegnazione funzionale della persona fisica ad un'unità organizzativa, specificando i trattamenti che tale unità è autorizzato ad effettuare.

La designazione scritta deve inoltre contenere le istruzioni per il trattamento dei dati personali. Tali istruzioni devono contenere un espresso richiamo alle policy dell'Università in materia di sicurezza informatica e protezione dei dati personali e possono prevedere ulteriori dettagli diversificati in relazione alle specificità dei singoli trattamenti.

I Soggetti autorizzati al trattamento svolgono i seguenti compiti:

a) fornire agli interessati le informative relative al trattamento dei dati personali nel rispetto dell'art. 13 e 14 del Regolamento;
b) acquisire il consenso, ove necessario, per il trattamento dei dati personali, nel rispetto dell'art. 7 del Regolamento;
c) supportare il titolare/designato per rispondere alle istanze degli interessati inerenti all'esercizio dei diritti previsti dalla normativa;
d) segnalare tempestivamente ai Servizi informativi la violazione di dati personali, qualora ne venga a conoscenza;
e) supportare il titolare/designato ai fini dell'eventuale valutazione d'impatto, fornendo tutte le informazioni allo stesso utili per determinare il rischio del trattamento effettuato nell'esercizio delle attività assegnate;
f) ogni altra attribuzione contenuta nell'atto di autorizzazione al trattamento dei dati personali.

6.5 Responsabili esterni del trattamento

Sono designati responsabili del trattamento di dati personali i soggetti esterni all'Università che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione, atto costitutivo o provvedimento di nomina, ad effettuare trattamenti di dati personali per conto del titolare.

Pertanto, qualora sia necessario affidare un incarico che comporti anche trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando l'esperienza, la capacità e l'affidabilità del soggetto cui affidare l'incarico in materia di protezione dei dati, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni, ivi compreso il profilo della sicurezza.

La designazione dei responsabili del trattamento deve essere effettuata all'interno di contratti o convenzioni e, in ogni caso, in costanza di formazione del rapporto contrattuale.

6.6Responsabile della Protezione dei dati (DPO)

Il Regolamento prevede l'obbligo per gli Enti pubblici di designare il Responsabile della protezione dei dati (o Data Protection Officer - DPO).

La designazione avviene con decreto rettorale, nel caso di DPO interno, oppure con contratto di servizi, nel caso di DPO esterno.

Il titolare del trattamento sostiene il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Il DPO svolge i seguenti compiti:

a) informare e fornire consulenza all'Università in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali;
b) sorvegliare l'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche dell'Università in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) cooperare con il Garante per la protezione dei dati personali;
d) fungere da punto di contatto per l'Autorità Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione;

e) promuovere la formazione di tutto il personale dell'Università in materia di protezione dei dati personali e sicurezza informatica;
f) formulare gli indirizzi per la realizzazione del Registro delle attività di trattamento di cui all'art. 30 del Regolamento;
g) partecipare allo svolgimento delle verifiche di sicurezza svolte dal personale della Ripartizione Servizi informatici o ne richiede di specifiche;
h) partecipare alla gestione degli incidenti di sicurezza nelle modalità previste da specifica policy dell'Università;
i) fornire i pareri obbligatori e facoltativi richiesti dall'Università secondo quanto specificato di seguito, entro il termine di 15 giorni.

Pareri obbligatori

Devono essere richiesti pareri in ordine a:

a) individuazione delle misure che abbiano un significativo impatto sulla protezione dei dati personali che l'Università intende adottare ai fini della tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Università stessa, anche a seguito di incidenti di sicurezza o analisi dei rischi;
b) adozione di policy e disciplinari in materia di protezione dei dati personali e sicurezza delle informazioni, redazione e aggiornamento dei disciplinari tecnici con impatto sulla sicurezza delle informazioni;
c) incidenti relativi alla sicurezza, compresi quelli che comportano la violazione di dati personali.

Pareri facoltativi

Possono essere richiesti pareri in ordine a:

a) progettazione di nuove applicazioni o modifica sostanziale di quelle esistenti, in aderenza al principio della privacy by design e by default;
b) valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 del Regolamento;
c) valutazione dell'eventuale pregiudizio che l'accesso civico potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alla tutela dei loro dati personali ai sensi dell'art. 5-bis co. 2 del D. Lgs. 33/2013 e, in via generale, del Regolamento;
d) opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti.

Le richieste di parere possono essere presentate dai designati al trattamento, per il tramite dell'Ufficio Legale, provvedimenti autorizzativi e disciplinari.

Laddove se ne ravvisi la necessità al Responsabile della Protezione dei dati possono essere attribuiti, con specifico contratto aggiuntivo, altri compiti e funzioni. Il titolare del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

6.7 Gruppo di lavoro trasversale in materia di privacy

E' stato creato un Gruppo di lavoro trasversale con i seguenti compiti:

a) supporta il Direttore Generale nella stesura del registro, attraverso la ricognizione periodica, dei trattamenti di dati personali effettuati dalle strutture dell'Ateneo tramite i responsabili interni;

b) assicura un presidio per le strutture dell'Università, studia e approfondisce gli aspetti normativi, organizzativi e procedurali e cura gli adempimenti derivanti dalle disposizioni normative vigenti;
c) collabora con le strutture per la risoluzione di problemi specifici e per la predisposizione della documentazione necessaria (a titolo di esempio informative, atti di contitolarità, ecc.);
d) formula proposte per la formazione in materia di protezione di dati personali;
e) coordina le richieste di parere al DPO formulate dai responsabili interni

6.8 Servizi informativi di Ateneo

I Servizi informativi di Ateneo svolgono i seguenti compiti:

a) adotta policy in materia di privacy e sicurezza informatica, con particolare riferimento all'utilizzo, alla sicurezza delle risorse informatiche e allo sviluppo delle applicazioni informatiche, da aggiornare periodicamente, ogni qualvolta l'evoluzione tecnica o normativa lo renda necessario; in particolare individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Università;
b) vigila sul corretto utilizzo della rete universitaria e controlla che il livello di sicurezza degli applicativi amministrativi sia adeguato ai rischi sui dati contenuti prevedendo la partecipazione del DPO e realizzando le verifiche raccomandate dallo stesso;
c) effettua le necessarie verifiche di sicurezza, avvalendosi, se necessario, del DPO;
d) gestisce gli incidenti di sicurezza, nelle modalità definite in apposito disciplinare, avvalendosi del DPO, qualora necessario;
e) supporta i responsabili interni nella valutazione di impatto e nella consultazione preventiva del Garante di cui agli artt. 35 e 36 del Regolamento;
f) partecipa nella valutazione dei rischi per i trattamenti informatici realizzati autonomamente dai Dipartimenti, in particolare al verificarsi di minacce di data-breach;
g) promuove la formazione di tutto il personale dell'Università in materia di sicurezza informatica, anche attraverso un piano di comunicazione e divulgazione all'interno dell'Università, coordinandosi con le azioni promosse dal DPO;
h) supporta il DPO mettendo a disposizione le proprie risorse strumentali e le proprie competenze.

7. Rinvio di norme

Per quanto non previsto si rinvia al Regolamento di Ateneo.