

POLICY ORGANIZZATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Emanata con Decreto Rettorale Rep. n. ----- Prot. n. ----- del -----

Entrata in vigore: -----

Sommario

1. Finalità della policy	2
2. Definizioni	2
3. Tipologie dei dati trattati dall'Università	2
4. Principi applicabili al trattamento dei dati	4
5. Ruoli e responsabilità	4
5.1 Ruoli previsti nel Regolamento	4
5.2 Titolare del trattamento	5
5.3 Designati al trattamento (Designati) e Referenti per il trattamento (Referenti)	6
5.4 Soggetti autorizzati al trattamento	8
5.5 Responsabili del trattamento	9
5.6 Responsabile della Protezione dei dati (DPO)	9
5.7 Ufficio Privacy	11
5.8 Direzione Servizi digitali integrati	12
5.9 Gruppo gestione incidenti ICT	12

1. Finalità della policy

Il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (di seguito “Regolamento”) e il D. Lgs. 196/03 e s.m.i (di seguito “Codice”) disciplinano la protezione dei dati personali, prevedendo molteplici obblighi a carico dei soggetti che trattano tali dati, ivi comprese le pubbliche amministrazioni.

Per garantire un’efficace protezione dei dati personali e dare attuazione ai suddetti obblighi, è opportuno definire una policy organizzativa in materia di protezione dei dati personali che definisca le tipologie dei dati trattati dall’Università, i principi applicabili al trattamento, nonché i ruoli e le rispettive competenze.

2. Definizioni

Il Regolamento, nell’art. 4, definisce:

- a) 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;
- b) trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di 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. 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 subordinato, parasubordinato o con rapporto di lavoro autonomo, ivi 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 studente e ai laureati, con particolare riferimento a:

- attività di orientamento;
- erogazione dei 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 protocollo e conservazione documentale;

- acquisto di 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 e alla ricerca (compresa la ricerca in ambito medico - sanitario).

4. 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).

5. Ruoli e responsabilità

5.1 Ruoli previsti nel Regolamento

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

- a) il 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) il responsabile del trattamento: definito dall'art. 4 del Regolamento come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- c) il 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) la persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile: figura che si desume implicitamente dalla definizione di "terzo" di cui al n. 10 del comma 1 art. 4 del Regolamento.

Il D. Lgs. 196/03 e s.m.i., nell'art. 2 *quaterdecies*, stabilisce che il titolare possa prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento dei dati personali siano attribuiti a persone fisiche espressamente designate.

5.2 Titolare del trattamento

Il titolare del trattamento di dati personali, ai sensi degli artt. 4 n. 7 e 24 del Regolamento, è l'Università degli Studi di Ferrara, nella persona del Rettore pro tempore, a cui spetta l'adozione di 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 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) designare, qualora opportuno, 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, con il supporto dei Designati al trattamento e 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.

5.3 Designati al trattamento (Designati) e Referenti per il trattamento (Referenti)

Il titolare, al fine di attuare gli adempimenti necessari per la conformità del trattamento dei dati personali al Regolamento e al Codice, può designare, con decreto rettorale, i seguenti Designati al trattamento (Designati), ciascuno per il proprio ambito di competenza:

- a) il Direttore Generale;
- b) i Dirigenti;
- c) i Direttori di Dipartimento;
- d) i Direttori dei Centri strategici.

Il Direttore Generale può designare, con proprio decreto, i seguenti Referenti per il trattamento (Referenti), ciascuno per il proprio ambito di competenza:

- a) i Responsabili di Ufficio e dei Poli bibliotecari;
- b) i Responsabili di Settore, nei casi in cui gli incarichi di responsabilità degli Uffici o dei Poli bibliotecari non siano attribuiti;
- c) i Responsabili delle strutture di coordinamento (Meta-strutture e IUSS);
- d) i Segretari Amministrativi di Dipartimento.

I Direttori di Dipartimento possono designare, con proprio decreto, i seguenti Referenti per il trattamento (Referenti), ciascuno per il proprio ambito di competenza:

- a) i Direttori dei Centri ordinari (dipartimentali e interdipartimentali);
- b) i Responsabili Scientifici dei Laboratori del Tecnopolo;
- c) specifici soggetti individuati dal Consiglio di Dipartimento.

Gli eventuali decreti di designazione di Referenti devono essere trasmessi per conoscenza all'Ufficio competente dell'Amministrazione centrale.

I Designati 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;

Il Direttore Generale, con il supporto dell'Ufficio privacy e degli eventuali Referenti, tiene il registro delle attività amministrative degli uffici dell'amministrazione centrale e dei dipartimenti che prevedono un trattamento di dati personali.

Ciascun Direttore di Dipartimento, con il supporto degli eventuali Referenti, tiene il registro delle attività di ricerca e di didattica che prevedono un trattamento di dati personali;

- b) effettuare una valutazione dei rischi connessi al trattamento dei dati, con il supporto della Direzione Servizi digitali integrati 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, del supporto dei soggetti autorizzati al trattamento e della Direzione Servizi digitali integrati;
- 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 della Direzione Servizi digitali integrati;
- e) comunicare alla Direzione Servizi digitali integrati, 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, e di nomina a Responsabile del trattamento, ai sensi dell'art. 28 del Regolamento;
- k) designare i Responsabili del trattamento, ai sensi dell'art. 28 del Regolamento, e determinare, congiuntamente a uno o più titolari del trattamento, le finalità e i mezzi del trattamento mediante accordi di contitolarità, in conformità all'art. 26 del Regolamento;

- l) adottare, se necessario, specifici Disciplinari tecnici di settore, anche congiuntamente con altri Designati, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi alla propria area di competenza;
- m) segnalare tempestivamente alla Direzione Servizi digitali integrati la violazione di dati personali, qualora ne venga a conoscenza;
- n) 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;
- o) provvedere, anche con il supporto degli incaricati, a dare riscontro alle istanze degli interessati inerenti all'esercizio dei diritti previsti dalla normativa;
- p) adottare i provvedimenti imposti dal Garante;
- q) 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;
- r) verificare la legittimità dei trattamenti effettuati nella struttura di riferimento;
- s) vigilare sull'attuazione delle istruzioni impartite ai soggetti autorizzati;
- t) collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
- u) garantire alla Direzione Servizi digitali integrati, al DPO e al gruppo di gestione incidenti ICT i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza.

I Designati possono delegare ai Referenti solo i compiti di cui ai punti f), g), h), i), j).

5.4 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, tecnopolo che effettuano operazioni di trattamento in relazione alle attività di propria competenza, e che operano sotto la diretta autorità del titolare o dei Designati/Referenti.

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/Referenti.

I soggetti autorizzati sono designati:

- a) tramite individuazione nominativa delle persone fisiche specificando i trattamenti che lo stesso è autorizzato ad effettuare;
- b) tramite assegnazione funzionale della persona fisica ad una unità organizzativa/gruppo/commissione, specificando i trattamenti che tale unità/gruppo/commissione 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 i Designati per rispondere alle istanze degli interessati inerenti all'esercizio dei diritti previsti dalla normativa;
- d) segnalare tempestivamente alla Direzione Servizi digitali integrati la violazione di dati personali, qualora ne venga a conoscenza;
- e) supportare il 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.

5.5 Responsabili 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 o provvedimento di designazione, 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.

5.6 Responsabile 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 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 Direzione Servizi digitali integrati 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 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 alle tutele 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 oppositori.

Le richieste di parere possono essere presentate dai Designati/Referenti, per il tramite dell'Ufficio competente dell'Amministrazione centrale. I pareri sono espressi nel rispetto delle seguenti codifiche:

NC: acronimo di "non conformità", nei casi in cui siano rilevati elementi di non conformità alla normativa e alle policy in materia di protezione dei dati personali;

OS: acronimo di "osservazione", nei casi in cui vi siano elementi di miglioramento che garantiscono una maggiore aderenza alla normativa e alle policy in materia di protezione dei dati personali, non costituendo vincolo di attuazione;

PO: acronimo di "positivo", nei casi in cui siano prospettati elementi valutati come conformi alla normativa e alle policy dell'Università in materia di protezione dei dati personali.

Nei casi in cui il DPO esprima pareri “NC” e “OS” il Designato/Referente deve formalizzare, nelle medesime forme utilizzate dal DPO per l’espressione del parere, le motivazioni che giustificano l’esecuzione dell’attività o l’implementazione della soluzione tecnologica in contrasto con le indicazioni fornite dal DPO.

I pareri espressi dal DPO sono conservati agli atti dall’Ufficio competente dell’Amministrazione centrale.

5.7 Ufficio privacy

L’Ufficio privacy svolge 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 Referenti;
- 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 Designati/Referenti.

5.8 Direzione Servizi digitali integrati

La Direzione Servizi digitali integrati svolge 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 sull’osservanza del Regolamento d’uso delle risorse informatiche, 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 Designati 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.

5.9 Gruppo gestione incidenti ICT

L'Università, con provvedimento del Direttore Generale, costituisce un gruppo di gestione incidenti ICT (G-ICT), composto da persone con competenze informatiche, giuridiche e in materia di pubbliche relazioni con lo scopo di gestire gli incidenti di sicurezza e i data breach dal punto di vista organizzativo, legale e tecnico.