UNIVERSITÀ DEGLI STUDI DI BRESCIA

DECRETO

Oggetto: Adozione dell'Organigramma Privacy di Ateneo

IL RETTORE

VISTI

- il D.Lgs. 30 giugno 2003, n. 196 s.m.i. "*Codice in materia di protezione dei dati personali*";
- il Regolamento UE 2016/679 (General Data Protection Regulation) del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (in seguito soltanto "GDPR");

RICHIAMATI

- lo Statuto dell'Università degli Studi di Brescia, emanato con D.R. del 6 febbraio 2024, n. 107;
- il Regolamento in materia di protezione dei dati personali, emanato con D.R. del 01 luglio 2024, n. 554;

RICHIAMATI, inoltre

- il D.R. 1241 del 21 Dicembre 2023 avente ad oggetto "*Designazione Responsabile della Protezione Dati (Data Protection Officer – RPD/DPO) – Liguria Digitale SpA*";
- il D.R. 1174 del 03 dicembre 2024 avente ad oggetto "*Aggiornamento nomina dei referenti del Responsabile della protezione dei dati (RPD) e degli addetti alla gestione del Registro dei Trattamenti per l'attuazione del Regolamento UE 2016/679 – GDPR*";
- il D.R. 195 del 14 marzo 2025 avente ad oggetto "*Designazione di tutto il personale dipendente tecnico-amministrativo, docente, contrattista di ricerca, collaboratore e altre forme contrattuali a "Persona autorizzata al trattamento di dati personali" ai sensi del Regolamento Generale sulla protezione dei dati personali n. 679/2016 e del D. Lgs. n.196/2003 (Codice Privacy) così come novellato dal D. Lgs. n.101/2018*";

PREMESSO che

- l'art. 24 del GDPR prescrive che "i*l titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*";
- tali misure includono "*l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento*" (art. 24, par. 2, GDPR);
- l'art. 2-quaterdecies del d.lgs. 196/20023 dispone, inoltre, che "*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.";*

DATO ATTO che, nella "*Relazione di Assessment iniziale dell'Università degli Studi di Brescia*" (prot.

108621 del 12 aprile 2024), il Responsabile per la Protezione dei Dati ha consigliato l'adozione di un documento relativo al sistema organizzativo privacy dell'Università degli Studi di Brescia;

PRECISATO che, anzitutto, l'Università ha emanato un Regolamento in materia di protezione dei dati personali (DR 554/2024) per definire i principi, i ruoli e compiti, nonché le modalità di trattamento dei dati personali all'interno dell'organizzazione;

RILEVATO che, a seguire, l'Università ha aggiornato le nomine dei referenti interni e disposto la designazione del personale come autorizzato al trattamento;

RAVVISATA la necessità di adottare anche un Organigramma Privacy che descriva l'organizzazione interna, le funzioni e le competenze di strutture, uffici e personale di ateneo nel trattamento dei dati personali;

VISTO l'Organigramma Privacy (Allegato 1) e ritenuto che lo stesso definisca adeguatamente la struttura e le competenze interne per i trattamenti dei dati personali effettuati dall'Università degli Studi di Brescia, tanto in qualità di titolare (art.24 GDPR) quanto di responsabile del trattamento (art. 28 GDPR);

EVIDENZIATO che il documento è stato condiviso con il Responsabile per la Protezione dei Dati;

DECRETA

- di adottare l'Organigramma Privacy (Allegato 1), parte integrante e sostanziale del presente provvedimento;
- di disporre la pubblicazione dell'Organigramma Privacy e darne ampia diffusione all'interno dell'Ateneo.

Brescia, data protocollo

IL RETTORE
(Prof. Francesco Castelli)

Firmato digitalmente da Francesco Castelli
Data: 15.05.2025 21:35:52 CEST
Organizzazione: UNIVERSITA' DEGLI STUDI DI BRESCIA/0177371017

F.to digitalmente ex art. 24 D.Lgs 82/05

UNIVERSITÀ DEGLI STUDI DI BRESCIA

ORGANIGRAMMA PRIVACY E DISPOSIZIONI PER I REFERENTI PRIVACY

Scopo

Lo scopo del presente documento è illustrare l'**Organigramma Privacy** e le disposizioni per i Referenti Privacy dell'Università degli Studi di Brescia (a seguire "Università" o "Ateneo"), aggiornato in base alle disposizioni in materia di trattamento dei dati personali ai sensi del Regolamento Generale sulla protezione dei dati personali n.679/2016 (per brevità, "GDPR" o "Regolamento"), del D.lgs. n.196/2003, così come novellato dal D.lgs. n.101/2018 e delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati.

Compiti e responsabilità

Quanto contenuto nella presente disposizione organizzativa esplicita i compiti e le responsabilità delle funzioni rappresentate nell'Organigramma Privacy.

Le istruzioni contenute nel presente documento si applicano quando l'Università opera in qualità di Titolare del Trattamento e/o di Responsabile del Trattamento.

Principale documentazione di riferimento

- Statuto di autonomia
- Regolamento in materia di protezione dei dati personali
- Regolamento dei servizi informatici e di rete
- Procedura di gestione dell'esercizio dei diritti dell'interessato
- Procedura di gestione delle violazioni (Data Breach)
- Linee guida "Rispetto e gestione del segreto d'ufficio nell'attività amministrativa"
- Designazione del personale autorizzato al trattamento
- Designazione dei referenti RPD
- Procedura "Accesso alle immagini di videosorveglianza"

Struttura organizzativa

In conformità al dettato normativo e sulla base dell'organizzazione aziendale vigente, l'Organigramma Privacy si articola nelle figure di seguito descritte:

1. Titolare del Trattamento;
2. Responsabile del Trattamento;
3. RPD – Responsabile della Protezione dei Dati;
4. U.O.C. Protezione Dati, Anticorruzione e Trasparenza;
5. Referente Privacy;
6. Referente per la ricerca;
7. Comitato Etico per la Ricerca di Ateneo;
8. Servizi ICT;
9. Persona autorizzata al trattamento dei dati personali;
10. Amministratore di Sistema.

Inoltre, sono previste le seguenti attività a dimostrazione dell'accountability aziendale:

11. Formazione Privacy;
12. Misure di sicurezza generali;
13. Misure minime di sicurezza AgID (circolare AgID 2/2017);
14. Tavoli di lavoro;
15. Disciplina del trasferimento dei dati personali al di fuori del SEE.

1. Titolare del Trattamento

Secondo quanto previsto dall'art. 4, punto 7, del Regolamento, il Titolare del Trattamento è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che determina le finalità e i mezzi del trattamento dei dati personali*".

L'Università agisce in qualità di Titolare del Trattamento quando assume ogni decisione in ordine alle finalità e modalità di trattamento sui dati oggetto del trattamento stesso; inoltre, al Titolare compete la messa in atto di misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al dettato normativo.

Qualora l'Università decida di affidare all'esterno determinati servizi che prevedono il trattamento di dati personali di cui detiene la titolarità (es. dati personali dei dipendenti, studenti, ..), l'Università è tenuta a nominare il fornitore quale Responsabile del Trattamento mediante apposito atto giuridico (art. 28 del Regolamento).

La Titolarità è esercitata dal legale rappresentante *pro tempore*, quindi dal Rettore o dalla Rettrice in carica.

2. Responsabile del Trattamento

Il Responsabile del Trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che trattano dati personali per conto del Titolare del Trattamento (art. 4, punto 8, del Regolamento).

L'Università agisce in qualità di "Responsabile del Trattamento" quando tratta dati personali per conto di altri soggetti che detengono la titolarità dei dati; anche in questo caso, la nomina dell'Università quale Responsabile del Trattamento avviene mediante atto giuridico.

3. RPD – Responsabile della Protezione dei Dati

Ai sensi dell'art. 37 del Regolamento, il Titolare del trattamento ha nominato il Responsabile della Protezione dei Dati (in seguito "RPD") o anche Data Protection Officer (DPO).

I dati di contatto del RPD sono inseriti nelle informative sul trattamento dei dati, pubblicate sul sito internet (https://www.unibs.it/it/protezione-dati-personali).

Il Responsabile della Protezione dei Dati ha il compito di informare e fornire consulenza al Titolare del Trattamento in merito agli obblighi normativi, fungere da punto di contatto con l'Autorità di Controllo e gli interessati, assicurare l'osservanza del Regolamento, delle normative in materia di protezione dei dati e delle politiche attuate dal Titolare.

Nell'esecuzione dei propri compiti il RPD è tenuto a:

- informare e fornire consulenza al Titolare del Trattamento, ai referenti, ai responsabili nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- vigilare sull'osservanza del Regolamento, di altre disposizioni nazionali o dell'Unione Europea relative alla protezione dei dati nonché delle politiche del Titolare 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, anche per il tramite dei Referenti;
- fornire parere in merito alla Valutazione d'impatto sulla protezione dei dati;
- cooperare con l'Autorità di Controllo;
- fungere da punto di contatto con il Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del Regolamento, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Oltre a questo, il Responsabile per la Protezione dei Dati provvede a:

- relazionare sull'attività svolta e sullo stato di attuazione in Ateneo della normativa sulla protezione dei dati personali, redigendo report settimanali;
- in caso di *data breach* svolgere i compiti previsti dalla relativa procedura di Ateneo.

4. U.O.C. Protezione Dati, Anticorruzione e Trasparenza

La U.O.C. Protezione Dati, Anticorruzione e Trasparenza (in seguito anche solo "U.O.C. Protezione Dati") è la struttura interna di riferimento in merito alla protezione dei dati personali e ha il compito di supportare l'Ateneo negli adempimenti previsti dalla normativa vigente e opera in sinergia con il RPD.

In questo ambito, le principali attività della struttura sono:

- rendere consulenza tramite *helpdesk* per la corretta gestione dei dati personali di Ateneo nel rispetto del GDPR;
- collaborare e supportare il RPD nello svolgimento delle attività di competenza di quest'ultimo;
- supportare gli uffici di ateneo per la corretta tenuta del registro di trattamento (GDP Cineca);
- aggiornare la regolamentazione interna e rendere le indicazioni in materia di protezione dei dati;
- monitorare la corretta attuazione della normativa in materia di trattamento dati;
- elaborare schede ed approfondimenti su novità giuridico-amministrative in tema di protezione dei dati.

Oltre a questo, la U.O.C. Protezione Dati, Anticorruzione e Trasparenza supporta il RPD nella

verifica dei risultati dei rispettivi *audit* per favorire la compliance in un'ottica di miglioramento continuo.

5. Referente Privacy

Attribuzione di funzioni e compiti a "Referente Privacy"

Il Titolare del Trattamento ha previsto, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la sua autorità (*Art. 2-quaterdecies*, Attribuzione di funzioni e compiti a soggetti designati, D.lgs. n.196/2003 così come novellato dal D.lgs. n.101/2018).

Sono nominati Referenti Privacy i dirigenti responsabili di Settore, i funzionari responsabili di Servizio e i responsabili di U.O.C. afferenti alla Direzione Generale (*Art. 2-quaterdecies*, Attribuzione di funzioni e compiti a soggetti designati, D.lgs. n.196/2003 così come novellato dal D.lgs. n.101/2018).

Il Referente Privacy assicura che le attività di trattamento dei dati avvengano nel rispetto della normativa in tema di protezione dei dati personali, impegnandosi a mantenere la riservatezza rispetto a tutte le informazioni apprese durante lo svolgimento dei compiti a esso assegnati.

Il Referente Privacy, in ossequio alle proprie funzioni e responsabilità, ha l'onere e il dovere di:

a) conoscere e rispettare la normativa in materia di protezione dei dati personali;
b) osservare il patto di riservatezza e le istruzioni impartite dal titolare del trattamento;
c) vigilare sul rispetto della normativa e delle istruzioni impartite da parte dei dipendenti e collaboratori afferenti alla struttura di cui sono responsabili;
d) adottare le opportune misure di sicurezza per garantire la protezione dei dati personali trattati nell'ambito della struttura di cui sono responsabili;
e) provvedere, se incaricati, alla tenuta e all'aggiornamento del registro dei trattamenti di cui all'art. 30 del Regolamento. Laddove non autorizzati ad agire sul registro dei trattamenti, comunicare all'RPD e al Titolare del Trattamento gli elementi essenziali del trattamento da inserire, aggiornare o cancellare;
f) tenere e aggiornare gli archivi di dati personali, cartacei e informatizzati, e dei server attivi gestiti in maniera autonoma dalla struttura di cui sono referenti;
g) aggiornare la modulistica di propria competenza;
h) nel caso di strutture didattiche e di ricerca, vigilare sul rispetto degli adempimenti previsti dall'Ateneo in materia di mappatura dei progetti di ricerca;

i) qualora riceva segnalazioni di violazione di dati personali, darne tempestiva comunicazione all'RPD e al titolare del trattamento con le modalità previste dalla procedura di *Data Breach*;
j) formulare proposte al Titolare del trattamento circa i bisogni formativi del personale della propria struttura;
k) partecipare alle sessioni informative, formative e di sensibilizzazione in materia di protezione dei dati personali;
l) segnalare al Titolare del Trattamento e all'RPD ogni variazione organizzativa che può avere un impatto sulle modalità di trattamento dei dati;
m) per i trattamenti che hanno come base giuridica il consenso, predisporre le misure organizzative atte a dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei dati personali, sulla base del principio di accountability ai sensi dell'art. 7, par. 1, del Regolamento;
n) nominare personale autorizzato al trattamento dei dati coloro che hanno rapporti di servizio, collaborazione, studio e ricerca con la struttura di riferimento, qualora le sottese attività siano connesse al trattamento di dati personali. A tal fine si avvale di uno schema tipo di autorizzazione, trasmettendo agli autorizzati le correlate istruzioni, anche mediante procedure informatiche.

Sempre nell'ambito delle sue funzioni, il Referente Privacy è tenuto a:

- informare tempestivamente il RPD, la U.O.C. Protezione Dati e i Servizi ICT quando, in considerazione della natura dei dati o, comunque, delle modalità del trattamento o degli effetti che esso può determinare, ritenga vi sia il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati;
- garantire l'adozione, nel trattamento dei dati personali, di tutte le misure di sicurezza indicate e quelle che successivamente verranno presentate in aggiornamento a quelle previste oggi dal Titolare, in particolare:
  a) comunicare immediatamente al RPD e alla U.O.C. Protezione Dati tutte le iniziative, non rientranti nella normale gestione dei dati e di ogni fatto e circostanza rilevante occorsa nel trattamento dei dati;
  b) fornire al RPD, a semplice richiesta e secondo le modalità indicate, tutte le informazioni relative all'attività svolta, al fine di consentirne l'attività di controllo; più in generale, prestare la più ampia e completa collaborazione al RPD al fine di compiere quanto sia necessario e opportuno in relazione agli adempimenti imposti dalla normativa in materia di trattamento di dati personali;
  c) verificare che vengano applicate efficacemente le misure di sicurezza adottate in conformità alla normativa di protezione dei dati personali e segnalare al RPD, alla U.O.C. Protezione Dati e ai Servizi ICT eventuali circostanze che rendano necessario o opportuno l'aggiornamento delle predette misure di sicurezza al fine

di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Le prescrizioni impartite al Referente Privacy sono valide per le/i attività/trattamenti svolte/effettuati dall'Università in qualità di Titolare e analogamente per quelle/i affidate/i all'Università in qualità di Responsabile del Trattamento. In questa ultima fattispecie, qualora si riscontrassero disallineamenti tra quanto prescritto dalle istruzioni del Titolare e le prassi o procedure aziendali, occorre richiedere chiarimenti al RPD, alla U.O.C. Protezione Dati e ai Servizi ICT.

Obblighi nell'ambito dei rapporti con le persone autorizzate

Il Referente Privacy deve far adottare e far rispettare dalle persone autorizzate al trattamento, che risultino sottoposte al suo coordinamento, le opportune misure di sicurezza previste dalla normativa in materia di trattamento dei dati personali, per ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità del trattamento.

A tale scopo dovrà assicurarsi che ciascuno riceva ed esegua opportune istruzioni sulle modalità pratiche di trattamento dei dati, tra cui:

a) raccogliere e in qualsiasi modo trattare dati personali non oltre quanto necessario alle esigenze ed allo svolgimento delle proprie mansioni/attività lavorative;
b) comunicare dati personali ai soli soggetti indicati nel Registro del Trattamento;
c) conservare i supporti informatici e/o cartacei contenenti dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
d) effettuare una comunicazione al RPD, alla U.O.C. Protezione Dati e ai Servizi ICT nel caso di incidente di sicurezza, di una violazione o sospetta violazione dei dati personali e seguire scrupolosamente le relative procedure;
e) comunicare al RPD, se viene a conoscenza del fatto che uno o più persone autorizzate al trattamento dei dati personali abbiano violato la normativa in materia di trattamento dei dati personali e/o le istruzioni ricevute dal Titolare, cui sono essi tenuti in base alla relativa autorizzazione o abbiano commesso fatti gravi che possano pregiudicare la sicurezza di dati o banche dati, affinché vengano adottate tutte le misure preventive e/o riparatorie necessarie. Nel caso in cui si verifichino violazione o fatti gravi, il RPD avvisa la Direzione Generale.

Obblighi nell'ambito dei rapporti con gli interessati

a) assicurare che le persone debitamente autorizzate ai sensi della normativa sul trattamento dei dati personali, che risultano sottoposte al suo coordinamento e che sono sotto la sua area di responsabilità, supportino il RPD per la gestione dell'esercizio dei diritti degli interessati ai sensi degli artt. 15 e ss. del Regolamento (tra cui le richieste di opposizione al trattamento, di limitazione, di rettifica dei dati

o di loro cancellazione) nei tempi e nei modi previsti dalle norme e dalle procedure aziendali. Qualora uno o più interessati denunci situazioni o fatti rilevanti di particolare gravità, il Referente Privacy dovrà informarne tempestivamente la U.O.C. Protezione Dati e il RPD e adottare tutte le misure precauzionali e/o riparatorie necessarie;

b) assicurare, qualora necessario, per le attività per le quali l'Università riveste il ruolo di Titolare del Trattamento, che le persone debitamente autorizzate rendano all'interessato l'informativa e, ove necessario, ottengano il consenso al trattamento dei dati. Per le attività per le quali l'Università riveste il ruolo di Responsabile del trattamento, assicurare che le persone autorizzate rilascino l'informativa fornita e redatta dal Titolare del Trattamento, secondo le modalità indicate dallo stesso.

L'attività del Referente Privacy potrà essere oggetto di confronto e verifica da parte del RPD allo scopo di assicurarne la conformità alla presente disposizione organizzativa, alle istruzioni e alla normativa in materia di trattamento dei dati personali.
Si ricorda che l'inosservanza di quanto sopra può costituire violazione dei doveri di ufficio e comportare sanzioni disciplinari sulla base del vigente contratto di lavoro. In caso di sanzioni amministrative e di pagamento di danni agli interessati, il Titolare potrebbe rivalersi sui singoli per danno erariale.

6. Referente per la ricerca

Il Titolare ha ritenuto di individuare un referente RPD per la ricerca per ciascun Dipartimento.
I Referenti per la ricerca sono docenti o ricercatori afferenti ai singoli dipartimenti e nominati con Decreto Rettorale, dietro indicazione del Direttore di Dipartimento.
I Referenti per la ricerca contribuiscono a sensibilizzare il personale docente afferente ai rispettivi dipartimenti per la protezione dei dati personali nell'attività di ricerca scientifica; in particolare a:

a) conoscere e rispettare la normativa in materia di protezione dei dati personali;
b) osservare il patto di riservatezza e le istruzioni impartite dal titolare del trattamento;
c) costituire un punto di riferimento per il personale docente e ricercatore del rispettivo Dipartimento per la protezione dei dati personali nello svolgimento della ricerca scientifica;
d) collaborare con il RPD e con l'U.O.C. Protezione Dati attenzionando casi specifici;
e) collaborare al rispetto degli adempimenti previsti dall'Ateneo in materia di mappatura dei progetti di ricerca;
f) qualora vengano a conoscenza di una violazione di dati personali, darne tempestiva comunicazione al RPD, alla U.O.C. Protezione Dati e ai Servizi ICT con le modalità previste dalla procedura di *Data Breach*;

g) formulare proposte al Titolare del trattamento circa i bisogni formativi del personale docente del proprio dipartimento;
h) partecipare alle sessioni informative, formative e di sensibilizzazione in materia di protezione dei dati personali, soprattutto relative allo svolgimento dell'attività di ricerca.

7. Comitato Etico per la Ricerca di Ateneo

Il Comitato Etico per la Ricerca di Ateneo (CERA) è un organismo indipendente costituito presso l'Università degli Studi di Brescia, secondo criteri di competenza e interdisciplinarità. Opera nel rispetto della normativa vigente, conformemente ai princìpi etici, giuridici e deontologici contenuti nei documenti nazionali, comunitari e internazionali in materia di ricerca scientifica, con la finalità di salvaguardare, nell'àmbito delle attività di ricerca di Ateneo:

a) i diritti, la dignità, l'integrità e il benessere degli esseri umani coinvolti;
b) il rispetto di ogni altro organismo vivente;
c) il rispetto dell'ambiente in ogni sua dimensione e componente;
d) l'integrità, la libertà e la promozione della scienza.

Fornisce pareri, valutazioni e verifiche su richiesta del/della Responsabile scientifico/a di una ricerca, al fine di assicurare che quest'ultima sia condotta in accordo con i princìpi etici definiti in sede internazionale e nazionale e dal Codice etico interno.

Pur non avendo competenze dirette in materia di protezione dei dati personali, si coordina con la UOC Protezione Dati per promuovere una corretta tutela della privacy nello svolgimento dell'attività di ricerca scientifica.

8. Servizi ICT

La struttura Servizi ICT gestisce i sistemi informatici di Ateneo e garantisce la sicurezza delle informazioni. Tra l'altro, i Servizi ICT provvedono a:

- definire, implementare, e mantenere il programma di governance e la struttura per la gestione della sicurezza delle informazioni;
- definire *policy* di sistema per il *backup* e *Disaster Recovery*;
- gestire, progettare e condurre i *Data Center* e i sistemi per il *backup* e *Disaster Recovery*;
- implementare le politiche interne di sicurezza informatica;
- collaborare alle analisi di impatto della introduzione e sviluppo di sistemi informatici;
- monitorare con costanza i bollettini di vulnerabilità e i sistemi informatici ai fini della sicurezza informatica;

- supportare gli utenti e essere riferimento tecnico nella gestione di incidenti informatici su segnalazioni esterne (GARR, autorità di polizia, ecc.) o interne;
- condurre iniziative di formazione, informazione e verifica sulle problematiche di sicurezza informatica verso gli utenti;
- provvedere, almeno annualmente, all'aggiornamento delle relative modalità di implementazione delle prescrizioni della Circolare AgID 2/2017 "*Misure minime di sicurezza ICT per le pubbliche amministrazioni" con il supporto delle Strutture coinvolte.*

Secondo quanto previsto da apposita procedura, la struttura Servizi ICT è coinvolta nella gestione di eventuali *data breach* svolgendo i seguenti compiti:

- valutare le minacce ed elaborare un piano di intervento in caso di attacchi, incidenti informatici e *Data Breach* (violazione di dati personali);
- supportare il RPD e l'U.O.C. Protezione Dati nella valutazione di eventuali segnalazioni di *Data Breach* che riguardano la sicurezza informatica seguendo scrupolosamente le relative procedure;
- provvedere, in caso di *Data Breach* inerente la sicurezza informatica, a mettere in atto le procedure di gestione del rischio e le misure tecniche adeguate per minimizzare gli impatti negativi sui diritti e le libertà fondamentali delle persone fisiche.

9. Persona autorizzata al trattamento dei dati personali

I soggetti autorizzati al trattamento dei dati personali ("Autorizzati") operano sotto la diretta autorità del Referente ed effettuano, con riferimento alle attività di propria competenza, i trattamenti dei dati personali nel rispetto delle misure di sicurezza previste e delle istruzioni ricevute.

Gli Autorizzati sono tenuti a:

a) trattare i dati personali in modo lecito e corretto, mantenendo assoluto riserbo sui dati stessi e attenendosi alle istruzioni fornite dall'Università o dai/dalle Referenti Privacy;
b) utilizzare le sole banche dati ed i soli strumenti ai quali si è preventivamente autorizzati;
c) trattare esclusivamente i dati necessari allo svolgimento della mansione lavorativa e non trattare o diffondere alcun tipo di informazione di cui si è in possesso per motivi di servizio al di fuori di quanto strettamente necessario per lo svolgimento dell'attività;
d) non condividere, comunicare, inviare dati personali a persone che non ne necessitano per lo svolgimento delle proprie attività svolte nell'ambito dell'Ateneo (anche se queste persone sono a loro volta autorizzate al

trattamento); non comunicare i dati personali all'esterno dell'Università e comunque a soggetti terzi, se non previa autorizzazione;

e) conservare i dati personali per un periodo di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
f) non acquisire dati e informazioni che non siano di competenza della propria unità organizzativa/struttura e strettamente necessari allo svolgimento della propria attività professionale, anche qualora essi risultino tecnicamente accessibili;
g) non lasciare incustoditi o accessibili a terzi non autorizzati gli strumenti elettronici mentre è in corso una sessione di lavoro;
h) custodire e non divulgare né cedere a terzi le proprie credenziali di autenticazione;
i) procedere all'archiviazione definitiva, nei luoghi predisposti, dei supporti cartacei e dei supporti magnetici una volta terminate le ragioni della consultazione;
j) non asportare in alcun modo i supporti informatici o cartacei contenenti dati personali degli/delle Interessati/e, senza la preventiva autorizzazione del/la Titolare e/o del/la Referente;
k) osservare scrupolosamente tutte le misure di sicurezza già predisposte, o che saranno successivamente comunicate dal/la Titolare e/o dal/la Referente, in particolare per quanto riguarda i trattamenti effettuati da ciascun soggetto autorizzato;
l) non modificare i trattamenti in essere senza specifica indicazione del/la Titolare e/o del/la Referente;
m) seguire la formazione di base disponibile per il personale strutturato sulla piattaforma "Moodle";
n) rispettare il "*Regolamento di utilizzo dei servizi informatici e di rete*";
o) trattare dati personali unicamente sulle cartelle di rete messe a disposizione dall'Ateneo;
p) rispettare tutte le misure di sicurezza previste per poter garantire la confidenzialità, disponibilità, integrità dei dati trattati;
q) informare il/la Titolare e/o il/la Referente nel caso si verifichino incidenti relativi alla sicurezza delle informazioni trattate;
r) in caso di violazione della sicurezza, che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati personali trasmessi, conservati o comunque trattati (art. 4, par. 12, del Regolamento) attivarsi nel rispetto della "Procedura per la gestione delle violazioni di dati personali (Personal Data Breach)" adottata dall'Università e consultabile alla pagina https://www.unibs.it/it/protezione-dati-personali;
s) adottare e rispettare le seguenti regole di "scrivania pulita": al termine del lavoro o durante lunghe pause, non deve essere lasciata alcuna documentazione riservata sulle scrivanie (documentazione cartacea) o su supporti rimovibili (documentazione digitale);

Con riferimento alla documentazione cartacea, gli autorizzati sono tenuti a:

a) stampare dati personali solo se strettamente necessario per l'esecuzione dei trattamenti;

b) custodire il materiale cartaceo contenente dati personali e aziendali affinché nessun terzo non autorizzato possa prenderne visione, possa manipolarlo o riprodurlo;
c) custodire il materiale cartaceo contenente categorie particolari di dati personali in archivi e/o stanze dotati/e di chiusura a chiave;
d) non lasciare documenti incustoditi presso la propria postazione (o comunque altre scrivanie, tavoli di lavoro) qualora sia previsto un allontanamento per un lasso di tempo tale da consentirne eventualmente la visione da parte di terzi non autorizzati;
e) custodire i dati oggetto del trattamento in luoghi non accessibili a personale non autorizzato;
f) distruggere il materiale cartaceo in modo da non rendere comprensibile il contenuto del documento.

Tutti coloro che trattano dati personali nell'ambito del rapporto con l'Ateneo sono comunque ritenuti autorizzati al trattamento dei dati e sono obbligati a osservare quanto previsto dal presente articolo anche in assenza di formale designazione.

Si ricorda inoltre che gli obblighi relativi alla riservatezza e alla protezione dei dati personali dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro e che tale autorizzazione cesserà automaticamente con il venir meno del rapporto intercorrente tra l'Università e il dipendente.

10. Amministratore di Sistema

Come previsto dal Provvedimento del Garante del 27 novembre 2008, l'Amministratore di Sistema è "*una figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali*".

L'attribuzione delle funzioni di Amministratore di Sistema avviene 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.

Gli estremi identificativi delle persone fisiche Amministratori di Sistema, con l'elenco delle funzioni ad essi attribuite, sono riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

11. Formazione Privacy

La normativa privacy prevede l'obbligo di formare tutte le figure presenti a vario titolo nell'organizzazione. L'Università garantisce la formazione obbligatoria in materia privacy somministrando corsi di formazione proposti dal RPD e dal U.O.C. Protezione Dati.

12. Misure di sicurezza generali

Misure per garantire la protezione dei dati

Sono le misure di sicurezza volte a minimizzare i rischi che le informazioni siano rivelate o modificate senza autorizzazione, ovvero perse o alterate accidentalmente o intenzionalmente.

Queste comprendono un sistema di autenticazione per assicurare che la persona che accede al sistema nelle sue diverse articolazioni sia identificata con certezza, basato su codice identificativo e password individuale segreta, nonché un sistema di autorizzazione che preveda che a ciascuna persona che accede al sistema sia assegnato un profilo di accesso che definisca i dati ai quali l'utente è autorizzato ad accedere e, ove applicabile, le operazioni che per ciascun dato o gruppo di dati è autorizzato ad eseguire (consultazione, inserimento, modifica, cancellazione).

Per ridurre i rischi di indisponibilità (parziale o totale) nell'accesso al sistema informatico dell'Ente, sono previste una serie di attività, in particolare al momento dell'assunzione o della dimissione del personale, con la procedura di attivazione o dismissione dell'utenza personale. Sempre al fine di controllo, si procede a verificare che la lista dei dipendenti cessati sia coerente con le utenze disabilitate.

Scrivania sgombra e schermo inattivo (clean desk & clear screen Policy)

La politica della scrivania sgombra (*Clean Desk Policy*) e dello schermo inattivo (*Clear Screen Policy*) è una delle migliori strategie da attuare per ridurre il rischio di violazioni della sicurezza della postazione di lavoro.

Lo scopo di tale politica è stabilire requisiti minimi per prevenire violazioni accidentali o dolose dei dati personali (*Data Breach*) e responsabilizzare i soggetti che nelle attività lavorative si trovano a loro contatto.

Livelli di sicurezza

L'amministrazione della sicurezza logica segue i seguenti criteri generali:

- applicazione del principio “need to know” o del minimo privilegio, secondo cui la definizione dei profili standard da assegnare agli utenti, con le autorizzazioni necessarie all’espletamento delle rispettive mansioni (definite per ruoli e competenze), avviene alla luce delle effettive esigenze operative. A tal scopo viene limitato l’accesso logico a reti, sistemi e basi dati;
- la validità delle richieste di accesso alla rete è verificata automaticamente dal sistema stesso prima di consentire l’accesso ai dati, tramite un sistema di autenticazione costituito da User-ID e password;
- sono adottate delle indicazioni per la gestione delle password che indicano la lunghezza, la complessità, la durata, la conservazione sicura richiesta nel caso di trattamenti dei dati effettuati con strumenti elettronici;
- sono previsti sistemi per la periodica validazione e il censimento delle utenze e delle abilitazioni;
- sono adottate tecniche e metodologie per la verifica continua dell’utilizzo dei sistemi applicativi e per il controllo del traffico di rete generato, al fine di garantire un pronto intervento in caso di attività anomale;
- sono previsti presidi rafforzati per l’accesso da remoto, in particolare nei confronti di utenti appartenenti a soggetti terzi;
- è prevista la revisione periodica delle misure di sicurezza, anche attraverso esercizi di *penetration test*, al fine di prevenire violazioni dei dati personali (*Data Breach*);
- sono organizzate sessioni di formazione dei dipendenti, nonché regolamenti e altre forme di documentazione interna, al fine di rendere gli stessi edotti dei rischi in materia di sicurezza delle informazioni e di protezione dei dati personali;
- sono previsti periodici controlli al fine di verificare l’adeguatezza, l’affidabilità complessiva e la tutela del sistema informativo.

13. Misure minime di sicurezza ICT AGID per le pubbliche amministrazioni

Oltre a quanto previsto nel paragrafo precedente, l’Università rispetta le prescrizioni della Circolare AgID 2/2017 “Misure minime di sicurezza ICT per le pubbliche amministrazioni”. Queste indicazioni possono essere assunte come “stato dell’arte” per la protezione dei dati personali di cui all’art. 32 del Regolamento.

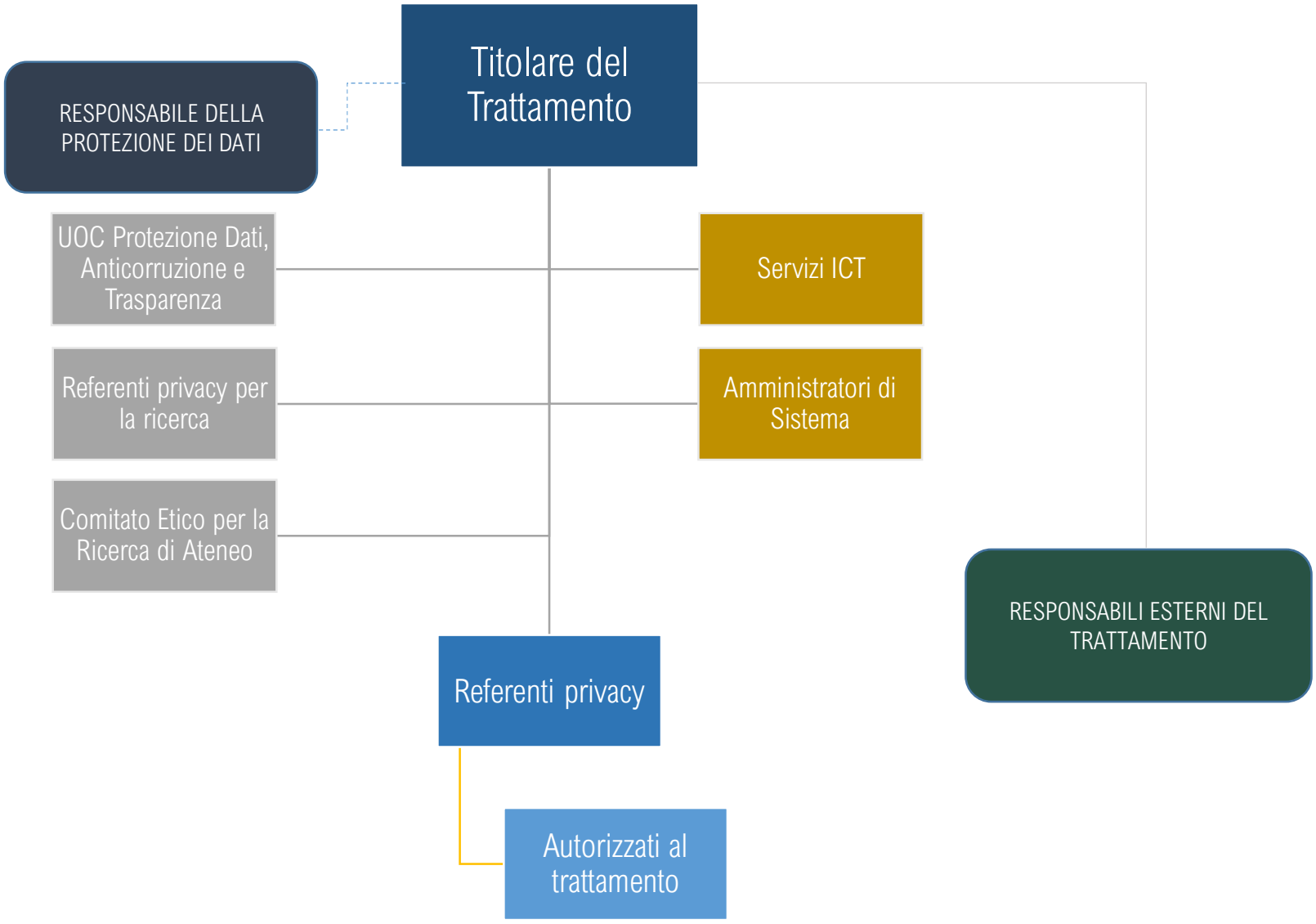
È compito dei Servizi ICT provvedere, almeno annualmente, all’aggiornamento delle relative modalità di implementazione con il supporto delle Strutture coinvolte.

14. Tavoli di lavoro

Per favorire l'adeguamento dell'Università alla normativa privacy vigente possono essere istituiti dei Tavoli di Lavoro che si occupino di tematiche relative alla Privacy, Tecnologia e Sicurezza.

15. Disciplina sul trasferimento dei dati al di fuori dello Spazio Economico Europeo

Ai sensi dell'art. 44 GDPR, i trasferimenti al di fuori del SEE sono generalmente vietati, a meno che non intervengano specifiche garanzie.

L'Università, qualora agisca in qualità di Titolare del trattamento, deve assicurarsi che eventuali fornitori esteri o che utilizzano servizi erogati da aziende estere, garantiscano l'adeguatezza della protezione dei dati, rimanendo responsabile nei confronti degli interessati in caso contrario.

UNIVERSITÀ DEGLI STUDI DI BRESCIA