DECRETO RETTORALE

Dati desumibili da registrazione a protocollo:
Numero Repertorio, Numero di Protocollo, Titolo,
Classe Fascicolo Allegati e Riferimenti
MP/AA

Oggetto: Decreto rettorale di emanazione del Regolamento in materia di protezione dei dati personali dell'Università degli studi di Bergamo.

IL RETTORE

PREMESSO che il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (abrogativo della vigente direttiva 95/46 CE) ha introdotto un nuovo quadro giuridico nella materia della protezione dati personali applicabile dal 25 maggio 2018 ai sensi di quanto disposto dall'Art. 99, paragrafo 2 del Regolamento (UE) 2016/679;

PREMESSO che la piena applicazione della normativa europea determina la necessità per gli Stati dell'Unione di adeguare la vigente legislazione interna in materia di tutela dati personali, oltre che la necessità da parte di tutti i soggetti/operatori, pubblici o privati che trattano dati personali di ottemperare alle nuove prescrizioni europee;

VISTO il Regolamento Europeo 679/2016 (cd GDPR), direttamente efficace e vincolante per gli Stati membri, che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché le norme relative alla libera circolazione di tali dati;

VISTO il D.lgs. 196/2003 come novellato dal D.lgs. n. 101/2018 (cd Codice privacy) che lo ha adeguato alla disciplina europea per garantire che il trattamento dei dati si svolga nel rispetto dei diritti e delle libertà fondamentali nonché della dignità dell'interessato con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali;

VISTO l'art. 19 dello Statuto che disciplina le attribuzioni specifiche del Consiglio di Amministrazione;

DATO ATTO che le principali novità introdotte dal Regolamento (UE) 2016/679 sono da collegarsi sostanzialmente alla centralità del principio di responsabilizzazione ex art. 5, paragrafo 2 del Regolamento (accountability nella accezione inglese), che può tradursi nell'adozione di comportamenti proattivi e tali da dimostrare la concreta definizione di misure finalizzate ad assicurare l'applicazione del regolamento" (così il Garante per la Protezione dei Dati personali nella sua Guida all'applicazione del Regolamento europeo);

CONSIDERATO che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale e che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;

CONSIDERATA l'opportunità che l'Università si doti di un regolamento in materia di protezione dei dati personali per disciplinare gli aspetti relativi al trattamento sui quali la normativa comunitaria e nazionale rimette alla discrezionalità dell'Ente;

VISTA la delibera del Consiglio di amministrazione 30.7.2021 che ha approvato il Regolamento in materia di protezione dei dati personali;

VISTO l'art. 12 dello Statuto che disciplina l'approvazione e emanazione dei Regolamenti di Ateneo e le loro modifiche;

DECRETA

Art. 1

E' emanato il **Regolamento in materia di protezione dei dati personali dell'Università degli studi di Bergamo**, nel testo approvato dal Consiglio di Amministrazione nella seduta del 30.7.2021 ed allegato al presente decreto.

Art. 2

Il presente decreto è pubblicato sul sito web dell'Università nella sezione "Albo di Ateneo" ed entra in vigore con decorrenza immediata.

Art. 3

Il testo del predetto Regolamento è contestualmente pubblicato sul sito web dell'Università al seguente pagina: Università > Statuto e regolamenti> Regolamenti >interesse generale.

Bergamo, *come da registrazione di protocollo*

IL RETTORE
Prof. Sergio Cavalieri

Firmato digitalmente da: Sergio Cavalieri
Limitazioni d'uso: Explicit Text: Il titolare fa uso del presente certificato solo per le finalità di lavoro per le quali esso è rilasciato. The certificate holder must use the certificate only for the purposes for which it is issued.
Data: 21/12/2023 14:43:14

REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI DELL'UNIVERSITÀ DEGLI STUDI DI BERGAMO

SEZIONE I - PRINCIPI E DISPOSIZIONI GENERALI

SEZIONE II MODELLO ORGANIZZATIVO INTERNO

SEZIONE I - PRINCIPI E DISPOSIZIONI GENERALI

Articolo 1 - Oggetto

L'Università degli studi di Bergamo adotta il presente Regolamento quale misura organizzativa necessaria a dare attuazione alla protezione dei dati di carattere personale trattati in Ateneo, direttamente o indirettamente riconducibili a persone fisiche, secondo le previsioni del Regolamento (UE) 27 aprile 2016, n. 679 e del D. Lgs. n. 196/2003, come novellato dal D. Lgs. n. 101/2018.

Articolo 2 - Riferimenti normativi

Le principali fonti normative di riferimento sono costituite da:

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE ("Regolamento Generale sulla Protezione dei Dati Personali");
- D.Lgs. 30 giugno 2003 n. 196, "Codice in materia di protezione dei dati personali", così come modificato e integrato dal D.Lgs. n. 101/2018, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al Trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".

L'Ateneo osserva altresì le Linee Guida e i Provvedimenti adottati dal Garante per la Protezione dei Dati Personali, i provvedimenti del Comitato Europeo per la Protezione dei Dati e il "Codice Etico" e il "Codice di Comportamento" dell'Università degli studi di Bergamo.

Articolo 3 - Ambito di applicazione

L'Ateneo svolge attività di Trattamento dei dati personali nell'ambito delle proprie finalità istituzionali. Sono da considerarsi "attività con finalità istituzionali" le attività di didattica, ricerca, terza missione, amministrazione e servizio, nonché le ulteriori attività previste in convenzioni e contratti stipulati dall'Ateneo con soggetti pubblici o privati, sia in ambito nazionale che internazionale. Rientrano tra le attività istituzionali anche le attività di informazione e comunicazione istituzionale finalizzate a promuovere gli obiettivi strategici, il nome, l'immagine e le attività svolte dall'Ateneo in qualità di Titolare del Trattamento o Contitolare del Trattamento. L'Ateneo svolge attività di Trattamento dei dati personali nell'ambito di attività in "conto terzi", ovvero attività di interesse prevalente del committente e per le quali l'Ateneo percepisce un corrispettivo, disciplinate da contratti sottoscritti con soggetti pubblici e privati. Tali attività sono svolte dall'Ateneo in qualità di Responsabile del Trattamento.

I dati potranno essere altresì trattati da soggetti pubblici e privati (es: fondazioni, associazioni), nominati Responsabili del Trattamento ai sensi e per gli effetti di cui all'art. 28 del Regolamento (UE) 2016/679, per la gestione di attività di natura istituzionale proprie dell'Ateneo e per l'affidamento di servizi di propria competenza in *out-sourcing*.

Articolo 4 - Definizioni

Ai fini del presente Regolamento si intende per:

- "Ateneo": l'Università degli studi di Bergamo articolata in tutti i suoi Uffici e Strutture;

- "Struttura": le Aree dell'Amministrazione Centrale e i relativi Uffici, i Dipartimenti, le Strutture didattiche interdipartimentali; Scuole e Centri di Ateneo e interateneo;
- "Codice Privacy": il D.Lgs. 30 giugno 2003 n. 196, "*Codice in materia di protezione dei dati personali*", così come modificato e integrato dal D.Lgs. n. 101/2018, recante "*Disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al Trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*", nonché da ss.mm.ii.;
- "GDPR": il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio relativo al Trattamento dei dati personali, che ha abrogato la Direttiva 95/46/CE;
- "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).
- "Dati Personali Comuni": tutte le informazioni relative a persone fisiche o giuridiche che non appartengono alle "Categorie Particolari di Dati Personali" e a "Dati Personali Giudiziari";
- "Dati Personali Giudiziari": i dati personali relativi a condanne penali e reati o a connesse misure di sicurezza;
- "Categorie Particolari di Dati Personali": i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale. Vi rientrano anche i dati genetici, dati biometrici, intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- "Dati Genetici": i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla fisiologia o sulla salute e che risultano, in particolare, dall'analisi di un campione biologico della persona fisica in questione;
- "Dati Biometrici": i dati personali ottenuti da un Trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentano o confermino l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- "Dati relativi alla salute": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelino informazioni relative al suo stato di salute;
- "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;

- "Profilazione": qualsiasi forma di Trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare, per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- "Pseudonimizzazione": il Trattamento dei dati personali in modo tale che gli stessi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- "Archivio": qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- "Titolare del Trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di dati personali; quando le finalità e i mezzi di tale Trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del Trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- "Contitolare del Trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altro/i titolare/i del Trattamento, determina le finalità e i mezzi del Trattamento dei dati personali;
- "Responsabile per la Protezione dei Dati" o "*Data Protection Officer*" ("RPD" o "DPO"): figura indipendente che svolge attività di consulenza, supporto e controllo per il corretto adeguamento dell'Ateneo al GDPR nonché di raccordo con il Garante per la Protezione dei Dati Personali;
- "Responsabile del Trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del Trattamento;
- "Referente per la protezione dei dati (Referente privacy)": figura nominata dal Titolare o dal Responsabile 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;
- "Designato al Trattamento": chiunque agisca sotto l'autorità diretta del Titolare del o del Responsabile del Trattamento che operi attenendosi alle istruzioni impartite al fine di realizzare in modo diretto i processi gestionali e di elaborazione del Dato Personale;
- "Autorità di controllo": autorità pubblica indipendente, individuata ai sensi dell'articolo 51 del Regolamento UE, incaricata di sorvegliare l'applicazione del Regolamento stesso, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche, con riguardo al Trattamento, e di agevolare la libera circolazione

dei dati personali all'interno dell'Unione. Per l'Italia, l'Autorità di controllo è individuata dal Codice nella figura del Garante per la Protezione dei Dati Personali (art. 153 D. Lgs. n. 196/2003);

- "Consenso dell'Interessato": qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva, che i dati personali che lo riguardano siano oggetto di Trattamento;
- "Terzo": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'Interessato, il Titolare del Trattamento, il Responsabile del Trattamento e gli Autorizzati al Trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;
- "Violazione dei dati personali": l'evento che comporta, accidentalmente o in modo illecito, la distruzione; la perdita; la modifica; la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- "Comunicazione": il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'Interessato, dal Rappresentante del Titolare nel territorio dell'Unione europea, dal Responsabile o dal suo Rappresentante nel territorio dell'Unione europea, dalle persone autorizzate ai sensi del Codice Privacy, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
- "Diffusione": il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "Registro delle attività di Trattamento": l'elenco dei trattamenti di dati in forma cartacea o telematica effettuati dal Titolare e dal Responsabile del Trattamento secondo i rispettivi ambiti del Trattamento;
- "Valutazione d'impatto sulla protezione dei dati": procedura atta a descrivere il Trattamento, a valutarne la necessità e proporzionalità e a garantire la gestione dei rischi per i diritti e le libertà degli interessati;
- "Amministratore di sistema": la 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;
- "Istituto o ente di ricerca": un organismo pubblico o privato per il quale la finalità di statistica o di ricerca scientifica risulta dagli scopi dell'istituzione e la cui attività scientifica è documentabile;
- "Società scientifica", un'associazione che raccoglie gli studiosi di un ambito disciplinare, ivi comprese le relative associazioni professionali;
- "Ricerca scientifica": un progetto di ricerca istituito conformemente alle pertinenti norme etiche e metodologiche settoriali, in conformità delle buone prassi.

Articolo 5 - Tipologia dei trattamenti in ambito universitario

L'Università degli studi Bergamo quale istituzione pubblica con finalità specifiche per le attività di didattica e formazione, ricerca, terza missione, elaborazione critica, diffusione delle conoscenze, sviluppo delle competenze ed educazione della persona, nel proseguire i suoi fini istituzionali tratta anche di particolari tipologie di dati personali quali, a titolo esemplificativo e non esaustivo:

a) dati dei dipendenti dell'Ateneo relativi al rapporto di lavoro pubblico;

b) dati del personale operante a vario titolo nell'Università;

c) dati relativi a studenti ivi compresi coloro che hanno già terminato gli studi;

d) dati relativi alla didattica e a tutta l'attività di ricerca nessuna esclusa e tutti gli altri trattamenti di dati svolti dall'Università.

Articolo 6 - Principi generali applicabili al Trattamento dei Dati Personali

1.L'Ateneo tratta i Dati Personali nel rispetto dei principi e delle libertà fondamentali così come previsti in modo puntuale e specifico dall'art. 5, paragrafo 1, del GDPR.

2. Spetta al Titolare e al Responsabile del Trattamento predisporre misure tecniche e organizzative finalizzate a garantire un livello di sicurezza adeguato alla natura, all'oggetto, al contesto e alle finalità del Trattamento e assicurare percorsi di formazione in materia di privacy e protezione dei dati per tutto il personale che a qualsiasi titolo tratta i dati, di cui all'art. 5 del presente Regolamento in ragione della funzione o dell'ufficio al quale è preposto.

Articolo 7 - Principi generali riguardanti l'esecuzione di un compito di interesse pubblico

1.L'Ateneo è legittimato al Trattamento dei dati personali nei casi disciplinati e previsti dall'art. 6 par. 1 del GDPR. E' inoltre legittimato al Trattamento di Categorie Particolari di Dati Personali, sulla base dell'art. 9 par. 2 del GDPR dalla lettera a) alla lettera j).
2. L'Ateneo è altresì legittimato al Trattamento dei dati personali e particolari quando il Trattamento è necessario per motivi di interesse pubblico, rilevante in relazione alla previsione dell'art. 2-sexies comma 1 del Codice Privacy come novellato dal D. Lgs. 101/2018 per l'accesso ai Dati Personali e Particolari.

Articolo 8 - Privacy by design e privacy by default nella progettazione degli impianti di elaborazione dell'Ateneo

1.Chiunque progetti o sviluppi impianti di elaborazione o suoi componenti hardware e software, su autorizzazione preventiva del Titolare, è tenuto a mettere in atto

misure tecniche ed organizzative adeguate, e nel rispetto delle previsioni di cui all'art. 25 del GDPR, verificare la rispondenza della soluzione alla normativa sul Trattamento di Dati Personali sin dalla fase di progettazione e sviluppo dell'impianto, ivi compresi i profili relativi alla sicurezza.
2. Nella fase di progettazione degli impianti di elaborazione o suoi componenti hardware e software è tenuto a informare il DPO ad acquisirne il parere e a provvedere in merito a tutte le prescrizioni impartite o approfondimenti consigliati d'intesa con il titolare tenendo conto dello stato dell'arte e delle dotazioni già in possesso dell'Ateneo e dei costi di adeguamento delle soluzioni nuove proposte.

Articolo 9 - Modalità di acquisizione del consenso dell'interessato da parte degli uffici

1.L'Ateneo nei casi previsti dalla legge o da regolamento può effettuare il Trattamento dei dati sulla base del consenso prestato da parte dell'Interessato. Quando il Trattamento si fonda sul consenso, il Titolare, il Responsabile o il Designato deve accertare che il consenso reso sia stato prestato dall'effettivo Interessato e che sia un valido presupposto per il Trattamento, in relazione alle finalità per cui viene concesso. Il consenso dato deve essere libero, specifico, informato e inequivocabile. L'Ateneo raccoglie e conserva la relativa documentazione, comprovante la manifestazione del consenso stesso, al fine di dimostrare tale adempimento.
2.Non è ammesso il consenso tacito o presunto, ma il consenso deve sempre essere reso e manifestato attraverso dichiarazione o azione positiva inequivocabile e concludente. Il Consenso al Trattamento dei Dati Personali Comuni è validamente prestato solo qualora l'Interessato abbia preventivamente preso visione dell'informativa. Il Titolare del Trattamento è tenuto a fornire l'informativa all'interessato, indipendentemente dall'obbligo di acquisirne il consenso, salvo nei casi in cui l'Interessato sia già in possesso delle informazioni (art. 13 paragrafo 4 del GDPR) o nei casi particolari descritti nel GDPR (art. 14 paragrafo 5).
3. Il Titolare, il Responsabile o i Designati al Trattamento sono obbligati ad acquisire il consenso esplicito degli interessati nel caso in cui debbano effettuare un Trattamento che richieda il consenso esplicito degli interessati nei seguenti:
a) il Trattamento sia relativo a Categorie Particolari di Dati Personali;
b) i dati debbano essere trasferiti verso Paesi Terzi o verso un'organizzazione internazionale;
c) attività automatizzate, inclusa la profilazione.
4. Il Titolare, il Responsabile e i Designati al Trattamento quando intendano trattare i dati per fini ulteriori e diversi, rispetto a quelli per cui sono stati raccolti, dovranno fornire preventivamente all'interessato informazioni in merito a tale diversa finalità. Se i dati non sono stati forniti dall'interessato sarà necessario indicare la fonte da cui hanno origine e se si tratta di una fonte di pubblico accesso.

Articolo 10 - Basi giuridiche legittimanti il Trattamento dei Dati

1. I Dati Personali vengono trattati dall'Ateneo solo in presenza di una base giuridica che ne renda lecito il Trattamento, sulla base di quanto previsto dall'art. 6 del GDPR e per tutte le altre ipotesi previste dall'art. 9 del GDPR.
2. In particolare, la base giuridica legittimante il Trattamento di Categorie Particolari di Dati Personali da parte dell'Ateneo è costituita dall'art. 9, par. 2 lett. g) del GDPR: quando *"il Trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, [che] deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato".*
L'Ateneo è autorizzato al Trattamento dei dati in vista di un interesse pubblico quando i Dati Personali o Particolari attengono a uno dei profili consentiti sulla base delle deroghe previste all'art. 2-sexies del D. Lgs. 196/2003.
3. Il Trattamento dei Dati Personali Giudiziari da parte dell'Ateneo avviene solo se autorizzato da una norma di legge o di regolamento riguardanti in particolare:
● l'adempimento di obblighi e l'esercizio di diritti da parte del Titolare del Trattamento o dell'Interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi, secondo quanto previsto dall'art. 9, par. 2, lett. b), e dall'art. 88 del GDPR;
● l'adempimento degli obblighi in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali;
● la verifica o l'accertamento dei requisiti di onorabilità, dei requisiti soggettivi e dei presupposti interdittivi;
● l'accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana, nonché la prevenzione, l'accertamento e il contrasto di frodi o di situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa;
● l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
● l'esercizio del diritto di accesso ai dati e ai documenti amministrativi;
● l'esecuzione di investigazioni, le ricerche o la raccolta di informazioni per conto di terzi ai sensi dell'art. 134 del Testo Unico delle Leggi di Pubblica Sicurezza;
● l'adempimento di obblighi previsti da disposizioni di legge o da regolamenti in materia di:
- comunicazioni e informazioni antimafia;
- prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale;
- produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto;
- accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto;
- attuazione della disciplina di attribuzione del rating di legalità delle imprese ai sensi dell'art. 5-ter del Decreto Legge 24 gennaio 2012, n. 1, convertito, con modificazioni, dalla Legge 24 marzo 2012, n. 27;
- prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

4.In mancanza delle predette disposizioni di legge o di regolamento, per il Trattamento dei dati, si farà riferimento a quanto disposto nel Decreto del Ministero della Giustizia così come previsto dall'articolo 2-octies, comma 2, del Codice Privacy.

SEZIONE II – MODELLO ORGANIZZATIVO INTERNO

Articolo 11- Figure di riferimento del Trattamento dei dati

1.Tenuto conto del modello organizzativo interno, di cui all'allegato A, le figure di riferimento per la protezione dei dati personali sono le seguenti:

a. Titolare;
b. Responsabile del Trattamento;
c. Referente privacy;
d. Designato al Trattamento;
e. Responsabile della Protezione dei dati personali;
f. Responsabili esterni al Trattamento;
g. Amministratori di sistema.

Articolo 12- Titolare del Trattamento

1. Titolare del Trattamento è l'Università degli studi di Bergamo nella persona del Magnifico Rettore *pro tempore*, in qualità di legale rappresentante dell'Ateneo, al quale spetta determinare le finalità e i mezzi del Trattamento.

2. Nei casi in cui il Magnifico Rettore, anche a seguito di attività di controllo e audit, rilevi comportamenti difformi, da parte di una o più Strutture dell'Ateneo, a quanto previsto nel presente Regolamento, definisce, con la collaborazione del DPO, i necessari interventi correttivi e ne dispone l'attuazione.

Articolo 13– Responsabile del Trattamento

1. Il Titolare del Trattamento può nominare, con apposito atto giuridico, il Responsabile interno del Trattamento nella figura del Direttore Generale quale figura apicale ovvero, a sua discrezione, altra figura di comprovata esperienza, capacità e affidabilità a garanzia del pieno rispetto delle vigenti disposizioni in materia di Trattamento e tutela dei diritti dell'Interessato.

2. Il Responsabile del Trattamento esterno è nominato con apposito atto del Titolare del Trattamento ed è individuato tra soggetti che per esperienza, capacità e affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di Trattamento e tutela dei diritti dell'Interessato.

3. I compiti affidati al Responsabile del Trattamento sono vincolanti e specifici.

Articolo 14 – Referente e Team di supporto al RPD

1. Il Titolare o il Responsabile del Trattamento dei dati possono nominare un Referente per la protezione dei dati personali sulla base di quanto previsto dall'art. 2-quaterdecies del D.Lgs. 196/2003 aggiornato al D.Lgs. 101/2018.

2. Il Titolare o il Responsabile del Trattamento individuano, ricorrendone l'opportunità, anche specifici referenti del RPD, all'interno delle varie strutture dell'Ateneo, che possano svolgere un ruolo di supporto e di raccordo, sulla base di precise istruzioni del RPD, anche operando quali componenti di un gruppo di lavoro (Team), al quale destinare risorse interne con competenze giuridiche, amministrative o in ambito informatico.

Articolo 15- Designati al Trattamento

1. Il Titolare e il Responsabile al Trattamento dell'Ateneo, individuano i Designati nei responsabili apicali di struttura di cui all'Allegato A, i quali hanno il compito di vigilare, monitorare e garantire, all'interno della struttura a cui sono preposti, il rispetto delle norme vigenti e delle istruzioni del Titolare e del Responsabile del Trattamento, in materia di protezione dei dati personali.

2. Con apposito atto di nomina, sottoscritto dal Magnifico Rettore, o del Direttore Generale, per le singole finalità perseguite in relazione ai compiti assegnati possono essere Designati anche coloro che appartengono al personale tecnico-amministrativo, compresi i tecnologi, i Collaboratori ed Esperti Linguistici (CEL), il personale docente, i ricercatori, i dottorandi, gli assegnisti, i consulenti e collaboratori e gli eventuali altri soggetti che intrattengono rapporti di lavoro con l'Ateneo nonché gli studenti.

3. I Designati che opereranno sotto la diretta responsabilità e direzione del Titolare o del Responsabile del Trattamento dovranno garantire il rispetto delle misure di sicurezza adottate dall'Ateneo, un'adeguata conoscenza della normativa sulla protezione dei dati e di avere ricevuto una formazione qualificata in materia di protezione dei Dati Personali in osservanza delle Linee Guida diramate dal RPD d'intesa con il Titolare o il Responsabile del Trattamento.

4. Tutti i dipendenti dell'Ateneo sono tenuti a seguire le indicazioni e le disposizioni dell'Ateneo in materia di protezione dei dati personali e sicurezza informatica e ad agire in modo conforme alla normativa vigente anche quando svolgono attività lavorativa da remoto (smart-working o telelavoro).

Articolo 16 - Responsabile della Protezione dei Dati o *Data Protection Officer* ("RPD" o "DPO")

1. Il Responsabile della Protezione dei Dati o Data Protection Officer ("RPD" o "DPO"), la cui designazione è obbligatoria per l'Università degli studi di Bergamo, ai sensi della dell'art. 37, par. 1, lett a) del GDPR, è la persona fisica indipendente designata dal

Titolare o dal Responsabile del Trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR, nonché di raccordo con il Garante per la Protezione dei Dati Personali. Il Responsabile della Protezione dei Dati riferisce direttamente al Titolare del Trattamento o al Responsabile del Trattamento.

2. Il DPO è designato in funzione delle qualità professionali e, in particolare, della conoscenza specialistica della normativa e delle prassi in materia di Protezione dei Dati e della capacità di assolvere ai propri compiti di cui all'art. 39 del GDPR.

3. Il DPO può essere un dipendente del Titolare del Trattamento o del Responsabile del Trattamento oppure un soggetto esterno che assolve i suoi compiti sulla base di un contratto di servizi.

4. Il DPO è nominato con Decreto del Magnifico Rettore con il quale sono assegnati i seguenti compiti:
a) informare e fornire consulenza al Titolare del Trattamento, al Responsabile del Trattamento, e ai Designati al Trattamento in merito agli obblighi derivanti dal presente Regolamento nonché dalla normativa europea e nazionale relativa alla protezione dei Dati Personali;
b) sorvegliare l'osservanza del presente Regolamento e di altre disposizioni derivanti dalla normativa europea e nazionale relative alla protezione dei dati nonché delle politiche del Titolare del Trattamento o del Responsabile del Trattamento in materia di protezione dei Dati Personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione dei Designati al Trattamento;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
d) cooperare con il Garante per la Protezione dei Dati Personali;
e) fungere da punto di contatto per il Garante per la Protezione dei Dati Personali per questioni connesse al Trattamento, tra cui la consultazione preventiva di cui all'art. 36 del GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
f) collaborare alla redazione e all'aggiornamento dei registri del Trattamento;
g) svolgere ogni ulteriore compito attribuitogli dal Titolare del Trattamento solo se compatibile con le sue funzioni e il suo ruolo.

5.Nell'eseguire i propri compiti, il DPO considera debitamente i rischi inerenti al Trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

6. Al DPO sono garantiti supporto, risorse e tempi di lavoro adeguati allo svolgimento della relativa funzione. È garantita, inoltre, nel caso in cui si tratti di un soggetto interno, una formazione permanente per permettergli l'aggiornamento costante sugli sviluppi nel settore della protezione dei Dati Personali.

7. Il DPO ha ampio accesso alle informazioni ed è interpellato per ogni problematica inerente la protezione dei Dati Personali nonché consultato per ogni nuovo Trattamento che si intende avviare.

9. L'Ateneo garantisce che il DPO, quando ricorre ad un professionista esterno, eserciti le proprie funzioni in autonomia e indipendenza e, in particolare, non assegna allo stesso attività o compiti che risultino in contrasto con l'Ateneo o in eventuale conflitto di interessi con lo stesso. Il DPO non deve ricevere, dal Titolare o dal Responsabile o da altri, alcuna istruzione per quanto riguarda l'esecuzione dei compiti a lui affidati ai sensi dell'art. 39 del GDPR. Il DPO non può essere rimosso o penalizzato in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni, salvo che per comprovati e documentati gravi e reiterati inadempimenti degli obblighi previsti nel contratto di affidamento del servizio.

10. In caso di scadenza dell'incarico e in attesa della nuova nomina del RPD, nelle more della procedura di selezione, l'incarico è prorogato al DPO in carica per il periodo necessario allo svolgimento della procedura di selezione. Il nominativo e i dati di contatto del DPO sono comunicati, senza ritardo, al Garante per la Protezione dei Dati Personali e gli stessi dati sono inseriti, senza ritardo, nelle informative pubblicate sul sito istituzionale dell'Ateneo.

Articolo 17 - Amministratori di sistema

1. Sono Amministratori di sistema le figure professionali finalizzate alla gestione e manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente Regolamento sono da considerarsi tali anche gli amministratori di database, gli amministratori di rete, gli amministratori di apparati di sicurezza, gli amministratori di sistemi software complessi.

2. L'Amministratore di sistema sviluppa e gestisce l'impianto di elaborazione o i suoi componenti hardware e software mediante i quali vengono effettuati i Trattamenti di Dati Personali, applicando, per i profili relativi alla sicurezza, le direttive del Titolare.

3. Il Titolare o il Responsabile del Trattamento individuano gli amministratori di sistema, nell'ambito dei servizi informativi dell'Ateneo, con atto di designazione individuale che definisce analiticamente i compiti e gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

4. L'Amministratore di sistema è componente di diritto nel Team a supporto del DPO ed è il Referente Privacy per i sistemi informativi dell'Ateneo.

Articolo 18 -Privacy e sicurezza informatica

1. Tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del Trattamento, nonché della probabilità e della gravità del rischio per i diritti e le libertà delle persone fisiche, il Titolare mette in atto misure tecniche e organizzative che garantiscano un livello di sicurezza adeguato al rischio, tutelino il patrimonio informativo dell'Ateneo e prevengano l'accadimento di incidenti di sicurezza. Tali misure sono testate e verificate regolarmente per garantire la sicurezza del Trattamento, con facoltà per l'Ateneo di prescrivere correttivi e bloccare temporaneamente o definitivamente un Trattamento e il sistema che concorre ad effettuarlo, fino al rientro in parametri di sicurezza accettabili.

2. Le misure di sicurezza sono descritte, unitamente alle direttive e alle procedure cui attenersi, sul sito istituzionale di Ateneo.

Articolo 19- Contitolari del Trattamento

1. La contitolarità nel Trattamento dei dati delle persone fisiche 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 i Contitolari con determinazione delle rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, 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, e le rispettive funzioni di comunicazione delle Informazioni di cui al successivo art. 28. Il contenuto essenziale dell'accordo di Contitolarità è messo a disposizione dell'Interessato, se richiesto.

2. I Contitolari condividono le decisioni relative alle finalità e modalità del Trattamento di dati e sono obbligati a predisporre e mantenere aggiornati tutti gli adempimenti previsti dal GDPR e dalle disposizioni di legge vigenti in materia di tutela dei dati personali. In particolare la gestione e il supporto reciproco per la gestione dei reclami e le richieste di esercizio dei diritti presentati saranno gestiti da ognuno dei Contitolari, ai sensi dell'art. 26, paragrafo 3, del GDPR.

3. Nell'accordo di contitolarità - ai sensi dell'art. 26 del GDPR - saranno determinati i profili di responsabilità per ciascuno dei Contitolari e dell'ammontare del danno da ciascuno eventualmente determinato in caso di violazione, al fine di garantire il risarcimento effettivo dell'interessato. Saranno determinati, inoltre, i profili e le misure di sicurezza tecniche e organizzative adeguate per mantenere la segretezza e proteggere i dati personali raccolti, trattati e utilizzati in virtù del rapporto di contitolarità instaurato con l'accordo.

Articolo 20 - Autorità di controllo

1. L'Autorità di controllo di riferimento per l'Ateneo è il Garante per la Protezione dei Dati Personali.

Articolo 21 - Informativa

1. Nel rispetto del principio di trasparenza, per ogni tipologia di Trattamento di Dati Personali l'Ateneo fornisce agli Interessati un'apposita informativa nel rispetto delle previsioni contenute agli art. 13 e 14 del GDPR.

2. L'informativa deve essere concisa, trasparente, intellegibile, facilmente accessibile e redatta con un linguaggio chiaro e semplice. Le informazioni sono fornite per iscritto o con altri mezzi, anche elettronici.

3. Se i dati vengono raccolti presso l'Interessato, ciascuna Struttura fornisce l'informativa agli Interessati al momento della raccolta dei dati. È necessario rendere agli Interessati una nuova informativa quando il Titolare del Trattamento intenda trattare i dati già acquisiti per una finalità diversa da quella per cui sono stati raccolti ovvero vengano modificati elementi fondamentali del Trattamento originario rappresentato agli Interessati.

4. Se i Dati Personali non sono stati raccolti presso l'Interessato, il Titolare o il Responsabile del Trattamento forniscono all'Interessato l'informativa di cui all'art. 14 del GDPR.

5. Non si dovrà fornire l'informativa nei casi previsti dal paragrafo 5 lettere a), b), c) d) dell'articolo 14 del GDPR.

Articolo 22- Registro delle attività di Trattamento del Titolare

1. L'Ateneo, Titolare del Trattamento, ha predisposto il Registro delle attività di Trattamento, in conformità delle prescrizioni contenute nell'art. 30 del GDPR e delle altre disposizioni ivi richiamate. Il Registro è sia in formato elettronico che in formato cartaceo.

2. Il Registro delle attività di Trattamento, redatto dall'Ateneo quale Titolare del Trattamento, deve contenere tutti i trattamenti relativi alle Strutture dell'Ateneo. Spetta a ciascuno dei Designati individuare i trattamenti della propria struttura e dare incarico all'interno delle strutture di competenza al fine di completare e aggiornare i relativi trattamenti di competenza.

3. Il Registro è sottoposto a revisione e/o aggiornamento semestrale con il supporto del RPD.

4. Il Registro è a disposizione del Titolare, del Responsabile, dei Designati, del DPO e dell'Autorità Garante ed ispettori o delegati dall'Autorità Garante. Il Registro dei trattamenti è sottratto da ogni forma e tipo di accesso civico e da qualsiasi altra forma di accesso agli atti.

Articolo 23 -Informazione necessaria

Il Titolare, i Responsabili e i Designati ogni qualvolta debbano porre in essere un Trattamento di Dati Personali o Particolari che preveda l'utilizzo di nuove tecnologie ovvero trattamenti di dati in forma cartacea o informatica, banche dati o altro che, considerati la natura, l'oggetto, il contesto e le finalità del Trattamento, possano presentare un rischio per i diritti e le libertà dell'Interessato, prima di procedere al Trattamento, ne devono dare comunicazione al DPO e acquisirne il parere anche in ordine alla procedura di valutazione di impatto o di consultazione preventiva al Garante Privacy.

Articolo 24- Valutazione d'impatto

1. L'Ateneo effettua una valutazione di impatto ogni qualvolta le attività di Trattamento dei Dati Personali prevedono l'utilizzo di nuove tecnologie, ovvero ogni qualvolta in ragione della natura, oggetto, contesto e finalità del Trattamento, si possa presentare un rischio elevato per i diritti e le libertà dell'Interessato. Prima di procedere al Trattamento, l'Ateneo effettua, consultandosi con il DPO, una valutazione dell'impatto sulla protezione dei Dati Personali. Può anche essere condotta una singola valutazione di impatto per un insieme di trattamenti simili che presentino rischi elevati analoghi.

2. Fatte salve le tipologie di Trattamento individuate dal Garante, la valutazione d'impatto viene effettuata dall'Università, ai sensi e con il procedimento descritto all'art. 35 del GDPR, nei seguenti casi: a) valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un Trattamento automatizzato, compresa la profilazione, e sulla quale, si fondano decisioni che hanno effetti giuridici o incidono in modo significativamente analogo suddette persone; b) Trattamento su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali e a reati; c) sorveglianza o videosorveglianza sistematica su larga scala di una zona accessibile al pubblico; d) Trattamento di dati relativi alla salute a fini di ricerca scientifica in campo medico, biomedico e epidemiologico.

3. La valutazione di impatto contiene i seguenti elementi: a) una descrizione sistematica del Trattamento e delle sue finalità; b) una valutazione in ordine alla necessità e alla proporzionalità del Trattamento in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati; d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone coinvolte.

4. Se necessario, l'Università procede a un riesame per valutare se il Trattamento dei Dati Personali sia effettuato conformemente alla valutazione d'impatto, quando insorgono variazioni del rischio rappresentato dalle attività di Trattamento.

Articolo 25 - Consultazione preventiva

1. L'Università, per il tramite del DPO, prima di procedere al Trattamento, quando lo ritiene conforme alle prescrizioni del GDPR o alla normativa vigente, ovvero sulla base di provvedimenti del Garante Nazionale ed Europeo, valutata la necessità del consulto preventivo al Garante, ovvero qualora la valutazione d'impatto indichi che il Trattamento presenterebbe un rischio elevato in assenza di misure adottate per attenuare il rischio, può fare, nell'interesse dell''Ateneo, richiesta preventiva di valutazione al Garante.

2. IL DPO se ritiene che il Trattamento previsto violi il GDPR, in particolare qualora l'Università non abbia identificato o attenuato sufficientemente il rischio, chiede un parere scritto al Garante che deve trasmetterlo entro un termine di otto settimane dal ricevimento della richiesta di consultazione. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del Trattamento previsto. Il Garante informa l'Università di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte del Garante delle informazioni richieste ai fini della consultazione.

3. In sede di consultazione, l'Università comunica al Garante: a) le rispettive responsabilità dell'Università, in qualità di Titolare, nonché di eventuali Contitolari e Responsabili del Trattamento; b) le finalità e i mezzi del Trattamento; c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati; d) i dati di contatto del DPO; e) la valutazione d'impatto sulla protezione dei dati; f) ogni altra informazione richiesta dal Garante.

Articolo 26 - Diritti dell'interessato

1. L'Ateneo garantisce il rispetto dei diritti degli Interessati disciplinati dagli artt. 12-22 del GDPR, ove applicabili, e, in particolare, di:

● essere informati circa le attività di Trattamento svolte sui propri Dati Personali tramite l'informativa ("diritto a essere informato");

● avere conferma dal Titolare del Trattamento che sia o meno in corso un'attività di Trattamento sui propri Dati Personali e ottenere l'accesso a tali dati ("diritto di accesso ai dati personali");

● ottenere la rettifica dei dati inesatti e l'integrazione dei dati incompleti ("diritto alla rettifica");

● ottenere la cancellazione dei propri Dati Personali ("diritto all'oblio");

● ottenere la limitazione al Trattamento dei propri dati ("diritto alla limitazione");

● ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i relativi Dati Personali forniti a un Titolare del Trattamento e trasmettere

tali dati a un altro Titolare del Trattamento senza impedimenti da parte del Titolare del Trattamento cui li ha forniti ("diritto alla portabilità");

● opporsi in qualsiasi momento, per motivi connessi alla propria situazione particolare, al Trattamento dei propri Dati Personali ai sensi dell'art. 6, paragrafo 1, lett. e) o f), del GDPR, compresa la Profilazione ("diritto all'opposizione");

● non essere sottoposto a una decisione basata unicamente sul Trattamento automatizzato, compresa la Profilazione, che produca effetti giuridici nei confronti dell'interessato stesso o che incida in modo analogo significativamente sulla propria persona, fatti salvi i casi in cui ciò è previsto dalla legge ("diritto a non essere sottoposti a Trattamento automatizzato").

2. L'Interessato presenta istanza di esercizio dei diritti al DPO, senza alcuna formalità, previa dimostrazione della propria identità. Per rendere agevole e immediata la risposta può utilizzare uno dei moduli di richiesta pubblicati sul sito di Ateneo.

3. L'Ateneo risponde tempestivamente alle richieste di esercizio dei diritti e, comunque, entro un mese dal ricevimento dell'istanza. Tale termine può essere prorogato di ulteriori due mesi (per un totale di tre mesi), tenuto conto della complessità e del numero delle richieste. In ogni caso, l'Ateneo dovrà comunicare tale proroga all'Interessato entro un mese dal ricevimento dell'istanza, indicando i motivi del ritardo.

4. L'Ateneo può negare la risposta a una richiesta di esercizio dei diritti solo nel caso in cui quest'ultima risulti manifestamente infondata o eccessiva, in particolare per il suo carattere ripetitivo. Sarà onere dell'Ateneo dimostrare il carattere manifestamente infondato o eccessivo della richiesta e comunicare i motivi del diniego all'Interessato.

5. L'Ateneo non richiede un contributo spese per dare riscontro a richieste di esercizio dei diritti, fatti salvi i casi di istanze manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo.

Articolo 27 - Circolazione dei dati personali all'interno dell'Ateneo

1. L'accesso ai Dati Personali, da parte delle Strutture e dei dipendenti dell'Università è limitato e finalizzato al perseguimento dei fini istituzionali sebbene ispirato al principio della libera circolazione delle informazioni all'interno dell'Ateneo, per lo svolgimento dei compiti istituzionali. L'Università provvede all'organizzazione, gestione e condivisione delle informazioni e dei dati a propria disposizione mediante strumenti, anche di carattere informatico, atti a facilitarne l'accesso e la fruizione in relazione alle attività a cui il richiedente o l'ufficio della struttura appartiene.

2. Ogni accesso ai Dati Personali da parte delle strutture e dei dipendenti dell'Università, deve essere connessa allo svolgimento dell'attività inerente alla specifica funzione, e deve essere soddisfatta in via diretta e senza ulteriori formalità

nella misura necessaria al perseguimento dell'interesse istituzionale, ferma restando la responsabilità di chi tratta i dati in caso di utilizzo improprio.

3. Laddove l'accesso fosse finalizzato ad un utilizzo diverso dei Dati personali, il richiedente è tenuto a presentare una formale richiesta e attendere l'autorizzazione che sarà concessa o negata a seconda che il fine della richiesta rientri o meno nell'attività istituzionale dell'Università.

Articolo 28 – Comunicazione dei dati personali al di fuori dell'Ateneo

La comunicazione dei Dati Personali al di fuori dell'Ateneo può avvenire solo ove sussista una specifica base giuridica. Ogni richiesta, rivolta da soggetti esterni all'Ateneo, finalizzata a ottenere la comunicazione di Dati Personali, salvi i casi espressamente previsti da una norma di legge o di regolamento, deve essere trasmessa per iscritto e motivata e l'accoglibilità della richiesta sarà valutata dalla Struttura in collaborazione con il DPO.

Articolo 29 – Diffusione dei dati personali

1. La diffusione dei Dati Personali può avvenire solo ove prevista da una norma di legge applicabile alla fattispecie concreta. Per la pubblicazione degli atti e la circolazione delle informazioni nonché per la disciplina degli accessi sarà fatto riferimento alle Linee Guida del Garante Privacy e dei Provvedimenti del Garante Privacy sentito il DPO dell'Ateneo.

2. L'Ateneo può diffondere, anche sui propri siti web, i Dati Personali del personale docente, tecnico amministrativo, collaboratori ed esperti linguistici nonché di collaboratori, assegnisti, dottorandi, laureati, stagisti e studenti, in ottemperanza a obblighi di legge. Nei casi di procedure di valutazione e selezione, l'Ateneo procede alla pubblicazione di documenti e graduatorie, anche sui propri siti web, nel rispetto delle prescrizioni normative in materia.

Articolo 30 - Trasferimento di Dati Personali verso Paesi terzi od organizzazioni internazionali

1. Il trasferimento di Dati Personali verso Paesi al di fuori dell'Unione o organizzazioni internazionali o altri destinatari in paesi terzi, deve avvenire assicurandosi che non sia compromesso il livello di tutela delle persone fisiche assicurato dalle normative europee e nazionali per la protezione dei dati personali, come previsto dal Capo V del GDPR.

2. Il trasferimento di Dati Personali, come ogni Trattamento, deve essere innanzitutto conforme alle disposizioni generali inerenti la Protezione dei Dati Personali, in relazione alle finalità per cui viene effettuato.

3. La valutazione dell'adeguatezza della tutela offerta da un Paese Terzo va considerata in funzione di tutte le circostanze relative ad un trasferimento o ad una

categoria di trasferimenti, che riguardano anche la modalità, la frequenza, la durata e il contesto del trasferimento.

4. Sia nella valutazione del rischio sia nelle garanzie attuabili, il Titolare deve prestare attenzione anche ai trasferimenti che potrebbero subentrare tra l'importatore dei dati e un successivo subincaricato, in virtù di un subcontratto dell'importatore.

SEZIONE III - MISURE DI SICUREZZA E NOTIFICA DI VIOLAZIONE DEI DATI PERSONALI

Articolo 31 - Misure, tecniche e organizzative per la protezione dei dati personali

1. L'Ateneo adotta misure, tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio, tenuto conto dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del Trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

2. Ciascuna Struttura è responsabile della concreta adozione delle misure organizzative necessarie a proteggere i Dati Personali oggetto di Trattamento. Tali misure sono individuate in collaborazione con il Titolare del Trattamento, il Responsabile del Trattamento, i Servizi Informativi e con il supporto del DPO.

3. Ciascuna Struttura è responsabile del rispetto delle misure tecniche individuate dai Sistemi informativi di Ateneo, nonché di quelle individuate dalla Struttura stessa, in collaborazione con il Titolare o il Responsabile del Trattamento e con il supporto del DPO.

Articolo 32 - Conservazione dei Dati Personali

1. L'Ateneo conserva i Dati Personali solo per il tempo necessario al conseguimento delle finalità del Trattamento e/o per il periodo indicato dalla legge. Adeguate misure vengono adottate per assicurare la sicurezza dei Dati Personali durante la loro conservazione.

2. Al termine del periodo di conservazione, i Dati Personali vengono cancellati, distrutti o resi anonimi.

3. Il periodo di conservazione dei Dati Personali oggetto di Trattamento è individuato nel "*Massimario - elenco descrittivo della documentazione da conservare perennemente oppure da scartare*", allegato al Manuale di Gestione documentale dell'Università degli Studi di Bergamo.

Articolo 33 - Violazione dei Dati Personali ("*Data Breach*")

1. Ai sensi degli artt. 33 e seguenti del GDPR, il Titolare adotta la Procedura di comunicazione del Data Breach per consentire a chiunque la segnalazione di un evento che comporti, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la rivelazione o l'accesso non autorizzato ai dati personali trasmessi, memorizzati o comunque elaborati. La suddetta Procedura è pubblicata sul sito internet istituzionale.

2. Il Titolare predispone una procedura interna di gestione di tali segnalazioni e degli incidenti di sicurezza informatica, individuando le risorse organizzative alle quali, per le competenze possedute, sia possibile assegnare le attività richieste per la valutazione del rischio per i diritti e le libertà degli interessati, per la loro mitigazione nonché per la corretta e tempestiva gestione delle azioni complessive da intraprendere per far fronte alla violazione occorsa.

3. Compete alle stesse risorse organizzative, individuate nella procedura, la valutazione della necessità di procedere alla notifica all'Autorità garante per la protezione dei dati personali, di cui all'art. 33 del GDPR, senza ingiustificato ritardo e, ove possibile, entro 72 ore dall'avvenuta conoscenza della violazione, come pure la valutazione della necessità di comunicare la violazione all'Interessato, nel rispetto delle previsioni di cui all'art. 34 del GDPR.

4. Il Titolare provvede alle notifiche di cui al precedente comma e documenta in un apposito "Registro degli incidenti" qualsiasi violazione di dati personali, comprese le circostanze in cui si è verificata, le conseguenze e i provvedimenti adottati per attenuarne le conseguenze.

SEZIONE IV - CONTROLLI, SANZIONI E DISPOSIZIONI FINALI

Articolo 34 - Controlli ammessi

Il Titolare del Trattamento dei dati, i soggetti da questo delegato, ovvero il DPO, effettuano i controlli, anche preventivi, necessari a garantire la tutela dei dati personali oggetto di Trattamento da parte dell'Ateneo nello svolgimento delle attività istituzionali.

Articolo 35 - Sanzioni

Fermo restando quanto previsto dagli artt. 58, 82, 83 e 84 del GDPR e dal Codice in materia di protezione dei dati personali, le sanzioni disciplinari e amministrative a carico del personale in caso di violazione delle leggi e delle procedure in tema di protezione dei dati personali saranno definite dall'Università anche sulla base di quanto disposto dai CCNL, dal Codice etico e dai Codici di comportamento.

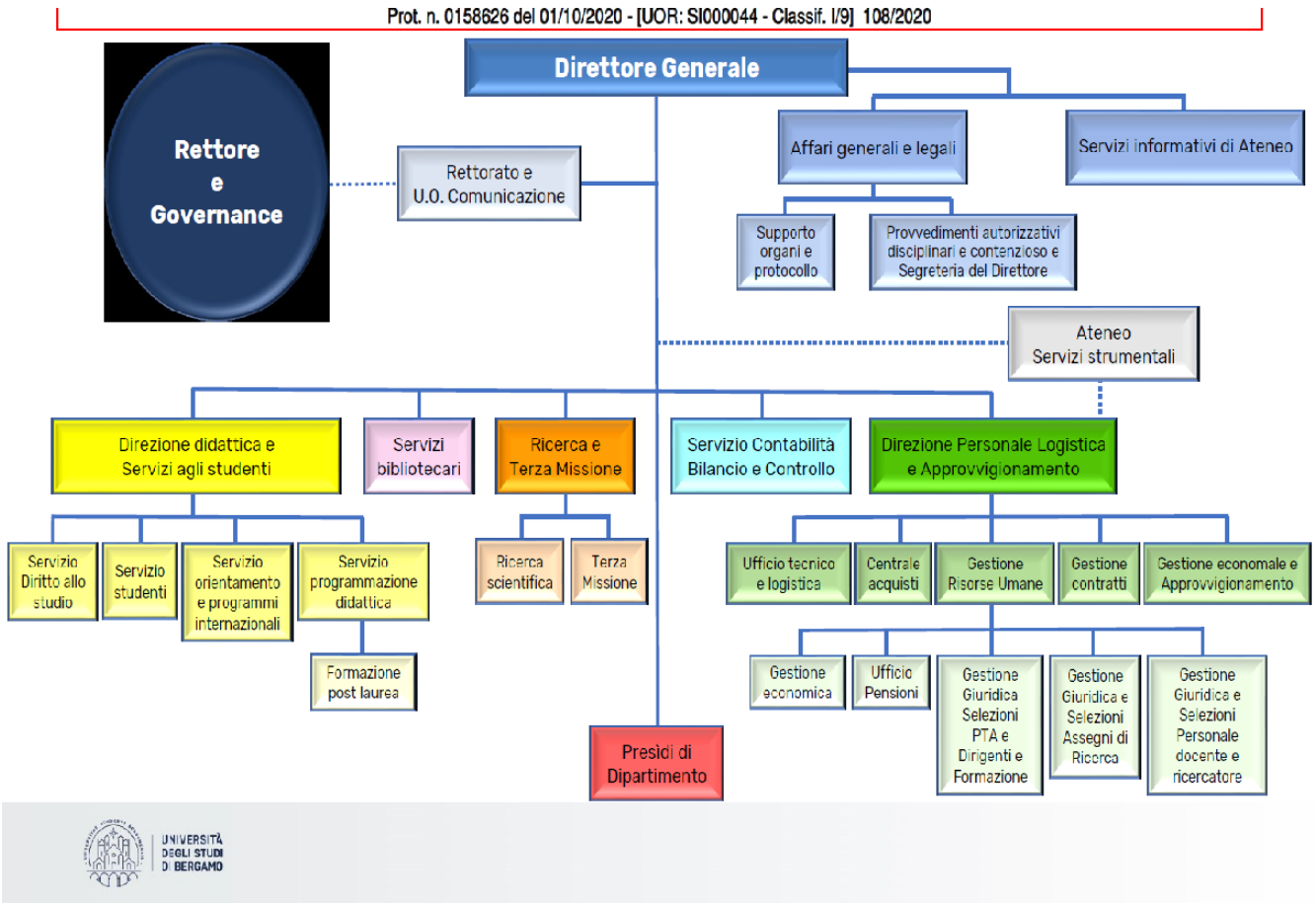
Articolo 36 - Modalità di approvazione e aggiornamento del presente Regolamento

1. Il presente Regolamento è approvato dal Consiglio di Amministrazione a maggioranza assoluta dei componenti.

2. Il Regolamento potrà essere aggiornato a seguito di:

- modifiche normative sopravvenute;
- introduzione di nuove pratiche volte a migliorare l'azione amministrativa;
- inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti.

Allegato A


Prot. n. 0158626 del 01/10/2020 - [UOR: SI000044 - Classif. I/9] 108/2020
Rettore e Governance
Direttore Generale
Rettorato e U.O. Comunicazione
Affari generali e legali
Servizi informativi di Ateneo
Supporto organi e protocollo
Provvedimenti autorizzativi disciplinari e contenzioso e Segreteria del Direttore
Ateneo Servizi strumentali
Direzione didattica e Servizi agli studenti
Servizi bibliotecari
Ricerca e Terza Missione
Servizio Contabilità Bilancio e Controllo
Direzione Personale Logistica e Approvvigionamento
Servizio Diritto allo studio
Servizio studenti
Servizio orientamento e programmi internazionali
Servizio programmazione didattica
Formazione post laurea
Ricerca scientifica
Terza Missione
Ufficio tecnico e logistica
Centrale acquisti
Gestione Risorse Umane
Gestione contratti
Gestione economale e Approvvigionamento
Gestione economica
Ufficio Pensioni
Gestione Giuridica Selezioni PTA e Dirigenti e Formazione
Gestione Giuridica e Selezioni Assegni di Ricerca
Gestione Giuridica e Selezioni Personale docente e ricercatore
Presidi di Dipartimento
UNIVERSITÀ DEGLI STUDI DI BERGAMO