

**REGOLAMENTO IN MATERIA
DI PROTEZIONE DEI DATI PERSONALI
DELL'UNIVERSITÀ CA' FOSCARI
VENEZIA**

Sommario

REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI DELL'UNIVERSITÀ CA' FOSCARI VENEZIA	0
TITOLO I - PRINCIPI E DISPOSIZIONI GENERALI	5
CAPO I - RIFERIMENTI NORMATIVI E AMBITO DI APPLICAZIONE	5
Articolo 1 - Oggetto	5
Articolo 2 - Riferimenti normativi	5
1. 6	
Articolo 4 - Ambito di applicazione oggettivo	5
CAPO II – DEFINIZIONI	5
Articolo 5 - Definizioni	5
CAPO III - PRINCIPI GENERALI	8
Articolo 6 - Principi generali applicabili al Trattamento dei Dati Personali	8
Articolo 7 - Principio di responsabilizzazione (“ <i>Accountability</i> ”)	9
Articolo 8 - Principi di <i>privacy by design</i> e <i>privacy by default</i>	9
Articolo 9 - Basi giuridiche del Trattamento dei Dati Personali Comuni	9
Articolo 10 – Eccezioni al divieto di Trattamento di Categorie Particolari di Dati Personali	9
Articolo 11 - Basi giuridiche del Trattamento per i Dati Personali Giudiziari	10
Articolo 12 - Principi generali riguardanti l'esecuzione di un compito di interesse pubblico	11
Articolo 13 - Principi generali riguardanti il Consenso dell'Interessato	11
TITOLO II - TRATTAMENTO DEI DATI PERSONALI	12
CAPO I - ORGANIZZAZIONE E RESPONSABILITÀ	12
Articolo 14 - Titolare del Trattamento	12
Articolo 15 - Referenti di Struttura e Referenti Interni	12
Articolo 16 - Autorizzati al Trattamento	13
Articolo 17 - Amministratori di Sistema	13
Articolo 18 - Responsabile della Protezione dei Dati o <i>Data Protection Officer</i> (“RPD” o “DPO”)	13
Articolo 19 - Responsabile del Trattamento	14
Articolo 20 - Sub-Responsabile del Trattamento	15
Articolo 21 - Contitolari del Trattamento	15
Articolo 22 - Autorità di controllo	15
CAPO II - ADEMPIMENTI	15
Articolo 23 – Informazioni da fornire all'Interessato	15
Articolo 24 - Registro delle attività di Trattamento	16

Articolo 25 - Valutazione di impatto	17
CAPO III - DIRITTI DELL'INTERESSATO	18
Articolo 26 - Diritti dell'Interessato	18
CAPO IV – CIRCOLAZIONE, COMUNICAZIONE, DIFFUSIONE E TRASFERIMENTO DI DATI PERSONALI	18
Articolo 27 - Circolazione dei Dati Personali all'interno dell'Ateneo	18
Articolo 28 - Comunicazione dei Dati Personali al di fuori dell'Ateneo	18
Articolo 29 - Diffusione dei Dati Personali	18
Articolo 30 - Trasferimento di Dati Personali verso Paesi terzi od organizzazioni internazionali	19
TITOLO III - MISURE DI SICUREZZA E NOTIFICA DI VIOLAZIONE DEI DATI PERSONALI	19
Articolo 31 - Misure di sicurezza	19
Articolo 32 - Conservazione dei Dati Personali	20
Articolo 33 - Violazione dei Dati Personali (“Data Breach”)	20
TITOLO IV - CONTROLLI, SANZIONI E DISPOSIZIONI FINALI	20
Articolo 34 - Controlli ammessi	20
Articolo 35 - Sanzioni	20
Articolo 36 - Modalità di approvazione e aggiornamento del presente Regolamento e relativi Allegati	20
ALLEGATO A	21
VIDEOSORVEGLIANZA NELLE SEDI UNIVERSITARIE	21
Articolo 1 - Principi generali	21
Articolo 2 - Titolare del Trattamento	21
Articolo 3 - Responsabile del Trattamento	21
Articolo 4 - Conservazione delle immagini	21
Articolo 5 - Controllo degli accessi alle immagini	21
Articolo 6 - Informazioni agli Interessati	22
Articolo 7 - Basi giuridiche	22
Articolo 8 - Diritti dell'Interessato	22
Articolo 9 - Collocazione delle telecamere	22
ALLEGATO B	23
ATTRIBUZIONE DELLE CREDENZIALI DI ATENEEO E DELLE CASELLE DI POSTA ELETTRONICA	23
Articolo 1 - Premessa	23
Articolo 2 - Account utente	23
Articolo 3 - IDEM e EduGAIN	24

Articolo 4 - Credenziali	25
Articolo 4.1 - Modalità di rilascio dell' <i>account</i>	26
Articolo 4.2 - Rinnovo	27
Articolo 4.3 - Scadenza e dismissione dell' <i>account</i>	27
Articolo 4.4 - Ruoli e diritti di accesso	27
Articolo 4.5. - Revoca delle credenziali di autenticazione	30
Articolo 5 - Caratteristiche degli account di amministratore di sistema	30
Articolo 6 - Caratteristiche degli <i>account</i> sui sistemi di servizio	31
Articolo 7 - Verifica degli <i>account</i>	31
ALLEGATO C	32
INFRASTRUTTURE E RISORSE INFORMATICHE	32
Articolo 1 - Gestione e implementazione dei servizi di rete delle strutture di Ateneo	32
Articolo 2 - Utilizzo di cartelle condivise e spazi personali	32
Articolo 3 - Utilizzo postazioni di lavoro dell'Ateneo	33
Articolo 4 - Utilizzo della rete Internet	34
ALLEGATO D	36
UTILIZZO DELLA POSTA ELETTRONICA	36
Articolo 1 - Principi generali	36
Articolo 2 - Gestione tecnica del servizio	36
Articolo 3 - Validità dei profili autorizzativi per l'uso del servizio di posta elettronica	36
Articolo 4 - Uso del sistema di posta elettronica	36
ALLEGATO E	39
CONTROLLI SULL'UTILIZZO DELLE INFRASTRUTTURE, DELLE RISORSE INFORMATICHE E DELLA POSTA ELETTRONICA	39
Articolo 1 - Principi generali	39
Articolo 2 - Controlli relativi alla posta elettronica	39
Articolo 2.1. - <i>Dati rilevati</i>	39
Articolo 3 - Controlli relativi all'utilizzo dei sistemi informatici	40
ALLEGATO F	43
PRESENTAZIONE E GESTIONE DELLE ISTANZE DI ESERCIZIO DEI DIRITTI	43
Articolo 1 - Oggetto	43
TITOLO I – ADEMPIMENTI PER LA PRESENTAZIONE E LA GESTIONE DELLE ISTANZE	43
Articolo 2 - Legittimazione all'esercizio dei Diritti e modalità di presentazione dell'istanza	43
Articolo 3 - Legittimazione e presentazione delle istanze relative a Dati Personali di Interessati deceduti ovvero dichiarati morti presunti	43

Articolo 4 - Soggetti coinvolti nella gestione delle istanze di esercizio dei Diritti	44
Articolo 5 - Adempimenti preliminari	44
Articolo 6 - Adempimenti generali	45
Articolo 7 - Modalità di riscontro	45
Articolo 8 - Tempi di riscontro alle istanze di esercizio dei Diritti	46
Articolo 9 - Contributo spese	46
Articolo 10 - Limitazioni al riscontro alle istanze di esercizio dei Diritti	47
Articolo 11 - Registro delle richieste di esercizio dei Diritti	47
TITOLO II – I DIRITTI DI CUI AGLI ARTT. 15-22 DEL GDPR	47
Articolo 12 - Diritto di accesso	47
Articolo 13 - Diritto di rettifica	47
Articolo 14 - Diritto alla cancellazione	48
Articolo 15 - Diritto di limitazione di Trattamento	48
Articolo 16 - Diritto alla portabilità dei Dati Personali	49
Articolo 17 - Diritto di opposizione	49
Articolo 18 - Diritti relativi ai processi decisionali automatizzati, compresa la profilazione	49
ALLEGATO G	51
GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI (“ <i>DATA BREACH</i> ”)	51
Articolo 1 - Premessa	51
Articolo 2 - Ambito di applicazione	51
Articolo 3 - Principi generali	51
Articolo 4 - Rilevazione di un incidente di sicurezza	51
Articolo 5 - Valutazione preliminare	52
Articolo 6 - Valutazione del <i>Data Breach</i> e analisi del rischio	52
Articolo 7 – Notifica al Garante	53
Articolo 8 – Comunicazione agli interessati	54
Articolo 9 – Azioni di mitigazione	54
Articolo 10 – Misure di <i>remediation</i>	54
Articolo 11 – Registro degli incidenti di Sicurezza e dei <i>Data Breach</i>	54
Articolo 12 – Gestione di un <i>Data Breach</i> occorso in regime di contitolarità	55
Articolo 13 – Gestione di un <i>Data Breach</i> occorso presso un Responsabile del Trattamento dell’Ateneo	55

TITOLO I - PRINCIPI E DISPOSIZIONI GENERALI

CAPO I - RIFERIMENTI NORMATIVI E AMBITO DI APPLICAZIONE

Articolo 1 - Oggetto

1. Il presente Regolamento e i relativi Allegati recano i principi e le disposizioni ai quali l'Università Ca' Foscari Venezia deve attenersi con riguardo alle attività di trattamento dei dati personali.

Articolo 2 - Riferimenti normativi

1. Le principali fonti normative di riferimento sono costituite da:
 - a. 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");
 - b. 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)".
2. L'Ateneo osserva altresì eventuali altre norme europee o nazionali che regolamentano il trattamento dei dati personali, nonché 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 di Comportamento" dell'Università Ca' Foscari Venezia.

Articolo 3 - Ambito di applicazione soggettivo

1. Il presente Regolamento si applica a tutti coloro che svolgono attività di Trattamento dei Dati Personali – su supporto cartaceo e/o tramite procedure informatizzate – nell'ambito delle mansioni ovvero delle attività assegnate loro dall'Università Ca' Foscari Venezia.
2. Tutte le cariche, professioni e titoli inerenti a funzioni nominate nel presente Regolamento e declinate al genere maschile devono intendersi riferite anche al corrispondente termine di genere femminile.

Articolo 4 - Ambito di applicazione oggettivo

1. L'Università Ca' Foscari Venezia svolge attività di Trattamento dei Dati Personali nell'ambito delle proprie finalità istituzionali. Ai fini del presente Regolamento, 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'Università stessa 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'Università. Le predette attività sono svolte dall'Università in qualità di Titolare del Trattamento o di Contitolare del Trattamento ovvero, in determinati casi residuali, di Responsabile del Trattamento.
2. Inoltre, l'Università 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'Università stessa percepisce un corrispettivo, disciplinate da contratti sottoscritti con soggetti pubblici e privati. Le predette attività sono svolte dall'Università in qualità di Responsabile del Trattamento.

CAPO II – DEFINIZIONI

Articolo 5 - Definizioni

1. Ai fini del presente Regolamento si intende per:
 - a. "**Ateneo**": l'Università Ca' Foscari Venezia in tutte le sue articolazioni;

- b. **“Struttura”**: le Aree dell'Amministrazione Centrale e i relativi Uffici, i Dipartimenti, le Scuole, il Sistema Bibliotecario dell'Ateneo, i Centri aventi sede amministrativa presso l'Ateneo, il Collegio Internazionale Ca' Foscari e i gruppi di ricerca dell'Ateneo che fanno capo a un Responsabile Scientifico di Attività di Ricerca;
- c. **“GDPR”**: il 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; il Regolamento (UE) 2016/679 abroga la Direttiva 95/46/CE;
- d. **“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.;
- e. **“Dato Personale”**: qualsiasi informazione riguardante una persona fisica identificata o identificabile (**“Interessato”**); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- f. **“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, 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;
- g. **“Dati Personali Comuni”**: dati personali che non appartengono alle categorie particolari di dati personali e non sono relativi a condanne penali e a reati o a connesse misure di sicurezza;
- h. **“Dati Genetici”**: i dati relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- i. **“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;
- j. **“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 rivelano informazioni relative al suo stato di salute;
- k. **“Dati Personali Giudiziari”**: i dati personali relativi a condanne penali e reati o a connesse misure di sicurezza;
- l. **“Trattamento”**: qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- m. **“Profilazione”**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali 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;
- n. **“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

- sogette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- o. **“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;
 - p. **“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;
 - q. **“Contitolare del Trattamento”**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altro/altri titolare/titolari del trattamento, determina le finalità e i mezzi del trattamento dei dati personali;
 - r. **“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;
 - s. **“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;
 - t. **“Sub-Responsabile del Trattamento”**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo a cui il responsabile del trattamento ricorre per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento;
 - u. **“Referente di Struttura”**: il Referente della Struttura nell'ambito della quale i dati personali sono gestiti per finalità istituzionali o in “conto terzi”; il Referente di Struttura è individuato sulla base della funzione organizzativa o carica istituzionale che ricopre ed esercita prevalentemente attività programmatiche e di controllo in relazione al trattamento dei dati personali all'interno della propria Struttura;
 - v. **“Referente Interno”**: Il Referente Interno agisce sulla base delle linee programmatiche determinate dal Referente di Struttura e si occupa di garantire la corretta gestione operativa dei dati personali;
 - w. **“Responsabile Scientifico di Attività di Ricerca”**: è il ricercatore ovvero il docente responsabile delle attività di ricerca definite nel progetto di ricerca o dallo stesso presiedute, nonché delle attività compiute dagli altri soggetti impegnati nell'attività stesse;
 - x. **“Autorizzato al Trattamento”**: chiunque agisca sotto l'autorità diretta del Titolare del Trattamento o del Responsabile del Trattamento che abbia accesso ai dati personali; non può trattare tali dati se non è istruito in tale senso dal Titolare del Trattamento;
 - y. **“Amministratori di Sistema”**: figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti e figure equiparabile dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, che, pertanto, svolgono attività tecniche quali il salvataggio dei dati (*backup/recovery*), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione *hardware*;
 - z. **“Autorità di controllo”**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51 del GDPR; in Italia l'autorità di controllo è il Garante per la Protezione dei Dati Personali;
 - aa. **“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 inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
 - bb. **“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;

- cc. **“Destinatario”**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi; tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerati destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- dd. **“Violazione dei dati personali” o “Data Breach”**: 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;
- ee. **“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 dell'art. 2-*quaterdecies* del Codice Privacy, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
- ff. **“Diffusione”**: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- gg. **“ASIT”**: Area Servizi Informatici e Telecomunicazioni.

CAPO III - PRINCIPI GENERALI

Articolo 6 - Principi generali applicabili al Trattamento dei Dati Personali

1. L'Ateneo tratta i Dati Personali nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento al rispetto della riservatezza e dell'identità personale. In particolare, l'Ateneo svolge le attività di Trattamento dei Dati Personali nel rispetto dei principi previsti dall'art. 5, c. 1 del GDPR, ovvero i Dati Personali sono:
 - a. trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato (“principio di liceità, correttezza e trasparenza”);
 - b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore Trattamento dei Dati Personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali (“limitazione delle finalità”);
 - c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (“principio di minimizzazione dei dati”);
 - d. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (“principio di esattezza”);
 - e. conservati in una forma che consenta l'identificazione degli Interessati per un arco temporale non superiore a quello necessario per il conseguimento delle finalità per le quali sono trattati; i Dati Personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'Interessato (“principio di limitazione della conservazione”);
 - f. trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante adeguate misure tecniche e organizzative da Trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (“principio di integrità e riservatezza”).

Articolo 7 - Principio di responsabilizzazione (“Accountability”)

1. L'Ateneo, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del Trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in

grado di dimostrare, che il Trattamento è effettuato conformemente alle prescrizioni del GDPR (“principio di responsabilizzazione”).

2. Le Strutture possono dotarsi di proprie disposizioni specifiche a integrazione e nel rispetto del presente Regolamento. Il TITOLO II, CAPO I del presente Regolamento individua le responsabilità di ciascuna Struttura, con specifico riferimento al ruolo e alle attribuzioni dei Referenti di Struttura, dei Referenti Interni e degli Autorizzati al Trattamento.

Articolo 8 - Principi di *privacy by design* e *privacy by default*

1. L'Ateneo, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del Trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal Trattamento, sia al momento di determinare i mezzi del Trattamento, sia all'atto del Trattamento stesso, mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, come la minimizzazione, e a integrare nel Trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli Interessati (“principio di *privacy by design*”).
2. L'Ateneo mette in atto le misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i Dati Personali necessari per ogni specifica finalità di Trattamento. Tale obbligo vale per la quantità dei Dati Personali raccolti e l'accessibilità a questi ultimi, la portata del Trattamento e il periodo di conservazione. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili Dati Personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica (“principio di *privacy by default*”).
3. Ciascuna Struttura deve: (i) individuare e implementare, con la collaborazione del Titolare del Trattamento e del DPO, le predette misure tecniche e organizzative; (ii) vigilare, unitamente ai predetti soggetti, sul rispetto delle stesse; nonché (iii) predisporre, ove necessario, la valutazione d'impatto ai sensi dell'art. 35 del GDPR, così come disciplinata all'art. 25 del presente Regolamento.

Articolo 9 - Basi giuridiche del Trattamento dei Dati Personali Comuni

1. L'Ateneo tratta i Dati Personali solo in presenza di una base giuridica che renda lecito il Trattamento effettuato.
2. La principale base giuridica che legittima i Trattamenti di Dati Personali Comuni effettuati dall'Ateneo è costituita dall'art. 6, c. 1, lett. e) del GDPR (“*esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del Trattamento*”) (meglio specificata all'art. 12 del presente Regolamento).
3. Potranno, in considerazione delle caratteristiche del Trattamento, costituire idoneo fondamento di liceità per il Trattamento dei Dati Personali Comuni anche le altre basi giuridiche previste dall'art. 6, c. 1, del GDPR.
4. L'Ateneo, con la collaborazione delle Strutture e del DPO, individua la corretta base giuridica per le attività di Trattamento in oggetto.

Articolo 10 – Eccezioni al divieto di Trattamento di Categorie Particolari di Dati Personali

1. Il Trattamento di Categorie Particolari di Dati Personali da parte dell'Ateneo è vietato ai sensi dell'art. 9, c. 1 del GDPR, salvo il verificarsi di uno dei casi indicati dall'art. 9, c. 2 del GDPR stesso.
2. La principale eccezione al divieto di trattamento di Categorie Particolari di Dati Personali per lo svolgimento di attività con finalità istituzionali è rappresentata per l'Ateneo dall'art. 9, c. 2, lett. g), del GDPR (“*il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione europea 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*”). Ove le predette attività di Trattamento non siano contenute nei testi normativi dell'Unione europea o nella legislazione nazionale, l'Ateneo sopperisce a tale mancanza con quanto disposto nel Regolamento “Trattamento dei dati sensibili e giudiziari in attuazione del D.L. 196/2003” disponibile alla pagina <https://www.unive.it/pag/8249/>.

In particolare, in relazione al Trattamento delle Categorie Particolari di Dati Personali del personale dell'Ateneo, possono costituire, inoltre, adeguate eccezioni al divieto anche l'art. 9, c. 2, lett. b), del GDPR (*"il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato"*) e l'art. 9, c. 2, lett. h), del GDPR (*"il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3"*).

Infine, per quanto riguarda l'ambito della ricerca scientifica, costituiscono adeguate eccezioni l'art. 9, c. 2, lett. a), del GDPR (*"l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche"*) in connessione con l'art. 7.2 dell'Allegato A5 al Codice privacy "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica" e l'art. 9, c. 2, lett. j), del GDPR (*"il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato"*).

L'art. 9, c. 2, lett. a), del GDPR può essere utilizzato anche in altri casi in cui è facoltativo fornire Categorie Particolari di Dati Personali all'Ateneo.

Articolo 11 - Basi giuridiche del Trattamento per i Dati Personali Giudiziari

1. Il Trattamento dei Dati Personali Giudiziari da parte dell'Ateneo è lecito solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, riguardanti, in particolare:
 - a. 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, c. 2, lett. b), e dall'art. 88 del GDPR;
 - b. l'adempimento degli obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali;
 - c. la verifica o l'accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti;
 - d. 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 situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
 - e. l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
 - f. l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
 - g. l'esecuzione di investigazioni o le ricerche o la raccolta di informazioni per conto di terzi ai sensi dell'art. 134 del Testo Unico delle Leggi di Pubblica Sicurezza;
 - h. l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto;
 - i. l'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti;
 - j. l'attuazione della disciplina in materia 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;

- k. l'adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.
2. Ove le predette norme di legge o regolamento non individuino i Trattamenti nonché le garanzie appropriate per i diritti e le libertà degli Interessati, si farà riferimento a quanto disposto nell'emanando Decreto del Ministero della Giustizia così come previsto dall'articolo 2-*octies*, c. 2, del Codice Privacy.

Articolo 12 - Principi generali riguardanti l'esecuzione di un compito di interesse pubblico

1. Il Trattamento dei Dati Personali Comuni da parte dell'Ateneo, la cui base giuridica è rappresentata dall'art. 6, c. 1, lett. e), del GDPR, può avvenire quando il *"compito di interesse pubblico"* è regolato da una norma di legge o, nei casi previsti dalla legge, di regolamento, nonché all'interno di atti amministrativi generali adottati dall'Ateneo, ai sensi dell'art. 2-*ter* del Codice Privacy, come emendato dal D.L. n. 139/2021, convertito con modificazioni dalla L. n. 205/2021.
2. Il Trattamento di Categorie Particolari di Dati Personali da parte dell'Ateneo, la cui eccezione al divieto di Trattamento è rappresentata dall'art. 9, c. 2, lett. g), del GDPR, può avvenire quando il *"compito di interesse pubblico rilevante"* è regolato dal diritto dell'Unione europea, da una norma di legge o, nei casi previsti dalla legge, di regolamento che specifichi i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'Interessato. L'art. 2-*sexies*, c. 2, lett. bb), del Codice Privacy riconosce espressamente le attività di Trattamento svolte nel campo *"dell'istruzione e formazione in ambito scolastico, professionale, superiore o universitario"* come attività compiute in esecuzione di un compito di interesse pubblico rilevante. Inoltre, l'art. 2-*sexies*, c. 2 lett. cc), del Codice Privacy riconosce quali attività di Trattamento compiute in esecuzione di un compito di interesse pubblico *"i trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale"*.

Articolo 13 - Principi generali riguardanti il Consenso dell'Interessato

1. L'Ateneo ottiene il Consenso dell'Interessato quando lo stesso costituisce base giuridica idonea per le attività di Trattamento.
2. Per essere considerato valido, il Consenso deve consistere in una manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva indubbia, affinché i Dati Personali che lo riguardano siano oggetto di Trattamento; il Consenso, inoltre, deve essere dimostrabile.
3. Il Consenso si applica a tutte le attività di Trattamento svolte per la stessa finalità. Qualora il Trattamento abbia più finalità, il Consenso deve essere prestato per ciascuna di esse.
4. Il Consenso al Trattamento dei Dati Personali Comuni è validamente prestato solo qualora l'Interessato abbia preventivamente preso visione dell'informativa.
5. Il Consenso dell'Interessato deve essere, invece, necessariamente esplicito nei seguenti casi: (i) attività di Trattamento dei Dati Personali a fini di Profilazione, che produca effetti giuridici per l'Interessato o conseguenze analoghe; (ii) Trattamento di Categorie Particolari di Dati Personali; (iii) trasferimento dei dati verso paesi terzi (ad esempio, extra Unione europea) o verso una organizzazione internazionale.
6. Il Consenso non è validamente prestato in caso di: (i) caselle preselezionate e (ii) silenzio e/o inattività dell'Interessato.
7. Il Consenso al Trattamento dei Dati Personali deve essere raccolto separatamente da quello prestato per altre attività.
8. Quando il Consenso costituisce la base giuridica che legittima le attività di Trattamento, ciascuna Struttura provvede a raccogliarlo e a conservare la relativa documentazione, composta dall'informativa resa all'Interessato e la prova della manifestazione del Consenso stesso, in modo da

poter dimostrare tale adempimento e, su richiesta, metterla a disposizione del Garante per la Protezione dei Dati Personali.

TITOLO II - TRATTAMENTO DEI DATI PERSONALI

CAPO I - ORGANIZZAZIONE E RESPONSABILITÀ

Articolo 14 - Titolare del Trattamento

1. Il Titolare del Trattamento è l'Università Ca' Foscari Venezia nella persona del Magnifico Rettore *pro tempore*, quale legale rappresentante dell'Ateneo.
2. Nei casi in cui il Magnifico Rettore, anche a seguito di attività di controllo e *audit*, rilevi comportamenti difformi a quanto previsto nel presente Regolamento da parte di una o più Strutture dell'Ateneo, definisce, con la collaborazione del DPO, i necessari interventi correttivi e ne dispone l'attuazione.

Articolo 15 - Referenti di Struttura e Referenti Interni

1. Per ogni Struttura è individuato un Referente di Struttura, nella persona: del Direttore Generale, dei Dirigenti delle Aree dell'Amministrazione Centrale e del Sistema Bibliotecario, dei Direttori dei Dipartimenti, dei Responsabili dei Centri e delle Scuole di Ateneo con funzioni di rappresentanza.
2. I Direttori degli Uffici, i Segretari dei Dipartimenti, delle Scuole e dei Centri e i Direttori di Biblioteca sono nominati Referenti Interni. Sono, inoltre, nominati Referenti Interni i Responsabili Scientifici di Attività di Ricerca che comportino un trattamento di Dati Personali di cui l'Ateneo è Titolare.
3. I Referenti di Struttura e i Referenti Interni sono designati con apposito atto di nomina sottoscritto dal Magnifico Rettore e sono responsabili degli adempimenti della propria Struttura indicati nel presente Regolamento.
4. I Referenti di Struttura sono responsabili del rispetto del presente Regolamento da parte della propria Struttura e predispongono gli interventi programmatici e di controllo relativi alle attività di Trattamento dei Dati Personali nell'ambito di quest'ultima in conformità al presente Regolamento.
5. Il Referenti Interni predispongono gli interventi operativi, sulla base delle linee programmatiche determinate dal Referente di Struttura, relativi alle attività di Trattamento dei Dati Personali specifici per il proprio ambito di lavoro, in conformità al presente Regolamento.
6. I Referenti di Struttura e i Referenti Interni organizzano, ove necessario, in collaborazione con il DPO, eventi formativi per gli Autorizzati al Trattamento della propria Struttura affinché vengano illustrati il contenuto del presente Regolamento e le regole operative relative alle attività di Trattamento di Dati Personali effettuate dalla Struttura stessa, per garantire il rispetto di quanto ivi stabilito.
7. Nei casi in cui i Referenti di Struttura o i Referenti Interni, anche a seguito di attività di controllo e *audit*, rilevino comportamenti difformi da quanto previsto dal presente Regolamento o dalle regole operative applicabili da parte degli Autorizzati al Trattamento all'interno della propria Struttura, definiscono, in collaborazione con il DPO, gli eventuali interventi correttivi e ne dispongono l'attuazione.
8. Quando il Referente di Struttura o il Referente Interno sia oggettivamente impossibilitato ad adottare adeguate misure di protezione a tutela dei Dati Personali trattati, è tenuto a darne tempestiva comunicazione al DPO, affinché vengano congiuntamente valutate le possibili soluzioni tecnologiche e organizzative per adempiere alla normativa vigente.

Articolo 16 - Autorizzati al Trattamento/Autorizzate al Trattamento

1. Tutto il personale tecnico-amministrativo, compresi i tecnologi di cui all'art. 24-*bis* della L. n. 240/2010, i Collaboratori ed Esperti Linguistici (CEL), i professori universitari, i ricercatori anche a tempo determinato, i docenti a contratto, i *visiting professor*, i *visiting scholar*, i dottorandi, gli assegnisti, i borsisti, i consulenti e collaboratori e gli eventuali altri soggetti che intrattengono rapporti di lavoro o collaborazione con l'Ateneo, compresi gli studenti nello svolgimento delle attività di supporto ai servizi universitari e gli stagisti nonché i volontari del servizio civile assegnati

all'Università sono designati Autorizzati al Trattamento con apposito atto di nomina sottoscritto dal Rettore.

2. L'Ateneo può procedere a nominare ad Autorizzati al Trattamento soggetti che svolgono particolari attività di Trattamento per conto dell'Ateneo (es: membri delle Commissioni di selezione e della Commissione Ispettiva di Ateneo), fornendo loro specifiche istruzioni.
3. Gli Autorizzati al Trattamento: (i) operano sotto la diretta autorità del Titolare del Trattamento rappresentato dal Referente di Struttura e Referente Interno; (ii) devono osservare le disposizioni contenute nel presente Regolamento e nelle regole operative applicabili; (iii) devono effettuare il Trattamento in osservanza delle misure di sicurezza adottate dall'Ateneo; (iv) ricevono, ove necessario, formazione in materia di protezione dei Dati Personali specifica per la Struttura di appartenenza.

Articolo 17 - Amministratori di Sistema/Amministratrici di Sistema

1. In ottemperanza al Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 e s.m.i. "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*", l'Ateneo provvede alla designazione delle persone fisiche che svolgono funzioni di Amministratori di Sistema, previa valutazione delle caratteristiche di esperienza, capacità e affidabilità dei soggetti designati (i quali devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza informatica). In particolare, per l'Amministrazione Centrale, le funzioni di Amministratore di Sistema sono attribuite con Decreto del Direttore Generale o suo delegato; per le strutture decentrate, invece, con Decreto del Direttore del Dipartimento o del relativo Referente di Struttura.
2. Gli estremi identificativi delle persone fisiche designate quali Amministratori di Sistema, con l'elenco delle funzioni ad esse attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante per la Protezione dei Dati Personali.

Articolo 18 - Responsabile della Protezione dei Dati o Data Protection Officer ("RPD" o "DPO")

1. L'Ateneo nomina un Responsabile della Protezione dei Dati o *Data Protection Officer* ("RPD" o "DPO"), che opera quale soggetto di supporto al Titolare del Trattamento con funzioni di raccordo con il Garante per la Protezione dei Dati Personali.
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.
3. Il DPO può essere un Dirigente dell'Ateneo – o comunque una figura interna dotata di particolari competenze – o un soggetto esterno con incarico affidato sulla base di un contratto di servizi. Il DPO è nominato con Decreto del Magnifico Rettore.
4. Il DPO svolge i seguenti compiti:
 - a. informare e fornire consulenza al Titolare del Trattamento, al Responsabile del Trattamento, ai Referenti di Struttura, ai Referenti Interni, agli Amministratori di Sistema e agli Autorizzati 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 degli Autorizzati al Trattamento; in particolare, il DPO organizza incontri di formazione *ad hoc* con i componenti delle varie Strutture di Ateneo;
 - c. fornire al Titolare, 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 con 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 delle schede del Registro delle attività di 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 alla protezione dei Dati Personali nonché consultato per ogni nuovo Trattamento che si intende avviare, fin dalla progettazione dello stesso.
 8. L'Ateneo garantisce che il DPO eserciti le proprie funzioni in autonomia e indipendenza e, in particolare, non assegna allo stesso attività o compiti che risultino in contrasto o conflitto di interessi.
 9. Il DPO non riceve alcuna istruzione per quanto riguarda l'esecuzione dei compiti allo stesso affidati ai sensi dell'art. 39 del GDPR.
 10. L'Ateneo non rimuove o penalizza il DPO in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni.
 11. Il nominativo e i dati di contatto del DPO sono comunicati al Garante per la Protezione dei Dati Personali. I dati di contatto istituzionali del DPO sono inseriti nelle informative e pubblicati sul sito internet di Ateneo.

Articolo 19 - Responsabile del Trattamento

1. Qualunque soggetto esterno che esegua – in base a un contratto, una convenzione o altro atto giuridico – attività di Trattamento dei Dati Personali per conto del Titolare del Trattamento deve essere designato Responsabile del Trattamento ai sensi dell'art. 28 del GDPR.
2. Il Responsabile del Trattamento è nominato con apposito atto del Titolare del Trattamento e fornisce adeguate garanzie, in particolare, per quanto riguarda le misure tecniche e organizzative atte a consentire il rispetto delle disposizioni del GDPR e la tutela dei diritti dell'Interessato.
3. Il Responsabile del Trattamento risponde per l'eventuale danno causato dal Trattamento solo se non ha adempiuto alle prescrizioni del GDPR specificatamente allo stesso indirizzate o ha agito in modo difforme o contrario rispetto alle istruzioni impartite dal Titolare del Trattamento. Il Responsabile del Trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
4. Il Responsabile del Trattamento risponde in solido con il Titolare del Trattamento al fine di garantire il risarcimento effettivo del danno patito dall'Interessato. Qualora il Titolare del Trattamento o il Responsabile del Trattamento abbia pagato, conformemente all'art. 82, c. 4, del GDPR, l'intero risarcimento del danno, quest'ultimo ha diritto di reclamare dall'altro soggetto coinvolto nello stesso Trattamento la parte del risarcimento corrispondente alla sua parte di responsabilità, conformemente alle condizioni di cui all'art. 82, c. 2, del GDPR.
5. Il Responsabile del Trattamento che non rispetti o ecceda nelle attività di Trattamento le istruzioni allo stesso impartite dal Titolare del Trattamento diventa, a sua volta, Titolare del Trattamento per la parte delle attività relative ai Dati Personali non previste nell'atto di nomina.

Articolo 20 - Sub-Responsabile del Trattamento

1. Il Responsabile del Trattamento può ricorrere ad altro Responsabile del Trattamento ("Sub-Responsabile") per l'esecuzione di specifiche attività di Trattamento per conto del Titolare del Trattamento, previa autorizzazione scritta di quest'ultimo, specifica o generale, mediante contratto o altro atto giuridico con il quale vengano imposti gli stessi obblighi in materia di protezione dei dati contenuti nel contratto tra il Titolare del Trattamento e il Responsabile del Trattamento.

2. Il Responsabile del Trattamento risponde dinanzi al Titolare del Trattamento dell'inadempimento del Sub-Responsabile, anche ai fini del risarcimento di eventuali danni causati.

Articolo 21 - Contitolari del Trattamento

1. Quando uno o più Titolari del Trattamento determinano congiuntamente con l'Ateneo le finalità e i mezzi del Trattamento, gli stessi sono Contitolari del Trattamento.
2. L'Ateneo stipula con il Contitolare o Contitolari del Trattamento un accordo che determini i rispettivi ruoli, rapporti e responsabilità ai fini dell'osservanza della normativa, ai sensi dell'art. 26 del GDPR.
3. L'Interessato può esercitare i diritti riconosciuti dal GDPR nei confronti di ciascun Contitolare del Trattamento.

Articolo 22 - Autorità di controllo

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

CAPO II - ADEMPIMENTI

Articolo 23 – Informazioni da fornire all'Interessato/all'Interessata

1. Nel rispetto del principio di trasparenza, per ogni tipologia di Trattamento di Dati Personali l'Ateneo fornisce agli Interessati le informazioni individuate al c. 5 del presente articolo.
2. L'informativa deve essere concisa, trasparente, intelligibile, facilmente accessibile e redatta con un linguaggio chiaro e semplice. Le informazioni sono fornite per iscritto o con altri mezzi, anche elettronici. L'Interessato potrà chiedere che le informazioni siano fornite oralmente.
3. Se i Dati Personali 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.
4. Se i Dati Personali vengono raccolti presso Terzi, ciascuna Struttura fornisce l'informativa agli Interessati: (i) al momento della prima comunicazione con gli stessi, nel caso in cui i Dati Personali siano destinati alla comunicazione con l'Interessato (ad esempio, invio di una *newsletter*); (ii) al momento della prima comunicazione ad altro destinatario; (iii) negli altri casi, entro un termine ragionevole dall'ottenimento dei Dati Personali, ma, al più tardi, entro un mese, in considerazione delle specifiche circostanze in cui i Dati Personali sono trattati. Non si dovrà fornire l'informativa nei seguenti casi: (i) l'Interessato dispone già delle informazioni; (ii) comunicare tali informazioni risulti impossibile o implichi uno sforzo sproporzionato; (iii) l'ottenimento dei dati o la comunicazione degli stessi sono previsti espressamente dal diritto europeo o nazionale; (iv) i Dati Personali debbano rimanere riservati, conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o nazionale, compreso un obbligo di segretezza previsto per legge.
5. L'informativa deve contenere:
 - a. l'identità e i dati di contatto del Titolare del Trattamento;
 - b. i dati di contatto del Responsabile della Protezione dei Dati;
 - c. le finalità e la base giuridica del Trattamento;
 - d. le categorie di Dati Personali raccolte, e, nei casi in cui i dati non siano stati direttamente conferiti dall'Interessato, anche la fonte da cui hanno origine i Dati Personali e l'eventualità che i dati provengano da fonti accessibili al pubblico;
 - e. gli eventuali destinatari o le eventuali categorie di destinatari dei Dati Personali;
 - f. ove applicabile, l'intenzione del Titolare del Trattamento di trasferire i Dati Personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui agli artt. 46, 47 o 49 del GDPR, il riferimento alle garanzie appropriate od opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili;
 - g. il periodo di conservazione dei Dati Personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

- h. i diritti che l'Interessato può esercitare, quali l'accesso ai Dati Personali, la rettifica o la cancellazione degli stessi, la limitazione del Trattamento dei dati che lo riguardano o l'opposizione al Trattamento degli stessi, il diritto alla portabilità dei dati (ove applicabile) nonché il diritto di proporre reclamo al Garante per la Protezione dei Dati Personali. Qualora il Trattamento sia basato sull'art. 6, c. 1, lett. a), del GDPR, oppure sull'art. 9, c. 2, lett. a), del GDPR, il diritto di revocare il Consenso in qualsiasi momento senza pregiudicare la liceità del Trattamento basata sul Consenso prestato prima della revoca. Qualora il Trattamento sia basato sull'art. 6, c. 1, lett. e), del GDPR il diritto di opporsi in qualsiasi momento al Trattamento dei Dati Personali che lo riguardano deve essere esplicitamente portato all'attenzione dell'Interessato e presentato chiaramente e separatamente da qualsiasi altra informazione;
 - i. se la comunicazione dei Dati Personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'Interessato ha l'obbligo di fornire i Dati Personali nonché le possibili conseguenze della mancata comunicazione di tali dati
 - j. l'esistenza di un processo decisionale automatizzato, compresa la Profilazione, e la logica utilizzata, nonché l'importanza e le conseguenze previste da tale Trattamento.
6. Le informative per le attività di Trattamento di competenza delle Strutture sono predisposte e aggiornate dai Referenti Interni, in collaborazione con il DPO.
7. Gli Autorizzati al Trattamento possono trattare i Dati Personali solo per le specifiche finalità indicate nell'informativa fornita all'Interessato.

Articolo 24 - Registro delle attività di Trattamento

1. L'Ateneo, quale Titolare del Trattamento, istituisce e aggiorna periodicamente il Registro delle attività di Trattamento, che descrive le operazioni di Trattamento svolte presso l'Ateneo e ne delinea le principali caratteristiche. Il Registro è tenuto in formato elettronico.
2. Il Registro delle attività di Trattamento, redatto dall'Ateneo quale Titolare del Trattamento, contiene le seguenti informazioni:
 - a. dati identificativi e di contatto dell'Ateneo, degli eventuali Contitolari e del DPO e dei Referenti di Struttura e/o dei Referenti Interni;
 - b. le finalità del Trattamento;
 - c. la descrizione delle categorie degli Interessati e delle categorie di Dati Personali;
 - d. le categorie di Destinatari, a cui i Dati Personali sono stati o saranno comunicati, compresi Destinatari di paesi terzi od organizzazioni internazionali;
 - e. l'eventuale trasferimento di Dati Personali verso un paese terzo o un'organizzazione internazionale, indicando i dati identificativi del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui all'art. 49, c. 2, del GDPR, la documentazione delle garanzie adeguate;
 - f. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
 - g. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate, di cui all'art. 32, c. 1, del GDPR.
3. L'Ateneo istituisce e aggiorna periodicamente, inoltre, il Registro delle attività di Trattamento in qualità di Responsabile del Trattamento, nel quale sono descritte le attività di Trattamento svolte in qualità di Responsabile per conto di altri Titolari del Trattamento.
4. Il Registro delle attività di Trattamento, redatto dall'Ateneo quale Responsabile del Trattamento, contiene le seguenti informazioni:
 - a. dati identificativi e di contatto dell'Ateneo, del Titolare del Trattamento, di eventuali altri Responsabili del Trattamento e del DPO dell'Ateneo e del Titolare del Trattamento per conto del quale agisce l'Ateneo;
 - b. le categorie di Trattamenti effettuati per conto di ogni Titolare del Trattamento;
 - c. l'eventuale trasferimento di Dati Personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale, e, per i trasferimenti di cui all'art. 49, c. 2, del GDPR, la documentazione delle garanzie adeguate;

- d. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate di cui all'art. 32, c. 1, del GDPR.
5. Ciascuna Struttura collabora alla redazione e all'aggiornamento delle schede dei predetti Registri delle attività di Trattamento, in collaborazione con il DPO.
6. I Registri delle attività di Trattamento devono essere messi a disposizione, su richiesta, al Garante per la Protezione dei Dati Personali.

Articolo 25 - Valutazione di impatto

1. L'Ateneo effettua una valutazione di impatto quando le attività di Trattamento dei Dati Personali che prevedono in particolare l'utilizzo di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del Trattamento, possono presentare un rischio elevato per i diritti e le libertà dell'Interessato.
2. L'art. 35 del GDPR specifica che la valutazione di impatto è obbligatoria nei seguenti casi:
 - a. valutazione sistematica e globale degli 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 analogo significativamente su dette persone fisiche;
 - b. Trattamento, su larga scala, di Categorie Particolari di Dati Personali, quali l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il Trattamento di 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 relativi a condanne penali e a reati o a connesse misure di sicurezza;
 - c. sorveglianza sistematica su larga scala di una zona accessibile al pubblico (videosorveglianza).
3. L'Ateneo, con la collaborazione delle Strutture e del DPO, determinerà i casi nei quali si rende necessario procedere a una valutazione di impatto nel rispetto di quanto previsto dalle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017 e modificate il 4 ottobre 2017, nonché dal Provvedimento n. 467 dell'11 ottobre 2018 (9058979) del Garante per la Protezione dei Dati Personali.
4. Qualora una Struttura ritenesse di trovarsi in uno dei suddetti casi, consulterà il DPO per decidere se effettuare la valutazione di impatto. La decisione deve essere documentata per iscritto e conservata per poter essere prodotta in caso di richiesta da parte del Garante per la Protezione dei Dati Personali.
5. Nei casi in cui, al termine della valutazione di impatto e dell'adozione delle misure di sicurezza, si ritenesse che le attività di Trattamento comportino un rischio elevato per gli Interessati, il Titolare del Trattamento, in collaborazione con il DPO, procederà a consultare il Garante per la Protezione dei Dati Personali ai sensi dell'art. 36 del GDPR.

CAPO III - DIRITTI DELL'INTERESSATO/DELL'INTERESSATA

Articolo 26 - Diritti dell'Interessato/dell'Interessata

1. L'Ateneo garantisce il rispetto dei diritti degli Interessati disciplinati dagli artt. 12-22 del GDPR, ove applicabili, e, in particolare, di:
 - a. essere informati circa le attività di Trattamento svolte sui propri Dati Personali ("diritto a essere informato") (vedasi art. 23 del presente Regolamento);
 - b. 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");
 - c. ottenere la rettifica dei dati inesatti e l'integrazione dei dati incompleti ("diritto alla rettifica");
 - d. ottenere la cancellazione dei propri Dati Personali ("diritto all'oblio");
 - e. ottenere la limitazione al trattamento dei propri dati ("diritto alla limitazione");

- f. 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");
 - g. opporsi in qualsiasi momento, per motivi connessi alla propria situazione particolare, al Trattamento dei propri Dati Personali ai sensi dell'art. 6, c. 1, lett. e), del GDPR, compresa la Profilazione ("diritto all'opposizione");
 - h. 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. Per la gestione delle richieste di esercizio dei diritti si rimanda a quanto stabilito nell'Allegato F al presente Regolamento.

CAPO IV – CIRCOLAZIONE, COMUNICAZIONE, DIFFUSIONE E TRASFERIMENTO DI DATI PERSONALI

Articolo 27 - Circolazione dei Dati Personali all'interno dell'Ateneo

1. L'accesso ai Dati Personali da parte delle Strutture e degli Autorizzati al Trattamento dall'Ateneo è ispirato al principio del *need-to-know*: le informazioni devono essere rese disponibili esclusivamente ai soggetti che hanno necessità di accedervi, per lo svolgimento dell'attività lavorativa, mediante strumenti, sia cartacei sia informatici, atti a facilitarne la fruizione.

Articolo 28 - Comunicazione dei Dati Personali al di fuori dell'Ateneo

1. La comunicazione dei Dati Personali al di fuori dell'Ateneo nei confronti di determinati soggetti esterni può avvenire solo ove sussista una specifica base giuridica o un'eccezione al divieto di trattamento (vedasi artt. 9, 10, 11, 12 e 13 del presente Regolamento).
2. 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 regolamento, deve essere sottoposta per iscritto e motivata; l'accogliibilità della richiesta sarà valutata dalla Struttura competente in collaborazione con il DPO.

Articolo 29 - Diffusione dei Dati Personali

1. La diffusione di Dati Personali, con conseguente conoscibilità degli stessi da parte di soggetti indeterminati, può avvenire solo ove prevista da una norma di legge o di regolamento applicabile alla fattispecie concreta ovvero in conformità ad un atto amministrativo generale adottato dall'Ateneo.

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

1. Il trasferimento di Dati Personali verso un Paese terzo o un'organizzazione internazionale avviene sulla base di una delle misure adeguate previste dal Capo V del GDPR, quali:
 - a. decisione di adeguatezza adottata a norma dell'art. 45, c. 3, del GDPR e delle decisioni adottate sulla base dell'art. 25, c. 6, della Direttiva 95/46/CE;
 - b. uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche od organismi pubblici;
 - c. le norme vincolanti di impresa;
 - d. le clausole contrattuali standard adottate dalla Commissione Europea o da un'Autorità di controllo e approvate dalla Commissione Europea secondo la procedura d'esame di cui all'art. 93, c. 2, del GDPR;
 - e. un codice di condotta approvato a norma dell'art. 40 del GDPR, unitamente all'impegno vincolante ed esecutivo da parte del Titolare del Trattamento o del Responsabile del Trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli Interessati;
 - f. un meccanismo di certificazione approvato a norma dell'art. 42 del GDPR, unitamente all'impegno vincolante ed esigibile da parte del Titolare del Trattamento o del Responsabile

- del Trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli Interessati.
2. Il trasferimento di Dati Personali che non può basarsi su una decisione di adeguatezza o su una garanzia adeguata, che si verifica in condizioni particolari e in casi di trasferimenti sporadici, può avvenire ove ricorra una delle seguenti condizioni:
 - a. l'Interessato ha esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;
 - b. il trasferimento è necessario all'esecuzione di un contratto concluso tra l'Interessato e il Titolare del Trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'Interessato;
 - c. il trasferimento è necessario per la conclusione o l'esecuzione di un contratto stipulato tra il Titolare del Trattamento e un'altra persona fisica o giuridica a favore dell'Interessato;
 - d. il trasferimento è necessario per importanti motivi di interesse pubblico;
 - e. il trasferimento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
 - f. il trasferimento è necessario per tutelare gli interessi vitali dell'Interessato o di altre persone, qualora l'Interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio Consenso;
 - g. il trasferimento è effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può essere consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.
 3. Nel caso di trasferimento di Dati Personali verso un paese terzo o un'organizzazione internazionale, ciascuna Struttura individua, in collaborazione con il DPO, l'ideale misura per garantire la tutela dei Dati Personali.

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

Articolo 31 - Misure di sicurezza

1. L'Ateneo adotta misure di sicurezza, 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 e con il supporto del DPO.
3. Ciascuna Struttura è responsabile del rispetto delle misure tecniche individuate da ASIT, nonché di quelle individuate dalla Struttura stessa, in collaborazione con il Titolare del Trattamento e con il supporto di ASIT.

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 di sicurezza 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 di selezione e scarto dell'Ateneo.

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

1. Per la gestione degli incidenti di sicurezza e delle Violazioni dei Dati Personali si rimanda a quanto stabilito nell'Allegato G al presente Regolamento.

TITOLO IV - CONTROLLI, SANZIONI E DISPOSIZIONI FINALI

Articolo 34 - Controlli ammessi

1. Il Titolare del Trattamento o altri soggetti da quest'ultimo delegati hanno facoltà di effettuare controlli, anche preventivi, circa l'adozione delle corrette misure per garantire il rispetto dei diritti e delle libertà fondamentali degli Interessati, i cui Dati Personali sono oggetto di Trattamento da parte dell'Ateneo.
2. I controlli possono avere a oggetto anche le risorse informatiche messe a disposizione dall'Ateneo, nel rispetto di quanto disposto nell'Allegato E del presente Regolamento.

Articolo 35 - Sanzioni

1. I comportamenti in violazione della normativa vigente in tema di protezione dei Dati Personali, del presente Regolamento, dei suoi Allegati e delle regole operative che hanno una rilevanza disciplinare sono sanzionati secondo le forme e le modalità previste dagli ordinamenti delle varie tipologie di personale coinvolto, fermi restando i diversi profili di responsabilità civile e penale.
2. Tali comportamenti sono segnalati, oltre all'organo disciplinarmente competente, anche al Magnifico Rettore e al Direttore Generale, che valuteranno le modalità di intervento più idonee, anche a tutela di eventuali danni economici e/o di immagine subiti dall'Ateneo.

Articolo 36 - Modalità di approvazione e aggiornamento del presente Regolamento e relativi Allegati

1. Il presente Regolamento è approvato dal Consiglio di Amministrazione dell'Ateneo a maggioranza assoluta dei componenti. Sulle materie per cui si renda necessario, verrà siglato un accordo con i Sindacati.
2. Il presente Regolamento potrà essere aggiornato o integrato, previa approvazione da parte del Consiglio di Amministrazione, a seguito di:
 - a. modifiche normative sopravvenute;
 - b. introduzione di nuove pratiche volte a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
 - c. inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti;
 - d. introduzione di nuovi Allegati.
3. Le eventuali modifiche e/o gli eventuali aggiornamenti degli Allegati del presente Regolamento non costituiscono modifica di quest'ultimo e vengono emanati con provvedimento del Direttore Generale.

ALLEGATO A

VIDEOSORVEGLIANZA NELLE SEDI UNIVERSITARIE

Articolo 1 - Principi generali

1. Il presente Allegato disciplina il Trattamento dei Dati Personali realizzato mediante impianti di videosorveglianza installati presso le sedi dell'Ateneo.
2. Al Trattamento dei Dati Personali realizzato mediante impianti di videosorveglianza si applicano le disposizioni di carattere generale contenute nel Regolamento così come integrate da quelle del presente Allegato.
3. È lecito installare impianti di videosorveglianza solo al fine di:
 - a. garantire un adeguato grado di sicurezza alla popolazione universitaria (dipendenti, studenti, ecc.);
 - b. prevenire eventuali atti delittuosi e vandalici presso le sedi dell'Ateneo nonché garantire l'esercizio del diritto di difesa;
 - c. tutelare gli immobili di proprietà o in gestione all'amministrazione universitaria;
 - d. tutelare il patrimonio dei beni mobili presenti nelle sedi universitarie.
4. Non è possibile installare sistemi di videosorveglianza ovvero utilizzare i dati raccolti con questi ultimi per finalità ulteriori rispetto a quelle indicate.

Articolo 2 - Titolare del Trattamento

1. Il Titolare del Trattamento dei Dati Personali raccolti tramite gli impianti di videosorveglianza attivi all'interno e all'esterno dei locali dell'Ateneo è l'Università Ca' Foscari Venezia nella persona del Magnifico Rettore.
2. Ad ASIT è affidato il compito di garantire l'osservanza delle norme di legge in materia e di quanto stabilito nel presente Allegato.
3. Il Titolare conserva la documentazione che dimostri le ragioni dell'installazione di tali sistemi e la conformità agli adempimenti prescritti dal GDPR, dal Codice Privacy e dalle Linee Guida n. 3/2019 del Comitato Europeo per la Protezione dei Dati, oltre a quelli previsti dal presente Regolamento. Tale documentazione dovrà essere esibita nell'eventualità di visite ispettive da parte del Garante per la Protezione dei Dati Personali o di altre Autorità.

Articolo 3 - Responsabile del Trattamento

1. L'Ateneo può affidare la gestione degli impianti o altre attività connesse alla videosorveglianza a soggetti terzi nominati Responsabili del Trattamento con apposito atto che specifichi le istruzioni a cui il Responsabile del Trattamento stesso è soggetto. L'Ateneo conserva l'atto di nomina ed eventuali ulteriori documenti connessi che dovranno essere esibiti in caso di visite ispettive da parte del Garante per la Protezione dei Dati Personali o di altre Autorità.

Articolo 4 - Conservazione delle immagini

1. Le immagini registrate mediante le telecamere collocate presso le sedi dell'Ateneo dovranno essere conservate in appositi sistemi di registrazione per un periodo non superiore a quarantotto ore successive alla loro rilevazione; decorso il predetto periodo, le stesse dovranno essere automaticamente cancellate. Restano salve particolari esigenze di ulteriore conservazione in relazione a festività o a chiusure delle sedi universitarie, nonché nel caso di specifiche richieste da parte dell'Autorità Giudiziaria o per l'eventuale difesa in giudizio.

Articolo 5 - Controllo degli accessi alle immagini

1. L'accesso ai locali e/o agli armadi dove sono collocati gli strumenti di registrazione e/o dove sono conservate le immagini già registrate deve essere autorizzato dall'Ateneo. In particolare, i soggetti che potranno avere accesso alle immagini e il personale addetto alla gestione delle predette immagini e dei predetti impianti dovranno essere nominati Autorizzati al trattamento e/o Amministratori di Sistema con apposito atto.

Articolo 6 - Informazioni agli Interessati

1. Il Titolare si assicura che gli Interessati, ovvero coloro le cui immagini vengono registrate dagli strumenti di videosorveglianza, siano sempre informati prima di accedere a un'area videosorvegliata.
2. L'informativa è fornita attraverso cartelli affissi alle pareti recanti, come minimo, indicazioni sull'identità del Titolare del Trattamento, sulla finalità perseguita e sui diritti dell'Interessato. I supporti con l'informativa: (i) sono collocati prima del raggio di azione della telecamera, anche nelle immediate vicinanze e non necessariamente a contatto con le stesse; (ii) hanno un formato e un posizionamento tale da essere chiaramente visibili in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno; (iii) inglobano un simbolo o un'icona di facile e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.
3. In presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, potranno essere installati più cartelli.
4. L'informativa estesa, che illustra le principali caratteristiche dell'impianto di videosorveglianza e che contiene tutti gli elementi prescritti dall'art. 13 del GDPR, è reperibile sul sito web di Ateneo.

Articolo 7 - Basi giuridiche

1. Con riferimento all'utilizzo di impianti di videosorveglianza per le finalità di cui all'art. 1 del presente Allegato, la base giuridica è rappresentata dall'art. 6, c. 1, lett. c), del GDPR, ossia "*adempimento a un obbligo di legge*", ai sensi del D.Lgs. n. 81/2008 in materia di tutela della salute e della sicurezza nei luoghi di lavoro, nel rispetto dell'art. 4 dello Statuto dei Lavoratori (L. n. 300/1970), così come richiamato dall'art. 114 del Codice Privacy; il Trattamento delle immagini rilevate dagli impianti di videosorveglianza, inoltre, avviene nel rispetto di quanto prescritto dalle Linee Guida n. 3/2019 sul "*trattamento dei dati personali attraverso dispositivi video*" dell'*European Data Protection Board* (adottate il 29 gennaio 2020).

Articolo 8 - Diritti dell'Interessato/dell'Interessata

1. L'Interessato può esercitare i diritti di cui al TITOLO II, CAPO III, art. 26, del presente Regolamento con riguardo alle immagini riprese dagli impianti di sorveglianza, ad esclusione del diritto di rettifica. Sono sempre fatti salvi gli eventuali diritti dei terzi.

Articolo 9 - Collocazione delle telecamere

1. La collocazione delle telecamere è riportata in appositi documenti predisposti e aggiornati dal Dirigente di ASIT. L'integrazione o la modifica della collocazione delle telecamere viene preventivamente sottoposta all'attenzione dei Sindacati, con i quali viene sottoscritto apposito accordo.
2. L'angolo visuale delle telecamere dovrà essere regolato in modo tale da non ledere la riservatezza e la dignità degli Interessati. Non dovranno pertanto, per esempio, essere riprese postazioni fisse di lavoro ovvero aree destinate ad attività ricreative e personali (ad esempio, servizi igienici).

ALLEGATO B

ATTRIBUZIONE DELLE CREDENZIALI DI ATENEO E DELLE CASELLE DI POSTA ELETTRONICA

Articolo 1 - Premessa

1. L'Ateneo promuove l'utilizzo della rete informatica e telematica, di Internet e della posta elettronica quali strumenti utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali.
2. L'Ateneo, quale datore di lavoro, è tenuto ad assicurare la funzionalità e il corretto impiego degli strumenti informatici di sua proprietà, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa e adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informativi, nel rispetto dei generali principi di proporzionalità, pertinenza, necessità e non eccedenza delle attività di Trattamento dei Dati Personali, applicando ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati di proprietà.
3. Il presente documento, stilato in conformità alla *policy* di utilizzo della rete GARR, in quanto fornitore di connettività, regola la concessione delle credenziali di accesso alla rete dati dell'Ateneo e l'attribuzione di caselle di posta elettronica, con l'obiettivo di proteggere la riservatezza, l'integrità e la disponibilità di tutti gli elementi della rete informatica dell'Ateneo da accessi non autorizzati.

Articolo 2 - Account utente

1. La creazione degli account e il rilascio delle credenziali è gestito da ASIT ed è riservato a specifiche tipologie di utenti elencate di seguito nel presente Allegato.
2. L'accesso ai servizi online dell'Ateneo avviene mediante un codice di identificazione attribuito all'utente (*username*), una parola chiave (*password*) e una *one-time-password* (per le tipologie di utenza che lo prevedono). In alternativa è possibile utilizzare l'autenticazione via SPID o CIE e successivamente selezionare uno degli account associati alla persona.
3. Nel momento dell'attribuzione di uno *username*, l'utente riceve un PIN che gli permette di impostare la propria *password* che dovrà cambiare almeno ogni 180 giorni, o immediatamente nei casi in cui se ne sospetti la compromissione, scegliendone una che osservi le seguenti regole:
 - a. la *password* deve essere composta da almeno 10 caratteri alfanumerici;
 - b. l'utente deve utilizzare, nella composizione della propria *password*, almeno un carattere numerico, un carattere maiuscolo, un carattere minuscolo e un carattere speciale all'interno di un insieme definito e indicato all'utente in fase di inserimento;
 - c. la *password* non deve contenere parole o parti di parola di uso comune (es. venez123) o sequenze comuni di caratteri o numeri (es. 123456 qwerty aaaaa) e non deve essere stata utilizzata nei precedenti 12 mesi;
 - d. la *password* non deve contenere elementi agevolmente riconducibili all'utente o riferimenti basati su informazioni facilmente deducibili, quali il proprio nome, il nome dei famigliari, la data di nascita, il codice fiscale.
4. Se la *password* non viene cambiata entro la sua scadenza utilizzando la procedura www.unive.it/newpass, l'*account* verrà disattivato e lo stesso sarà bloccato fino alla riattivazione, che può avvenire tramite una procedura basata su una *one-time-password* inviata automaticamente tramite SMS, tramite l'account SPID o CIE dell'utente (collegandosi al sito web www.unive.it/newpass) oppure richiesta contattando il servizio di Help Desk di ASIT, che provvederà a fornire un nuovo PIN previo riconoscimento dell'utente.
5. Gli *account* bloccati per scadenza *password* e non più riattivati dopo 6 mesi vengono definitivamente eliminati dagli Amministratori di Sistema.
6. L'utente è responsabile della conservazione e della riservatezza delle proprie credenziali e, conseguentemente, rimane il solo responsabile per tutti gli usi a esse connessi o correlati (e per eventuali danni e conseguenze pregiudizievoli arrecati all'Ateneo e/o a terzi).
7. L'utente dovrà custodire diligentemente la propria *password* nonché adottare le necessarie cautele per preservarne la sicurezza e la segretezza. In particolare, l'utente:

- a. ha l'obbligo di mantenere la propria *password* riservata e non divulgarla a terzi né trascriverla su supporti fisici (es. fogli, post-it, agende, ecc.);
 - b. non deve permettere ad altri (es. colleghi, familiari, ecc.) di operare con il proprio identificativo utente;
 - c. si impegna a modificare immediatamente la *password* ogni qualvolta ritenga che sussista il rischio che questa sia stata conosciuta da terzi ovvero su richiesta esplicita di ASIT ove vengano rilevate compromissioni delle *password*;
 - d. ove rilevi problematiche relative alla propria *password* (compromissione ovvero debolezza della stessa), dovrà immediatamente informare ASIT utilizzando il sistema di richiesta di supporto utenti.
 - e. Per le tipologie di *account* che prevedono l'attivazione dell'OTP l'utente dovrà conservare con cura il pdf (o la sua stampa su carta) contenente il QRCode con il *seed* per l'attivazione. Tale documento è strettamente personale e non deve essere divulgato o mostrato a terzi, serve esclusivamente all'utente per attivare l'OTP in un nuovo dispositivo, ad esempio in caso di sostituzione dello *smartphone*.
8. Gli *account* di accesso ai servizi informatici dell'Ateneo si suddividono in otto gruppi:
- a. *account* per il personale (che comprende i Dirigenti, il personale tecnico-amministrativo, il personale docente e ricercatore, i collaboratori ed esperti linguistici, nonché i collaboratori dell'Ateneo);
 - b. *account* per gli studenti;
 - c. *account* per ex studenti;
 - d. *account* per gli ospiti wifi;
 - e. *account* per gli ospiti biblioteche;
 - f. *account* per i registrati al sito;
 - g. *account* per gli Amministratori di Sistema;
 - h. *account* di servizio.
9. A ogni *account* sono associati dei diritti di accesso che dipendono dal ruolo dell'utente e dall'uso dell'*account* stesso (vedasi tabella all'art. 4.4).
10. Agli utenti sono attribuiti gli *account* secondo il gruppo di appartenenza. È possibile che un singolo utente sia in possesso di *account* di diversi tipi (es. dipendenti iscritti a un corso di laurea); in questo caso, l'utente dovrà utilizzare l'*account* corretto in base alla situazione in cui si trova a operare.
11. Oltre all'*account* primario, è possibile che vengano attribuiti all'utente *account* aggiuntivi (detti *account* secondari) abilitati esclusivamente all'uso di servizi specifici. L'utente a cui è stato attribuito un *account* di questo tipo ne è responsabile in maniera del tutto analoga rispetto all'*account* primario.

Articolo 3 - IDEM e EduGAIN

1. L'Ateneo aderisce al servizio IDEM (IDentity Management per l'accesso federato), l'infrastruttura di autorizzazione e autenticazione della rete GARR.
2. Nell'ambito della Federazione IDEM, GARR agisce da coordinatore, fornendo l'infrastruttura centrale e i servizi e sottoscrivendo i contratti d'adesione. I servizi raggiungibili attraverso la Federazione sono resi disponibili dai membri e *partner* di IDEM. Il sistema, a ogni richiesta di accesso ai servizi, mostrerà all'utente la lista dettagliata delle informazioni che verranno trasferite al titolare del servizio e l'utente potrà accettare o meno tale trasferimento. Maggiori informazioni sulla Federazione IDEM sono disponibili alla pagina <https://www.unive.it/pag/31755>.
3. IDEM a sua volta aderisce a EduGain, ovvero la federazione europea delle federazioni nazionali. Le funzionalità e le regole sugli attributi sono le medesime di IDEM, con la differenza che l'offerta di servizi disponibili tramite l'autenticazione federata si allarga a livello europeo. Maggiori informazioni sulla federazione EduGain sono rinvenibili alla pagina: http://www.geant.org/Services/Trust_identity_and_security/eduGAIN.

Articolo 4 - Credenziali

1. Il nome utente attribuito a un *account* coincide con lo *username* di un eventuale indirizzo di posta elettronica collegato all'*account* stesso.
2. L'indirizzo di posta elettronica è completato dal dominio, che può essere @unive.it oppure @stud.unive.it a seconda della tipologia di utente.
3. Sono previste le seguenti tipologie di *account*:

Personale

Username: nome.cognome
Dominio email: @unive.it
OTP: obbligatorio
SPID/CIE: facoltativo

Studenti

Username: matricola
Dominio email: @stud.unive.it
OTP: facoltativo
SPID/CIE: facoltativo

EX-Studenti

Username: matricola
OTP: non previsto (obbligo SPID / CIE)
SPID/CIE: obbligatorio

Ospiti wifi

Username: wifi00000
OTP: non previsto
SPID/CIE: non previsto

Ospiti biblioteche

Username: ucf.000000
OTP: obbligatorio
SPID/CIE: facoltativo

Registrati al sito

Username: unive.000000
OTP: non previsto
SPID/CIE: obbligatorio

Amministratori di Sistema

Username: adm_cognome
OTP: obbligatorio
SPID/CIE: facoltativo

Account di servizio

Username: libero
OTP: facoltativo
SPID/CIE: facoltativo

4. Nel caso in cui l'utente abbia più nomi e/o cognomi, quest'ultimi generalmente vengono uniti senza spazi (es: nome1 nome2 cognome1 cognome2 diventa nome1nome2.cognome1cognome2).
5. L'utente può decidere, al momento della richiesta dell'*account*, di escludere alcuni nomi o cognomi dal nome utente; inoltre, la procedura di creazione dell'*account* potrà guidare l'utente nella scelta di un *username* alternativo nel caso superi la lunghezza massima (di 20 caratteri) o di omonimie.

6. Non è possibile creare nomi utente che contengano nomi di fantasia o *alias*, fatti salvi i nomi utenti già creati e in utilizzo.

Articolo 4.1 - Modalità di rilascio dell'*account*

Articolo 4.1.a. - *Account Personale*

1. È compito dell'utente richiedere l'*account* utilizzando la procedura guidata disponibile alla pagina <http://www.unive.it/account>.
2. L'*account* può essere richiesto a partire dal giorno di inizio del rapporto di lavoro o di collaborazione.
3. Ogni *account* viene autorizzato da un responsabile individuato in base al ruolo e alla struttura di appartenenza secondo la tabella disponibile alla pagina <https://apps.unive.it/utenti/listaruoli>.
4. È responsabilità di chi autorizza la richiesta dell'*account* procedere al riconoscimento dell'utente e garantire l'appartenenza al ruolo per cui viene richiesto l'*account*.
5. L'autorizzazione può essere:
 - a. implicita (utente già inserito in un applicativo gestionale); in tal caso l'*account* verrà rilasciato immediatamente;
 - b. esplicita (non esiste un *database* di riferimento); in tal caso il responsabile dovrà autorizzare esplicitamente (tramite apposita procedura via e-mail) il rilascio dell'*account* entro 14 giorni. In caso di mancata risposta, l'autorizzazione si intenderà negata.
6. La durata dell'*account* dipende dal tipo di rapporto di lavoro o di collaborazione.

Articolo 4.1.b. - *Account Studenti*

1. Il numero di matricola e la *password* vengono inviati agli studenti, al momento del perfezionamento dell'immatricolazione, via e-mail all'indirizzo fornito dagli stessi all'atto dell'immatricolazione stessa.
2. L'*account* da studenti rimane attivo fino ai 6 mesi successivi al termine della carriera, trascorsi i quali l'*account* viene trasformato in *account* da ex studente.
3. Lo *username* corrisponde al numero di matricola. Nel caso in cui lo studente abbia avuto nel corso delle sue carriere più numeri di matricola, lo *username* di riferimento è l'ultimo numero di matricola assegnato allo studente.

Articolo 4.1.c. - *Account Ex Studenti*

1. Nel caso di ex studenti, a casella email viene disattivata e successivamente eliminata trascorsi 6 mesi dal termine della carriera, i servizi forniti agli studenti vengono disattivati, la *password* viene rimossa e l'accesso (limitato ad alcuni servizi in area riservata) rimane a vita utilizzando SPID o CIE.

Articolo 4.1.d. - *Account Ospiti Wifi*

1. Per gli eventi di Ateneo è previsto l'accesso a internet via Wifi per gli ospiti, l'organizzatore dell'evento può richiedere ad ASIT il rilascio di uno o più *account*. Tali *account* possono avere la durata massima di 14 giorni (rinnovabili su richiesta) e sono abilitati solo all'accesso a internet via Wifi e opzionalmente all'accesso ai PC delle aule (se usato ad esempio da un relatore). Gli *account* vengono intestati al richiedente che ne è responsabile.

Articolo 4.1.e. - *Account Ospiti biblioteche*

1. Le biblioteche rilasciano account agli ospiti del servizio (cittadini, esterni non studenti, o dipendenti dell'Ateneo). Tali account hanno le medesime regole di gestione password del personale, ma sono limitati esclusivamente all'accesso ai servizi di prenotazione accesso e gestione prestiti in area riservata.

Articolo 4.1.f. - *Account Registrati al sito*

1. Chiunque può registrarsi da <https://www.unive.it/registrazione> e ottenere un *account* da registrati. Tali *account* sono abilitati esclusivamente all'accesso al portale ESSE3 per l'iscrizione ad attività formative e ad alcuni servizi dedicati a futuri studenti. Non viene rilasciata *username* e *password*, l'accesso deve avvenire esclusivamente via SPID/CIE. Utenti che non possono avere SPID o CIE

(es. minorenni e stranieri) possono richiedere il rilascio di *username* e *password* previo riconoscimento tramite la procedura <https://www.unive.it/nospidaccess>.

2. Gli *account* da registrati vengono cancellati automaticamente se la persona conclude la fase di immatricolazione, o dopo 2 anni se non effettua alcuna operazione. In ogni caso, gli *account* si possono ricreare in qualsiasi momento.

Articolo 4.1.g. - Account Amministratori di Sistema

1. Ai soggetti nominati Amministratori di Sistema, per motivi di sicurezza, viene rilasciato un secondo *account* distinto da quello personale da usarsi esclusivamente per l'accesso ai sistemi che ospitano tali servizi.

Articolo 4.1.h. - Account di servizio

1. Gli *account* di servizio sono *account* speciali utilizzati nello scambio di dati tra sistemi (anche detti *machine-to-machine* o *M2M*); per tale motivo non hanno uno schema preciso nella composizione dell'*username* e non sono vincolati alle regole standard di gestione delle *password* (che dipendono dalle caratteristiche dei sistemi coinvolti). Sono associati a una persona che ne è responsabile, ma non si possono usare per autenticarsi manualmente a servizi dedicati a utenti "umani".

Articolo 4.2 - Rinnovo

1. Per gli *account* che hanno una durata prefissata, qualora l'utente continui ad avere necessità di utilizzare l'*account*, e ferma restando l'eleggibilità dell'utente, sarà necessario richiedere il rinnovo, seguendo le indicazioni che verranno inviate via e-mail 30 giorni prima della disattivazione dello stesso.

Articolo 4.3 - Scadenza e dismissione dell'*account*

1. Una volta scaduto l'*account*, i dati correlati verranno conservati per 6 mesi per poter intervenire in caso di necessità o a fronte di richiesta di rinnovo tardivo. Trascorso tale periodo, l'*account* viene cancellato definitivamente e tutti i dati connessi (es. messaggi di e-mail, documenti presenti sul *Google Drive* personale, ecc.) verranno cancellati definitivamente.

Articolo 4.4 - Ruoli e diritti di accesso

1. La tabella sottostante riporta i ruoli e i diritti di accesso che possono essere associati a ciascun *account* utente.

Ruolo	Area riservata	Email Istituzionale	Wifi/VPN	Accesso biblioteche	PC lezione frontale	Durata
Assegnista	✓	✓	✓	✓	✓	1 anno
Cultore della materia	✓	✓	✓	✓		1 anno
Stagista	✓	✓	✓	✓		1 anno
Borsista	✓	✓	✓	✓		1 anno

Volontario servizio civile	✓	✓	✓	✓		1 anno
Tutor specialistici	✓	✓	✓	✓	✓	1 anno
Prestatori d'opera, partite IVA, collaboratori autonomi	✓					1 anno
Supervisor di tirocinio Servizio Sociale	✓	✓	✓	✓		1 anno
Tutor informativi	✓		✓	✓	✓	1 anno
Collaboratore Fondazione	✓	✓	✓			1 anno
Visiting professor	✓	✓	✓	✓	✓	1 anno
Teaching Assistant	✓	✓	✓	✓	✓	1 anno
Visiting scholar			✓	✓		1 anno
Collaboratori progetti di ricerca	✓		✓			1 anno
Ambasciatori di Ca' Foscari nelle scuole superiori	✓		✓	✓		1 anno
Docenti SIE	✓	✓	✓	✓	✓	1 anno
Collaboratori didattici CLA	✓	✓	✓			1 anno
Collaboratori Ciset	✓	✓	✓			1 anno

Personale esterno istituto Confucio	✓	✓				1 anno
Dipendenti cooperative portinerie	✓		✓			1 anno
Dipendenti cooperativa call center/URP			✓			1 anno
Dipendenti Terra			✓			1 anno
Dipendenti Euro&Promos			✓			1 anno
Utenti banca dati studenti per la verifica delle autocertificazioni (ESSE3PA)	✓					1 anno
Personale Start-UP			✓			1 anno
Componente organi collegiali, o di altri organi o commissioni dell'Ateneo	✓	✓	✓	✓		1 anno
Docente a contratto o supplente di altre università	✓	✓	✓	✓	✓	2 anni accademici
Collaboratore a contratto	✓	✓	✓			1 anno
Dottorando	✓	✓	✓		✓	rapporto + 1 anno
Manutentori esterni	✓		✓			1 anno

Docenti e ricercatori	✓	✓	✓	✓	✓	rapporto + 1 anno
Personale tecnico amministrativo e tecnologi	✓	✓	✓	✓	✓	rapporto + 1 anno
Collaboratori ed Esperti Linguistici	✓	✓	✓	✓	✓	rapporto + 1 anno
Personale in quiescenza		✓	✓	✓		a vita
Studenti	✓	✓	✓	✓		rapporto + 6 mesi
Ex studenti	✓					a vita
Ospiti biblioteche				✓		1 anno
Ospiti WIFI			✓			14 giorni

2. Gli utenti che non rientrano in nessuno dei ruoli sopra indicati possono richiedere l'*account* esclusivamente come "Registrati al sito" e accedere tramite SPID o CIE. Tali *account* non hanno alcun privilegio e possono accedere solo ad alcuni servizi dedicati a tutti i cittadini.

3. Nel caso di specifiche e documentate necessità di ottenere un *account* con diritti particolari al di fuori dei ruoli stabiliti, è necessario contattare direttamente ASIT che, di concerto con la Direzione Generale o il Rettorato, valuterà la richiesta. In generale, non è possibile assegnare un indirizzo email @unive.it a utenti diversi da quelli citati nella tabella che precede, salvo specifici accordi o convenzioni in essere.

Articolo 4.5. - Revoca delle credenziali di autenticazione

1. Per gli *account* autorizzati in modo esplicito, chi ha autorizzato l'*account* può richiederne la revoca anche prima della naturale scadenza aprendo un *ticket* da www.unive.it/ticket alla voce "Servizi personali: *account*".
2. In ogni caso, gli *account* degli utenti saranno sospesi o bloccati:
 - a. trascorsi sei mesi dall'ultimo *login* dell'utente (tranne che per gli *account* utilizzati per la manutenzione);
 - b. nel caso in cui vengano rilevate dai sistemi dell'Ateneo, o siano segnalate da terzi, attività dannose per l'Ateneo o che violino qualsiasi regolamento dell'Ateneo o norma della legislazione italiana;
3. Qualora venga rilevato dai sistemi dell'Ateneo o segnalato ad ASIT l'uso improprio dell'*account* utente, fatti i dovuti controlli nel rispetto di quanto previsto nell'Allegato E al presente Regolamento, gli Amministratori di Sistema, oltre alla sospensione delle credenziali, procederanno alla segnalazione alla segreteria studenti o ad ARU per le necessarie verifiche e le eventuali successive azioni disciplinari.

Articolo 5 - Caratteristiche degli account di amministratore di sistema

1. Agli Amministratori di Sistema sono assegnati degli *account* personali con privilegi specifici sui *server* e sull'infrastruttura di rete dell'Ateneo.
2. Gli *account* degli Amministratori di Sistema devono essere utilizzati esclusivamente quando si svolgono funzioni di gestione dei sistemi informatici dell'Ateneo. Nel caso in cui un utente cessi la sua attività di amministratore il relativo *account* viene cancellato.
3. Gli *account* degli Amministratori locali di Sistema devono essere, ove possibile, disabilitati. Quando questo non è possibile, verrà impostata una *password* di servizio (vedasi art. 6 del presente Allegato). In ogni caso l'accesso attraverso tali *account* sarà possibile solo tramite *console* locale della macchina.
4. Nel caso si sospetti un accesso non autorizzato a un qualunque *account* di sistema, amministrativo o dell'utente, tutte le *password* potenzialmente compromesse dovranno essere immediatamente modificate.

Articolo 6 - Caratteristiche degli account sui sistemi di servizio

1. Alcuni sistemi per la gestione dell'infrastruttura informatica prevedono la definizione di *account* per la loro amministrazione. Laddove tecnicamente fattibile, a tali *account* saranno applicate le stesse regole richieste per gli *account* standard, compresa la lunghezza della *password*, la complessità e la tempistica per la modifica. In caso contrario, l'Amministratore di Sistema che abilita il servizio dovrà procedere alla generazione *random* di una *password* estremamente complessa (almeno 16 caratteri e rispondente ai requisiti standard di complessità delle *password*) e ad assegnarla al servizio. La *password* così generata non sarà cambiata se non quando strettamente necessario, ad esempio a causa della riconfigurazione del servizio. Nei sistemi in cui non è possibile prevedere *account* multipli di amministrazione, la *password* dell'unico *account* dovrà essere cambiata ogni volta che un amministratore cessa il suo incarico.
2. L'elenco degli *account* di servizio utilizzati verrà mantenuto aggiornato dagli Amministratori di Sistema ed esibito in caso di eventuali controlli.

Articolo 6.1. - Autenticazione tramite chiave

1. In specifici contesti, per gli *account* di servizio e/o di amministrazione, è possibile l'autenticazione attraverso sistemi di crittografia asimmetrica. Questo sistema sostituisce l'uso della *password* e lega la verifica dell'identità dell'utente al possesso di una chiave privata preventivamente autorizzata. Tale chiave privata è conservata in forma di *file*, al quale vanno applicate tutte le opportune protezioni per tutelarne la riservatezza.
2. Le chiavi utilizzate dovranno avere dimensione minima di 2048 bit se di tipo RSA, 384 bit se di tipo ECSDA, o il numero massimo di bit consentiti dal sistema ove questo sia minore di quelli precedentemente citati.
3. Nel caso un utente/amministratore cessi il proprio servizio le relative chiavi andranno cancellate da tutti i sistemi in cui erano presenti.

Articolo 7 - Verifica degli account

1. L'Ateneo, al fine di garantire il corretto funzionamento delle risorse informatiche aziendali, effettuerà attività di verifica periodica dell'attribuzione degli *account* utente, esclusivamente finalizzate a individuare e rimuovere eventuali *account* non più necessari o privilegi autorizzativi in eccesso attribuiti erroneamente agli utenti.
2. A tal riguardo si ricorda che gli *account* rilasciati a utenti il cui ruolo non è gestito in *database* ufficiali dell'Ateneo vanno rinnovati di anno in anno e i responsabili dovranno esplicitamente autorizzare il rinnovo.
3. Con la stessa frequenza verranno verificati gli *account* dei *database* e quelli di sistema, siano essi riconducibili a una singola persona piuttosto che a un servizio o a un'applicazione. Qualora gli *account* siano riconducibili a una specifica persona, è richiesto, se tecnicamente possibile, di

impostare la scadenza dell'*account* a 90 o 180 giorni a seconda dei privilegi attribuiti e del tipo di informazioni trattate.

4. Sempre con cadenza almeno annuale saranno verificati gli *account* appartenenti al gruppo degli Amministratori di Sistema per controllare l'appropriatezza del privilegio.

ALLEGATO C

INFRASTRUTTURE E RISORSE INFORMATICHE

Articolo 1 - Gestione e implementazione dei servizi di rete delle strutture di Ateneo

1. Le strutture di Ateneo utilizzano i servizi messi a disposizione da ASIT. Qualora il responsabile di una delle Strutture dell'Ateneo ritenga necessaria l'attivazione di un servizio informatico non fornito da ASIT o di un servizio che, sebbene disponibile attraverso ASIT, abbia funzionalità non coincidenti con quelle fornite, deve comunicare tale esigenza al Dirigente di ASIT, evidenziando gli obiettivi che intende raggiungere mediante tale attivazione.
2. ASIT, a seguito di tale comunicazione, provvede alternativamente a:
 - a. programmare l'implementazione dei nuovi servizi richiesti, laddove si rilevi un interesse concreto e diffuso;
 - b. estendere le funzionalità di servizi già esistenti;
 - c. consigliare alla Struttura l'utilizzo di servizi già implementati o in fase di implementazione anche in altre Strutture;
 - d. declinare, fornendo adeguate giustificazioni, la richiesta di attivazione del nuovo servizio, lasciando alla Struttura la decisione sulla possibilità di implementarlo autonomamente secondo quanto definito di seguito;
 - e. vietare l'installazione del sistema/l'erogazione del servizio per documentati motivi di sicurezza od opportunità, proponendo (ove possibile) delle soluzioni alternative.
3. Nel caso in cui ASIT declini la richiesta di attivazione, ma non ne vieti esplicitamente l'installazione/ erogazione, la singola Struttura può attivarsi per ottenere autonomamente servizi informatici richiesti nel rispetto della normativa vigente, anche in termini di sicurezza dei sistemi informatici, delle Linee Guida dell'Agenzia per l'Italia Digitale (AGID) e dell'Agenzia per la Cybersicurezza Nazionale (CSIRT), in osservanza del presente Regolamento.
4. Ogni Struttura è tenuta a dare notifica ad ASIT dell'elenco dei propri servizi informatici erogati mediante la rete dati di Ateneo (es. posta elettronica, domini, siti Web, DNS, FTP, DHCP, NAT, ecc.), attraverso le modalità che saranno comunicate da ASIT stessa.
5. Eventuali servizi erogati autonomamente dalle Strutture devono essere mantenuti aggiornati e configurati correttamente al fine di garantire un adeguato livello di sicurezza. Verranno effettuati controlli periodici per verificare l'aggiornamento e il grado di sicurezza dei sistemi nella rete di Ateneo, o comunque associati all'immagine pubblica dell'Ateneo, avvisando tempestivamente i responsabili di eventuali problemi rilevati. I responsabili di sistemi o servizi destinatari di tali avvertimenti sono tenuti a intervenire nel più breve tempo possibile in seguito alle segnalazioni di ASIT; qualora questo non avvenisse, ASIT si riserva la possibilità di interrompere la connettività verso i sistemi problematici.

Articolo 2 - Utilizzo di cartelle condivise e spazi personali

1. L'Ateneo, tramite ASIT e/o propri fornitori esterni ovvero mediante i servizi informatici implementati localmente dalle Strutture, può mettere a disposizione dei propri utenti cartelle di rete a uso esclusivo o condiviso: unità di memoria accessibili dall'interno della rete dati di Ateneo mediante le quali è possibile condividere e/o conservare *file* inerenti alla propria attività lavorativa memorizzandoli su un *server* dedicato.
2. Tali spazi possono essere utilizzati esclusivamente per finalità istituzionali. Non devono essere memorizzati, nemmeno per brevi periodi, *file* di natura personale. Pertanto l'Ateneo si riserva il diritto di rimuovere, in qualunque momento, i *file* di natura non istituzionale.
3. Sulle cartelle in oggetto vengono svolte regolari attività di controllo, nel rispetto di quanto previsto nell'Allegato E al presente Regolamento, relativamente ad amministrazione e *backup* da parte dell'amministratore del servizio. Gli utenti che salvano *file* privati in violazione del predetto divieto accettano il rischio che l'amministratore possa visualizzare il contenuto delle cartelle e cancellare senza preavviso alcuno i *file* di natura non istituzionale.
4. L'amministratore del servizio è tenuto a effettuare il *backup* delle sole informazioni di natura istituzionale presenti sul *file server*. Altre unità di memorizzazione a uso personale, come ad

esempio il disco rigido della propria postazione di lavoro o eventuali dischi rigidi esterni, non sono soggetti a *backup* e, pertanto, la responsabilità del salvataggio dei dati ivi contenuti è a carico del singolo utente.

5. Le cartelle personali legate al proprio *account* – e i dati in esse contenuti – verranno eliminate al momento della cancellazione dell'*account*, secondo le tempistiche indicate all'art. 4.3 dell'Allegato B al presente Regolamento. Resta facoltà dell'utente procedere alla cancellazione dei propri dati ovvero chiedere ad ASIT la chiusura dell'*account* in qualunque momento una volta terminato il rapporto con l'Ateneo.

Articolo 3 - Utilizzo postazioni di lavoro dell'Ateneo

1. Sulle postazioni di lavoro messe a disposizione dall'Ateneo non è consentito installare alcun tipo di *software* senza preventiva autorizzazione da parte di ASIT o del tecnico informatico della Struttura Decentrata di riferimento.
2. Non è altresì consentito riprodurre, tradurre, adattare, trasformare e distribuire *software* in licenza d'uso all'Ateneo.
3. È fatto assoluto divieto di installare strumenti *hardware* e/o *software* atti a intercettare e a modificare le comunicazioni informatiche oppure ad aggirare o a neutralizzare sistemi di protezione (es. programmi di *recovery password*, *cracking*, *sniffing*, *spoofing*, ecc.). In generale, è fatto divieto di installare, sviluppare o utilizzare sui sistemi messi a disposizione dall'Ateneo programmi che interferiscano con l'attività di altri utenti, che modifichino parti dei sistemi informatici esistenti, o che accedano a informazioni private o riservate alle quali l'utente non sia esplicitamente autorizzato. Gli illeciti che possono essere commessi tramite il *computer* o i sistemi informativi (*computer crimes*) sono regolati dal codice penale in tema di criminalità informatica.
4. È vietato utilizzare il *personal computer* per trasmettere, ricevere, scaricare, stampare o diffondere in qualunque altro modo contenuti di carattere indecente, osceno, razzista, sessualmente esplicito, illegale, immorale o discriminatorio.
5. Su ogni *personal computer* devono essere installati, configurati e attivati strumenti software di protezione dalle minacce informatiche individuati dall'Ateneo (ad esempio *firewall* e/o antivirus/*antimalware*); è vietato disabilitare o inibire il corretto funzionamento di tali software e interferire con il loro aggiornamento.
6. Il *personal computer* non deve essere lasciato incustodito durante una sessione di lavoro e anche in caso di breve assenza deve essere bloccato tramite le funzionalità di sistema (come ad esempio la combinazione di tasti [windows]+L); il sistema deve inoltre essere configurato affinché lo schermo venga bloccato automaticamente dopo al massimo 10 minuti di inattività, chiedendo le credenziali dell'utente per essere sbloccato. Al termine dell'attività lavorativa le sessioni di lavoro devono essere chiuse tramite le opportune procedure di *log-off*.
7. I supporti di memoria rimovibili (es. chiavette USB, *compact disk*, ecc.) devono essere conservati in luoghi protetti (es. armadi e cassettiere chiusi a chiave).
8. Qualora i supporti di memoria rimovibili vengano utilizzati per memorizzare e/o movimentare dati appartenenti a Categorie Particolari di Dati Personali o comunque di natura riservata ovvero quest'ultimi debbano essere trasmessi elettronicamente all'esterno dell'Ateneo, è necessario utilizzare appropriate tecniche di cifratura per limitare i danni derivanti da accessi non autorizzati o accidentali. ASIT mette a disposizione procedure e guide specifiche al riguardo, disponibili alla pagina <https://www.unive.it/criptarearchivi>.
9. Qualora nello svolgimento delle finalità istituzionali si utilizzino *computer* portatili non forniti da ASIT, sarà necessario verificare che sia attivata o attivare la *Full Disk Encryption*.
10. È sempre necessario verificare il contenuto informativo dei supporti di memoria prima: (i) della loro consegna a terzi per il riutilizzo del supporto ovvero della loro eliminazione/distruzione (in questo caso il dispositivo non dovrà più contenere dati leggibili o comunque in qualsiasi modo recuperabili); (ii) della loro consegna a terzi per il trasferimento dei dati (in questo caso il dispositivo deve contenere esclusivamente i dati a cui il terzo ha diritto di accedere).
11. I dati contenuti nei supporti rimovibili, quando non più necessari, devono essere cancellati secondo le seguenti indicazioni: se contengono dati appartenenti a Categorie Particolari di Dati Personali, distruggendo definitivamente tutte le copie della chiave usata per la cifratura; se non contengono dati

- appartenenti a Categorie Particolari di Dati Personali, ricorrendo alla formattazione a basso livello utilizzando eventualmente la funzione *Secure Erase* prevista dallo standard ATA.
12. I supporti di memorizzazione non rimovibili (es. *hard disk*) utilizzati all'interno dei sistemi *server* vengono fisicamente distrutti al momento della dismissione.
 13. I supporti di memorizzazione non rimovibili utilizzati all'interno di sistemi *desktop*, poiché alcune applicazioni (es. *Google Filestream*) potrebbero aver fatto *caching* di dati sul disco anche senza l'intervento dell'utente, vanno dismessi secondo le seguenti indicazioni:
 - a. se il dispositivo di memorizzazione è un *hard disk* "classico" a rotazione, può essere formattato a basso livello con gli strumenti opportuni e riutilizzato;
 - b. se il dispositivo è di tipo SSD/NVMe e ha eventualmente ospitato Dati Personali ma non appartenenti a Categorie Particolari, può essere formattato a basso livello utilizzando inoltre la funzione *Secure Erase* prevista dallo standard ATA e riutilizzato;
 - c. se il dispositivo è di tipo SSD/NVMe e ha ospitato dati appartenenti a Categorie Particolari di Dati Personali ed è stato usato un *filesystem* cifrato o i dati sono stati mantenuti in archivi cifrati come descritto in <https://www.unive.it/criptarearchivi>, è possibile riutilizzarlo previa formattazione a basso livello utilizzando inoltre la funzione *Secure Erase* prevista dallo standard ATA e distruzione definitiva di tutte le copie della chiave usata per la cifratura;
 - d. se il dispositivo è di tipo SSD/NVMe e ha ospitato dati appartenenti a Categorie Particolari di Dati Personali su *filesystem* non cifrato, va fisicamente distrutto.
 14. Nell'eventualità in cui si rilevi l'esistenza di programmi che violino il diritto d'autore, ASIT o l'Amministratore di Sistema della Struttura interessata dovrà tempestivamente informare il Referente di Struttura, il quale provvede a:
 - a. inviare avvisi collettivi, all'interno della struttura di riferimento, mediante i quali l'utenza sarà richiamata all'osservanza di corrette norme di comportamento;
 - b. richiedere la rimozione del software, senza alcun preavviso all'utente, nei casi in cui software e file possano limitare l'utilizzo di risorse o possano recare danno all'Ateneo;
 - c. effettuare, nei casi in cui i comportamenti non corretti si ripetano nel tempo o risultino particolarmente gravi, una segnalazione al Rettore o al Direttore Generale, per i rispettivi ambiti di competenza, che adotteranno i provvedimenti più opportuni.
 15. Nel caso in cui, per motivi di sicurezza o affidabilità del sistema, si renda opportuno sostituire la postazione di lavoro di un utente, il tecnico informatico di Struttura Decentrata potrà procedere alla sostituzione, garantendo il trasferimento nella nuova postazione dei soli dati di rilevanza istituzionale.

Articolo 4 - Utilizzo della rete Internet

1. La connessione a Internet è un sistema di supporto per lo svolgimento delle attività degli utenti. Gli utenti dei servizi informatici dell'Ateneo possono accedere a Internet per favorire l'effettivo ed efficiente svolgimento dell'attività lavorativa, di studio e di ricerca.
2. L'Ateneo consente l'uso sporadico od occasionale di Internet per motivi personali e/o non collegati alle attività lavorative, di studio o di ricerca.
3. L'uso personale è vietato se esso:
 - a. interferisce con la produttività o con la prestazione professionale dell'utente o di qualsiasi altro dipendente;
 - b. incide negativamente sul buon funzionamento del computer;
 - c. viola le norme oggetto del presente Regolamento.
4. Nell'uso dei servizi Internet gli utenti devono osservare le seguenti regole:
 - a. l'accesso alla rete dati è personale; è fatto divieto di rivelare le proprie credenziali a soggetti non autorizzati; l'utente è responsabile, sia nei confronti di terzi che dell'Ateneo, dei fatti illeciti commessi in prima persona o da chiunque utilizzi le sue credenziali;
 - b. è fatto divieto agli utenti di servirsi o dar modo ad altri di servirsi della rete dell'Ateneo e dei servizi da essa messi a disposizione per utilizzi illeciti che violino diritti d'autore, marchi di fabbrica, brevetti o altri diritti tutelati dalla normativa applicabile, per utilizzi contro la morale e l'ordine pubblico, ovvero che arrechino offesa, danno o molestie a chicchessia, e in generale tutti gli utilizzi o comportamenti contrari alla legge;

- c. è vietato accedere, scaricare, stampare o salvare informazioni dall'esplicito contenuto sessuale, pedopornografico o che inciti alla violenza e all'odio razziale;
 - d. è vietato scaricare o trasmettere immagini o messaggi fraudolenti, minacciosi, osceni, intimidatori, diffamatori, molesti, discriminatori o altrimenti illegali;
 - e. le risorse informatiche dell'Ateneo non devono essere utilizzate per finalità connesse all'attività di propaganda di partiti od organizzazioni religiose;
 - f. salva e impregiudicata l'applicazione della vigente normativa penale, è comunque fatto espressamente divieto all'utente di compromettere in tutto o in parte il funzionamento di sistemi e reti informatiche, falsificare o utilizzare l'autenticazione, le credenziali e le chiavi di accesso di altri utenti, compromettere e/o violare le misure di sicurezza presenti in un sistema informatico e/o interferire in qualsivoglia maniera con la trasmissione o l'utilizzo della rete e dei sistemi informatici da parte di altri utenti; gli utenti, in particolare: (i) non devono inserire, modificare o rimuovere apparati di rete senza preventiva autorizzazione degli amministratori di rete; (ii) non devono attuare attività intenzionali mirate a conseguire il blocco o la saturazione dei sistemi di elaborazione e trasmissione dati, rendendo anche solo temporaneamente indisponibili risorse di uso comune;
 - g. a livello nazionale e internazionale esistono comunità informatiche a cui l'Ateneo aderisce per fini istituzionali di ricerca e di didattica e con cui interagisce prevalentemente tramite le reti informatiche; tali comunità hanno definito norme e regolamenti per l'utilizzo delle risorse messe in comune: l'Ateneo è quindi tenuto ad adeguare le proprie attività e azioni alle suddette norme; di particolare rilievo risulta il rapporto con la comunità di rete scientifica e di ricerca italiana, rappresentata dall'ente denominato GARR (Gruppo Armonizzazione Reti di Ricerca italiano), e il rispetto delle regole (*Acceptable User Policy* <https://www.garr.it/it/regole-di-utilizzo-della-rete-aup>) da tale ente definite, a cui gli utenti devono conformarsi.
5. Gli Amministratori di Sistema e/o di rete possono temporaneamente interdire l'accesso e l'uso delle risorse informatiche a un utente qualora, sulla base di comprovati motivi, se ne evidenzi la necessità per garantire la sicurezza dei sistemi o della rete. In caso di eventi di particolare gravità o urgenza, gli interventi suddetti possono dover essere attuati senza specifico preavviso. Gli Amministratori di Sistema devono comunque notificare per iscritto la situazione ed eventuali azioni intraprese al Dirigente di ASIT e ai responsabili delle Strutture coinvolte, in modo che l'utente possa essere opportunamente informato.

ALLEGATO D

UTILIZZO DELLA POSTA ELETTRONICA

Articolo 1 - Principi generali

1. L'Ateneo, tramite ASIT, rende disponibile agli studenti, al personale docente e ricercatore, al personale tecnico-amministrativo, ai collaboratori ed esperti linguistici e ad altri soggetti autorizzati un indirizzo di posta elettronica istituzionale appartenente al dominio "unive.it" o a suoi eventuali sotto-domini.
2. Le comunicazioni ufficiali e istituzionali da parte dell'Ateneo sono inviate esclusivamente all'indirizzo di posta istituzionale di cui al paragrafo precedente, salvo in presenza di determinati casi specifici e motivati (ad es. recupero *password*, invio di sms in casi di emergenza, ecc.). Analogamente, i soggetti autorizzati, di cui al comma 1 che precede, possono inviare e ricevere le comunicazioni ufficiali e istituzionali esclusivamente utilizzando l'indirizzo di posta elettronica istituzionale appartenente al dominio "unive.it" o a suoi eventuali sottodomini. È fatto, inoltre, divieto agli utenti di gestire e conservare le predette comunicazioni con strumenti diversi da quelli forniti dall'Ateneo.
3. Tutti gli utenti abilitati possono accedere al servizio di posta elettronica utilizzando le proprie credenziali istituzionali.
4. In caso di assenza, il personale e i collaboratori sono invitati ad attivare sistemi di risposta automatica ai messaggi di posta elettronica, indicando eventuali indirizzi istituzionali alternativi a cui fare riferimento per l'invio di comunicazioni. Qualora, in casi eccezionali, la persona titolare dell'*account* non possa inserire in autonomia tale messaggio (es. casi di malattia grave, decesso, ecc.), gli Amministratori di Sistema potranno, previa autorizzazione del Titolare del Trattamento, anche tramite delega al Referente di Struttura competente, accedere all'*account* al solo fine di inserire un messaggio di risposta automatica.
5. Al fine di agevolare la comunicazione istituzionale e favorire la circolazione delle informazioni, sono altresì forniti indirizzi per unità/strutture organizzative o indirizzi legati al ruolo, il cui accesso può essere consentito a uno o più utenti. A titolo esemplificativo, indirizzo di posta elettronica può essere fornito a:
 - a. cariche (es. *rettore@unive.it*);
 - b. organi (es. *presidio.qualita@unive.it*);
 - c. soggetti/strutture/unità organizzative dell'Ateneo che nell'ambito di progetti, ricerche o altre forme di attività di collaborazione necessitano di tale strumento di lavoro.
6. L'Ateneo ha, inoltre, facoltà di fornire ai propri utenti altri servizi di posta elettronica a supporto dell'attività di collaborazione con l'Ateneo.

Articolo 2 - Gestione tecnica del servizio

1. ASIT implementa misure di protezione automatizzate *antivirus* e *antispam* per il servizio di posta istituzionale, individuando le tecnologie e le modalità operative per contrastare la ricezione di messaggi di posta elettronica non desiderati contenenti *virus*, comunicazioni e/o materiali pubblicitari o altro materiale dal contenuto potenzialmente dannoso.
2. È compito di ASIT adottare idonee politiche di *backup* dei messaggi, esplicitandone le modalità di attuazione sulle pagine web di Ateneo dedicate al servizio di posta.

Articolo 3 - Validità dei profili autorizzativi per l'uso del servizio di posta elettronica

1. Il servizio di posta elettronica istituzionale sarà disattivato secondo i termini previsti all'Allegato B al presente Regolamento.

Articolo 4 - Uso del sistema di posta elettronica

1. Il sistema di posta elettronica deve essere utilizzato esclusivamente per lo svolgimento dell'attività lavorativa e di studio. È tollerato, nei limiti di quanto di seguito indicato, un utilizzo a fini privati, che non dovrà però in alcun modo interferire con il normale svolgimento dell'attività lavorativa e di studio o con gli scopi cui gli stessi sono destinati. Coloro che dovessero utilizzare il sistema di posta elettronica a fini privati accettano, quindi, il rischio che l'Ateneo possa, anche involontariamente o

nello svolgimento dei controlli di cui all'Allegato E al presente Regolamento, venire a conoscenza di informazioni private dell'utente che costituiscono Dati Personali, anche particolari. Per tutelare la *privacy* di eventuali messaggi privati si consiglia di conservare tale corrispondenza esclusivamente per il tempo strettamente necessario, provvedendo a eliminare quanto prima la stessa per evitare che l'Ateneo possa inavvertitamente prendere conoscenza del contenuto.

2. Nell'uso del servizio di posta elettronica, gli utenti devono osservare le seguenti norme comportamentali:
- a. è vietato l'utilizzo dell'e-mail istituzionale per veicolare messaggi il cui contenuto sia lesivo dell'immagine dell'Ateneo;
 - b. l'accesso alle caselle nome.cognome@unive.it (o alias@unive.it) o matricola@stud.unive.it è strettamente personale. Ciascun utente accede alla propria casella elettronica previa autenticazione tramite le credenziali di Ateneo. È fatto assoluto divieto di rivelare a terzi le proprie credenziali. L'utente che violi tali disposizioni ne risponde anche in via disciplinare. L'utente riceve al momento dell'attivazione dell'account un PIN che gli permetterà di selezionare una *password* personale, secondo quanto previsto dall'art. 2 dell'Allegato B;
 - c. l'*account* personale non può essere condiviso o ceduto ad altri; è fatto divieto di scambiare messaggi utilizzando l'*account* personale tentando di travisare od occultare la propria identità;
 - d. è assolutamente vietato inviare o archiviare immagini e messaggi di natura oltraggiosa, minacciosa, oscena, intimidatoria, diffamatoria, molesta e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o comunque ritenuti illegali secondo la normativa vigente;
 - e. è assolutamente vietato servirsi o dar modo di servirsi della rete istituzionale e dei relativi servizi per usi che violino o trasgrediscano diritti d'autore, di proprietà intellettuale e/o industriale o, in generale, altri diritti tutelati dalla normativa vigente;
 - f. è espressamente proibito inviare messaggi non richiesti, invadenti, molesti o eccessivamente frequenti (*junk mail*, *spam*) di qualsiasi tipo (es. pubblicità commerciale, propaganda politica, annunci) o spedire lo stesso messaggio o messaggi simili a un elevato numero di destinatari (interscambio o invii multipli o c.d. "Catene di Sant'Antonio");
 - g. l'utente è tenuto a esercitare particolare cautela nell'interagire con i messaggi di posta elettronica, ad esempio aprendo gli allegati o seguendo i collegamenti ipertestuali eventualmente contenuti nel messaggio. Per favorire un uso sicuro della posta elettronica l'utente si impegna a seguire le indicazioni riportate all'URL <https://www.unive.it/pag/42238/>;
 - h. al fine di garantire il corretto funzionamento della posta elettronica istituzionale e di evitare la proliferazione del traffico indebito (*spam*), si fa presente che l'Ateneo ha in uso un sistema *antispam* che filtra i messaggi sospetti depositandoli in un'apposita cartella; è responsabilità dell'utente verificare che il filtro abbia operato in modo corretto esaminando periodicamente la cartella in questione;
 - i. il protocollo di posta elettronica non può garantire l'uso di crittografia per la trasmissione dei contenuti, né l'obbligo di identificazione dei mittenti; pertanto il sistema non garantisce la riservatezza dei messaggi inviati o ricevuti, né la verifica dell'identità degli interlocutori; è quindi fatto divieto di inviare materiali che non siano compatibili con tali caratteristiche del servizio, se non adottando le misure indicate alla pagina <https://www.unive.it/criptarearchivi/>;
 - j. è suggerito utilizzare il seguente *disclaimer* privacy nei messaggi in uscita:

**** Riservatezza - Confidentiality notice ****

In ottemperanza al GDPR (Regolamento UE 2016/679) e al D.Lgs. n. 196 del 30/6/2003 in materia di protezione dei dati personali, le informazioni contenute in questo messaggio sono strettamente riservate ed esclusivamente indirizzate al destinatario indicato (oppure alla persona responsabile di rimmetterlo al destinatario). Vogliate tener presente che qualsiasi uso, riproduzione o divulgazione di questo messaggio è vietato. Nel caso in cui aveste ricevuto questo messaggio per errore, vogliate cortesemente avvertire il mittente e distruggere il presente messaggio.

In compliance with the GDPR (EU Regulation 2016/679) and with Legislative Decree No. 196/2003 on personal data protection, the content of this e-mail is confidential and is solely

for the use of the addressee (or other individuals responsible for the delivery of the message to such person). Any disclosure, copy, distribution of this communication is prohibited. If you receive this in error, please contact the sender and delete the material from any computer;

- k. per garantire la riservatezza e la disponibilità delle informazioni, l'utente è tenuto a non archiviare i documenti allegati ai messaggi di posta elettronica (o gli stessi messaggi di posta elettronica) sui dispositivi locali (disco fisso del computer, chiavette o dischi usb personali o di lavoro): al fine di assicurare il *backup* dei documenti e di ridurre così al minimo il rischio di perdita anche accidentale degli stessi, tutti i *file* devono essere mantenuti nella casella di posta elettronica o salvati nei *server* preposti e non nell'*hard disk* dei *personal computer* nonché sui *server* di Ateneo/Google Drive, in quanto risorse sottoposte a regolari *backup*;
- l. l'utente dovrà utilizzare l'indirizzo email della propria unità/struttura organizzativa in tutte le comunicazioni relative a pratiche in gestione alla struttura stessa, in modo da assicurare la condivisione delle informazioni e che, in caso di sua assenza e/o impedimento, l'ufficio sia in grado di assicurare la continuità lavorativa;
- m. in caso di comunicazioni con molti destinatari, è necessario verificare preventivamente che tutti i destinatari siano autorizzati ad avere accesso alle informazioni e ai documenti inviati; andrà inoltre valutata l'opportunità di inserire gli indirizzi dei destinatari nel campo ccn, al fine di garantire la riservatezza di questa informazione.

ALLEGATO E

CONTROLLI SULL'UTILIZZO DELLE INFRASTRUTTURE, DELLE RISORSE INFORMATICHE E DELLA POSTA ELETTRONICA

Articolo 1 - Principi generali

1. Come previsto dall'art. 34 del presente Regolamento, il Titolare del Trattamento o altri soggetti da quest'ultimo delegati hanno facoltà di effettuare controlli, anche preventivi, circa l'adozione delle corrette misure per garantire il rispetto della normativa vigente e la sicurezza dell'infrastruttura informatica di Ateneo e dei suoi utenti. A tal fine, i controlli possono avere a oggetto anche le infrastrutture, le risorse informatiche e la posta elettronica messe a disposizione dall'Ateneo.

Articolo 2 - Controlli relativi alla posta elettronica

Articolo 2.1. - Dati rilevati

1. L'Ateneo si appoggia a Google come servizio esterno di posta elettronica. Google rende accessibili agli Amministratori di Sistema dell'Ateneo i *log* e i metadati relativi alla posta elettronica per 6 mesi; in particolare, Google attualmente raccoglie e mette a disposizione dell'Ateneo le seguenti informazioni riguardanti il singolo messaggio: oggetto, mittente, destinatario (in campo A: e CC:), data e ora di invio/ricezione, ID messaggio, dimensione messaggio, presenza di allegati, IP server di destinazione, classificazione SPAM. In casi specifici potrebbero essere raccolti ulteriori metadati, come ad esempio l'orario di lettura di un messaggio.
2. Informazioni aggiornate sui dati trattati dall'Ateneo possono essere richieste in qualunque momento ad ASIT attraverso l'apertura di un *ticket* di supporto.

Articolo 2.2. - Controlli periodici

1. Il presente articolo si applica a tutti i soggetti che utilizzano le risorse informatiche di Ateneo.
2. L'Ateneo si riserva di procedere, con cadenza periodica e/o occasionale, a controlli per verificare che l'utilizzo dello strumento di posta elettronica sia conforme a quanto prescritto nell'Allegato D al presente Regolamento e comunque al presente Regolamento, per esigenze di manutenzione e/o sicurezza dei sistemi nonché al fine di prevenire atti illeciti. I controlli verranno effettuati da ASIT. Gli accertamenti hanno natura periodica e, se non in presenza di fondati motivi, non potranno essere mirati sul singolo utente. Tali verifiche saranno quindi effettuate su dati aggregati che si riferiscono all'intera struttura informatica o a determinate aree o settori.
3. L'Ateneo, laddove venissero rilevate anomalie, comunicherà agli utenti l'esito dei controlli effettuati sui dati aggregati e adotterà, ove richiesto, le necessarie misure.
4. Ove vengano rilevati utilizzi in violazione dell'Allegato D al presente Regolamento o comunque delle previsioni del Regolamento, l'Ateneo nella predetta comunicazione inviterà nuovamente tutti gli utenti ad astenersi da tali comportamenti, annunciando ulteriori controlli. Ove a seguito di tali verifiche, vengano rilevati ulteriori utilizzi anomali, l'Ateneo procederà, senza ulteriore preavviso, a identificare l'utente o gli utenti che abusano del servizio, con le modalità indicate all'articolo seguente.

Articolo 2.3. - Controlli straordinari

1. Laddove vi sia il sospetto di violazioni, di particolare gravità, di norme di legge, delle disposizioni dell'Allegato D al Regolamento o comunque delle previsioni del Regolamento, l'Ateneo potrà effettuare controlli straordinari.
2. I controlli straordinari saranno, in ogni caso, improntati ai principi di correttezza, pertinenza e non eccedenza nel trattamento dei Dati Personali, evitando quindi modalità di accesso indiscriminato a ogni contenuto. Verranno privilegiate modalità di verifica selettive, mediante l'utilizzo di parole chiave, nonché saranno adottate misure opportune per garantire la tutela dei dati attinenti alla vita privata dell'utente eventualmente presenti nella posta elettronica.
3. I controlli straordinari potranno avvenire a opera di ASIT, anche avvalendosi di soggetti esterni (es. consulente informatico e società di *auditing*).

4. Dei predetti controlli verrà redatto verbale, che riporterà la data di inizio della verifica, il motivo dell'indagine, una descrizione sintetica delle attività poste in essere e dei soggetti che vi hanno partecipato, il relativo arco temporale, la data di chiusura dell'indagine e l'indicazione dell'esito della stessa.
5. La documentazione acquisita durante i controlli straordinari verrà conservata per un periodo di tempo non superiore a quello necessario agli scopi per i quali la stessa è stata raccolta e successivamente trattata. Resta fermo, in ogni caso, il diritto dell'Ateneo di conservare la memoria di massa del *computer* o di altro strumento informatico affidato in dotazione all'utente per far valere o difendere un diritto in sede giudiziaria e consentire all'autorità giudiziaria di accedervi con le modalità dalla stessa ritenute opportune.

Articolo 2.4. - Sanzioni

1. Le prescrizioni contenute nel presente Allegato hanno una rilevanza disciplinare, fermi restando i diversi profili di responsabilità civile e penale, e sono sanzionati secondo le forme e le modalità previste dagli ordinamenti delle varie categorie di personale coinvolto.

Articolo 3 - Controlli relativi all'utilizzo dei sistemi informatici

Articolo 3.1. - Controlli dati rilevati

1. Per la fornitura dei servizi informatici, l'Ateneo registra l'associazione tra utente e risorse/servizi impegnati secondo le seguenti specifiche e può utilizzare tali dati per finalità di controllo.
 - a. Fornitura di hardware:
 - nome utente;
 - codice inventariale del materiale.
 - b. Accesso alla rete Internet tramite connessione WiFi:
 - nome utente;
 - indirizzo IP associato;
 - MAC del dispositivo utilizzato;
 - data e ora di inizio sessione;
 - data e ora di fine sessione.
 - c. Accesso alla rete intranet tramite connessione VPN:
 - nome utente;
 - indirizzo IP di origine;
 - indirizzo IP assegnato dalla VPN;
 - data e ora di inizio sessione;
 - data e ora di fine sessione.
 - d. Accesso in modalità virtuale ai PC aziendali:
 - nome utente;
 - data e ora di accesso;
 - data e ora di disconnessione;
 - specifici eventi legati alla sicurezza del sistema operativo;
 - per la durata della sessione sul PC vengono registrati dal sistema i dati di utilizzo secondo le impostazioni standard del sistema operativo utilizzato, questi dati vengono cancellati al termine della sessione stessa.
 - e. Accesso ai PC istituzionali fisici:
 - nome utente;
 - data e ora di accesso;
 - data e ora di disconnessione;
 - specifici eventi legati alla sicurezza del sistema operativo;
 - per la durata della sessione sul PC vengono registrati dal sistema i dati di utilizzo secondo le impostazioni standard del sistema operativo utilizzato, i dati vengono mantenuti sulla macchina stessa
 - f. Ai fini di garantire ottimizzazione e diagnostica dell'infrastruttura di rete vengono raccolti in modo aggregato (informazioni di flusso):
 - IP di partenza;

- IP di destinazione;
 - protocollo utilizzato;
 - quantità di dati scambiati;
 - data e ora di inizio e fine connessione.
- vii. Autenticazioni ai servizi tramite il sistema di autenticazione di Ateneo:
- nome utente;
 - esito del tentativo di autenticazione;
 - URL del servizio che richiede l'autenticazione;
 - data e ora del tentativo.
- viii. Operazioni sull'*account* utente (es. cambio *password*):
- nome utente autore dell'operazione;
 - nome *account* interessato;
 - tipo di operazione;
 - attributo interessato;
 - data e ora dell'operazione.
- ix. Accesso a file nelle aree di *storage* condivise:
- nome utente;
 - IP del device utilizzato;
 - riferimento alla risorsa acceduta;
 - tipo di accesso;
 - data e ora dell'operazione.

Si sottolinea che non viene raccolto il contenuto dei pacchetti scambiati.

2. Tutte le informazioni, di cui al comma 1 che precede, vengono conservate fino a 6 mesi. L'Ateneo effettua un *backup* mensile dei propri *server* conservandoli per 12 mesi. Pertanto, parte delle informazioni indicate al comma 1 che precede potrebbe essere presente nelle copie di *backup* dei predetti *server*. Alle copie di *backup* accedono gli Amministratori di Sistema, debitamente nominati, solamente a fronte di comprovate necessità e le informazioni in esse contenute, non potendo essere aggregate, non consentono una ricostruzione completa dei *log*.
3. Un eventuale prolungamento dei tempi di conservazione sopra indicati deve considerarsi come eccezionale e può aver luogo solo in relazione a esigenze tecniche o di sicurezza del tutto particolari, dell'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria, oppure all'obbligo di custodire o consegnare i dati per ottemperare a una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Articolo 3.2. - Controlli periodici

1. L'Ateneo si riserva di procedere, con cadenza periodica e/o occasionale, a controlli per verificare che l'utilizzo delle infrastrutture e degli strumenti informatici sia conforme a quanto prescritto dall'Allegato C o comunque dal presente Regolamento per esigenze di manutenzione e/o sicurezza dei sistemi nonché al fine di prevenire la commissione di atti illeciti. I controlli verranno effettuati da ASIT. Gli accertamenti avranno natura periodica e, se non in presenza di fondati motivi, non potranno essere mirati sul singolo utente. L'Ateneo potrà effettuare, senza alcun preavviso, periodiche analisi aggregate (e quindi anonime) dei *log* di accesso e utilizzo del sistema e dei suoi servizi. Tali verifiche saranno effettuate su dati aggregati che si riferiscono all'intera struttura informatica, o a determinate aree o settori.
2. L'Ateneo, laddove venissero rilevate anomalie, comunicherà agli utenti l'esito dei controlli effettuati sui dati aggregati e adotterà, ove richiesto, le necessarie misure.
3. Ove vengano rilevati utilizzi in violazione del presente Regolamento e/o dei suoi Allegati, l'Ateneo, nella predetta comunicazione, inviterà nuovamente tutti gli utenti ad astenersi da tali comportamenti, annunciando ulteriori controlli. Ove, a seguito di tali verifiche, vengano rilevati ulteriori utilizzi anomali, l'Ateneo procederà, senza ulteriore preavviso, a identificare l'utente o gli utenti che abusano del servizio, con le modalità indicate al punto seguente.

Articolo 3.3. - Controlli straordinari

1. Laddove vi sia il sospetto di violazioni di norme di legge, delle disposizioni del presente Regolamento e/o dei suoi Allegati, di particolare gravità, l'Ateneo potrà effettuare controlli straordinari.
2. I controlli straordinari saranno, in ogni caso, improntati ai principi di correttezza, pertinenza e non eccedenza nel trattamento dei Dati Personali, evitando quindi modalità di accesso indiscriminato a ogni contenuto. Verranno privilegiate modalità di verifica selettive, mediante l'utilizzo di parole chiave, nonché saranno adottate misure opportune per garantire la tutela dei dati attinenti alla vita privata dell'utente eventualmente presenti sullo strumento informatico.
3. I controlli straordinari potranno avvenire a opera di ASIT, anche avvalendosi di soggetti esterni (es. consulente informatico e società di *auditing*).
4. Dei predetti controlli verrà redatto processo verbale, che riporterà la data di inizio della verifica, il motivo dell'indagine, una descrizione sintetica delle attività poste in essere e dei soggetti che vi hanno partecipato, il relativo arco temporale, la data di chiusura dell'indagine e l'indicazione dell'esito della stessa.
5. La documentazione acquisita durante i controlli straordinari verrà conservata per un periodo di tempo non superiore a quello necessario agli scopi per i quali la stessa è stata raccolta e successivamente trattata. Resta fermo, in ogni caso, il diritto dell'Ateneo di conservare la memoria di massa del *computer* o di altro strumento informatico affidato in dotazione all'utente per far valere o difendere un diritto in sede giudiziaria e consentire all'autorità giudiziaria di accedervi con le modalità dalla stessa ritenute opportune.

Articolo 3.4. - Sanzioni

1. Le prescrizioni contenute nel presente Allegato hanno una rilevanza disciplinare, fermi restando i diversi profili di responsabilità civile e penale, e sono sanzionati secondo le forme e le modalità previste dagli ordinamenti delle varie tipologie di personale coinvolto.

ALLEGATO F

PRESENTAZIONE E GESTIONE DELLE ISTANZE DI ESERCIZIO DEI DIRITTI

Articolo 1 - Oggetto

1. Il presente Allegato disciplina le modalità di presentazione, da parte degli Interessati o di altri soggetti legittimati, delle istanze di esercizio dei diritti previsti dagli artt. 15-22 del GDPR (“**Diritti**”), nonché le modalità di gestione delle stesse da parte dell'Ateneo. Gli Interessati sono informati in merito ai Diritti loro riconosciuti dal GDPR e alle modalità di esercizio degli stessi.
2. Nella prima parte dell'Allegato sono descritti gli adempimenti di carattere generale applicabili a qualsiasi istanza; nella seconda parte, invece, è esaminato ciascun Diritto nel dettaglio.
3. Il presente Allegato non si applica direttamente alle richieste di esercizio dei Diritti relative a Dati Personali contenuti in segnalazioni di condotte illecite (istituto del “*whistleblowing*”), pur recando principi e indicazioni utili per l'evasione delle stesse; le richieste in questione, infatti, saranno gestite dal Responsabile della Prevenzione della Corruzione e della Trasparenza (“RPCT”) di Ateneo (in quanto unico soggetto che può conoscere l'identità del segnalante e i contenuti della segnalazione), eventualmente potendo chiedere supporto al DPO di Ateneo sul merito dell'istanza e sul processo di evasione.

TITOLO I – ADEMPIMENTI PER LA PRESENTAZIONE E LA GESTIONE DELLE ISTANZE

Articolo 2 - Legittimazione all'esercizio dei Diritti e modalità di presentazione dell'istanza

1. L'istanza di esercizio dei Diritti può essere presentata direttamente dall'Interessato o tramite suo delegato (munito di apposita delega corredata di copia di un documento di riconoscimento del soggetto delegante; il delegato dovrà altresì allegare copia del suo documento di riconoscimento; copia del documento di identità del delegato non è necessaria se quest'ultimo firma digitalmente o se trasmette l'istanza dal proprio domicilio digitale iscritto in uno degli elenchi di cui all'articolo 6-bis, 6-ter o 6-quater del D.Lgs. 82/2005 ovvero da un indirizzo di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato).
2. L'istanza non necessita di motivazione per essere presentata, salvo nei casi previsti all'art. 3 del presente Allegato.
3. L'istanza di esercizio dei Diritti può essere presentata oralmente (di persona o telefonicamente) ovvero per iscritto (con mezzi elettronici o analogici) all'attenzione del DPO di Ateneo o dell'Università (in qualità di Titolare del Trattamento).
4. Qualora venga avanzata oralmente un'istanza al personale di una Struttura di Ateneo, quest'ultimo dovrà mettere in contatto il richiedente (di persona o telefonicamente) con il DPO o con lo Staff di supporto al DPO.
5. L'istanza avanzata per iscritto può essere recapitata:
 - a. tramite posta elettronica semplice, scrivendo all'indirizzo dpo@unive.it;
 - b. tramite posta elettronica certificata, scrivendo all'indirizzo PEC protocollo@pec.unive.it;
 - c. tramite raccomandata A/R, scrivendo al seguente recapito: Università Ca' Foscari Venezia, Dorsoduro n. 3246, 30123, Venezia, c.a. Responsabile della Protezione dei Dati.

Articolo 3 - Legittimazione e presentazione delle istanze relative a Dati Personali di Interessati deceduti/Interessate decedute ovvero dichiarati morti presunti

1. In caso di Interessati deceduti o dichiarati morti presunti, i Diritti possono essere esercitati da:
 - a. chi abbia un interesse proprio;
 - b. chi agisca a tutela dell'Interessato in qualità di suo mandatario;
 - c. chi agisca per ragioni familiari meritevoli di protezione.

Nel caso di esercizio del Diritto di accesso a Dati Personali presenti nella corrispondenza del soggetto defunto/dichiarato morto presunto (contenuta in caselle di posta elettronica o in altri strumenti o su altri supporti), trova applicazione il DPR 29 marzo 1973, n. 156, per cui nessuno può prendere visione e ottenere copia della corrispondenza in genere, ad eccezione del mittente, del

destinatario, dei loro eredi e dei loro rappresentanti legali, nonché delle altre persone indicate dalla legge.

2. L'esercizio dei Diritti non è ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della società dell'informazione, l'Interessato lo abbia espressamente vietato con dichiarazione scritta presentata al Titolare del Trattamento o a quest'ultimo comunicata. Tale volontà deve risultare in modo non equivoco e deve essere specifica, libera e informata. Il divieto può riguardare l'esercizio soltanto di alcuni dei Diritti. L'Interessato, finché in vita, ha in ogni momento il diritto di revocare o modificare il divieto. In ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'Interessato nonché del diritto di difendere in giudizio i propri interessi.
3. L'istanza deve riportare la specifica dei Dati Personali di interesse, le motivazioni alla base della stessa ed eventuale documentazione utile per comprovare la propria posizione.
4. In applicazione di quanto disposto dal DPR 29 marzo 1973, n. 156, qualora l'istanza abbia ad oggetto l'accesso a Dati Personali contenuti in corrispondenza del soggetto defunto o dichiarato morto presunto, la stessa deve essere corredata, inoltre, da: (i) una dichiarazione sostitutiva di atto notorio in cui vengano specificati tutti gli eredi (anche legittimari) nonché l'eventuale esistenza di esecutori testamentari; (ii) il consenso all'apertura della corrispondenza del soggetto defunto o dichiarato morto presunto, espresso per iscritto dagli altri eventuali coeredi o, comunque, dagli aventi diritto ad autorizzare tale apertura.
5. Per avanzare una richiesta di esercizio dei Diritti relativa a Dati Personali di soggetti defunti o dichiarati morti presunti l'Ateneo mette a disposizione sul proprio sito web istituzionale apposita modulistica da poter utilizzare.
6. La richiesta deve essere presentata necessariamente per iscritto al DPO di Ateneo o all'Università (in qualità di Titolare del Trattamento) e recapitata secondo le modalità indicate all'art. 2, c. 5, del presente Allegato.

Articolo 4 - Soggetti coinvolti nella gestione delle istanze di esercizio dei Diritti

1. Ai fini del riscontro alle richieste di esercizio dei Diritti, sono coinvolti i seguenti soggetti:
 - a. l'Ateneo, Titolare del Trattamento, per il tramite di:
 - o DPO e Staff di supporto al DPO;
 - o Referenti di Struttura e Referenti Interni ("**Referenti**"), per i trattamenti di loro competenza, da individuarsi in funzione della tipologia dei Dati Personali oggetto della richiesta e delle finalità per cui quest'ultimi sono trattati;
 - o eventuali ulteriori Referenti di altre Strutture di Ateneo la cui collaborazione è necessaria per poter fornire riscontro alla richiesta avanzata;
 - o eventuali Amministratori di Sistema di Ateneo, qualora sia necessario un intervento a livello di sistemi informatici dell'Università;
 - b. eventuali Contitolari, Responsabili del Trattamento e/o altri destinatari dei Dati Personali.

Articolo 5 - Adempimenti preliminari

1. Qualora l'istanza sia presentata oralmente, il DPO o lo Staff di supporto al DPO formalizza la richiesta in apposito verbale, da inviare tempestivamente al Settore Protocollo per la sua assunzione al sistema di protocollo di Ateneo.
2. Qualora l'istanza sia avanzata per iscritto e giunga:
 - a) all'indirizzo di posta elettronica dpo@unive.it, lo Staff di supporto al DPO inoltra tempestivamente la comunicazione al Settore Protocollo per la sua registrazione a protocollo;
 - b) all'indirizzo PEC protocollo@pec.unive.it o tramite raccomandata A/R, la stessa è protocollata dal Settore Protocollo assegnandola allo Staff di Supporto al DPO;
 - c) a un'altra Struttura di Ateneo (anche attraverso canali diversi dalla posta elettronica semplice o certificata, come, ad esempio, un sistema di *ticketing*), i relativi Referenti la inoltrano tempestivamente allo Staff di Supporto al DPO, che procede a inviarla al Settore Protocollo per la protocollazione.
3. Nel caso in cui vi siano dubbi sulla genuinità della richiesta (ad esempio, nel caso di istanze avanzate dagli Interessati tramite portali che li supportano nell'invio di richieste relative all'esercizio

dei Diritti), lo Staff di supporto al DPO procede alla richiesta di protocollazione solo dopo aver effettuato le dovute verifiche contattando il richiedente.

4. Lo Staff di Supporto al DPO annota tutte le istanze pervenute (comprese quelle di cui al precedente comma) all'interno del Registro delle richieste di esercizio dei Diritti di cui all'art. 11 del presente Allegato.
5. Lo Staff di supporto al DPO procede a coinvolgere tempestivamente i Referenti e gli eventuali Amministratori di Sistema di Ateneo competenti, al fine di ottenere il loro supporto per la gestione dell'istanza.
6. Nel caso in cui i Dati Personali oggetto dell'istanza siano condivisi con Contitolari del Trattamento e/o Responsabili del Trattamento e/o altri destinatari, quest'ultimi, qualora necessario, vengono coinvolti dal DPO e/o dallo Staff di supporto al DPO e/o dai Referenti nel minor tempo possibile e, comunque, non oltre 10 giorni lavorativi.

Articolo 6 - Adempimenti generali

1. Il DPO e lo Staff di Supporto al DPO verificano, in collaborazione con i Referenti competenti, l'identità del soggetto richiedente. In particolare, è possibile chiedere di esibire o di presentare copia di un documento di riconoscimento solo se l'identità del richiedente non possa essere verificata altrimenti: l'ottenimento del documento non è infatti necessario se la richiesta è presentata da un soggetto già noto (ad esempio, un dipendente o un collaboratore di Ateneo che utilizzi l'indirizzo di posta elettronica istituzionale di Ateneo o un soggetto i cui dati anagrafici e di contatto siano già presenti negli archivi associati all'anagrafica dell'Interessato). In caso di istanza presentata per iscritto e firmata digitalmente o trasmessa tramite PEC non sarà necessario richiedere copia del documento d'identità.
2. Nel caso di istanza presentata dall'Interessato tramite proprio delegato, è inoltre necessario verificare che la procura sia validamente conferita (controllando delega e copia del documento di riconoscimento del soggetto delegante e, eventualmente, copia del documento di riconoscimento del delegato).
3. Nel caso di istanza relativa a Dati Personali dell'Interessato deceduto ovvero dichiarato morto presunto, occorre inoltre verificare la documentazione presentata dall'istante.
4. Ai fini della gestione dell'istanza, il DPO e lo Staff di Supporto al DPO verificano, in collaborazione con i Referenti competenti, la fondatezza della richiesta avanzata e la non ricorrenza di uno dei casi previsti all'art. 10 del presente Allegato.
5. Se nell'istanza il richiedente non circoscrive i Dati Personali oggetto della richiesta, il DPO e lo Staff di Supporto al DPO provvedono a ottenere chiarimenti. Nel caso in cui non si ottenga un riscontro adeguato, l'istanza sarà considerata estesa a tutti i dati oggetto di Trattamento.
6. L'Ateneo, se richiesto, deve fornire copia dei Dati Personali oggetto di Trattamento. La trasmissione di tale copia deve avvenire con modalità sicure.
7. Nel caso in cui l'istanza coinvolga anche Dati Personali di terzi, tali dati devono essere rimossi od oscurati, ad eccezione dei seguenti casi:
 - a. la scomposizione o la privazione di alcuni elementi renda impossibile o estremamente difficile comprendere i Dati Personali relativi all'Interessato;
 - b. la richiesta faccia esplicito riferimento anche a Dati Personali relativi a soggetti terzi e dimostri la necessità di accedere a tali dati; in questi casi, l'Ateneo deve compiere un bilanciamento tra i diversi interessi implicati nel caso di specie e stabilire le modalità del riscontro.
8. Nel compimento delle valutazioni preliminari dell'istanza presentata, è necessario, inoltre, considerare che il riscontro alla stessa non leda i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, come anche i diritti d'autore.
9. Il DPO e lo Staff di supporto al DPO possono chiedere la collaborazione dei Referenti, delle Strutture competenti, degli Amministratori di Sistema nonché degli eventuali Contitolari o Responsabili del trattamento qualora si renda necessario estrarre i dati.

Articolo 7 - Modalità di riscontro

1. Il riscontro all'istanza è fornito per iscritto dal DPO e/o dallo Staff di Supporto al DPO con la collaborazione dei Referenti competenti. In casi specifici (ad esempio, istanza avanzata tramite

sistema di *ticketing*), è possibile valutare l'opportunità che il riscontro sia fornito dai Referenti competenti con la collaborazione del DPO.

2. Qualora, per evadere la richiesta, si debbano attuare azioni da cui derivino impatti a livello amministrativo (ad esempio, relativi ad aspetti contabili per la richiesta di un contributo secondo quanto previsto al successivo art. 9 o a interventi su applicativi o basi di dati per la cancellazione di dati personali) ovvero impatti sull'Interessato o sul richiedente (ad esempio, in caso di diniego dell'istanza o compimento di un bilanciamento di interessi a fronte di una richiesta di opposizione), il riscontro al richiedente è previamente autorizzato da un provvedimento interno adottato da un Referente di Struttura.
3. Il riscontro al richiedente è inviato per iscritto tramite email, PEC o raccomandata A/R.
4. Il riscontro deve essere reso in forma concisa, trasparente, intelligibile e facilmente accessibile.
5. Il riscontro è positivo se l'Ateneo accetta l'istanza avanzata dal richiedente.
6. Il riscontro è negativo se l'Ateneo ritiene di non poter accogliere l'istanza del richiedente in quanto:
 - a. non risulta possibile l'identificazione del richiedente;
 - b. l'istanza è manifestamente infondata;
 - c. l'istanza è manifestamente eccessiva, in particolare per il suo carattere ripetitivo.

L'Ateneo deve indicare le motivazioni del rifiuto e informare il richiedente che potrà proporre reclamo avanti all'Autorità di Controllo o ricorso giurisdizionale.

7. Lo Staff di supporto al DPO protocolla la comunicazione di riscontro e archivia tutta la documentazione riguardante la gestione dell'istanza (compresa, nel caso l'Ateneo ritenga di non accogliere la richiesta dell'Interessato, la documentazione riportante le considerazioni che hanno portato a tale decisione).
8. In caso di ispezione, se richiesto, la documentazione di cui al precedente c. 7, congiuntamente al Registro delle richieste di esercizio dei Diritti, deve essere resa disponibile all'Autorità di Controllo.

Articolo 8 - Tempi di riscontro alle istanze di esercizio dei Diritti

1. L'Ateneo fornisce riscontro (sia in caso di esito positivo che in caso di esito negativo) all'istanza di esercizio dei Diritti senza ritardo e comunque entro 30 giorni dalla ricezione della stessa.
2. Il termine di cui al precedente c. 1 può essere sospeso nel caso in cui l'Ateneo prenda contatto con il richiedente per ottenere informazioni utili all'identificazione ovvero per ricevere chiarimenti sull'oggetto dell'istanza. Tale sospensione dovrà essere comunicata al richiedente.
3. Il termine di cui al c. 1 può essere prorogato di 60 giorni (per un totale di 90 giorni dalla data di presentazione della richiesta) per comprovati motivi, tenuto conto della complessità della richiesta. L'Ateneo informa il richiedente di tale proroga e dei motivi del ritardo entro 30 giorni dal ricevimento dell'istanza.

Articolo 9 - Contributo spese

1. Il riscontro all'istanza di esercizio dei Diritti è gratuito. In casi specifici, secondo quanto di seguito indicato, i Referenti competenti, sentito anche il DPO, possono decidere di richiedere all'istante un contributo spese previa adozione di un provvedimento interno ai sensi dell'art. 7, c. 2.
2. In caso di riscontro negativo, in quanto non risultino presenti nei *database* o negli archivi cartacei dell'Ateneo Dati Personali relativi all'Interessato, potrà essere richiesto al richiedente il pagamento di un contributo spese. Non potrà essere chiesto alcun contributo quando i Dati Personali siano stati cancellati o comunque non siano più reperibili, ma siano stati trattati in precedenza.
3. In particolari casi connessi a istanze manifestamente eccessive, anche per il loro carattere ripetitivo, l'Ateneo potrà valutare di esigere dal richiedente il pagamento di un contributo spese.
4. In caso di riscontro positivo che comprenda la trasmissione di copia dei Dati Personali, la prima copia deve essere trasmessa a titolo gratuito. Se l'istante richiede ulteriori copie dei medesimi Dati Personali, allo stesso verrà chiesto di versare un contributo spese sulla base di quanto stabilito dal "*Tariffario relativo al rimborso dei costi di ricerca, visura, riproduzione e spedizione delle copie di documenti nell'ambito dei procedimenti di accesso documentale e civico generalizzato*" di Ateneo, disponibile sul sito web istituzionale. Se l'Interessato presenta la richiesta mediante mezzi elettronici, salvo indicazione diversa dello stesso, le informazioni sono fornite in un formato elettronico di uso comune.

Articolo 10 - Limitazioni al riscontro alle istanze di esercizio dei Diritti

1. La portata dei Diritti degli Interessati è limitata nei casi previsti dall'art. 23 del GDPR e dall'art. 2-undecies del Codice Privacy, ai quali si rimanda.

Articolo 11 - Registro delle richieste di esercizio dei Diritti

1. L'Ateneo ha istituito un Registro in cui vengono annotate le informazioni relative alle richieste di esercizio dei Diritti ricevute, compresi i tempi di riscontro alle stesse.
2. Il Registro è tenuto e aggiornato tempestivamente dal DPO e dallo Staff di Supporto al DPO.
3. Il Registro, su richiesta, deve essere messo a disposizione dell'Autorità di Controllo congiuntamente alla documentazione riguardante la gestione delle istanze.

TITOLO II – I DIRITTI DI CUI AGLI ARTT. 15-22 DEL GDPR¹

Articolo 12 - Diritto di accesso

1. Ai sensi dell'art. 15 del GDPR, l'Interessato ha il diritto di ottenere dall'Ateneo la conferma che sia o meno in corso un Trattamento di Dati Personali che lo riguardi e, in tal caso, di ottenere l'accesso ai dati e alle seguenti informazioni:
 - a. le finalità del Trattamento;
 - b. le categorie di Dati Personali oggetto di Trattamento;
 - c. i destinatari o le categorie di destinatari a cui i Dati Personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi od organizzazioni internazionali;
 - d. quando possibile, il periodo di conservazione dei Dati Personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
 - e. l'esistenza del diritto dell'Interessato di chiedere all'Ateneo la rettifica o la cancellazione dei Dati Personali o la limitazione del Trattamento dei Dati Personali che lo riguardano o di opporsi al loro Trattamento;
 - f. il diritto di proporre reclamo all'Autorità di Controllo;
 - g. qualora i Dati Personali non siano raccolti presso l'Interessato, tutte le informazioni disponibili sulla loro origine;
 - h. l'esistenza di un processo decisionale automatizzato, compresa la Profilazione, e, almeno in tal caso, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale Trattamento per l'Interessato.
2. Qualora i Dati Personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'Interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'art. 46 del GDPR relative al trasferimento.
3. L'Ateneo fornisce una copia dei Dati Personali oggetto di trattamento secondo quanto previsto dall'art. 9, c. 3, del presente Allegato.
4. Qualora la richiesta riguardi un vasto campione di Dati Personali e potrebbe essere complesso per l'Interessato ricevere tutte le informazioni insieme, l'Ateneo, dopo aver informato l'Interessato, può utilizzare un "*layered approach*", ovvero presentare le informazioni a scaglioni, in modo da dare la possibilità all'Interessato di comprenderle.

Articolo 13 - Diritto di rettifica

1. Ai sensi dell'art. 16 del GDPR, l'Interessato ha il diritto di ottenere dall'Ateneo la rettifica dei Dati Personali inesatti che lo riguardano senza ingiustificato ritardo, e comunque entro i tempi definiti all'art. 8 del presente Allegato. Tenuto conto delle finalità del Trattamento, l'Interessato ha il diritto di ottenere dall'Ateneo l'integrazione dei Dati Personali eventualmente incompleti, anche fornendo una dichiarazione integrativa.
2. Nel caso in cui l'istanza riguardi documentazione con valore legale (ad esempio, certificati di laurea), l'Ateneo procederà a modificare il documento in caso di errore materiale e nei casi previsti dalla normativa, mantenendo agli atti la documentazione originale.

¹ Nel Titolo II si fa riferimento ai Diritti dell'Interessato; resta inteso che, nel caso di richieste relative a Dati Personali di Interessati deceduti ovvero dichiarati morti presunti, i Diritti possono essere esercitati anche dai soggetti legittimati di cui all'art. 3 del presente Allegato.

3. L'Ateneo comunica a ciascuno dei destinatari cui sono stati trasmessi i Dati Personali le eventuali rettifiche del trattamento, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. L'Ateneo comunica all'Interessato tali destinatari qualora l'Interessato lo richieda.

Articolo 14 - Diritto alla cancellazione

1. Ai sensi dell'art. 17 del GDPR, l'Interessato ha il diritto di ottenere dall'Ateneo la cancellazione dei Dati Personali che lo riguardano e l'Ateneo ha l'obbligo di cancellare tali Dati Personali senza ingiustificato ritardo, e comunque entro i tempi definiti all'art. 8 del presente Allegato, se sussiste uno dei motivi seguenti:
 - a. i Dati Personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
 - b. l'Interessato revoca il consenso su cui eventualmente si basa il Trattamento svolto dall'Ateneo e se non sussiste altro fondamento giuridico per il trattamento;
 - c. l'Interessato si oppone al Trattamento;
 - d. i Dati Personali sono stati trattati illecitamente;
 - e. i Dati Personali devono essere cancellati per adempiere a un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del Trattamento.
2. L'Ateneo non procede a cancellare i Dati Personali il cui Trattamento sia necessario:
 - a. per l'esercizio del diritto alla libertà di espressione e di informazione;
 - b. per l'adempimento di un obbligo giuridico che richieda il Trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del Trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del Trattamento;
 - c. per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'art. 9, c. 2, lett. h) e i) del GDPR, e dell'art. 9, c. 3 del GDPR;
 - d. a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui la cancellazione dei Dati Personali rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale Trattamento;
 - e. per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
3. L'Ateneo comunica a ciascuno dei destinatari cui sono stati trasmessi i Dati Personali le eventuali cancellazioni del trattamento, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. L'Ateneo comunica all'Interessato tali destinatari qualora quest'ultimo lo richieda.
4. L'Ateneo, qualora abbia reso pubblici Dati Personali e sia obbligato a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, adotta le misure ragionevoli, anche tecniche, per informare i Titolari del Trattamento che stanno trattando i Dati Personali della richiesta dell'Interessato di cancellare qualsiasi *link*, copia o riproduzione dei suoi Dati Personali.

Articolo 15 - Diritto di limitazione di Trattamento

1. Ai sensi dell'art. 18 del GDPR, l'Interessato ha il diritto di ottenere dall'Ateneo la limitazione del Trattamento quando ricorre una delle seguenti ipotesi:
 - a. l'Interessato contesta l'esattezza dei Dati Personali per il periodo necessario al Titolare del Trattamento per verificare l'esattezza di tali Dati Personali;
 - b. il Trattamento è illecito e l'Interessato si oppone alla cancellazione dei Dati Personali e chiede invece che ne sia limitato l'utilizzo;
 - c. benché il Titolare del Trattamento non ne abbia più bisogno ai fini del Trattamento, i Dati Personali sono necessari all'Interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
 - d. l'Interessato si è opposto al Trattamento ed è in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del Trattamento rispetto a quelli dell'Interessato.
2. Se il Trattamento viene limitato, i Dati Personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'Interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i Diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante.

3. L'Interessato che ha ottenuto la limitazione del Trattamento è informato dall'Ateneo prima che detta limitazione sia revocata.
4. L'Ateneo comunica a ciascuno dei destinatari cui sono stati trasmessi i Dati Personali le eventuali limitazioni del trattamento, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. L'Ateneo comunica all'Interessato tali destinatari qualora l'Interessato lo richieda.

Articolo 16 - Diritto alla portabilità dei Dati Personali

1. Ai sensi dell'art. 20 del GDPR, l'Interessato ha il diritto di richiedere all'Ateneo la ricezione in un formato strutturato, di uso comune e leggibile da dispositivo automatico i Dati Personali che lo riguardano e di trasmetterli a un altro Titolare del trattamento senza impedimenti da parte dell'Ateneo, qualora:
 - a. il Trattamento si basi sul consenso, ai sensi dell'art. 6, c 1, lett. a), o dell'art. 9, c 2, lett. a), o su un contratto ai sensi dell'art. 6, c. 1, lett. b), del GDPR; e
 - b. il Trattamento sia effettuato con mezzi automatizzati.
2. In caso di esercizio di tale diritto, l'Interessato ha il diritto di ottenere la trasmissione diretta dei Dati Personali da un Titolare del Trattamento all'altro, se tecnicamente fattibile.
3. L'esercizio del diritto alla portabilità lascia impregiudicato l'art. 17 del GDPR. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del Trattamento.
4. Il diritto alla portabilità non deve ledere i diritti e le libertà altrui.

Articolo 17 - Diritto di opposizione

1. Ai sensi dell'art. 21 del GDPR, l'Interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al Trattamento dei Dati Personali che lo riguardano ai sensi dell'art. 6, c. 1, lett. e), del GDPR compresa la profilazione sulla base di tali disposizioni. L'Ateneo si astiene dal trattare ulteriormente i Dati Personali salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al Trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'Interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Il DPO, di concerto con i Referenti competenti, valuta se sussistono o meno i predetti motivi cogenti documentandoli per iscritto.
2. Qualora i Dati Personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'art. 89, c. 1 del GDPR, l'Interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di Dati Personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.
3. In caso di ricezione di *newsletter* o di comunicazioni tramite *mailing list*, l'Interessato può esercitare il suo diritto di opposizione al ricevimento di futuri messaggi attraverso l'"*unsubscribe link*" contenuto nelle comunicazioni inviate dall'Ateneo. La richiesta di disiscrizione deve essere registrata dall'Università in apposita lista in modo da assicurarsi di non contattare nuovamente tale soggetto. Il diritto di opposizione non potrà essere esercitato dall'Interessato in relazione a comunicazioni di carattere istituzionale rispetto alle quali l'Ateneo abbia effettuato una valutazione in termini di rischi derivanti dalla mancata ricezione.

Articolo 18 - Diritti relativi ai processi decisionali automatizzati, compresa la profilazione

1. L'Interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul Trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
2. Il precedente comma non si applica nel caso in cui la decisione:
 - a. sia necessaria per la conclusione o l'esecuzione di un contratto tra l'Interessato e il Titolare del Trattamento;
 - b. sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del Trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'Interessato;
 - c. si basi sul consenso esplicito dell'Interessato.

3. Nei casi in cui tale Trattamento è concesso, l'Ateneo deve garantire l'attuazione di misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'Interessato, almeno il diritto di ottenere l'intervento umano da parte del Titolare del Trattamento, di esprimere la propria opinione e di contestare la decisione.
4. Le predette decisioni non si basano sulle Categorie Particolari di Dati Personali salvo che sia applicabile l'art. 9, c. 2, lett. a) o g), del GDPR, e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'Interessato.

ALLEGATO G

GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI (“DATA BREACH”)

Articolo 1 - Premessa

1. Le Violazioni di Dati Personali o *Data Breach*, così come definite all'art. 5 del presente Regolamento, sono incidenti di sicurezza che compromettono uno o più dei seguenti attributi: confidenzialità, integrità o disponibilità dei Dati Personali.
2. Il presente Allegato ha l'obiettivo di definire le procedure da seguire durante la gestione di un *Data Breach*. In particolare, sono individuate le seguenti fasi:
 - a. rilevazione dell'incidente;
 - b. valutazione dello stesso per stabilire se sono coinvolti Dati Personali e, pertanto, se lo stesso costituisce un *Data Breach* o un incidente di sicurezza;
 - c. ove possibile, implementazione tempestiva di misure di mitigazione per limitare gli effetti del *Data Breach*;
 - d. valutazione del rischio posto dal *Data Breach* agli Interessati coinvolti per stabilire la necessità di notifica all'Autorità di Controllo e/o di comunicazione agli Interessati stessi;
 - e. eventuale notifica all'Autorità di Controllo e comunicazione agli interessati;
 - f. implementazione delle misure di *remediation*;
 - g. compilazione del Registro degli incidenti di Sicurezza e dei *Data Breach*.
3. Nel presente Allegato, per ciascuna delle fasi sopra riportate, verranno definiti i ruoli e le responsabilità dei soggetti coinvolti.

Articolo 2 - Ambito di applicazione

1. Il presente Allegato si applica alle Violazioni di Dati Personali trattati dall'Ateneo, in qualità di Titolare del Trattamento e, per quanto compatibile, di Contitolare o Responsabile del Trattamento.
2. Il presente Allegato si applica ai Dati Personali trattati sia su supporti informatici sia cartacei.
3. Per gli incidenti di sicurezza che non coinvolgono Dati personali, si rimanda all'apposita *policy*.

Articolo 3 - Principi generali

1. La tempestività è un fattore determinante nella gestione di un *Data Breach* in quanto permette di limitare i rischi per gli Interessati e di rispettare la ridotta tempistica, prevista dall'art. 33 del GDPR, per procedere, qualora necessaria, alla notifica all'Autorità di Controllo e/o all'eventuale comunicazione agli Interessati. Pertanto, tutti i soggetti coinvolti nella gestione di un *Data Breach*, nell'ambito del proprio ruolo, devono attribuire alla stessa la massima priorità, rispettando le indicazioni contenute nel presente Allegato e ponendo attenzione a non ritardare per alcun motivo le iniziative di loro competenza.
2. I soggetti coinvolti nella gestione di un *Data Breach* devono mantenere la massima riservatezza sull'accaduto. Non devono, pertanto, essere condivisi dettagli relativi al *Data Breach* con colleghi e collaboratori non direttamente coinvolti nella sua gestione; a quest'ultimi dovrà semplicemente essere comunicato che si è verificato incidente e che le attività di risposta allo stesso sono in corso.

Articolo 4 - Rilevazione di un incidente di sicurezza

Articolo 4.1. - Rilevazione di un incidente di sicurezza che si sospetti essere un *Data Breach* e che comporti una violazione dei sistemi informatici dell'Ateneo

1. Il personale, i collaboratori e gli studenti dell'Ateneo qualora, nello svolgimento della propria attività lavorativa, di studio o a seguito di segnalazione di terzi, vengano a conoscenza di un incidente di sicurezza che comporti una violazione dei servizi informatici dell'Ateneo dovranno immediatamente:
 - (i) aprire un ticket con le modalità previste alla pagina <https://www.unive.it/pag/32842>; e (ii) chiamare il numero 041 234 7171.
2. L'operatore incaricato della gestione del ticket o del ricevimento della telefonata procederà a documentare l'evento, nel sistema di ticketing a disposizione, identificandolo con un numero di riferimento e inserendo informazioni dettagliate sullo stesso, quali data, orario, luogo, fonte della segnalazione, sistema informatico coinvolto e, ove possibile, stima dell'entità della violazione.

3. A seguito di tale attività, l'operatore provvederà immediatamente a contattare telefonicamente e/o via email il Dirigente di ASIT, il Direttore dell'Ufficio Sistemi e Infrastrutture di ASIT, il Responsabile della Sicurezza Informatica e i Referenti di Struttura delle strutture coinvolte. Il Referente di Struttura potrà decidere di coinvolgere i Referenti Interni eventualmente interessati. Se vi è il sospetto che nell'incidente siano coinvolti anche Dati Personali, il Referente di Struttura provvederà immediatamente a contattare telefonicamente e/o via email anche il DPO e lo Staff di Supporto al DPO.
4. Qualora l'incidente di sicurezza sia rilevato dal Direttore dell'Ufficio Sistemi e Infrastrutture e/o dal Responsabile della Sicurezza Informatica nello svolgimento delle proprie attività, lo stesso dovrà documentare l'accaduto in apposito *report* da lui sottoscritto, indicando data, orario, luogo, fonte della segnalazione, sistema informatico coinvolto e stimata entità della violazione, senza la necessità di aprire un ticket. Il Responsabile della Sicurezza Informatica provvederà immediatamente a contattare telefonicamente e/o via email il Dirigente di ASIT e il Referente di Struttura della struttura coinvolta. Il Referente di Struttura potrà decidere di coinvolgere i Referenti Interni eventualmente interessati. Se vi è il sospetto che nell'incidente siano coinvolti anche Dati Personali, il Responsabile della Sicurezza Informatica provvederà immediatamente a contattare telefonicamente e/o via email anche il DPO e lo Staff di Supporto al DPO.

Articolo 4.2. - Rilevazione di un incidente di sicurezza che si sospetti essere un *Data Breach* e che non comporti una violazione dei sistemi informatici dell'Ateneo

1. Il personale, i collaboratori e gli studenti dell'Ateneo qualora, nello svolgimento della propria attività lavorativa, di studio o a seguito di segnalazione di terzi, vengano a conoscenza di un incidente di sicurezza che si sospetti coinvolga Dati Personali e che non comporti una violazione dei servizi informatici dell'Ateneo (es. smarrimento di documentazione cartacea, ecc.), dovranno immediatamente contattare il proprio Referente di Struttura, che potrà decidere di coinvolgere i Referenti Interni eventualmente interessati, nonché inviare un'email all'indirizzo dpo@unive.it e telefonare al DPO di Ateneo e allo Staff di Supporto al DPO fino a che non si riceve risposta.

Articolo 5 - Valutazione preliminare

1. A seguito della rilevazione di un incidente di sicurezza che si sospetti coinvolga Dati Personali, il DPO, lo Staff di Supporto al DPO, il Referente di Struttura, gli eventuali Referenti Interni coinvolti e, nei casi di cui all'art. 4, c.1 che precede, il Dirigente di ASIT nonché il Responsabile della Sicurezza Informatica procederanno immediatamente, sulla base delle informazioni raccolte, alla valutazione preliminare dell'evento per stabilire se effettivamente si tratti di un *Data Breach*.
2. Se al termine della valutazione, si stabilisce che si tratta di *Data Breach* si dovrà procedere come descritto agli articoli che seguono. Se, invece, si stabilisce che non si tratta di un *Data Breach*, si procederà ad archiviare la documentazione comprovante il fatto che non sono coinvolti Dati Personali, nella quale verranno eventualmente indicate le misure correttive da adottare.
3. L'Ateneo si ritiene "venuto a conoscenza", ai sensi dell'art. 33 del GDPR, di una Violazione di Dati Personali solamente al termine della valutazione preliminare di cui ai commi che precedono. Pertanto, i termini di cui all'art. 33 del GDPR iniziano a decorrere da tale momento.

Articolo 6 - Valutazione del *Data Breach* e analisi del rischio

1. A seguito della valutazione preliminare compiuta ai sensi dell'art. 5 che precede, il Referente di Struttura e i Referenti Interni eventualmente coinvolti dovranno proseguire con l'attività di raccolta di informazioni dettagliate sull'accaduto, anche tramite attività di analisi demandate al Responsabile della Sicurezza Informatica e/o con l'ausilio del DPO e dello Staff di Supporto al DPO, al fine di acquisire i necessari elementi per compiere una valutazione complessiva del *Data Breach*. Le informazioni raccolte dovranno essere documentate in apposito *report* che dovrà essere concluso e sottoscritto dal Referente di Struttura competente entro e non oltre 36 ore dal termine della valutazione preliminare.
2. Il DPO e lo Staff di Supporto al DPO, sulla base delle informazioni del *report* sottoscritto dal Referente di Struttura, procederanno all'analisi del rischio secondo la metodologia suggerita dalla *European Union Agency for Cybersecurity* nel documento denominato "*Recommendations for a*

methodology of the assessment of severity of personal data breaches” del dicembre 2013. In particolare, la gravità dell'incidente viene calcolata attraverso la seguente equazione:

GI (gravità incidente) = **CDT** (contesto del trattamento) x **FDI** (facilità di identificazione) + **CDV** (circostanze della violazione)

3. Il rischio calcolato con la metodologia sopra citata può risultare: basso, medio, alto o molto alto. In particolare, i livelli di rischio possono essere così descritti:

Basso	I soggetti potrebbero non essere coinvolti oppure subire alcuni disagi che potranno essere superati senza grossi problemi (tempo necessario a inserire nuovamente le informazioni, fastidio, irritazione, ecc.).
Medio	I soggetti potrebbero riscontrare significativi disagi che riusciranno tuttavia a superare nonostante qualche difficoltà (costi aggiuntivi, impossibilità di accedere ai servizi, preoccupazione, mancata comprensione, stress, malattie di piccola entità, ecc.).
Alto	I soggetti potrebbero subire gravi conseguenze che dovrebbero tuttavia poter superare sebbene con serie difficoltà (sottrazione di fondi, “liste nere” di banche, danni alla proprietà, perdita dell'occupazione, citazione in giudizio, danni alla salute, ecc.).
Molto alto	I soggetti potrebbero subire conseguenze gravi o addirittura irreversibili, che potrebbero non riuscire a superare (difficoltà finanziarie tra cui debiti considerevoli o incapacità di lavorare, malattie a lungo termine psicologiche o fisiche, decesso, ecc.).

4. Nel caso in cui, a seguito del calcolo effettuato, il rischio risulti basso, il Referente di Struttura redige e sottoscrive un documento in cui dichiara la non necessità di procedere alla notifica all'Autorità di Controllo e alla comunicazione agli Interessati individuando, però, le necessarie misure di *remediation* che dovranno essere adottate per evitare il ripetersi dell'evento in futuro. Tale documento dovrà essere inviato dal Referente di Struttura al Rettore e al Direttore Generale entro 48 ore dal termine della valutazione preliminare di cui all'art. 5 che precede.
5. Nel caso in cui, a seguito del calcolo effettuato, il rischio risulti medio, il Referente di Struttura informerà tempestivamente, e, comunque, entro 48 ore dal termine della valutazione preliminare, di tale circostanza il Direttore Generale e il Rettore. Quest'ultimo procederà con la notifica all'Autorità di Controllo secondo quanto formulato nell'art. 7 che segue.
6. Nel caso in cui, a seguito del calcolo effettuato, il rischio risulti alto o molto alto, il Referente di Struttura informerà tempestivamente, e comunque entro 48 ore dal termine della valutazione preliminare, di tale circostanza il Direttore Generale e il Rettore. Quest'ultimo procederà con la notifica all'Autorità di Controllo secondo quanto formulato nell'art. 7 che segue e con la comunicazione agli Interessati, ove ne ricorrano i presupposti, secondo quanto previsto dall'art. 8 del presente Allegato

Articolo 7 – Notifica al Garante

1. Qualora un *Data Breach* presenti un rischio medio, alto o molto alto, il Rettore a seguito della segnalazione del Referente di Struttura, procederà, con la collaborazione del DPO e dello Staff di Supporto al DPO, alla notifica all'Autorità di Controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dalla avvenuta conoscenza dell'evento.
2. La notifica avverrà utilizzando il modulo messo a disposizione dall'Autorità di Controllo che dovrà riportare la firma digitale del Rettore. La notifica verrà inviata all'Autorità di Controllo via PEC.

3. La notifica dovrà necessariamente, ai sensi dell'art. 33, c. 3, del GDPR: *“a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; c) descrivere le probabili conseguenze della violazione dei dati personali; d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi”*.
4. Qualora non sia possibile trasmettere la notifica all'Autorità di Controllo con tutte le informazioni di cui al comma precedente, si dovrà procedere a una notifica per fasi. La necessità di procedere a tale tipologia di notifica dovrà essere motivata.
5. In casi particolarmente complessi, in cui si ha il sospetto che un *Data Breach* sia occorso ma, entro la tempistica prevista, non è possibile reperire informazioni certe, si procederà a notificare all'Autorità di Controllo quanto conosciuto entro le 72 ore e, successivamente, si trasmetteranno le informazioni acquisite. Qualora, a seguito di successive analisi, si dovesse appurare che non si è verificato alcun *Data Breach*, tale circostanza dovrà essere immediatamente comunicata all'Autorità di Controllo.
6. Qualora si dovessero verificare *Data Breach* multipli e consequenziali nell'arco di un brevissimo periodo di tempo, si potrà decidere di procedere con un'unica notifica all'Autorità di Controllo che descriva congiuntamente tutte le Violazioni di Dati Personali occorse.

Articolo 8 – Comunicazione agli interessati/alle interessate

1. Il Rettore procederà, sentito il DPO e con la collaborazione dei Referenti di Struttura o dei Referenti Interni competenti, alla comunicazione agli Interessati, senza ingiustificato ritardo, qualora un *Data Breach* presenti un rischio alto o molto alto, e ricorrano le condizioni di cui all'art. 34 del GDPR.
2. La comunicazione dovrà contenere un linguaggio semplice e chiaro e potrà essere trasmessa utilizzando i canali ritenuti più idonei.
3. La comunicazione, ai sensi degli articoli 34, c. 3, e 33, c. 3, del GDPR dovrà necessariamente riportare: *“il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; descrivere le probabili conseguenze della violazione dei dati personali; descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi”*.
4. Non sarà, invece, necessario comunicare agli interessati la Violazione dei Dati Personali subita nei seguenti casi: *“a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1; c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia”*.

Articolo 9 – Azioni di mitigazione

1. Durante tutte le fasi di gestione di un *Data Breach*, laddove possibile, si intraprenderanno azioni immediate per contenere e/o prevenire ulteriori danni. Tali azioni possono anche consistere nella messa fuori servizio di reti e sistemi.
2. Le azioni di mitigazione dovranno rimanere in essere fino alla risoluzione dell'incidente.

Articolo 10 – Misure di remediation

1. A seguito del verificarsi di un *Data Breach*, a prescindere dal suo livello di rischio, il Referente di Struttura dovrà sempre individuare delle azioni correttive, sia tecniche che organizzative, che dovranno essere adottate per prevenire il ripetersi dell'incidente. Nella definizione di tali misure, il Referente di Struttura si coordinerà con il DPO e ASIT.

2. L'adozione di tali azioni è di responsabilità del Referente di Struttura e degli eventuali Referenti Interni coinvolti, che possono richiedere il supporto di ASIT, del DPO nonché dello Staff di Supporto al DPO.

Articolo 11 – Registro degli incidenti di Sicurezza e dei *Data Breach*

1. L'Ateneo ha istituito, ai sensi dell'art. 33, c. 5 del GDPR, un registro in cui vengono documentati sia gli incidenti di sicurezza, sia le Violazioni di Dati Personali occorse, a prescindere dalla necessità di notificare le stesse all'Autorità di Controllo.
2. Il registro, con riferimento ai *Data Breach*, contiene la descrizione della Violazione dei Dati Personali occorsa, comprensiva delle circostanze a essa relative, delle sue conseguenze e dei provvedimenti adottati per porvi rimedio ed evitare che le violazioni possano ripetersi in futuro. La compilazione del registro avviene sulla base delle informazioni ricevute dal Referente di Struttura competente nel *report* di cui all'art. 6 che precede.
3. Il registro è tenuto dal Dirigente di ASIT e aggiornato tempestivamente dal personale di ASIT, al verificarsi di un incidente di sicurezza, e dallo Staff di Supporto al DPO, in caso di un *Data Breach*.
4. Il registro, su richiesta, dovrà essere messo a disposizione dell'Autorità di Controllo congiuntamente alla documentazione prodotta per documentare e valutare l'accaduto.

Articolo 12 – Gestione di un *Data Breach* occorso in regime di contitolarità

1. Gli accordi di contitolarità conclusi dall'Ateneo, ai sensi dell'art. 26 del GDPR, prevedono una clausola che disciplina il ruolo dei Contitolari del Trattamento con riferimento alla gestione di un *Data Breach* e le rispettive responsabilità.
2. L'Ateneo si impegna a collaborare, ove possibile, con l'altro Contitolare/gli altri Contitolari durante tutte le fasi di risposta a un *Data Breach*.

Articolo 13 – Gestione di un *Data Breach* occorso presso un Responsabile del Trattamento dell'Ateneo

1. Gli accordi stipulati dall'Ateneo, in qualità di Titolare del Trattamento, ai sensi dell'art. 28 del GDPR, contengono istruzioni specifiche per il Responsabile del Trattamento con riferimento alla gestione e comunicazione delle Violazioni di Dati Personali sui Dati Personali trattati per conto dell'Ateneo stesso.
2. Nei predetti accordi viene stabilito che il Responsabile del Trattamento debba informare il Titolare del Trattamento dell'avvenuta Violazione di Dati Personali senza ingiustificato ritardo dopo essere venuto a conoscenza del *Data Breach*. Ove possibile, nell'accordo si indicherà una tempistica definita entro la quale il Responsabile del Trattamento debba informare il Titolare del Trattamento dell'avvenuta Violazione di Dati Personali.
3. Gli accordi di nomina a Responsabile del Trattamento devono prevedere l'impegno per quest'ultimo a collaborare con l'Ateneo durante tutte le fasi di risposta a un *Data Breach*, tenendo conto della natura del Trattamento e delle informazioni a disposizione del Responsabile stesso.