Università Ca'Foscari Venezia

Università Ca' Foscari Venezia
Dorsoduro 3246, 30123 Venezia
P.IVA 00816350276 - CF 80007720271
www.unive.it

Decreto della Rettrice 2021

Oggetto: **Regolamento in materia di protezione dei dati personali dell'Università Ca' Foscari Venezia – Emanazione**

LA RETTRICE

VISTO 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 e che abroga la direttiva 95/46/CE ("Regolamento Generale sulla Protezione dei Dati Personali");

VISTO 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 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)";

CONSIDERATA la necessità dell'Ateneo di dotarsi di un proprio Regolamento interno recante i principi e le disposizioni ai quali l'Università deve attenersi con riguardo alle attività di trattamento dei dati personali nell'ambito sia delle proprie finalità istituzionali (didattica, ricerca, terza missione, amministrazione, servizi e ulteriori attività previste in convenzioni e contratti con soggetti pubblici o privati), sia delle attività in "conto terzi" svolte a favore di un committente;

VISTO lo Statuto di Ateneo;

VISTA la delibera del Consiglio di Amministrazione n. 17 del 05.02.2021, con la quale è stato approvato il "Regolamento in materia di protezione dei dati personali dell'Università Ca' Foscari Venezia";

VISTO il Decreto del Direttore Generale n. 409/2018;

PRESO ATTO che la struttura proponente ha attestato la conformità del provvedimento alla legislazione vigente e ai regolamenti di Ateneo;

DECRETA

Art. 1. È emanato il "Regolamento in materia di protezione dei dati personali dell'Università Ca' Foscari Venezia", secondo il testo allegato al presente Decreto, di cui costituisce parte integrante.

Art. 2. Il Regolamento, di cui al precedente art. 1, entra in vigore il settimo giorno successivo alla pubblicazione del presente Decreto all'Albo dell'Ateneo, che viene disposta nella data di protocollazione dello stesso.

Art. 3. Con l'entrata in vigore del Regolamento in oggetto, di cui al precedente art. 1, viene abrogato il "Regolamento per la Disciplina della videosorveglianza nelle sedi universitarie", emanato con D.R. n. 383 dell'11.07.2012.

LA RETTRICE
Prof.ssa Tiziana Lippiello
Firmato digitalmente da: Tiziana Lippiello
Organizzazione: UNIVERSITA' DEGLI STUDI DI VENEZIA/00816350276
Data: 22/02/2021 09:19:28

Allegato: Regolamento in oggetto

Direzione Generale/Ufficio Affari Generali
aff.generali@unive.it / T. 041 234 7506 / 8231 / 8060

VISTO: IL RESPONSABILE DEL PROCEDIMENTO AMMINISTRATIVO
Ing. Tommaso Piazza – Dirigente ad interim dell'Area Pianificazione e Programmazione Strategica

Digitally signed by Tommaso Piazza
Date: 2021.02.18 15:00:11 +01'00'

VISTO: IL RESPONSABILE DEL PROVVEDIMENTO DI EMANAZIONE
Dott.ssa Massimiliana Equizi – Direttrice dell'Ufficio Affari Generali

Firmato digitalmente da: Massimiliana Equizi
Organizzazione: UNIVERSITA' DEGLI STUDI DI VENEZIA/00816350276
Data: 19/02/2021 15:23:24

VISTO: IL DIRETTORE GENERALE
Dott. Gabriele Rizzetto

Firmato digitalmente da: RIZZETTO GABRIELE
Data: 19/02/2021 16:33:55

Università
Ca'Foscari
Venezia

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

Sommario

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 come di seguito definiti.

Articolo 2 - Riferimenti normativi

1. Le principali fonti normative di riferimento sono costituite da:
    - Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE ("Regolamento Generale sulla Protezione dei Dati Personali");
    - D.Lgs. 30 giugno 2003 n. 196, "Codice in materia di protezione dei dati personali", così come modificato e integrato dal D.Lgs. n. 101/2018, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".
2. L'Ateneo osserva altresì le Linee Guida e i Provvedimenti adottati dal Garante per la Protezione dei Dati Personali, i provvedimenti del Comitato Europeo per la Protezione dei Dati e il "Codice Etico e 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 assegnate loro dall'Ateneo.

Articolo 4 - Ambito di applicazione oggettivo

1. L'Ateneo 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'Ateneo con soggetti pubblici o privati, sia in ambito nazionale che internazionale. Rientrano tra le attività istituzionali anche le attività di informazione e comunicazione istituzionale finalizzate a promuovere gli obiettivi strategici, il nome, l'immagine e le attività svolte dall'Ateneo. Le predette attività sono svolte dall'Ateneo in qualità di Titolare del Trattamento o Contitolare del Trattamento.
2. Inoltre, l'Ateneo svolge attività di Trattamento dei Dati Personali nell'ambito di attività in "conto terzi", ovvero attività di interesse prevalente del committente e per le quali l'Ateneo percepisce un corrispettivo, disciplinate da contratti sottoscritti con soggetti pubblici e privati. Le predette attività sono svolte dall'Ateneo in qualità di Responsabile del Trattamento.

CAPO II – DEFINIZIONI

Articolo 5 - Definizioni

1. Ai fini del presente Regolamento si intende per:
    - **"Ateneo"**: l'Università Ca' Foscari Venezia in tutte le sue articolazioni;
    - **"Struttura"**: le Aree dell'Amministrazione Centrale e i relativi Uffici, i Dipartimenti, le Scuole, il Sistema Bibliotecario, i Centri dell'Ateneo e i gruppi di ricerca che fanno capo a uno Sperimentatore Principale;
    - **"Codice Privacy"**: il D.Lgs. 30 giugno 2003 n. 196, "Codice in materia di protezione dei dati personali", così come modificato e integrato dal D.Lgs. n. 101/2018, recante "Disposizioni per

l'adeguamento dell'ordinamento nazionale al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE", nonché da ss.mm.ii.;

- **"GDPR"**: il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio 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;
- "**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;
- **"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;
- **"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;
- **"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;
- **"Dati Biometrici**": i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentano o confermino l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- **"Dati relativi alla salute"**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria che rivelano informazioni relative al suo stato di salute;
- **"Dati Personali Giudiziari**": i dati personali relativi a condanne penali e reati o a connesse misure di sicurezza;
- **"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;
- **"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;
- **"Pseudonimizzazione"**: il trattamento dei dati personali in modo tale che gli stessi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- **"Archivio"**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- **"Titolare del Trattamento"**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto

dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

- **"Contitolare del Trattamento"**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altro/i titolare/i del trattamento, determina le finalità e i mezzi del trattamento dei dati personali;
- **"Responsabile per la Protezione dei Dati"** o **"*Data Protection Officer*" ("RPD" o "DPO")**: figura indipendente che svolge attività di consulenza, supporto e controllo per il corretto adeguamento dell'Ateneo al GDPR nonché di raccordo con il Garante per la Protezione dei Dati Personali;
- **"Responsabile del Trattamento"**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- **"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;
- **"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;
- **"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;
- **"Sperimentatore Principale" o "*Principal Investigator*":** è il ricercatore responsabile del progetto di ricerca e delle attività compiute dagli altri ricercatori impegnati nello stesso;
- **"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;
- **"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;
- **"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;
- **"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;
- **"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;
- **"Violazione dei dati personali"**: l'evento che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- **"Comunicazione"**: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare nel territorio dell'Unione europea, dal Responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate ai sensi 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;
- **"Diffusione"**: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

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:
    - trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato ("principio di liceità, correttezza e trasparenza");
    - 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");
    - adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("principio di minimizzazione dei dati");
    - 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");
    - 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");
    - 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 per 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 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, quali 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, la portata del Trattamento, il periodo di conservazione e l'accessibilità. 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. 24 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 tale Trattamento.
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, vale a dire "*l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del Trattamento*" (meglio specificati 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 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 e conserva la documentazione relativa all'individuazione della corretta base giuridica, che metterà a disposizione, su richiesta, al Garante per la Protezione dei Dati Personali.

Articolo 10 - Basi giuridiche del Trattamento per Categorie Particolari di Dati Personali

1. Il Trattamento di Categorie Particolari di Dati Personali da parte dell'Ateneo è vietato, salvo il verificarsi di uno dei casi indicati dall'art. 9, c. 2, del GDPR.
2. La principale base giuridica che legittima i Trattamenti di Dati Personali particolari effettuati dall'Ateneo è costituita 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/.

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:
    - 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;
    - l'adempimento degli obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali;
    - la verifica o l'accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdettivi nei casi previsti dalle leggi o dai regolamenti;
    - 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;
    - l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
    - l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
    - 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;

- 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;
- 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;
- l'attuazione della disciplina in materia di attribuzione del *rating* di legalità delle imprese ai sensi dell'art. 5-*te*r del Decreto Legge 24 gennaio 2012, n. 1, convertito, con modificazioni, dalla Legge 24 marzo 2012, n. 27;
- 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 (in particolare per la Comunicazione e la Diffusione di Dati Personali si faccia riferimento al TITOLO II, Capo IV del presente Regolamento).
2. Il Trattamento di Categorie Particolari di Dati Personali da parte dell'Ateneo, la cui base giuridica 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 o le stesse finalità. Qualora il Trattamento abbia più finalità, il Consenso deve essere prestato per tutte queste.
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 dovrà 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 raccoglierlo e a conservare la relativa documentazione, composta dall'informativa resa all'interessato e dalla documentazione comprovante la manifestazione del consenso stesso, in modo da poter dimostrare tale adempimento.

TITOLO II - TRATTAMENTO DEI DATI PERSONALI

CAPO I - ORGANIZZAZIONE E RESPONSABILITA'

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, dei Direttori dei Dipartimenti, dei Direttori o Responsabili dei Centri e delle Scuole di Ateneo.
2. I Direttori degli Uffici e i Segretari dei Dipartimenti, delle Scuole e dei Centri sono nominati Referenti Interni. Sono, inoltre, nominati Referenti Interni gli Sperimentatori Principali (*Principal Investigator*) dei progetti di ricerca.
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 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 devono organizzare, 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 alla 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 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

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), il personale docente, i ricercatori, i dottorandi, gli assegnisti, i consulenti e collaboratori e gli eventuali altri soggetti che intrattengono rapporti di lavoro con l'Ateneo

nonché gli studenti nello svolgimento di compiti assegnati dall'Ateneo stesso saranno Autorizzati al Trattamento, con apposito atto di nomina sottoscritto dal Magnifico Rettore.

2. Gli Autorizzati al Trattamento: (i) operano sotto la diretta autorità del proprio 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 e (iv) ricevono formazione in materia di protezione dei Dati Personali specifica per la Struttura di appartenenza.

Articolo 17 - 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"), 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 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, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
    d) cooperare con il Garante per la Protezione dei Dati Personali;
    e) fungere da punto di contatto per il Garante per la Protezione dei Dati Personali per questioni connesse al Trattamento, tra cui la consultazione preventiva di cui all'art. 36 del GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
    f) collaborare alla redazione e all'aggiornamento dei registri del Trattamento;
    g) svolgere ogni ulteriore compito attribuitogli dal Titolare del Trattamento solo se compatibile con le sue funzioni e il suo ruolo.
5. Nell'eseguire i propri compiti, il DPO considera debitamente i rischi inerenti al Trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
6. Al DPO sono garantiti supporto, risorse e tempi di lavoro adeguati allo svolgimento della relativa funzione. È garantita, inoltre, nel caso in cui si tratti di un soggetto interno, una formazione permanente per permettergli l'aggiornamento costante sugli sviluppi nel settore della protezione dei Dati Personali.
7. Il DPO ha ampio accesso alle informazioni ed è interpellato per ogni problematica inerente la protezione dei Dati Personali nonché consultato per ogni nuovo Trattamento che si intende avviare, 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 a lui 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 del DPO sono inseriti nelle informative e pubblicati sul sito internet istituzionale.

Articolo 18 - 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 a lui 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 19 - 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 20 - 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 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 21 - 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 22 - Informativa

1. Nel rispetto del principio di trasparenza, per ogni tipologia di Trattamento di Dati Personali l'Ateneo fornisce agli Interessati un'apposita informativa.
2. L'informativa deve essere concisa, trasparente, intellegibile, facilmente accessibile e redatta con un linguaggio chiaro e semplice. Le informazioni sono fornite per iscritto o con altri mezzi, anche elettronici. L'Interessato potrà chiedere che le informazioni siano fornite oralmente, purché sia comprovata l'identità dell'Interessato.

3. Se i dati vengono raccolti presso l'Interessato, ciascuna Struttura fornisce l'informativa agli Interessati al momento della raccolta dei dati. È necessario rendere agli Interessati una nuova informativa quando il Titolare del Trattamento intenda trattare i dati già acquisiti per una finalità diversa da quella per cui sono stati raccolti ovvero vengano modificati elementi fondamentali del Trattamento originario rappresentato agli Interessati.
4. Se i Dati Personali 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 comunicazione prima ad altro destinatario ovvero, 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 (la documentazione che illustra i motivi per cui si è ritenuto che lo sforzo fosse sproporzionato deve essere conservata dalla Struttura e, su richiesta, messa a disposizione del Garante per la Protezione dei Dati Personali); (iii) l'ottenimento dei dati o la comunicazione degli stessi sono previsti espressamente dal diritto europeo o nazionale; (iv) qualora 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:
    - l'identità e i dati di contatto del Titolare del Trattamento;
    - i dati di contatto del Responsabile della Protezione dei Dati;
    - le finalità e la base giuridica del Trattamento;
    - 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;
    - gli eventuali destinatari o le eventuali categorie di destinatari dei Dati Personali;
    - 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 all'art. 46 o 47, o all'art. 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;
    - il periodo di conservazione dei Dati Personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
    - 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, 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), oppure sull'art. 9, c. 2, lett. a), il diritto di revocare il Consenso in qualsiasi momento senza pregiudicare la liceità del Trattamento basata sul Consenso prestato prima della revoca (nei casi in cui i dati siano stati direttamente conferiti dall'Interessato nel momento in cui i Dati Personali sono ottenuti); qualora il Trattamento sia basato sull'art. 6, c. 1, lett. e), deve essere esplicitamente portato all'attenzione dell'Interessato e presentato chiaramente e separatamente da qualsiasi altra informazione il diritto di opporsi in qualsiasi momento al Trattamento dei Dati Personali che lo riguardano effettuato per tali finalità;
    - 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 (nei casi in cui i dati siano stati direttamente conferiti dall'Interessato nel momento in cui i Dati Personali sono ottenuti);
    - l'esistenza di un processo decisionale automatizzato, compresa la Profilazione, e la logica utilizzata, nonché l'importanza e le conseguenze previste da tale Trattamento per l'Interessato (nei casi in cui i dati siano stati direttamente conferiti dall'Interessato, nel momento in cui i Dati Personali sono ottenuti).

6. Le informative di competenza delle Strutture sono predisposte e aggiornate dai Referenti Interni, eventualmente con il supporto del DPO.
7. Gli Autorizzati al Trattamento possono trattare i Dati Personali solo per le specifiche finalità indicate nell'informativa fornita all'Interessato.

Articolo 23 - Registro delle attività di Trattamento

1. L'Ateneo, quale Titolare del Trattamento, istituisce e aggiorna il Registro delle attività di Trattamento, che descrive le attività di Trattamento svolte presso l'Ateneo e ne delinea le principali caratteristiche. Il Registro può essere tenuto sia in formato elettronico che cartaceo.
2. Il Registro delle attività di Trattamento, redatto dall'Ateneo quale Titolare del Trattamento, deve contenere le seguenti informazioni:
    - dati identificativi e di contatto dell'Ateneo, degli eventuali Contitolari e del DPO e dei Referenti di Struttura e/o dei Referenti Interni;
    - le finalità del Trattamento;
    - la descrizione delle categorie degli Interessati e delle categorie di Dati Personali;
    - le categorie di destinatari, a cui i Dati Personali sono stati o saranno comunicati, compresi destinatari di paesi terzi od organizzazioni internazionali;
    - 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;
    - ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
    - 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, 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, deve contenere le seguenti informazioni:
    - 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;
    - le categorie di Trattamenti effettuati per conto di ogni Titolare del Trattamento;
    - 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;
    - 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 redige i predetti Registri delle attività di Trattamento, in collaborazione con il DPO, e ne cura periodicamente l'aggiornamento. I Registri delle attività di Trattamento devono essere tenuti a disposizione del Garante per la Protezione dei Dati Personali.

Articolo 24 - 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 casi seguenti:
    - 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;
    - 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;
- 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 il 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

Articolo 25 - Diritti dell'Interessato

1. L'Ateneo garantisce il rispetto dei diritti degli Interessati disciplinati dagli artt. 12-22 del GDPR, ove applicabili, e, in particolare, di:
   - essere informati circa le attività di Trattamento svolte sui propri Dati Personali tramite l'informativa ("diritto a essere informato") (vedasi art. 22 del presente Regolamento);
   - avere conferma dal Titolare del Trattamento che sia o meno in corso un'attività di Trattamento sui propri Dati Personali e ottenere l'accesso a tali dati ("diritto di accesso ai dati personali");
   - ottenere la rettifica dei dati inesatti e l'integrazione dei dati incompleti ("diritto alla rettifica");
   - ottenere la cancellazione dei propri Dati Personali ("diritto all'oblio");
   - ottenere la limitazione al trattamento dei propri dati ("diritto alla limitazione");
   - ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i relativi Dati Personali forniti a un Titolare del Trattamento e trasmettere tali dati a un altro Titolare del Trattamento senza impedimenti da parte del Titolare del Trattamento cui li ha forniti ("diritto alla portabilità");
   - opporsi in qualsiasi momento, per motivi connessi alla propria situazione particolare, al Trattamento dei propri Dati Personali ai sensi dell'art. 6, c. 1, lett. e) o f), del GDPR, compresa la Profilazione ("diritto all'opposizione");
   - non essere sottoposto a una decisione basata unicamente sul Trattamento automatizzato, compresa la Profilazione, che produca effetti giuridici nei confronti dell'interessato stesso o che incida in modo analogo significativamente sulla propria persona, fatti salvi i casi in cui ciò è previsto dalla legge ("diritto a non essere sottoposti a trattamento automatizzato").
2. L'Interessato presenta istanza di esercizio dei diritti al DPO di Ateneo, senza alcuna formalità, previa dimostrazione della propria identità.
3. L'Ateneo risponde tempestivamente alle richieste di esercizio dei diritti e, comunque, entro un mese dal ricevimento dell'istanza. Tale termine può essere prorogato di ulteriori due mesi (per un totale di tre mesi), tenuto conto della complessità e del numero delle richieste. In ogni caso, l'Ateneo dovrà comunicare tale proroga all'Interessato entro un mese dal ricevimento dell'istanza, indicando i motivi del ritardo.
4. L'Ateneo può negare la risposta a una richiesta di esercizio dei diritti solo nel caso in cui quest'ultima risulti manifestamente infondata o eccessiva, in particolare per il suo carattere ripetitivo; sarà onere dell'Ateneo dimostrare il carattere manifestamente infondato o eccessivo della richiesta e comunicare i motivi del diniego all'Interessato.

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

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

Articolo 26 - Circolazione dei Dati Personali all'interno dell'Ateneo

1. L'accesso ai Dati Personali da parte delle Strutture e del personale dell'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 27 - Comunicazione dei Dati Personali al di fuori dell'Ateneo

1. La comunicazione dei Dati Personali al di fuori dell'Ateneo può avvenire solo ove sussista una specifica base giuridica (vedasi artt. 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'accoglibilità della richiesta sarà valutata dalla Struttura in collaborazione con il DPO.

Articolo 28 - Diffusione dei Dati Personali

1. La diffusione dei Dati Personali può avvenire solo ove prevista da una norma di legge applicabile alla fattispecie concreta.
2. L'Ateneo può diffondere, anche sui propri siti web, i Dati Personali del personale PTA, CEL e docente, nonché di collaboratori, assegnisti, dottorandi, laureati, stagisti e studenti, in ottemperanza a obblighi di legge (ad esempio, per finalità di trasparenza). Nei casi di procedure di valutazione e selezione, l'Ateneo procede alla pubblicazione di documenti e graduatorie, anche sui propri siti web, nel rispetto delle prescrizioni normative in materia.

Articolo 29 - 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:
    - 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;
    - uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche od organismi pubblici;
    - le norme vincolanti di impresa;
    - 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;
    - 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;
    - 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:
    - 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;

- 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;
- 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;
- il trasferimento è necessario per importanti motivi di interesse pubblico;
- il trasferimento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- 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;
- 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'idonea misura per garantire la tutela dei Dati Personali.

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

Articolo 30 - 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 dall'Area Sistemi Informatici e Telecomunicazioni (ASIT), nonché di quelle individuate dalla Struttura stessa, in collaborazione con il Titolare del Trattamento e con il supporto del DPO.

Articolo 31 - 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 Manuale di Conservazione dell'Ateneo.

Articolo 32 - 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 nella "*Policy per la gestione dei data breach*" di Ateneo pubblicata sul sito web di Ateneo alla pagina https://www.unive.it/pag/35006/.

TITOLO IV - CONTROLLI, SANZIONI E DISPOSIZIONI FINALI

Articolo 33 - 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 34 - 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 35 - 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, previo accordo con i Sindacati per quanto attiene alla tematica della videosorveglianza.
2. Il presente Regolamento potrà essere aggiornato a seguito di:
    - modifiche normative sopravvenute;
    - introduzione di nuove pratiche volte a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
    - inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti.
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. L'installazione di impianti di videosorveglianza è finalizzata a:
    - garantire un adeguato grado di sicurezza alla popolazione universitaria (dipendenti, studenti, ecc...);
    - prevenire eventuali atti delittuosi e vandalici presso le sedi dell'Ateneo nonché garantire l'esercizio del diritto di difesa;
    - tutelare gli immobili di proprietà o in gestione dell'amministrazione universitaria;
    - tutelare il patrimonio dei beni mobili presenti nelle sedi universitarie.
4. Non è possibile installare sistemi di videosorveglianza per finalità ulteriori rispetto a quelle indicate, ovvero utilizzare i dati raccolti per finalità ulteriori.

Articolo 2 - Titolare del Trattamento

1. Il Titolare del Trattamento dei Dati Personali raccolti tramite strumenti di videosorveglianza all'interno degli ambienti dell'Ateneo è l'Università Ca' Foscari Venezia nella persona del Magnifico Rettore.
2. L'Area Servizi Informatici e Telecomunicazioni (ASIT) garantisce l'osservanza delle norme di legge in materia e di quanto stabilito nel presente Allegato.
3. ASIT conserva la documentazione che dimostri le ragioni dell'installazione di tali sistemi e la conformità agli adempimenti del GDPR, del Codice Privacy, delle Linee Guida n. 3/2019 del Comitato europeo per la protezione dei dati e del Provvedimento in materia di videosorveglianza del Garante per la Protezione dei Dati Personali dell'8 aprile 2010, 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. Le attività di videosorveglianza possono essere affidate 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 per fornire assistenza alle Autorità; 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 la difesa in giudizio a seguito di commissione di reato.

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, gli Autorizzati

alla gestione delle predette immagini e dei predetti impianti verranno nominati con apposito atto sottoscritto dal Magnifico Rettore.

Articolo 6 - Informativa

1. Ciascuna Struttura si assicura che gli Interessati, ovvero coloro le cui immagini vengano registrate dagli strumenti di videosorveglianza, siano sempre informati prima di accedere a un'area videosorvegliata.
2. L'informativa può essere 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) devono essere collocati prima del raggio di azione della telecamera, anche nelle immediate vicinanze e non necessariamente a contatto con le stesse; (ii) devono avere 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) possono inglobare 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, unitamente alle planimetrie riportanti la collocazione delle telecamere, è reperibile nella portineria della sede interessata e 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 (D.Lgs. n. 196/2003); il trattamento delle immagini rilevate dagli impianti di videosorveglianza, inoltre, avviene nel rispetto di quanto prescritto dal Provvedimento generale del Garante dell'8 aprile 2010.

Articolo 8 - Diritti dell'Interessato

1. L'Interessato può esercitare i diritti di cui al TITOLO II, CAPO III, art. 25, del Regolamento di Ateneo con riguardo alle immagini riprese dagli impianti di sorveglianza.

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 autorizzata dal Direttore Generale di Ateneo su istanza del Dirigente di ASIT.
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 ACCESSO ALLA RETE 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, regolamenta 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. L'accesso alla rete dati di Ateneo è gestito dall'Area Servizi Informatici e Telecomunicazioni (ASIT) ed è riservato agli studenti e al personale docente, tecnico-amministrativo e bibliotecario che opera all'interno delle strutture appartenenti all'Ateneo stesso, oltre che a utenti temporanei esterni espressamente autorizzati.
2. L'accesso ai servizi avviene mediante un codice di identificazione attribuito all'utente (*username*) e una parola chiave (*password*).
3. L'utente deve modificare la propria *password* al primo utilizzo e, successivamente, almeno ogni 180 giorni o immediatamente nei casi in cui sia compromessa, scegliendone una che osservi le seguenti regole:
    i) la *password* deve essere composta da almeno 10 caratteri alfanumerici;
    ii) 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;
    iii) 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;
    iv) 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, la stessa verrà disattivata e l'*account* sarà bloccato fino alla riattivazione, che può avvenire tramite una procedura basata su una *One Time Password* inviata tramite SMS, tramite l'account SPID dell'utente (collegandosi al sito web www.unive.it/newpass) oppure contattando il servizio di Help Desk di ASIT, che provvederà a fornire un nuovo PIN previo riconoscimento dell'utente; a tal proposito si raccomanda agli utenti di inserire il proprio numero di cellulare nella procedura di rinnovo *password* o di dotarsi di un account SPID.
5. Gli *account* bloccati per scadenza *password* e non più riattivati dopo 12 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 al gestore 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:
    i) 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...);
    ii) non deve permettere ad altri (es. colleghi, familiari, ecc...) di operare con il proprio identificativo utente;
    iii) si impegna a modificare immediatamente la *password* ogni qualvolta ritenga che sussista il rischio che questa sia facilmente conoscibile o sia stata effettivamente conosciuta da terzi ovvero su richiesta esplicita di ASIT ove vengano rilevate compromissioni delle *password*; ove l'utente rilevi problematiche relative alla propria *password* (compromissione ovvero debolezza della stessa) dovrà immediatamente informare ASIT utilizzando il sistema di richiesta di supporto del supporto utenti.
8. Gli *account* di accesso ai servizi informatici dell'Ateneo si suddividono in cinque gruppi:
    i) *account* per il personale dipendente;
    ii) *account* per gli studenti;
    iii) *account* per gli ospiti;
    iv) *account* per gli amministratori di sistema;
    v) *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.
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.
11. Oltre all'*account* principale, è possibile vengano attribuiti all'utente *account* aggiuntivi abilitati esclusivamente alla posta elettronica o per la gestione di siti web, da utilizzare come *account* di ufficio o per servizi particolari. L'utente a cui è stato attribuito un *account* di questo tipo ne è responsabile in maniera del tutto analoga rispetto all'*account* personale.

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. IDEM è la prima Federazione italiana di infrastrutture di Autenticazione e Autorizzazione (Federazione IDEM) con lo scopo di consentire agli utenti della comunità scientifica e accademica nazionale di accedere più facilmente a servizi e contenuti in rete messi a disposizione da organizzazioni diverse.
3. L'adesione a IDEM offre agli utenti il vantaggio di utilizzare le sole credenziali istituzionali per accedere a tutte le risorse disponibili attraverso la Federazione IDEM.
4. 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.
5. Da ottobre 2011, IDEM ha a sua volta aderito 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 e l'indirizzo di posta elettronica hanno la seguente struttura in base alla tipologia di utenti:

Personale e collaboratori
Username: nome.cognome
e-mail: nome.cognome@unive.it
Studenti
Username: matricola
email: matricola@stud.unive.it

2. Per il solo accesso alla rete Internet attraverso la rete *wireless* di Ateneo agli ospiti possono essere assegnati degli *account*:
   Ospiti personali
   Username: wifi00000
   (e-mail non prevista)
   Ospiti wifi
   Username: guest00000
   (e-mail non prevista)
   Ospiti biblioteche
   Username: ucf.000000
   (e-mail non prevista)
3. Nel caso in cui l'utente abbia più nomi e/o cognomi, generalmente vengono uniti senza spazi (es: nome1 nome2 cognome1 cognome2 diventa nome1nome2.cognome1cognome2).
4. 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.
5. 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. - Studenti

1. Il numero di matricola e la *password* vengono spediti agli studenti al momento del perfezionamento dell'immatricolazione via e-mail all'indirizzo fornito all'atto dell'immatricolazione stessa. L'*account* da studenti rimane attivo fino ai 6 mesi successivi al termine della carriera. Una volta terminata la carriera, *username* e *password* rimangono invariate, ma i diritti di accesso diventano quelli da ex-studente e l'*account* rimarrà attivo a meno che l'utente non ne richieda la disattivazione.
2. Lo *username* corrisponde al numero di matricola. Nel caso lo studente abbia avuto nel corso delle sue carriere più numeri di matricola, l'*username* di riferimento è sempre l'ultimo rilasciato.

Articolo 4.1.b. - Personale dipendente e collaboratori

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.
3. Ogni *account* viene autorizzato da un responsabile individuato in base al ruolo e alla struttura di afferenza secondo la tabella visibile 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:
   i) implicita (utente già inserito in un applicativo gestionale); in tal caso l'*account* verrà rilasciato immediatamente;
   ii) 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.

Articolo 4.1.c. - Ospiti

1. Gli utenti con ruolo di ospite e tutti gli altri ruoli non elencati nell'art. 2, c. 8, del presente Allegato non possono utilizzare la procedura di richiesta *account* in quanto generalmente non ne hanno diritto. L'*account* ospite può essere ottenuto in casi particolari (conferenze, biblioteche, ecc…) seguendo le indicazioni fornite di volta in volta.
2. Nel caso di necessità particolare e documentata di ottenere un *account* al di fuori dei ruoli stabiliti, è necessario contattare direttamente ASIT che, di concerto con la Direzione Generale o il Rettorato, valuterà la possibilità di concedere l'*account*.

Articolo 4.1.d. - 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 4.2 - Scadenza e dismissione dell'account

1. Una volta scaduto l'*account*, i dati correlati verranno conservati per 1 anno 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 4.3 - 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	Wifi/VPN	Accesso biblioteche	PC lezione frontale	Durata
Titolari di borsa di ricerca	✓	✓	✓	✓	✓	1 anno
Professori affiliati	✓	✓	✓	✓	✓	1 anno
Visiting professors	✓	✓	✓	✓		1 anno
Teaching Assistant	✓	✓	✓	✓	✓	1 anno
Ricercatori a tempo det-Tesoro	✓	✓	✓	✓		rapporto + 1 anno
Ricercatori a tempo det-Legge 240/10	✓	✓	✓	✓	✓	rapporto + 1 anno
Personale Tec. Amm.vo a Comando	✓	✓	✓	✓		rapporto + 1 anno
Collaboratori Fondazione	✓	✓	✓			1 anno
Professori straordinari a tempo determinato	✓	✓	✓	✓	✓	rapporto + 1 anno
Docenti Emeriti	✓	✓	✓	✓	✓	1 anno
Docenti Onorari	✓	✓	✓	✓	✓	1 anno
Senior Researchers	✓	✓	✓	✓	✓	1 anno
Componenti Organi Collegiali	✓	✓	✓	✓		1 anno

Ruolo	Area riservata	Email	Wifi/VPN	Accesso bibliotec he	PC lezione frontale	Durata
Volontari servizio civile	✓	✓	✓	✓		1 anno
Dottorandi	✓	✓	✓	✓		rapporto + 1 anno
Ricercatori Universitari	✓	✓	✓	✓	✓	rapporto + 1 anno
Assistenti universitari	✓	✓	✓	✓	✓	rapporto + 1 anno
Collaboratori esterni	✓	✓	✓			rapporto + 1 anno
Dirigenti a contratto	✓	✓	✓	✓		rapporto + 1 anno
Lettori di scambio	✓	✓	✓			1 anno
Dipendenti in Comando	✓	✓	✓	✓		1 anno
Personale Tec. Amm.vo a tempo indet.	✓	✓	✓	✓		rapporto + 1 anno
Personale Tec. Amm.vo a tempo det.	✓	✓	✓	✓		rapporto + 1 anno
Professori Associati	✓	✓	✓	✓	✓	rapporto + 1 anno
Personale esterno			✓			1 anno
Professori Ordinari	✓	✓	✓	✓	✓	rapporto + 1 anno
Lettori di madre lingua	✓	✓	✓	✓	✓	rapporto + 1 anno
Dirigenti	✓	✓	✓	✓		rapporto + 1 anno
Prestatori d'opera, partite IVA, collaboratori autonomi	✓					1 anno
Professori a contratto	✓	✓	✓	✓	✓	rapporto + 1 anno
Supplente esterno-docente di altra Università	✓	✓	✓	✓	✓	rapporto + 1 anno
Collaboratore IDPA-CNR	✓	✓	✓			1 anno
Docenti SIE	✓	✓	✓	✓		1 anno
Collaboratori didattici CLA	✓	✓	✓			
Collaboratori CISET	✓	✓	✓			
Ambasciatori Scuole Superiori			✓	✓		

Ruolo	Area riservata	Email	Wifi/VPN	Accesso biblioteche	PC lezione frontale	Durata
Ospiti			✓			1 anno
Assegnisti	✓	✓	✓	✓		rapporto + 1 anno
Personale in quiescenza		✓	✓	✓		a vita
Cultori della materia	✓	✓	✓	✓		1 anno
Stagisti	✓	✓	✓			1 anno
Tutor Specialistici	✓		✓	✓	✓	1 anno
Tutor informativi	✓		✓	✓	✓	1 anno
Visiting researcher			✓	✓		1 anno
Collaboratori progetti di ricerca	✓	✓	✓	✓		1 anno
Dipendenti cooperative	✓		✓			1 anno
Studenti	✓	✓	✓	✓		rapporto + 6 mesi
Ex studenti	✓					a vita

Articolo 4.4. - Revoca delle credenziali di autenticazione

1. In caso di interruzione del rapporto di lavoro o collaborazione degli utenti prima della normale scadenza contrattuale o del pensionamento, l'Area Risorse Umane (ARU) ovvero la segreteria del Dipartimento che gestisce il contratto dovrà immediatamente richiedere all'Ufficio Supporto e Sviluppo Tecnologico di ASIT, aprendo un *ticket* all'indirizzo www.unive.it/aiuto alla voce "Autenticazione e *password*", di interrompere i relativi *account* di accesso. Gli *account* saranno disattivati tempestivamente.
2. In ogni caso, gli *account* degli utenti saranno sospesi o bloccati:
   iii) trascorsi sei mesi dall'ultimo *login* dell'utente (tranne che per gli *account* utilizzati per la manutenzione);
   iv) nel caso in cui vengano rilevate dai sistemi dell'Ateneo o siano segnalate attività dannose per l'Ateneo o che violino qualsiasi regolamento dell'Ateneo o norma della legislazione italiana;
   v) nel caso del decesso dell'utente.
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, gli amministratori di sistema, oltre alla sospensione delle credenziali, procederanno alla segnalazione alla segreteria studenti o ad ARU per le verifiche e le eventuali azioni disciplinari.

Articolo 5 - *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. Qualora un dipendente a cui sia stata assegnata una *password* per *account* di amministrazione di sistema termini il rapporto con l'Ateneo o sia assegnato ad altri ruoli, tutte le *password* per *account* di sistema a lui note devono essere cambiate.

3. Gli *account* 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 tramite tali *account* sarà possibile solo tramite *console* locale della macchina.
4. Le *password* degli *account* utilizzate dagli amministratori di sistema per le loro attività lavorative devono essere cambiate ogni 90 giorni.
5. Nel caso si sospetti un accesso non autorizzato a qualunque *account* di sistema, amministrativo o dell'utente, tutte le *password* potenzialmente compromesse dovranno essere immediatamente modificate.

Articolo 6 - 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 strettamente necessario, ad esempio, a causa della riconfigurazione del servizio. 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. Ove possibile, per gli *account* di servizio e/o di amministrazione, viene permessa l'autenticazione attraverso chiave pubblica. 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.

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 per controllare l'appropriatezza del privilegio.

ALLEGATO C

REGOLE PER IL CORRETTO USO DELLE INFRASTRUTTURE E DELLE RISORSE INFORMATICHE

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

1. Con esclusione delle attività collegate ai progetti di ricerca, le strutture di Ateneo utilizzano i servizi messi a disposizione dall'Area Servizi Informatici e Telecomunicazioni (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 a:
    i) programmare l'implementazione dei nuovi servizi richiesti, laddove si rilevi un interesse concreto e diffuso;
    ii) estendere le funzionalità di servizi già esistenti;
    iii) consigliare alla Struttura l'utilizzo di servizi già implementati o in fase di implementazione anche in altre Strutture;
    iv) 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;
    v) vietare l'installazione del sistema/l'erogazione del servizio per documentati motivi di sicurezza od opportunità e proponendo (ove possibile) delle soluzioni alternative.
3. Nel caso in cui ASIT declini la richiesta di attivazione ma non ne vieti esplicitamente l'installazione/ l'erogazione, la singola Struttura può erogare servizi informatici nel rispetto della normativa vigente, anche in termini di sicurezza dei sistemi informatici, delle Linee Guida di AGID e del CSIRT, in osservanza del presente Regolamento.
4. Ogni Struttura è tenuta a dare notifica ad ASIT dell'elenco dei propri servizi 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 applicando tempestivamente le *patch* di sicurezza; deve inoltre essere garantito un adeguato livello di sicurezza. Verranno effettuati controlli periodici per verificare l'aggiornamento e il grado di sicurezza dei sistemi in rete, avvisando tempestivamente i responsabili di eventuali problemi rilevati. I responsabili di *host* e di servizi sono tenuti a intervenire tempestivamente 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 o 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. Qualunque *file* che non sia legato all'attività lavorativa non può essere memorizzato, nemmeno per brevi periodi, in tali unità. 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, 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 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 Regolamento di Ateneo. 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 referente informatico della struttura, così come non è consentito riprodurre, tradurre, adattare, trasformare e distribuire *software* in licenza d'uso all'Ateneo.
2. 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*, *serial codes*, ecc...). In generale, gli utenti non devono sviluppare o usare programmi o utilità che interferiscano con l'attività di altri utenti o che modifichino parti dei sistemi informatici esistenti o che accedano a informazioni private o riservate. Gli illeciti che possono essere commessi tramite il *computer* o i sistemi informativi (*computer crimes*) sono regolati dal codice penale e dal codice di procedura penale in tema di criminalità informatica.
3. 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.
4. Su ogni *personal computer* deve essere installato il *software antivirus* standard individuato dall'Ateneo, correttamente configurato e aggiornato; è vietato disabilitare o inibire il corretto funzionamento del *software antivirus*.
5. 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 (Ctrl+Alt+Canc); al termine dell'attività lavorativa le sessioni di lavoro devono essere chiuse (*log-off*).
6. I supporti di memoria rimovibili (es. chiavette USB, compact disk, ecc...) devono essere conservati in luoghi protetti (es. armadi e cassettiere chiusi a chiave).
7. 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. Si ricorda che anche un *computer* portatile è considerato un supporto di memoria rimovibile.
8. 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).
9. 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.
10. I supporti di memorizzazione non rimovibili (es. *hard disk*) utilizzati all'interno dei sistemi *server* vengono fisicamente distrutti al momento della dismissione.
11. 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.

12. Nell'eventualità in cui si rilevi l'esistenza di programmi che violino il diritto d'autore, ASIT o l'Amministratore di Sistema della struttura, previa autorizzazione del proprio responsabile, può provvedere a:

i) inviare avvisi collettivi, all'interno della struttura di riferimento, mediante i quali l'utenza sarà richiamata all'osservanza di corrette norme di comportamento;
ii) rimuovere il *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;
iii) 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.

13. Nel caso in cui, per motivi di sicurezza o affidabilità del sistema, si renda opportuno sostituire la postazione di lavoro di un utente, il referente informatico di struttura 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 o non collegati alle attività lavorative, di studio o di ricerca.
3. L'uso personale è vietato se esso:
    i) interferisce con la produttività o con la prestazione professionale dell'utente o di qualsiasi altro dipendente;
    ii) incide negativamente sul buon funzionamento del *computer*;
    iii) viola le norme oggetto del presente Regolamento.
4. Nell'uso dei servizi Internet gli utenti devono osservare le seguenti regole:
    i) 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;
    ii) 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;
    iii) è vietato accedere, scaricare, stampare o salvare informazioni dall'esplicito contenuto sessuale, pedopornografico o che inciti alla violenza e all'odio razziale;
    iv) è vietato scaricare o trasmettere immagini o messaggi fraudolenti, minacciosi, osceni, intimidatori, diffamatori, molesti, discriminatori o altrimenti illegali;
    v) le risorse informatiche dell'Ateneo non devono essere utilizzate per finalità connesse all'attività di propaganda di partiti od organizzazioni religiose;
    vi) 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:

- non devono inserire, modificare o rimuovere apparati di rete senza preventiva autorizzazione degli amministratori di rete;
- 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;

vii) 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 se, sulla base di comprovati motivi, se ne evidenzia 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

LINEE GUIDA PER L'UTILIZZO DELLA POSTA ELETTRONICA

Articolo 1 - Principi generali

1. L'Ateneo, tramite l'Area Servizi Informatici e Telecomunicazioni (ASIT), rende disponibile agli studenti, al personale docente, 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 sottodomini.
2. Le comunicazioni ufficiali e istituzionali da parte dell'Ateneo sono inviate esclusivamente all'indirizzo di posta istituzionale di cui al paragrafo precedente.
3. L'Ateneo ha facoltà di fornire ai propri utenti altri servizi di posta elettronica a supporto dell'attività di collaborazione con l'Ateneo.
4. Tutti gli utenti abilitati possono accedere al servizio di posta elettronica utilizzando le proprie credenziali istituzionali.
5. Nel caso di assenza programmata, il personale e i collaboratori sono invitati ad attivare sistemi di risposta automatica ai messaggi di posta elettronica ricevuti nei quali indicare eventuali indirizzi istituzionali alternativi a cui fare riferimento per l'invio di comunicazioni.
6. Al fine di agevolare la comunicazione istituzionale e favorire la circolazione delle informazioni, sono altresì forniti indirizzi per unità/strutture organizzative o indirizzi legati alla carica, il cui accesso è consentito a uno o più lavoratori. A titolo esemplificativo, l'*account* di posta elettronica può essere fornito a:
    i) cariche (es. rettore@unive.it);
    ii) organi (es. presidio.qualita@unive.it);
    iii) soggetti/strutture/unità organizzative dell'Ateneo che nell'ambito di progetti, ricerche o altre forme di attività di collaborazione necessitino di tale strumento di lavoro.

Articolo 2 - Gestione tecnica del servizio

1. ASIT implementa misure di protezione automatizzate *antivirus* e *antispam* per il servizio di posta istituzionale, decidendo 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.

Articolo 4 - Uso del sistema di posta elettronica

1. Il sistema di posta elettronica deve essere utilizzato dai dipendenti/collaboratori esclusivamente per lo svolgimento dell'attività lavorativa. È tollerato, secondo quanto di seguito indicato, un limitato utilizzo da parte di tali soggetti a fini privati, che non dovrà però in alcun modo interferire con il normale svolgimento dell'attività lavorativa o con gli scopi cui gli stessi sono destinati. I dipendenti/collaboratori che dovessero utilizzare il sistema di posta elettronica a fini privati accettano, quindi, il rischio che l'Ateneo possa, anche involontariamente o nello svolgimento degli eventuali controlli di cui all'Allegato E, prendere 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 relativo contenuto.
2. Nell'uso del servizio di posta elettronica, gli utenti devono osservare le seguenti norme comportamentali:

i) è vietato l'utilizzo dell'e-mail istituzionale per veicolare messaggi il cui contenuto sia lesivo dell'immagine dell'Ateneo;
ii) l'accesso alle caselle nome.cognome@unive.it o matricola@stud.unive.it è strettamente personale. Ciascun utente accede alla propria casella elettronica previa autenticazione tramite nome utente e *password* di identificazione. È fatto assoluto divieto di rivelare a terzi le proprie credenziali (codice identificativo e *password*). L'utente che violi tali disposizioni ne risponde anche in via disciplinare. L'utente riceve inizialmente un PIN che gli permetterà di selezionare una *password* personale, secondo quanto previsto dall'art. 2 dell'Allegato B;
iii) l'*account* personale non può essere condiviso o ceduto ad altri; è illecito scambiare messaggi sotto mentite spoglie, ossia impersonando un mittente diverso da quello reale; è altresì vietato mandare messaggi in forma anonima;
iv) 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 altrimenti illegali;
v) è assolutamente vietato servirsi o dar modo di servirsi della rete istituzionale e dei relativi servizi per usi illeciti che violino o trasgrediscano diritti di autore di proprietà intellettuale e/o industriale o, in generale, altri diritti tutelati dalla normativa vigente;
vi) 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, anche noti come *usenet spam*, o c.d. "Catene di Sant'Antonio");
vii) l'utente è tenuto a esercitare cautela nell'aprire gli allegati ricevuti, dato che rappresentano un mezzo molto diffuso per la trasmissione di virus informatici; la posta elettronica in transito sul sistema istituzionale viene controllata da un sistema *antivirus* che blocca i messaggi contenenti allegati potenzialmente pericolosi (es. con estensioni .exe, .com, .vbs, .sys, .bin, ecc...), ma non può garantire una copertura completa delle minacce; nel caso di dubbi sulla provenienza dell'allegato, l'utente è tenuto a non aprirlo e a contattare il mittente per una verifica;
viii) 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 e prima di cancellare il messaggio;
ix) 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;
x) 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 rimetterlo 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.

xi) per garantire la riservatezza delle informazioni, l'utente è tenuto a evitare la copia e/o il salvataggio dei documenti allegati ai messaggi di posta elettronica (o gli stessi messaggi di posta elettronica) sui dispositivi in dotazione diretta (disco fisso del computer, chiavette o dischi usb personali o di lavoro); al fine, infatti, 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*; per garantire la riservatezza delle informazioni l'utente è tenuto a conservare gli allegati sui dispositivi in dotazione diretta per il minor tempo possibile e solo per quello necessario alla loro corretta gestione; l'archiviazione va gestita utilizzando il sistema di posta stesso o le cartelle disponibili sui *server* di Ateneo/*Google Drive*, in quanto risorse sottoposte a regolari *backup*;

xii) in caso di comunicazione a indirizzi plurimi, sarà necessario verificare che tutti i destinatari siano autorizzati alla ricezione delle informazioni e dei documenti; inoltre, sarà opportuno valutare l'opportunità di inserire gli indirizzi dei destinatari nel campo ccn, al fine di garantirne la riservatezza.

ALLEGATO E

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

Articolo 1 - Principi generali

1. Come previsto dall'art. 33 del Regolamento di Ateneo, 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. 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 i *log* agli amministratori dell'Ateneo per 30 giorni; in particolare, Google attualmente raccoglie e trasmette all'Ateneo le seguenti informazioni: oggetto, mittente, destinatario, data, ID messaggio, dimensione messaggio, presenza di allegati, IP server di destinazione, destinatari. Informazioni aggiornate sui dati trattati possono essere richieste in qualunque momento all'Area Servizi Informatici e Telecomunicazioni (ASIT) attraverso l'apertura di un *ticket* di supporto.

Articolo 2.2. - Controlli periodici

1. Il presente articolo si applica agli studenti, al personale docente, al personale tecnico-amministrativo, ai collaboratori ed esperti linguistici dell'Università e ad altri soggetti autorizzati con un indirizzo di posta elettronica istituzionale.
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, per esigenze di manutenzione e/o sicurezza dei sistemi nonché al fine di prevenire la commissione di atti che possono costituire fattispecie di reato e comunque atti illeciti. I controlli verranno effettuati da ASIT. Gli utenti sono informati che gli accertamenti avranno natura periodica e, inizialmente, non potranno essere mirati sul singolo utente. L'Ateneo potrà effettuare, senza alcun preavviso, periodiche analisi aggregate (e quindi anonime) del traffico di posta relativamente alla tipologia e dimensione degli allegati inviati (per esempio analizzando i dati aggregati prodotti dai *software* di *filtering*), presenza di *file* con estensione che faccia presumere l'estraneità degli stessi all'attività lavorativa. 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, 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 2.3. - Controlli straordinari

1. Laddove vi sia il sospetto di violazioni di norme di legge ovvero delle disposizioni dell'Allegato D 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 la 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 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 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 tipologie 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.
   i) Fornitura di *hardware*:
      - nome utente;
      - codice inventariale del materiale.
   ii) 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.

   Detti dati vengono mantenuti per 10 mesi.
   iii) 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.

   Detti dati vengono mantenuti per 10 mesi.
   iv) Accesso in modalità virtuale ai PC aziendali:
      - nome utente;
      - data e ora di accesso;
      - data e ora di disconnessione;
      - 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 di accesso vengono mantenuti per 6 mesi, i dati di sessione vengono cancellati al termine della sessione stessa.
   v) Accesso ai PC istituzionali fisici:
      - nome utente;
      - data e ora di accesso;
      - data e ora di disconnessione;
      - per la durata della sessione sul PC vengono registrati dal sistema i dati di utilizzo secondo le impostazioni standard del sistema operativo utilizzato.

Detti dati vengono mantenuti sulla macchina stessa.

vi) 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.

Detti dati vengono mantenuti in forma aggregata per 12 mesi. Si sottolinea che non viene raccolto il contenuto dei pacchetti scambiati.

2. Una volta decorso il tempo di conservazione sopra indicato, le informazioni verranno cancellate.
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, all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria, nonché 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 nell'Allegato C, per esigenze di manutenzione e/o sicurezza dei sistemi nonché al fine di prevenire la commissione di atti che possono costituire fattispecie di reato e comunque atti illeciti. I controlli verranno effettuati da ASIT. Gli utenti sono informati che i predetti controlli verranno effettuati con le modalità di seguito descritte: gli accertamenti avranno natura periodica e, inizialmente, 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; potrà inoltre avvalersi di sistemi di individuazione di *file* con estensione che faccia presumere l'estraneità degli stessi all'attività lavorativa. Tali verifiche saranno quindi 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 dell'Allegato C, 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 ovvero delle disposizioni dell'Allegato C 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 la 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

6. 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.