Università per Stranieri di Perugia

REGOLAMENTO IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI E DELL'UTILIZZO DELLE RISORSE INFORMATICHE E DEI SERVIZI DI COMUNICAZIONE DELL'UNIVERSITÀ PER STRANIERI DI PERUGIA

(Emanato con D.R. n. 39 del 07/02/2024)

Università per Stranieri di Perugia

SOMMARIO

SOMMARIO 2

TITOLO I - OGGETTO E AMBITO DI APPLICAZIONE 4

Articolo 1 Oggetto e finalità 4
Articolo 2 Ambito di applicazione 4
Articolo 3 Modello organizzativo privacy 5
Articolo 4 Definizioni 5

TITOLO II - TRATTAMENTO DEI DATI PERSONALI 7

Articolo 5 Titolare del Trattamento 7
Articolo 6 Responsabile protezione dati (DPO o RPD) 8
Articolo 7 Contitolare 8
Articolo 8 Responsabile interno del trattamento 8
Articolo 9 Responsabile esterno del trattamento 8
Articolo 10 Autorizzati al trattamento 9
Articolo 11 Referenti per la protezione dei dati personali 9
Articolo 12 Amministratori di sistema 9
Articolo 13 Area Sistemi Informativi e Supporto Tecnico 10
Articolo 14 Principi applicabili al trattamento dei dati personali 10
Articolo 15 Circolazione di dati personali nell'ambito dell'Università 11
Articolo 16 Comunicazione e diffusione di dati personali 11
Articolo 17 Sicurezza dei dati personali 11
Articolo 18 Violazione dei dati personali (Data Breach) 12

TITOLO III - REGOLE PER L'ACCESSO, L'UTILIZZO E LA SICUREZZA DELLE RISORSE INFORMATICHE E DEI SERVIZI DI COMUNICAZIONE 13

Articolo 19 Gestione e utilizzo risorse informatiche e dei servizi di comunicazione 13
Articolo 20 Misure tecniche e organizzative 13
Articolo 21 Modalità di utilizzo delle risorse telematiche 13
Articolo 22 Fornitori dei Servizi Informatici 14
Articolo 23 Servizi Cloud computing 14
Articolo 24 Utilizzo degli elaboratori personali forniti dall'Ateneo 14
Articolo 25 Utilizzo di dispositivi informatici non forniti dall'Ateneo 15
Articolo 26 Programmi per elaboratore 15
Articolo 27 Modalità di utilizzo delle risorse informatiche 16
Articolo 28 Rete dati di Ateneo 16
Articolo 29 Connessioni alla rete WiFi di Ateneo 17
Articolo 30 Accesso remoto alla Rete dati di Ateneo 18
Articolo 31 Monitoraggio e controlli 18
Articolo 32 Firma digitale 19

TITOLO IV - POSTA ELETTRONICA 19

Articolo 33 Obiettivi e ambito di applicazione 19

Articolo 34 Finalità del servizio di posta elettronica 19
Articolo 35 Proprietà dell'Ateneo 20
Articolo 36 Limitazioni di Responsabilità per l'Ateneo 20
Articolo 37 Restrizioni all'uso del servizio 20
Articolo 38 Assenso e conformità 20
Articolo 39 Limitazioni di accesso senza assenso 21
Articolo 40 Registro elettronico 21
Articolo 41 Soggetti titolari di una casella di posta elettronica 21
Articolo 42 Ambito di utilizzo del servizio di posta elettronica 22
Articolo 43 Ciclo di vita delle caselle di posta elettronica 23
Articolo 44 Chiusura anticipata 23
Articolo 45 Prolungamento 24
Articolo 46 Archiviazione e conservazione 24
Articolo 47 Uso Personale 24
Articolo 48 Caselle di servizio 25
Articolo 49 Proibizioni 25
Articolo 50 Monitoraggio e controlli 25

TITOLO V - IDENTITA' DIGITALI DI ATENEO 26
Articolo 51 Le identità digitali 26
Articolo 52 Titolari delle identità digitali 26
Articolo 53 Credenziali servizi web di Ateneo 26

TITOLO VI - RESPONSABILITÀ E CONTROLLI 27
Articolo 54 Responsabilità individuali 27
Articolo 55 Controllo e accesso ai dati 27
Articolo 56 Controllo e monitoraggio dei log 28

TITOLO VII - SANZIONI E DIRITTO DI DIFESA 28
Articolo 57 Sanzioni e diritto di difesa 28

Università per Stranieri di Perugia

TITOLO I - OGGETTO E AMBITO DI APPLICAZIONE

LE DISPOSIZIONI DEL PRESENTE REGOLAMENTO SI APPLICANO ANCHE AGLI ARCVHIVI IN FORMA ANALOGICA… (v. Regolamento GARANTE)

Articolo 1 Oggetto e finalità

1. L'Università per Stranieri di Perugia (d'ora in poi anche Ateneo o Università) tratta i dati personali in conformità a quanto previsto dal *Regolamento generale sulla protezione dei dati personali* - di seguito Regolamento (UE) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, e della relativa normativa nazionale "*Codice in materia di protezione dei dati personali",* D. Lgs. n. 196 del 30 giugno 2003 e s.m.i.., nonché della normativa vigente in materia e degli atti di soft law applicabili al contesto delle attività di trattamento.
2. Il presente regolamento detta regole interne relative alla definizione dei soggetti e delle modalità organizzate dell'Università finalizzate ad assicurare la conformità del trattamento dei dati personali alla normativa in materia.

3. Le disposizioni del presente regolamento disciplinano l'uso delle risorse informatiche e dei servizi di comunicazione dell'Ateneo, così come definite al successivo articolo 4.

4. Le risorse informatiche e i servizi di comunicazione di Ateneo sono messi a disposizione dei soggetti, così come definiti al successivo articolo 4, allo scopo di perseguire le finalità istituzionali.

Articolo 2 Ambito di applicazione

1. Il presente regolamento si applica a tutti i soggetti a vario titolo coinvolti nelle attività istituzionali dell'Ateneo ed a tutti coloro che ne utilizzano i servizi.

2. Nell'ambito del trattamento dei dati personali nell'esercizio dei suoi compiti istituzionali, l'Ateneo adotta:

    a) Atti organizzativi interni *per il trattamento dei dati sensibili e giudiziari;*

    b) Il *Modello organizzativo privacy dell'Università per Stranieri di Perugia;*

    c) Il *Disciplinare sull'impiego di sistemi di videosorveglianza negli ambienti dell'Università per Stranieri di Perugia.*
3. Il presente regolamento, in conformità con la normativa in materia di protezione dei dati personali, disciplina anche le condizioni per l'accesso, l'utilizzo e la protezione delle risorse informatiche e dei servizi di comunicazione.

4. Per le risorse informatiche e i servizi di comunicazione messi a disposizione o dati in uso all'Ateneo da altri enti od organizzazioni valgono gli accordi e le condizioni contrattuali stipulate fra le parti.

5. Per l'utilizzo, ove previsto, di dati, programmi e materiali valgono le condizioni di copyright.

6. Tutte le utilizzazioni delle risorse informatiche e dei servizi di comunicazione dell'Ateneo devono essere conformi a quanto previsto dalle norme vigenti.

Articolo 3 Modello organizzativo privacy

1. Il Codice in materia di protezione dei dati personali, ex. art 2-quaterdecies del D. Lgs. n. 196/2003 e s.m.i., prevede la possibilità che il Titolare deleghi compiti e funzioni a persone fisiche che collaborano col medesimo.
2. Il Titolare del trattamento, ai fini della gestione dei trattamenti di dati personali, considerate la complessità organizzativa dell'Università per Stranieri di Perugia, le funzioni istituzionali attribuita in ambito di Didattica, Ricerca, Terza Missione e di gestione logistico infrastrutturale, individua il seguente modello organizzativo:

    a) Autorizzati del trattamento
    b) Referenti privacy
    c) Amministratori di Sistema

3. L'Ateneo, con apposito atto adotterà il documento di dettaglio sul il "*Modello organizzativo privacy dell'Università per Stranieri di Perugia".*

4. Il modello di gestione della privacy viene sottoposto a costante monitoraggio al fine di intervenire rapidamente in caso di modifiche normative o a seguito dell'evoluzione tecnologica e per introdurre efficaci politiche di gestione dei dati.

Articolo 4 Definizioni

1. *Autorizzati al trattamento* - persone fisiche autorizzate a compiere operazioni di trattamento dati ai sensi dell'art 29 del GDPR;
2. *Credenziali di accesso* - dati utilizzati nelle operazioni di autenticazione utente (utente e password)*;*
3. *Dato* - tutte le informazioni, indipendentemente dal formato, che sono contenute o elaborate da risorse informatiche dell'Ateneo o che sono contenute o elaborate da risorse informatiche di altri soggetti per conto dell'Ateneo;
4. *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;

5. *Firma digitale* – (cfr. art.24 Codice Amministrazione Digitale) particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;
6. *Firma elettronica qualificata* - firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro (ad es.: smart card) per la creazione della firma;
7. *GARR* – Gruppo Armonizzazione Reti della Ricerca*;*
8. *Log* – Qualsiasi registrazione delle attività elaborative compiute da un'applicazione che permette di ricostruire le operazioni svolte da un utilizzatore identificato o identificabile;
9. *Paesi Terzi* – Paesi non appartenenti alla Spazio Economico Europeo (SEE, ossia UE + Norvegia, Liechtenstein, Islanda) e Organizzazioni internazionali;
10. *Referenti privacy* – persone fisiche, nominate dal Titolare, che hanno il compito di supporto il Responsabile in tutte le attività relative al trattamento dei dati personali, di interfacciarsi con il RPD per tutte le attività inerenti alla corretta gestione della tutela dei dati personali e per ogni comunicazione legata all'applicazione della normativa in materia;
11. *Responsabile esterno* - persona fisica o giuridica, autorità pubblica o organismo che tratta i dati per conto del Titolare del trattamento;
12. *Responsabili interni del trattamento* – persone fisiche designate nell'ambito del proprio assetto organizzativo che svolgono specifici compiti e funzioni connessi al trattamento di dati personali e operano sotto l'autorità del Titolare del trattamento
13. *Risorse informatiche* - Qualsiasi tipo di hardware, mezzo di comunicazione elettronica, rete di trasmissione dati, software, sistemi cloud (ibrido pubblico o privato) e informazione in formato elettronico;
14. *Servizio di Comunicazione Elettronica* - servizio consistente esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica. In tale nozione sono compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva;
15. *Servizi Telefonici* - servizi di trasmissione, a distanza e in tempo reale, della voce per mezzo di un opportuno impianto per telecomunicazioni. Nell'ambito dei servizi telefonici sono ricompresi: le chiamate telefoniche, incluse le chiamate vocali, di messaggeria vocale, in conferenza e di trasmissione dati tramite telefax; i servizi supplementari, inclusi l'inoltro e il trasferimento di chiamata; la messaggeria e i servizi multimediali, inclusi i servizi di messaggeria breve-sms;
16. *Servizi Telematici* - Servizio e tecnica di telecomunicazioni che prevede la presenza di grandi elaboratori centralizzati da cui gli utenti possono attingere informazioni per via telefonica o radiotelevisiva, visualizzandoli su un personal computer o sullo schermo televisivo. Nell'ambito dei servizi telefonici sono ricompresi: l'accesso alla rete Internet; la posta elettronica; i *fax* (nonché i messaggi *sms* e *mms*) via Internet; la telefonia via Internet (cd. *Voice over Internet Protocol*–VoIP);
17. Servizi Cloud Computing - modello di infrastrutture tecnologiche remote utilizzate come risorsa virtuale per la memorizzazione e/o l'elaborazione nell'ambito di un servizio. Le classi di servizio

più comuni che caratterizzano i servizi cloud sono IaaS, PaaS e SaaS. Tali servizi possono erogati ai soggetti secondo diverse modalità di fruizione: public cloud, private cloud e hybrid cloud

18. *Sistema Informativo* - insieme delle risorse e attività finalizzate alla gestione (raccolta, registrazione, elaborazione, conservazione, comunicazione) dell'informazione;
19. *Sistema Informatico* - l'insieme delle applicazioni software e degli strumenti hardware che gestiscono i dati e i flussi informativi;
20. *Soggetto/Utente* - Qualsiasi dipendente dell'Ateneo, di altro Ente, collaboratore, consulente, studente o fornitore di servizi all'Ateneo a qualsiasi titolo;
21. *Spid* - Sistema Pubblico d'Identità Digitale, ovvero la soluzione che permette di accedere a tutti i servizi online della Pubblica Amministrazione e di privati federati con un'unica Identità Digitale (username e password) utilizzabile da computer, tablet e smartphone;
22. *Strutture* – Qualsiasi unità organizzativa all'interno dell'organigramma Aziendale*;*
23. *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" (art. 4. par. 1 punto 7 del Regolamento (UE) 2016/679- RGPD)*;*
24. *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.
25. *Struttura* – l'unità organizzativa competente in materia di sistemi informativi e di policy in materia di privacy e sicurezza informatica.

TITOLO II - TRATTAMENTO DEI DATI PERSONALI

Articolo 5 Titolare del Trattamento

1. L'Università per Stranieri di Perugia, nella persona del Rettore è Titolare di tutti i trattamenti dei dati personali effettuati nell'ambito delle attività istituzionali.
2. In particolare, il Titolare del trattamento ha il compito di:

    a) adottare gli interventi necessari per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al Regolamento (UE) 2016/679, anche con riferimento alle disposizioni del Codice per la protezione dei dati personali e atti di soft law;
    b) nominare il Responsabile della protezione dei dati;
    c) nominare i soggetti ai quali è affidata l'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;
    d) effettuare, a mezzo della struttura competente, apposite verifiche sulla osservanza delle vigenti disposizioni in materia di trattamento di dati personali, ivi compreso i profili relativi alla sicurezza informatica, in collaborazione con il Responsabile della protezione dati nominato.

Articolo 6 Responsabile protezione dati (DPO o RPD)

1. L'Università per Stranieri di Perugia nomina un Responsabile della protezione dati (di seguito RPD o DPO) che sia riferimento all'interno dell'Ateneo per i compiti di consulenza nei confronti del Titolare e dei soggetti designati o autorizzati al trattamento e di sorveglianza sull'osservanza del Regolamento (UE) 2016/679.
2. Il RPD è nominato con decreto del Rettoren tra il personale, anche esterno, di alta qualificazione
3. Il modello organizzativo privacy può indicare ulteriori e specifici compiti nei confronti del RPD.
4. Il Titolare del trattamento assicura che il RPD sia coinvolto in tutte le questioni riguardanti la protezione dei dati personali. Il RPD deve essere consultato immediatamente qualora si verifichi la violazione dei dati o altro incidente che comporti un rischio per i diritti e le libertà degli interessati.

Articolo 7 Contitolare

1. Qualora l'Università determini le finalità e i mezzi di un trattamento dati congiuntamente ad altro soggetto – pubblico o privato – tale soggetto diviene contitolare del trattamento.
2. L'Università e il Contitolare del trattamento stabiliscono mediante accordo scritto le rispettive responsabilità, i rispettivi obblighi derivanti dal Regolamento (UE) 2016/679 e un punto di riferimento e di contatto per gli interessati.
3. Il contenuto essenziale dell'accordo è messo a disposizione degli interessati da ciascun Contitolare.

Articolo 8 Responsabile interno del trattamento

1. Sulla base dell'assetto organizzativo dell'Ateneo e nell'ambito delle rispettive funzioni ricoperte e competenze, i soggetti designati che assumono la qualità di "Responsabili interni del trattamento" sono:

    a) i Dirigenti;
    b) i Direttori di Dipartimento;
    c) i Responsabili di altre tipologie di strutture;
    d) Ogni altra figura interna individuata con apposito atto organizzativo.

2. Salvo quanto previsto dal modello organizzativo privacy, i Responsabili interni del trattamento, ciascuno per la propria area di competenza garantiscono, insieme al Titolare, l'osservanza della normativa europea in tema di protezione dei dati personali.

Articolo 9 Responsabile esterno del trattamento

1. I soggetti esterni all'amministrazione che siano tenuti, a seguito di convenzione, contratto, atto di aggiudicazione o provvedimento di nomina, ad effettuare trattamento di dati personali per conto del Titolare sono nominati "Responsabili esterni del trattamento dei dati personali".
2. La nomina di Responsabile esterno del trattamento deve essere effettuata con atto scritto, che individui, la natura, la finalità e la durata del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi del Responsabile e i diritti del titolare del trattamento, nel rispetto dell'art 28 del GDPR.

3. Ai Dirigenti, Direttori di Dipartimento, Responsabili di struttura, nell'ambito delle rispettive competenze di funzione in materia di stipulazione di contratti e in qualità di Responsabili Interni sono demandati i compiti di stipulare, con i soggetti esterni che collaborano con l'Ateneo per l'esercizio delle funzioni istituzionali, gli atti negoziali per la gestione dei trattamenti.

Articolo 10 Autorizzati al trattamento

1. I Responsabili interni provvedono ad individuare per iscritto, tra i soggetti afferenti alla propria struttura di riferimento, in ragione dell'incarico o dell'attività da svolgere le persone fisiche autorizzate a compiere operazioni di trattamento dati ai sensi dell'art. 29 del GDPR.

2. Gli Autorizzati al trattamento devono essere adeguatamente informati e ricevono al momento della nomina specifiche istruzioni.
3. Gli Autorizzati sono tenuti all'osservanza delle istruzioni impartite dal Titolare o dal Responsabile Interno che provvederà a sovraintendere e vigilare sull'attuazione delle istruzioni impartite.

Articolo 11 Referenti per la protezione dei dati personali

1. Al fine di garantire i corretti adempimenti normativi in materia di protezione dei dati personali, il Responsabile interno individua, all'interno della propria struttura di competenza, il Referente per la protezione dei dati personali. In assenza di una specifica indicazione del Referente privacy questo ruolo è svolto direttamente dal Responsabile della struttura (Dirigente, Direttore o un suo delegato).

2. Il Referente per la protezione dei dati personali, nell'esercizio delle ordinarie attività amministrativo/gestionali, ha il compito di supportare il Responsabile interno del trattamento in tutte le attività relative al trattamento dei dati personali, di interfacciarsi con il RPD per tutte le attività inerenti alla corretta gestione della tutela dei dati personali e per ogni comunicazione legata all'applicazione della normativa in materia.

3. Il modello organizzativo privacy definisce ulteriori compiti e attività assegnate ai Referenti nelle varie funzioni di supporto.

Articolo 12 Amministratori di sistema

1. Gli Amministratori di sistema (doc. web n. 1577499 del Garante della Privacy) sono degli Autorizzati al trattamento appositamente nominati e preposti alla gestione e alla manutenzione di un impianto di elaborazione di dati o di sue componenti.
2. L'Amministratore di sistema ha il compito di vigilare sul corretto utilizzo dei sistemi informatici dell'Ateneo e supporta i Responsabili Interni del trattamento e Autorizzati per gli aspetti di tipo tecnico informatico nelle normali attività operative.

3. La nomina individuale è disposta dai Responsabili di struttura e deve contenere l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Gli estremi identificativi delle persone fisiche Amministratori di sistema, ivi compresi i nominativi degli amministratori di sistema relativi ai servizi esternalizzati, devono essere riportati,

unitamente all'elenco delle funzioni ad essi attribuite, in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

4. Ulteriori previsioni di dettaglio sono previste nel modello organizzativo privacy.

Articolo 13 Area Sistemi Informativi e Supporto Tecnico

1. L'Area Sistemi Informativi e Supporto Tecnico è la struttura competente in materia di sistemi informativi ed ha il compito di attuare le policy in materia di privacy e sicurezza informatica, con particolare riferimento all'utilizzo, alla sicurezza delle risorse informatiche e allo sviluppo delle applicazioni informatiche, da aggiornare periodicamente, ogni qualvolta l'evoluzione tecnica o normativa lo renda necessario.
2. La struttura promuove la formazione di tutto il personale dell'Università per Stranieri di Perugia in materia di sicurezza informatica, ha un ruolo di supporto al RPD in tema di risorse strumentali e di competenze, prevedendo la partecipazione e realizzando le verifiche specifiche richieste dello stesso RPD.
3. L'Area Sistemi Informativi e Supporto Tecnico è tenuta a mettere in atto tutte le misure adeguate, tecniche ed organizzative, per garantire la sicurezza informatica nei termini previsti dalle norme in materia, predisponendo, nel rispetto dei principi di accountability, evidenze documentali circa le azioni intraprese, le attività svolte e le caratteristiche dei sistemi, da esibire in caso di eventuali attività ispettive da parte degli organi competenti o di sorveglianza sulla conformità al GDPR da parte del RPD.

Articolo 14 Principi applicabili al trattamento dei dati personali

1. L'Università per Stranieri di Perugia tratta i dati personali, in presenza di una base giuridica che renda lecito tale trattamento, esclusivamente per il perseguimento delle finalità istituzionali e dei compiti ad esse connesse nel rispetto delle previsioni normative in materia.
2. I dati personali oggetto del trattamento devono essere trattati in conformità alla normativa europea e nazionale, in materia di protezione dei dati personali, secondo le disposizioni dei regolamenti e delle procedure di Ateneo e secondo i principi di liceità, correttezza e trasparenza. In particolare i dati personali devono essere:

    a) trattati in modo lecito corretto e trasparente nei confronti dell'interessato;

    b) raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in altre operazioni del trattamento nei termini compatibili con tali scopi;

    c) esatti e, se necessario, aggiornati;

    d) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati (minimizzazione);

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

3. Qualsiasi dato è un bene dell'Ateneo, deve pertanto essere protetto da distruzioni o perdite anche accidentali, alterazioni, usi illeciti e divulgazioni non autorizzate.
4. Ai dati personali devono essere applicate tutte le prescrizioni di sicurezza previste dalla normativa vigente, anche in termini di sicurezza dei sistemi informatici.

Articolo 15 Circolazione di dati personali nell'ambito dell'Università

1. Il trattamento dei dati personali da parte di tutte le unità organizzative dell'Università è finalizzato al perseguimento delle finalità istituzionali e dei compiti ad esse connesse ed è ispirato al principio della libera circolazione delle informazioni all'interno dell'Ateneo nel rispetto dei principi di necessità e minimizzazione.
2. L'accesso ai dati personali da parte delle unità organizzative e del personale dell'Ateneo risponde al principio di necessità: le informazioni devono essere rese disponibili esclusivamente all'ufficio richiedente, per lo svolgimento dell'attività lavorativa, mediante strumenti atti a facilitarne la fruizione.
3. L'accesso e l'utilizzo di qualsiasi dato riservato deve essere espressamente autorizzato dal Responsabile del dato medesimo.

Articolo 16 Comunicazione e diffusione di dati personali

1. L'Università può comunicare, solo in presenza di precise condizioni (Cfr. art. 2-ter Codice privacy) ad altre pubbliche amministrazioni e diffondere, anche sui propri siti web: i nominativi del proprio personale e dei collaboratori, le informazioni sul ruolo ricoperto, i recapiti telefonici e indirizzi telematici istituzionali e il curriculum vitae dei professori e dei ricercatori dell'Ateneo.
2. Fermo restando le norme vigenti in materia di accesso ai documenti amministrativi, e le norme vigenti in materia di scambio di dati tra enti pubblici, la comunicazione o la diffusione di dati personali possono avvenire solo ove sussista una idonea base giuridica.
3. La comunicazione di dati personali è un'operazione del trattamento che consiste nel dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, ad opera di persone autorizzate.
4. La diffusione è un'operazione del trattamento che consiste nel dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Articolo 17 Sicurezza dei dati personali

1. Il Titolare fornisce ai Responsabili Interni e agli Autorizzati al trattamento misure organizzative adeguate a garantire un livello di sicurezza idoneo al rischio connesso al trattamento. Tali misure sono finalizzate a ridurre i rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
2. Nel caso in cui un particolare tipo di trattamento, anche connesso all'uso delle nuove tecnologie, per la sua natura, finalità, oggetto e contesto presenti un rischio elevato per i diritti e le libertà

delle persone fisiche, il Titolare in collaborazione con il RPD effettua in via preliminare una valutazione dell'impatto del trattamento stesso sulla protezione dei dati personali.

3. Qualora le risultanze della valutazione d'impatto sulla protezione dei dati indicano un rischio elevato il Titolare del trattamento prima di procedere ~~al trattamento~~ consulta l'autorità di controllo.
4. L'Area Sistemi Informativi e Supporto Tecnico fornisce supporto al Titolare, ai Responsabili e al RPD per lo svolgimento della valutazione d'impatto come da previsioni di dettaglio previste nel modello organizzativo privacy.

Articolo 18 Violazione dei dati personali (Data Breach)

1. Tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare sono tenuti nel caso di una concreta, potenziale o sospetta violazione dei dati personali ad informare dell'incidente il Responsabile della struttura, il quale si occuperà, di informare il Titolare del trattamento o un suo delegato e il RPD mediante la compilazione modulo di comunicazione di Data Breach presente sul sito di Ateneo.
2. Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Titolare del trattamento o un suo delegato dovrà coinvolgere anche il Responsabile dell'Area Sistemi Informativi e Supporto Tecnico o un suo delegato, in caso di assenza.
3. Nel caso in cui la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento deve notificare entro 72 ore la violazione al Garante per la protezione dati personali e, senza ingiustificato ritardo, dare comunicazione all'interessato nei casi previsti agli artt. 33 e 34 del GDPR.
4. La violazione di dati personali, ai sensi dell'art 33 del GDPR, deve essere documentata all'interno del Registro del Data Breach di Ateneo, come da previsioni di dettaglio previste nel modello organizzativo privacy.

Università per Stranieri di Perugia

TITOLO III - REGOLE PER L'ACCESSO, L'UTILIZZO E LA SICUREZZA DELLE RISORSE INFORMATICHE E DEI SERVIZI DI COMUNICAZIONE

Articolo 19 Gestione e utilizzo risorse informatiche e dei servizi di comunicazione

1. Le risorse informatiche e i servizi di comunicazione dell'Ateneo devono essere utilizzate per l'assolvimento delle finalità proprie dell'Ateneo.

2. È vietata qualsiasi attività che possa produrre danni alle risorse informatiche e ai servizi di comunicazione dell'Ateneo o che risulti in contrasto con le regole contenute nel presente testo o con le norme vigenti.
3. Ogni strumento ed ogni memoria esterna affidati dall'Ateneo agli utilizzatori, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti all'Area Sistemi Informativi e Supporto Tecnico che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento.

4. Il personale dell'Università per Stranieri di Perugia è tenuto ad adottare, nell'ambito delle proprie attività, tutte le misure di sicurezza atte a prevenire la possibilità di accessi non autorizzati, furti, frodi, danneggiamenti, distruzioni o altri abusi nei confronti delle risorse informatiche e telefoniche e ha il dovere di segnalare tempestivamente furti, danneggiamenti o smarrimenti di tali strumenti.

Articolo 20 Misure tecniche e organizzative

1. L'Ateneo, per tutte le risorse informatiche e i servizi di comunicazione, mette in atto misure tecniche e organizzative adeguate a garantire e dimostrare, che il trattamento è effettuato conformemente alle prescrizioni del Regolamento (UE) 2016/679 in materia di protezione dei dati personali (GDPR art. 5 "principio di responsabilizzazione").

2. Ciascuna struttura è responsabile della concreta adozione delle misure organizzative necessarie a proteggere i dati personali oggetto di trattamento in collaborazione con il Titolare del trattamento e con il supporto dell'Area Sistemi Informativi e Supporto Tecnico.

Articolo 21 Modalità di utilizzo delle risorse telematiche

1. L'Area Sistemi Informativi e Supporto Tecnico e Supporto Tecnico gestisce le infrastrutture telefoniche di Ateneo;
2. I servizi telematici messi a disposizione dell'Ateneo sono strumenti di lavoro e il loro utilizzo deve essere finalizzato allo svolgimento delle attività professionali e istituzionali dell'Università;

3. Ogni utilizzatore dei servizi telematici è tenuto ad adottare le necessarie misure per non interferire nel corretto funzionamento delle comunicazioni e per garantire l'integrità dei sistemi e l'accesso alle risorse da parte degli altri utenti.

Articolo 22 Fornitori dei Servizi Informatici

1. La delega di alcune attività che comportino il trattamento di dati personali a fornitori di servizi informatici (ad es. fornitori di servizi web, di servizi di hosting o cloud computing) deve essere fatta unicamente a soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate.

2. Per i fornitori di servizi informatici nominati responsabili del trattamento, nel rispetto di quanto richiesto all'art. 28 del RGPD, deve individuarsi una corretta ripartizione delle responsabilità tra Titolare e Responsabile, anche in relazione all'adozione di adeguate misure tecniche e organizzative volte a garantire all'Ateneo idonei strumenti di controllo delle attività di trattamento.
3. I trattamenti di dati personali effettuati dal Responsabile esterno devono essere presenti nel Registro dei trattamenti come da previsione di dettaglio previsto nel Modello organizzativo privacy adottato dall'Ateneo.
4. Per i fornitori di servizi stabiliti in Paesi terzi, ai fini della liceità del trasferimento dei dati personali in tali Paesi devono essere soddisfatte le condizioni previste dagli artt. 44 e ss. del RGPD.

Articolo 23 Servizi Cloud computing

1. L'utilizzo di servizi di cloud computing è subordinato alla verifica di tutte le indicazioni e prescrizioni previste dal Garante per la Protezione dei Dati Personali, dall'Agenzia per l'Italia Digitale (AGID) e dei Ministeri competenti.

2. L'Area Sistemi Informativi e Supporto Tecnico si riserva di identificare tecnologie e/o servizi cloud conformi alla normativa da mettere a disposizione dei soggetti anche al fine di supportare il personale nella gestione dei dati, consentendone tracciabilità, disponibilità, autenticità, e una conservazione appropriata, tenendo conto degli aspetti legati alla sicurezza (Data Management Plan).

Articolo 24 Utilizzo degli elaboratori personali forniti dall'Ateneo

1. Ai fini del presente articolo sono considerati elaboratori personali i dispositivi di proprietà dell'Ateneo assegnati ai soggetti.

2. Gli elaboratori personali sono strumenti di lavoro predisposti con la necessaria dotazione (*hardware)* e *(software)* tali da consentire il corretto funzionamento e garantire un adeguato livello di sicurezza.

3. Non è consentito utilizzare gli elaboratori per motivi non attinenti allo svolgimento delle mansioni assegnate e inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

4. Sugli elaboratori personali è consentito l'uso di programmi esclusivamente nel pieno rispetto degli obblighi imposti dalla vigente normativa sulla tutela giuridica del software e del diritto d'autore.

5. Sugli elaboratori personali contenenti dati personali devono essere applicate, in collaborazione con il Titolare del trattamento, tutte le idonee misure di sicurezza previste della normativa vigente in conformità al principio di *accountability,* ai sensi dell'art. 32 del Regolamento (UE) 2016/679, nonché quelle individuate dall'Ateneo.

6. L'Ateneo si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema informativo ovvero acquisiti o installati in violazione del presente regolamento.

Articolo 25 Utilizzo di dispositivi informatici non forniti dall'Ateneo

1. L'utilizzo di dispositivi informatici propri per lo svolgimento della prestazione lavorativa è possibile a condizione che siano garantiti adeguati livelli di sicurezza, al fine di proteggere il patrimonio informativo dell'Ateneo, nel rispetto dell'art. 32 del Regolamento (UE) 2016/679 e delle istruzioni fornite dall'Università.

Articolo 26 Programmi per elaboratore

1. Qualsiasi software, a qualsiasi titolo acquisito o realizzato dall'Ateneo, deve essere protetto da distruzioni o perdite anche accidentali, alterazioni, usi illeciti e divulgazioni non autorizzate.

2. Qualsiasi software non espressamente rilasciato con strumenti finalizzati alla diffusione pubblica è da intendersi riservato.

3. La riproduzione, installazione, duplicazione, distribuzione e ogni altra forma di utilizzo dei programmi per elaboratore, in quanto opere dell'ingegno tutelate dalla legge, può avvenire lecitamente solo nel rispetto dei diritti d'autore e delle licenze d'uso.
4. La distribuzione gratuita di software da parte di unità operative dell'Ateneo può avvenire purché, utilizzando di volta in volta gli strumenti più idonei e le formulazioni più appropriate, vengano informati i potenziali utilizzatori delle seguenti condizioni:

    a) l'Ateneo non fornisce alcuna garanzia sui software distribuiti gratuitamente e in particolare non garantisce la loro adeguatezza e fruibilità per scopi specifici;
    b) in nessun caso l'Ateneo potrà essere ritenuto responsabile per danni diretti, indiretti o derivanti dall'uso dei software distribuiti gratuitamente o dai risultati da essi forniti; in particolare non potrà essere ritenuto responsabile per eventuali ritardi,

inadempienze, perdita di dati e danni economici derivanti o in qualche modo collegati all'uso di tali software od ai risultati da essi forniti.

Articolo 27 Modalità di utilizzo delle risorse informatiche

1. L'accesso e l'uso di risorse informatiche esterne all'Ateneo e da essa non dipendenti è soggetto, nel rispetto del vigente ordinamento, alle norme e regolamentazioni fissate dai titolari di tali risorse.
   In particolare, a titolo esemplificativo e non esaustivo, è vietato:

   a) navigare in siti non pertinenti rispetto alle specifiche necessità di lavoro o di studio, soprattutto se idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché a rivelare lo stato di salute e la vita sessuale;

   b) compiere azioni in violazione delle norme e tutela delle opere protette dal diritto d'autore e da altri diritti connessi al suo esercizio quali opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro e alla cinematografia, qualunque ne sia il modo o la forma di espressione;
   c) trasferire o rendere disponibile materiale in violazione delle norme sulla proprietà intellettuale, con procedure non legali di programmi per elaboratore o altri strumenti

   d) memorizzare documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

   e) porre in essere qualsivoglia attività vietata dalle leggi vigenti.

2. L'utilizzo degli strumenti informatici sul luogo di lavoro, in particolare la posta elettronica e la navigazione internet dovranno ispirarsi al rispetto della normativa in materia di protezione dei dati personali nonché ai principi di diligenza, fedeltà e correttezza.
3. Chiunque intenda pubblicare contenuti su un qualsiasi sito Web di proprietà dell'Università per Stranieri di Perugia è tenuto al rispetto delle Linee guida per la gestione dei siti web dell'Università per Stranieri di Perugia e delle "Linee guida in materia di sicurezza e privacy dei siti Web di Ateneo". I siti web dell'Università non dovranno contenere materiale che esponga l'Ateneo a rischi di infrazione rispetto alla normativa vigente.

Articolo 28 Rete dati di Ateneo

1. L'Università per Stranieri di Perugia considera la rete dati di Ateneo un elemento strategico fondamentale per il perseguimento dei propri fini istituzionali e ne promuove lo sviluppo, il buon funzionamento e la sicurezza. La rete telematica di Ateneo è interconnessa alla rete Garr e, tramite quest'ultima, alla rete Internet.

2. L'uso delle risorse e l'accesso ai servizi Internet devono essere utilizzati per attività istituzionali o comunque strettamente correlate e funzionali all'Ateneo nel rispetto della normativa vigente nazionale e comunitaria, dal presente regolamento e dalle regole stabilite dall'Acceptable Use Policy del Consortium GARR.

3. Tutti gli utilizzatori della rete sono responsabili delle attività svolte e sono tenuti ad adottare le necessarie misure per non interferire nel corretto funzionamento delle comunicazioni e per garantire l'integrità dei sistemi e l'accesso alle risorse da parte degli altri utenti.

4. L'Università utilizza i social media con finalità istituzionali e di interesse generale per informare, comunicare, ascoltare e per consentire una relazione più diretta e una maggiore partecipazione della comunità accademica. Tutti gli utilizzatori sono tenuti a gestire spazi di comunicazione e dialogo all'interno dei profili social nel rispetto della normativa e delle Linee guida adottate dall'Ateneo.
5. Tutti gli utilizzatori della rete dati di Ateneo sono tenuti a segnalare immediatamente all'Area Sistemi Informativi e Supporto Tecnico e al RPD ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza.

6. Il responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D., ovvero, in sua assenza, il dirigente allo scopo designato, ha la responsabilità della attuazione delle Misure minime di sicurezza ICT per le pubbliche amministrazioni (AgID – Circolare 17 aprile 2017, n. 2/2017).

Articolo 29 Connessioni alla rete WiFi di Ateneo

1. L'Area Sistemi Informativi e Supporto Tecnico gestisce e mette a disposizione in tutti gli spazi interni ed esterni dell'Ateneo il servizio di accesso *wireless* denominato "*UNISTRAPG"*, *"EDUROAM" e "EASYUNISTRAPG".*

2. Nelle aree dell'Università per Stranieri di Perugia coperte dal servizio "*UNISTRAPG",* l'accesso all'infrastruttura Wi-Fi è consentito al Personale Docente, Tecnico-Amministrativo, Studenti, previa autenticazione con le proprie credenziali dei servizi on-line.

3. Nelle aree dell'Università per Stranieri di Perugia coperte dal servizio "*EASYUNISTRAPG*", l'accesso all'infrastruttura Wi-Fi è consentito agli ospiti o ai partecipanti a Convegni/Eventi previa autenticazione con le credenziali generate dalle segreterie dipartimentali o dalla UO Servizio Infrastrutture Informatiche dell'Area Sistemi Informativi e Supporto Tecnico previa richiesta della struttura o della segreteria organizzativa dell'evento.

4. Il servizio "*EDUROAM"* è un servizio internazionale che permette agli utenti mobili (roaming users) in tutte le organizzazioni partecipanti alla Federazione di accedere alla rete wireless locale utilizzando le credenziali fornite dalla propria organizzazione. Gli utenti che visitano un Ente aderente all'iniziativa potranno utilizzare la rete wifi della struttura ospitante usando le stesse credenziali (username e password) del proprio ente di appartenenza, senza ulteriori formalità presso l'istituto ospitante.

5. I log di accesso della rete wireless di Ateneo sono raccolti e conservati in conformità alla normativa vigente e a quanto definito nel Titolo VI RESPONSABILITÀ E CONTROLLI.

Articolo 30 Accesso remoto alla Rete dati di Ateneo

1. L'accesso remoto alle Rete dati di Ateneo è consentito esclusivamente utilizzando protocolli sicuri che garantiscono l'integrità e la confidenzialità dei dati veicolate su Internet.

2. L'Area Sistemi Informativi e Supporto Tecnico gestisce e mette a disposizione del personale strutturato un servizio di accesso remoto alla Rete dati di Ateneo mediante una connessione VPN (Virtual Private Network) con autenticazione tramite credenziali di Ateneo.

3. L'accesso è consentito da ogni rete esterna all'Ateneo previa richiesta all'Area Sistemi Informativi e Supporto Tecnico e successiva installazione e configurazione del client di accesso dedicato. Policy ad hoc vengono implementate e aggiornate dal personale dell'Area Sistemi Informativi e Supporto Tecnico su richiesta dell'utente. Tali accessi vengono attivati per attività di smartworking, telelavoro o attività di gestione/controllo di ditte manutentrici o di personale strutturato nell'ambito di progetti di ricerca o attività di laboratorio.

4. I log di accesso remoto alla rete in modalità VPN o assimilata sono raccolti e conservati in conformità alla normativa vigente e a quanto definito nel Titolo VI RESPONSABILITÀ E CONTROLLI.
5. È vietato l'utilizzo del servizio di accesso remoto alla rete di Ateneo per eludere anche solo in parte i sistemi e le policy di sicurezza di Ateneo.

Articolo 31 Monitoraggio e controlli

1. L'Università ha facoltà di effettuare controlli sulle attività svolte in rete nel rispetto dei diritti e delle libertà fondamentali degli utenti, ed in particolare dell'art. 4 dello Statuto dei Lavoratori, al fine di evitare usi impropri della rete o dei servizi di rete messi a disposizione dall'Ateneo.

2. La raccolta e conservazione dei log è, anche ai sensi dell'art. 132 del D. Lgs. 30 giugno 2003, n. 196 e s.m.i., un obbligo di legge al fine di coadiuvare le Autorità di Pubblica Sicurezza per l'indagine e la repressione dei reati informatici.
3. Viene tenuta traccia del traffico internet effettuato mediante rete WiFi di Ateneo.
4. Le copie di sicurezza delle registrazioni del traffico (file di log) delle consultazioni, contenenti la data, l'ora e gli estremi identificativi dell'utilizzatore e delle pagine Web visualizzate, effettuate per fini strettamente correlati alla gestione tecnica del servizio, sono conservate per un massimo di 365 giorni e nel rispetto della normativa vigente.

Articolo 32 Firma digitale

1. L'Università per Stranieri di Perugia ha avviato un sistema di firma digitale aperto a tutti i dipendenti che ne facciano motivata richiesta.

2. Gli assegnatari, nel rispetto dei poteri di firma derivanti dalla legge, dai regolamenti e dalle linee guida e dalle procedure di Ateneo, adottano tutte le misure organizzative e tecniche idonee all'utilizzo personale della firma per evitare l'uso fraudolento da parte di terzi.

TITOLO IV - POSTA ELETTRONICA

Articolo 33 Obiettivi e ambito di applicazione

1. L'Università per Stranieri di Perugia, tramite l'Area Sistemi Informativi e Supporto Tecnico, rende disponibile un servizio istituzionale di posta elettronica.

2. La posta elettronica è uno strumento istituzionale per la comunicazione interna ed esterna dell'Ateneo e l'utilizzo di tale casella costituisce "trattamento dei dati personali" e pertanto è da conformarsi alla normativa vigente in materia e al presente regolamento.

3. Le disposizioni del presente regolamento si applicano:
   a) a tutti i sistemi e i servizi di posta elettronica dell'Ateneo;

   b) indifferentemente ai contenuti dei messaggi di posta e alle informazioni transazionali (header dei messaggi, indirizzi di posta, dati dei destinatari e dei mittenti) relative a tali messaggi;
   c) agli amministratori e fornitori di tali servizi;

   d) tutti gli utenti dotati di una casella di posta elettronica, definiti nei domini appartenenti all'Ateneo;

   e) a ogni altra categoria di personale come ad esempio fornitori, consulenti, stagisti ecc. cui venga fornito in modo temporaneo un account di posta elettronica per lo svolgimento delle proprie attività;
   f) a tutti i messaggi di posta elettronica e alle altre registrazioni a questi connesse (indirizzi di posta elettronica, liste di distribuzione, notifiche e log dei messaggi, ecc.) in possesso di dipendenti o di altri utenti, amministratori o gestori del servizio di posta elettronica dell'Ateneo.

Articolo 34 Finalità del servizio di posta elettronica

1. L'Ateneo incoraggia l'uso della posta elettronica per scambiare informazioni, migliorare le comunicazioni, scambiare idee e per rendere più efficaci ed efficienti i processi di lavoro a supporto della missione istituzionale dell'Università.

Articolo 35 Proprietà dell'Ateneo

1. Il servizio di posta elettronica dell'Ateneo, erogato in proprio o per il tramite di fornitori dei servizi in outsourcing, è di proprietà dell'Università per Stranieri di Perugia. Pertanto ogni casella di posta elettronica associata all'Ateneo o a sue articolazioni organizzative o assegnata a individui o funzioni dell'Ateneo, sono di proprietà dell'Università.

Articolo 36 Limitazioni di Responsabilità per l'Ateneo

1. L'Ateneo non può essere ritenuto responsabile per qualsiasi danno, diretto o indiretto, arrecato all'utente ovvero a terzi e derivante:

a) dall'eventuale interruzione del servizio;

b) dall'eventuale smarrimento di messaggi diffusi per mezzo del servizio;

c) da messaggi inviati/ricevuti o da transazioni eseguite tramite il servizio;

d) da accesso non autorizzato ovvero da alterazione di trasmissioni o dati dell'utente.

Articolo 37 Restrizioni all'uso del servizio

1. Gli utenti del servizio di posta elettronica sono tenuti ad usarlo in modo responsabile, cioè rispettando le leggi, la presente e altre regole e procedure dell'Ateneo e secondo normali standard di cortesia, correttezza, appropriatezza, continenza, buona fede e diligenza professionale.
2. L'accesso ai servizi di posta elettronica può essere totalmente o parzialmente limitato dall'Ateneo, senza necessità di assenso da parte dell'utente e anche senza preavviso:

a) quando richiesto dalla legge e in conformità ad essa;

b) in caso di comprovati motivi che facciano ritenere la violazione dei criteri di cui al comma 1 del presente articolo o delle disposizioni di legge vigenti;

c) al venir meno delle condizioni in base alle quali si ha diritto di utilizzare il servizio;

d) in casi eccezionali, quando richiesto per esigenze operative critiche e improcrastinabili.

Articolo 38 Assenso e conformità

1. L'Ateneo è tenuto in generale ad ottenere l'assenso del titolare della casella di posta elettronica prima di ogni ispezione dei messaggi o accesso alle registrazioni o ai messaggi di posta elettronica, fatta eccezione per quanto disposto al successivo articolo. Il personale dell'Ateneo

fornisce collaborazione alle richieste riguardanti la fornitura di copie delle registrazioni di posta elettronica in suo possesso attinenti alle attività lavorative dell'Ateneo o necessarie per soddisfare obblighi di legge, indipendentemente dal fatto che tali registrazioni risiedano o meno su computer di proprietà dell'Università. Il mancato rispetto di tali richieste può portare all'applicazione delle misure di cui l'articolo successivo.

Articolo 39 Limitazioni di accesso senza assenso

1. L'Ateneo non ispeziona e non accede ai messaggi di posta elettronica dell'utente senza la sua autorizzazione. L'Ateneo potrà però permettere l'ispezione, il monitoraggio o l'accesso alla posta elettronica degli utenti, anche senza l'assenso del titolare, nei seguenti casi:
   a) su richiesta scritta dell'Autorità giudiziaria nei casi previsti dalla normativa vigente;

   b) per gravi e comprovati motivi che facciano credere che siano state violate le disposizioni di legge vigenti o le regole dell'Ateneo in materia di sicurezza;

   c) in situazioni critiche e di emergenza in assenza del titolare della casella e nel rispetto delle indicazioni contenute nelle *Linee Guida Posta Elettronica.*

Articolo 40 Registro elettronico

1. L'Ateneo può registrare e conservare i dati delle caselle di posta elettronica messe a disposizione dei propri utenti, tramite scrittura in appositi file di log, delle seguenti informazioni minime: mittente del messaggio, destinatario/i, giorno ed ora dell'invio e esito dell'invio.

Articolo 41 Soggetti titolari di una casella di posta elettronica

1. Il servizio di posta elettronica è fornito in funzione dell'attività didattica, dell'attività di ricerca, dell'attività amministrativa e delle altre attività strumentali o correlate ai fini istituzionali di Ateneo.
2. Al personale universitario in servizio attivo a tempo determinato o indeterminato, ai contrattisti e collaboratori, ai docenti in quiescenza, ai docenti emeriti, agli ospiti, stagisti, ai dipendenti cooperative, ai volontari del servizio civile, ai *collaboratori, ai* visiting professor è associato un indirizzo di posta elettronica afferente al dominio @unistrapg.it

3. Agli studenti iscritti a qualunque corso di studi (corsi di laurea, master, dottorati, scuole di specializzazione), è associato un indirizzo di posta elettronica afferente al dominio @studenti.unistrapg.it

4. Al fine di agevolare la comunicazione istituzionale e favorire la circolazione delle informazioni, sono altresì fornite su richiesta del Responsabile della unità organizzativa o suo delegato caselle di posta elettronica per strutture, laboratori, progetti, convegni, congressi e altre iniziative codificate nel formato base *nomestruttura@unistrapg.it.*

Università
per Stranieri
di Perugia

Articolo 42 Ambito di utilizzo del servizio di posta elettronica

1. Gli utenti del servizio di posta elettronica si avvalgono del medesimo nella consapevolezza che:

    a) la posta elettronica non è uno strumento sicuro poiché i messaggi spediti possono essere inoltrati ad altri destinatari. Gli utenti pertanto devono esercitare la massima cautela nell'uso della posta elettronica per comunicare informazioni riservate o dati sensibili;

    b) i messaggi di posta elettronica, creati e conservati sia su apparati elettronici forniti dall'Ateneo che su altri sistemi, possono costituire registrazioni di attività svolte dall'Università (ricezione o invio di informazioni scambiate tra uffici e personale dell'Ateneo, tra l'Università e enti o società esterne o singoli cittadini). È possibile che venga richiesto di accedere ai contenuti dei messaggi per un eventuale utilizzo nell'ambito di contenziosi che coinvolgano l'Ateneo. L'Università non darà corso automaticamente a tutte le richieste di accesso, ma le valuterà in relazione a precisi obblighi di legge quali la normativa in materia di privacy ed altre disposizioni applicabili. L'Ateneo non può garantire che non vi siano accessi alle informazioni personali degli utenti eventualmente presenti in messaggi di posta elettronica residenti sui sistemi dell'Università;
    c) l'Ateneo non si pone di norma come valutatore dei contenuti dei messaggi di mail scambiati, né può proteggere gli utenti dalla ricezione di messaggi che possano essere considerati offensivi. Gli utenti sono comunque fortemente incoraggiati a usare nella posta elettronica le stesse regole di cortesia che adopererebbero in altre forme di comunicazione;

    d) non c'è garanzia, a meno di utilizzare sistemi di posta certificata, che i messaggi ricevuti provengano effettivamente dal mittente previsto. Inoltre i messaggi di posta che arrivano come "inoltro" di precedenti messaggi, potrebbero essere stati modificati rispetto all'originale. Pertanto, in caso di dubbi, chi riceve un messaggio di posta elettronica dovrebbe verificare con il mittente l'autenticità delle informazioni ricevute.

2. I titolari di una casella di posta elettronica con un indirizzo riportante il proprio nominativo sono tenuti ad apportare in calce alle proprie e-mail una firma, generata da servizio firme di Ateneo, formata da: nome, cognome, struttura di appartenenza, numeri, indirizzo sede fisica, indirizzo mail, e sito web di Ateneo evitando di aggiungere altre informazioni non attinenti all'incarico lavorativo.
3. L'utilizzo degli indirizzi di posta elettronica @unistrapg.it e @studenti.unistrapg.it costituisce trattamento dei dati personali, pertanto, deve conformarsi alle disposizioni del RGPD e del D. Lgs. n. 196/2003 e s.m.i..

4. I titolari di una casella di posta elettronica sono tenuti ad indicare in calce alle proprie e-mail un avvertimento ai destinatari nel quale sia dichiarata la natura riservata del messaggio precisando che è vietato qualsiasi utilizzo improprio delle informazioni secondo le indicazioni contenute nelle buone prassi delle *Linee Guida Posta Elettronica.*

5. La trasmissione informatica di documenti e dati con particolari requisiti di riservatezza ("categorie particolari" secondo il Regolamento (UE) 2016/679), deve essere effettuata adottando idonee misure di sicurezza secondo le modalità indicate nella procedura preposta.
6. La sicurezza e riservatezza della posta elettronica non possono essere garantite in ogni circostanza, in particolare per quanto concerne i messaggi di posta scaricati sui Personal Computer. In questo caso è indispensabile che l'utente stesso provveda ad attuare le azioni adeguate a proteggere le informazioni usando tutti i mezzi disponibili, quali ad esempio password di accesso alle applicazioni e alla propria postazione di lavoro.

Articolo 43 Ciclo di vita delle caselle di posta elettronica

1. L'account di posta elettronica (username, password e indirizzo di posta) è fornito dall'Ateneo. Si distingue tra indirizzi di posta nominativi (ad personam) e indirizzi di posta impersonali (associati ad una struttura o ad una specifica funzione/progetto/servizio) con modalità di assegnazione automatica o su richiesta.

2. Le modalità di attivazione e disattivazione delle caselle di posta elettronica sono legate allo status di utente attivo, salvo eventuali casi particolari disciplinati secondo le indicazioni contenute nelle *Linee Guida Posta Elettronica.*

3. Il processo di revoca porta alla dismissione della casella di posta elettronica attraverso le fasi di disattivazione e cancellazione.
4. Per le caselle ad personam assegnate su richiesta il periodo standard di durata è definito nelle *Linee Guida Posta Elettronica*.

5. Le caselle impersonali rimangono attive fino a richiesta di disattivazione da parte del proprietario pro-tempore.

Articolo 44 Chiusura anticipata

1. L'utilizzo della casella di posta può essere revocato con decorrenza immediata nel caso in cui venga meno il rapporto di fiducia con l'Ateneo (ad esempio a titolo meramente esemplificativo e non esaustivo, in caso di licenziamento per giusta causa, illecito disciplinare, utilizzo illecito dei servizi), in caso di violazione della normativa vigente, del presente regolamento, per giustificate motivazioni tecniche o di sicurezza o per sospensione cautelare del dipendente dal servizio. In quest'ultimo caso il dipendente dovrà fornire all'Ateneo un indirizzo alternativo cui potranno essere inviate eventuali comunicazioni utili da parte dell'Ateneo stesso.

2. L'identificativo della casella disattivata sarà conservato dall'Ateneo allo scopo di evitare la riassegnazione di identificativo e/o indirizzo di posta elettronica a un soggetto omonimo.

3. Per le caselle assegnate su richiesta, la struttura o l'assegnatario possono chiedere la chiusura anticipata.

4. Situazioni specifiche saranno esaminate dagli Organi competenti di Ateneo.

Articolo 45 Prolungamento

1. Gli assegnatari di una casella afferenti a ruoli di docenza a tempo indeterminato (ricercatori, professori associati, professori ordinari), qualora persista un rapporto di collaborazione a qualsiasi titolo con l'Ateneo anche dopo la cessazione dal ruolo, continueranno ad avere normale accesso alla casella di posta elettronica fino al termine della collaborazione.

2. Gli assegnatari di una casella afferenti a ruoli non strutturati (assegnisti, dottorandi, borsisti, collaboratori, specializzandi, professori a contratto,…), qualora persista un rapporto di collaborazione a qualsiasi titolo con l'Ateneo anche dopo la cessazione dal ruolo, potranno far richiesta per il mantenimento della casella. La richiesta dovrà indicare il tipo di collaborazione e il suo termine.

3. Tutto il personale, nel caso in cui permanga un rapporto di necessità di utilizzo del servizio di posta elettronica, può richiedere tramite il Responsabile della struttura di appartenenza di prolungare la durata della casella oltre i limiti.

Articolo 46 Archiviazione e conservazione

1. Al fine di garantire un elevato livello di sicurezza della rete di Ateneo i sistemi di logging per il corretto esercizio del servizio di posta elettronica conservano i soli dati esteriori, contenuti nella cosiddetta "envelope" del messaggio.

Articolo 47 Uso Personale

1. È consentito l'utilizzo ragionevole dei propri account nei domini dell'Ateneo a fini privati e personali, purché, in aggiunta a quanto indicato nei punti precedenti, tale utilizzo non:
    a) sia causa, diretta o indiretta di disservizi dei sistemi elaborativi e dei servizi di posta elettronica;

    b) sia causa di oneri aggiuntivi per l'Ateneo;

    c) interferisca con le attività lavorative dell'utente o con altri obblighi dello stesso verso l'Università.

2. L'utente è edotto del fatto che l'Ateneo considererà, ai fini di eventuali ispezioni, tutti i messaggi di posta elettronica da lui gestiti come strettamente afferenti all'uso del servizio per scopi di lavoro.

3. L'Ateneo presuppone che l'utilizzo della posta elettronica istituzionale per scopi personali sia subordinato a una preliminare ed attenta valutazione delle opportunità da parte dell'utente.

Articolo 48 Caselle di servizio

1. Al fine di garantire il regolare svolgimento di attività lavorative o di studio l'Università rende disponibili anche indirizzi condivisi (caselle di servizio) tra più soggetti, rendendo così chiara la natura non privata della corrispondenza.
2. Gli indirizzi non nominativi di struttura o di incarichi accademici comprendono tra l'altro: Organi accademici, Prorettori, Strutture amministrative, didattiche e di ricerca dell'Ateneo e possono essere condivisi fra più utenti dotati di casella di posta nominativa dell'Ateneo. Gli indirizzi per Strutture amministrative, didattiche e di ricerca possono essere richiesti solo dal Responsabile di struttura.

Articolo 49 Proibizioni

4. È fatto divieto a tutti gli utenti di utilizzare il servizio di posta elettronica per inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione dell'Ateneo.

5. È vietato, inoltre, l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali e la fornitura (gratuita o a pagamento) a persone fisiche o giuridiche di qualsiasi lista o elenco degli Utenti del servizio.
6. Non è consentito fornire le proprie credenziali di accesso a sistemi o procedure, così come rispondere a messaggi e-mail che facciano richiesta di questo tipo di informazioni.

Articolo 50 Monitoraggio e controlli

1. I messaggi di posta elettronica possono essere soggetti ad un esame automatico da parte di software anti-virus e anti-spam; quelli rilevati infetti o indesiderati possono essere bloccati.
2. Nell'assolvimento dei propri compiti il personale che gestisce i sistemi di elaborazione e le reti di telecomunicazione può avere, saltuariamente, la necessità di analizzare i dati transazionali dei messaggi di posta per garantire il corretto funzionamento del servizio e in queste occasioni vi possono essere involontari accessi al contenuto stesso dei messaggi. Tale personale è tenuto comunque al rispetto di stretti vincoli di riservatezza qualora si verificassero i casi citati.

3. L'Ateneo laddove vi sia il sospetto di violazioni di norme di legge o delle disposizioni di cui al presente regolamento di particolare gravità, potrà effettuare controlli straordinari. 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.
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.

Università per Stranieri di Perugia

TITOLO V - IDENTITA' DIGITALI DI ATENEO

Articolo 51 Le identità digitali

1. L'identità digitale è costituita dalle informazioni o qualità relative a un utente utilizzate per rappresentarne l'identità, lo stato, la forma giuridica o altre caratteristiche peculiari ed è verificata attraverso un sistema di identificazione e autenticazione informatica.
2. L'identità digitale è strumentale all'accesso a uno o più servizi telematici.

3. L'Ateneo favorisce la partecipazione alle Federazioni di Autenticazione previste dall'ordinamento nazionale (SPID) o in uso sulle reti dell'università e della ricerca a livello nazionale, europeo e mondiale, quali ad esempio EDUROAM, che operano in una logica di identità federate.

4. La creazione di una identità digitale comporta un trattamento dei dati personali la cui liceità si basa sull'art 6 del Regolamento (UE) 2016/679.

Articolo 52 Titolari delle identità digitali

1. I titolari delle identità digitali sono tutti i soggetti che devono fruire dei servizi web di Ateneo.

2. I titolari delle identità digitali hanno l'onore e la responsabilità di adottare tutte le misure e comportamenti idonei per garantire l'integrità, la confidenzialità e la disponibilità delle identità nel tempo.
3. I servizi informatici erogati dall'Ateneo in collaborazione con soggetti terzi sono soggetti a condizioni e termini di servizio stabiliti con i relativi fornitori, di cui l'utente ne accetta i termini d'uso nel momento in cui accede al servizio.

Articolo 53 Credenziali servizi web di Ateneo

1. Le credenziali dei servizi web di Ateneo (account) sono il sistema di autenticazione principale per i servizi informatici erogati dall'Ateneo.
2. L'accesso ai servizi avviene mediante un codice di identificazione attribuito all'utente (username) e una parola chiave (password): firma elettronica semplice (FES).
3. La password dei servizi d'Ateneo può non coincidere con la password della posta elettronica.
4. L'utente deve modificare la propria password al primo utilizzo e, successivamente, almeno ogni 180 giorni o immediatamente nei casi in cui sia compromessa.
5. L'utente dovrà custodire diligentemente la propria password nonché adottare le necessarie cautele per preservarne la sicurezza e la segretezza. A ogni account sono associati dei diritti di accesso che dipendono dal ruolo dell'utente e dall'uso dell'account stesso.
6. La durata dell'account dipende dal tipo di rapporto in essere con l'Ateneo.

TITOLO VI - RESPONSABILITÀ E CONTROLLI

Articolo 54 Responsabilità individuali

1. I soggetti che utilizzano risorse informatiche e telefoniche devono rispettare le regole previste dal presente Regolamento e in particolare:

   a) mantenere una adeguata riservatezza dei dati;

   b) mantenere una adeguata riservatezza sulle misure di sicurezza adottate e sulle modalità di accesso ai servizi;

   c) utilizzare esclusivamente le risorse alla cui fruizione essi sono abilitati;

   d) segnalare ogni accertata violazione delle norme che regolano l'utilizzazione delle risorse informatiche e telefoniche.

Articolo 55 Controllo e accesso ai dati

1. L'Ateneo può utilizzare i dati relativi agli accessi ai propri sistemi informatici e telefonici, applicazioni, programmi, dati e transazioni da parte dei componenti la comunità universitaria per:

   a) motivi di sicurezza;

   b) la corretta gestione degli stessi dati e delle informazioni;

   c) la corretta gestione delle risorse informatiche e telefoniche;

   d) le statistiche d'uso relative ai sistemi informatici e telefonici;

   e) le attività relative a modifiche tecniche/operative;

   f) l'addebito dei costi relativi agli utilizzi informatici/telefonici alle strutture autonome. Tali accessi avverranno in conformità con le disposizioni del Garante per la Protezione dei Dati personali e in particolare delle "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)".

2. Nel pieno rispetto delle previsioni dell'art. 4, comma 2, della L. 300/70, i dati raccolti relativi agli accessi ai servizi informatici/telefonici non saranno in alcun caso utilizzati per controlli inerenti all'attività svolta dagli utilizzatori, né per fini diversi da quelli dichiarati nel presente regolamento esulano da ciò i trattamenti imposti da norme di legge nazionali e internazionali, nonché i trattamenti difensivi derivanti da comportamenti penalmente sanzionati.

3. Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la normale attività operativa, il personale incaricato avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni. Gli Amministratori di sistema possono, nei casi sopra indicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico (ad es. rimozione di file o applicazioni pericolosi).

4. Gli Amministratori di sistema sono altresì autorizzati ad accedere ai dati contenuti negli strumenti informatici restituiti dall'utente all'azienda per cessazione del rapporto, sostituzione delle apparecchiature, etc. e a cancellarne i contenuti.

Articolo 56 Controllo e monitoraggio dei log

1. Il monitoraggio e l'analisi dei *log* consentono di verificare il corretto funzionamento dei sistemi e di diagnosticare eventuali anomalie o abusi di servizi.

2. La raccolta e conservazione dei *log* è un obbligo di legge al fine di coadiuvare le autorità di Pubblica Sicurezza per l'indagine e la repressione dei reati informatici, ai sensi dell'art. 132 del D. Lgs. n. 196/2003 e s.m.i..
3. Qualunque struttura dell'Ateneo che, per obblighi di legge o regolamenti, è tenuta al mantenimento dei *log* deve trattarli conformemente alla normativa vigente.

4. Le strutture che raccolgo i *log* hanno l'obbligo di presentare all'utente l'informativa relativa alla gestione dei dati di traffico. Le copie di sicurezza delle registrazioni del traffico (file di log) delle consultazioni, contenenti la data, l'ora e gli estremi identificativi dell'utilizzatore e delle pagine Web visualizzate, effettuate per fini strettamente correlati alla gestione tecnica del servizio, sono conservate per un massimo di 365 giorni e nel rispetto della normativa vigente.

5. I sistemi di logging per il corretto esercizio del servizio di posta elettronica, conservano i soli dati esteriori, contenuti nella cosiddetta "envelope" del messaggio.

TITOLO VII - SANZIONI E DIRITTO DI DIFESA

Articolo 57 Sanzioni e diritto di difesa

1. Il personale che contravviene alle norme indicate nel presente regolamento e/o alle leggi vigenti, stanti le responsabilità individuali di tipo civile e penale verso terze parti offese, potrà essere oggetto di sanzioni di tipo disciplinare la cui entità e modalità di irrogazione saranno definite secondo la disciplina di stato giuridico propria della categoria cui appartiene il contravventore.

2. La contravvenzione alle presenti regole comporta l'applicazione delle disposizioni previste dal Codice Etico e dal Codice di Comportamento dell'Università, fermo restando l'obbligo dell'Ateneo di segnalare all'Autorità Giudiziaria eventuali violazioni a potenziale rilevanza penale.

3. Ai fini dell'esercizio del diritto di difesa, immediatamente dopo la contestazione, il materiale derivante dalla procedura di controllo sarà messo a disposizione dell'interessato.