ISTRUZIONI PER L'UTILIZZO DEGLI STRUMENTI AZIENDALI

RIFERIMENTI NORMATIVI:

- *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;*
- *Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) e successive modifiche e integrazioni;*
- ***Autorità Garante Privacy:*** *Lavoro: le linee guida del Garante per posta elettronica e internet Gazzetta Ufficiale n. 58 del 10 marzo 2007 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1387522;*
- ***Gruppo di lavoro sulla protezione dei dati - ARTICOLO 29:***
  - *Parere 8/2001 sul trattamento di dati personali nell'ambito dei rapporti di lavoro adottato il 13 settembre 2001 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1390186;*
  - *WP 55 Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro Adottato il 29 maggio 2002*
  - *Parere 2/2017 sul trattamento dati sul posto di lavoro adottato l'8 giugno 2017*

PREMESSE

Con il presente documento si intende portare a conoscenza di tutto il personale della Libera Università di Lingue e Comunicazione IULM (qui di seguito indicata per brevità **IULM** o **Titolare del trattamento**) incaricato di trattare dati personali, l'adozione di un disciplinare interno in materia di privacy, il quale regola, in particolare, il trattamento dei dati mediante strumenti aziendali, l'utilizzo della rete e della posta elettronica.

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete dai dispositivi, espone IULM e gli utenti a rischi di natura patrimoniale e a responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (come ad esempio la legge sul diritto d'autore e la normativa riguardante la privacy) con possibili ripercussioni sulla sicurezza e sull'immagine dell'Ateneo stesso.

Il disciplinare si applica a tutto il personale, compresi i lavoratori dipendenti, nonché a tutto il personale che a qualsiasi titolo - e quindi a prescindere dalla tipologia di rapporto contrattuale, - presti la propria attività lavorativa, anche saltuaria e/o consulenziale, presso la IULM, o che, per ragioni connesse all'espletamento delle proprie attività, risulti comunque autorizzato e abilitato all'uso, anche solo occasionale e/o temporaneo, delle risorse informatiche.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al **principio di diligenza e di correttezza,** comportamenti, questi, che normalmente si adottano nell'ambito dei rapporti di

lavoro, IULM ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Con specifico riguardo alla "Tutela del lavoratore":

> *" Le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell'uomo, può essere tracciata a volte solo con difficoltà. Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali."*

Scopo del presente Regolamento interno, quindi, è quello di organizzare il funzionamento e il corretto impiego degli strumenti elettronici e, in particolare, della posta elettronica e della navigazione in Internet da parte dei lavoratori, definendone le modalità d'uso. Ciò, tenendo conto dei diritti dei lavoratori e della disciplina in tema di relazioni sindacali, della normativa in materia di protezione dei dati personali, delle esigenze di tutela della sicurezza della disponibilità e dell'integrità dei sistemi informativi e dei dati, anche al fine di prevenire eventuali usi indebiti degli strumenti elettronici in parola.

Ulteriori scopi del presente Regolamento sono, da un lato, informare i lavoratori riguardo le finalità dei possibili controlli posti in essere a tutela della sicurezza della rete informatica e al fine di prevenire usi impropri degli strumenti da parte del personale e, dall'altro, sensibilizzare il medesimo personale su ulteriori aspetti, non meno rilevanti, relativi alla gestione dei sistemi informatici, quali il rispetto della normativa sulla tutela legale del software, e quella sulla tutela del know-how aziendale, quando queste importanti informazioni, di proprietà del titolare, sono custodite nel sistema informatico e informativo di Ateneo.

Secondo il testo dello statuto dei lavoratori (Legge 300/70) ART. 4. Impianti audiovisivi e altri strumenti di controllo

1. *Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale.*
2. *In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.*

3. *La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.*
4. *Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal Decreto Legislativo 30 giugno 2003, n. 196".*

SOMMARIO

0. Definizioni

Ai fini del presente Regolamento aziendale si intende per:

1) "**dato personale**", qualsiasi informazione riguardate 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, dati relativi all'ubicazione, un identificativo online, uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; **(C26, C27, C30)** [1].

2) "**trattamento**", qualunque 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;

3) "**limitazione di trattamento**", il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro; **(C67)**

4) "**profilazione**", qualsiasi forma di trattamento automatizzato di dati personali consistente nella valutazione di determinati aspetti relativi a una persona fisica, in particolare i dati sono utilizzati 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; **(C24, C30, C71-C72)**

5) "**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. Ciò 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; **(C26, C28-C29)**

6) "**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; **(C15)**

7) "**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,

[1] I codici si riferiscono ai "*considerandi*" che precedono l'articolazione del Reg. UE n. 679/2016.

il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; **(C74)**

8) "**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;

9) "**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 considerate 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; **(C31)**

10) "**terzo**", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, come il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) "**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, affinché i dati personali che lo riguardano siano oggetto di trattamento; **(C32, C33)**

12) "**violazione dei dati personali**", la violazione di sicurezza 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; **(C85)**

1. Utilizzo della postazione di lavoro

1.1 All'utente viene messa a disposizione una stazione di lavoro predisposta e configurata dall'Ufficio IT. **Ogni utilizzo della stessa non inerente all'attività lavorativa è vietato in quanto potenzialmente idoneo a innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza**. Gli strumenti della stazione di lavoro devono essere **custoditi con cura** evitando ogni possibile forma di danneggiamento.

La strumentazione messa a disposizione è configurata in modo tale da ridurre al minimo l'utilizzazione di dati personali e di dati identificativi e da escluderne il trattamento qualora le finalità perseguite nei singoli casi possano essere realizzate mediante dati anonimi o modalità che permettano di identificare l'interessato solo in caso di necessità.

1.3 L'infrastruttura tecnologica è a tutti gli effetti un bene dell'Università IULM.

1.4 La strumentazione data in affidamento all'utente permette **l'accesso alla rete dell'Ateneo solo attraverso specifiche credenziali di autenticazione** come meglio descritto al successivo punto 2 del presente Regolamento.

1.5 Il Titolare del trattamento rende noto che **il personale incaricato dell'Ufficio Information Technology**

(nel seguito per brevità "Ufficio IT") dell'Università IULM è stato autorizzato a compiere interventi nel sistema informatico e informativo diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware etc.). Detti interventi potranno anche comportare l'accesso, in caso di effettiva necessità, ai dati trattati da ciascuno, nonché la verifica riguardante i siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Università IULM, può essere esercitata, in caso di effettiva necessità, anche in caso di assenza prolungata o impedimento dell'utente.

Il personale incaricato dell'Ufficio IT ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza contro virus, spyware, malware, etc.. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità**,** a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso all'utente.

1.6 Salvo preventiva autorizzazione del personale dell'Ufficio IT**, non è consentito l'uso di programmi diversi da quelli ufficialmente installati per conto dell'Università IULM, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno**, sussistendo, infatti, il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone lo stesso Ateneo a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software, la quale impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

1.7 Salvo preventiva autorizzazione del personale dell'Ufficio IT, non è consentito all'utente di modificare le caratteristiche impostate e le configurazioni apportate, né di procedere ad installare dispositivi (come ad esempio masterizzatori, modem, etc.).

1.8 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale dell'Ufficio IT nel caso in cui fossero rilevati virus e adottando quanto previsto dal successivo punto 11 del presente Regolamento relativo alle procedure di protezione antivirus.

1.9 Premesso che lasciare incustodita la stazione di lavoro connessa alla rete può favorire l'utilizzo da parte di terzi, senza, tuttavia la possibilità di provare in seguito l'indebito uso, **si raccomanda di utilizzare la modalità manuale di blocco in ogni caso in cui si si allontana dalla propria postazione di lavoro**. La strumentazione informatica deve essere spenta ogni sera prima di lasciare gli uffici e in caso di assenze prolungate.

1.10 E' raccomandato che l'utente mantenga il proprio desktop ordinato, evitando di lasciare file isolati distribuiti sullo stesso, preferendo la creazione di cartelle e sotto cartelle suddivise a seconda della tipologia dei contenuti.

2. Gestione ed assegnazione delle credenziali di autenticazione

2.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale dell'Ufficio IT, previa comunicazione all'Ufficio IT da parte dell'Ufficio Risorse Umane a seguito della formalizzazione del rapporto contrattuale con l'Università IULM.

2.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dall'Ufficio IT, associato ad una parola chiave (password) riservata che dovrà essere custodita dall'incaricato con la massima diligenza e non divulgata.

2.3 La parola chiave, deve essere composta da almeno otto caratteri alfanumerici e non deve contenere riferimenti agevolmente riconducibili all'incaricato, inoltre deve essere diversa dalle ultime dodici inserite.

2.4 È necessario procedere alla **modifica della parola chiave** a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, **ogni tre mesi quando il sistema ne notifica la scadenza**.

2.5. Per evitare violazioni si consiglia di evitare l'utilizzo di username associati al dominio aziendale quando si accede a servizi interni di ogni tipo.

3. Utilizzo della rete del Titolare

3.1 Per l'accesso alla rete dell'Università IULM ciascun utente deve essere in possesso della specifica credenziale di autenticazione la quale non dovrà essere rivelata ad alcuno, neppure a colleghi o superiori.

3.2 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato.

3.3 Le cartelle utenti, dell'Università IULM, sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di amministrazione e back up da parte del personale dell'Ufficio IT. Si ricorda che **tutti i dischi o altre unità di memorizzazione locali non sono soggette a salvataggio da parte del personale incaricato dell' Ufficio IT, la responsabilità del salvataggio dei dati ivi contenuti è, pertanto, a carico del singolo utente.**

3.4 Il personale dell'Ufficio IT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà pericolosi per la Sicurezza dandone comunicazione all'utente che ne ha effettuato la creazione e/o l'inserimento.

3.5 Gli utenti si devono attenersi alle norme di comportamento sull'accesso alla rete pubblicate sul Portale IULM.

3.6 E' opportuno che, con regolare periodicità, ciascun utente provveda alla pulizia degli archivi digitali, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo, infatti, necessario evitare un'archiviazione ridondante.

4. Utilizzo di stampanti poste in rete

Al fine di assicurare la necessaria riservatezza delle informazioni pertinenti al singolo Ufficio, qualora gli utenti utilizzino una stampante in comune con Uffici diversi da quello di appartenenza devono utilizzare la **procedura di "stampa riservata".** Tale procedura prevede che la selezione della stampante e l'attivazione della richiesta di stampa avvenga dal PC della propria postazione ma il "rilascio" della stampa stessa avvenga - in propria presenza - mediante l'immissione sulla periferica del codice prescelto.

5. Utilizzo e conservazione dei supporti rimovibili

5.1 Tutti i supporti rimovibili, contenenti dati personali, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere violato.

5.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti rimovibili contenenti dati personali, ciascun utente dovrà contattare il personale dell'Ufficio IT e seguire le istruzioni da questo impartite.

5.3 In ogni caso, i supporti rimovibili contenenti dati personali devono essere adeguatamente custoditi dagli utenti in armadi chiusi e, nel caso siano portati esternamente all'Ateneo, protetti da password.

5.4 E' vietato l'utilizzo di supporti rimovibili personali senza esplicita autorizzazione.

5.5 L'utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

6. Utilizzo di PC portatili

6.1 L'utente è responsabile del PC portatile assegnatogli dall'Ufficio IT e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

6.2 Qualora i PC portatili siano utilizzati all'esterno (convegni, visite in azienda ecc.) devono essere **custoditi con diligenza,** adottando tutti i provvedimenti che le circostanze rendono necessari per evitare violazioni.

6.3 L'utente dovrà collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento Antivirus.

6.4 Tali disposizioni si applicano anche nei confronti di incaricati esterni.

6.5 Ai PC portatili si applicano le regole di utilizzo previste dal presente Regolamento con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna. La cancellazione di tutti i dati e file non necessari all'Università contenuti nel PC riconsegnato dal soggetto affidatario resta ad esclusivo carico del medesimo affidatario. Ogni eventuale responsabilità per violazione della normativa vigente in materia di tutela della privacy, derivante dall'omessa cancellazione dei dati contenuti nel PC restituito

dall'utente affidatario, resta a carico di quest'ultimo, fermi restando gli obblighi ricadenti in capo a IULM, ai sensi dal Provvedimento del Garante per la protezione dei dati personali, in materia di " Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008, *G.U. n. 287 del 9 dicembre 2008".*

7. Uso della posta elettronica

7.1 La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

7.2 **È fatto divieto di utilizzare le caselle di posta elettronica a dominio del Titolare del trattamento (anche se contenenti nome e/o cognome) per motivi diversi da quelli strettamente legati all'attività lavorativa.**

7.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti non compressi.

7.5 È obbligatorio **porre la massima attenzione nell'aprire i file attachments di posta elettronica prima del loro utilizzo (**non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

7.6 Al fine di garantire la funzionalità del servizio di posta elettronica e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, l'utente, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede) dovrà impostare la funzionalità che genera in automatico messaggi di risposta (out of office).

7.7 In casi eccezionali di particolare gravità e/o urgenza al fine di garantire la continuità operativa e di servizio dell'Ateneo, gli amministratori di sistema potranno consentire, previa espressa richiesta formale in forma scritta di un Responsabile di Ufficio e autorizzata dalla Direzione, l'accesso alle utenze di un incaricato temporaneamente assente o impedito ad accedere autonomamente. In questo caso si procederà alla cancellazione della password e all'inserimento di una nuova. Il cambiamento della password ad opera degli amministratori di sistema è garanzia, per l'utente, che è stato effettuato da terzi un accesso autorizzato.

7.8 Le email precedentemente archiviate nell'account del dipendente cessato potranno, tuttavia, essere consultate da un delegato degli Organi di Governo dell'Ateneo, qualora ciò si rivelasse necessario ai fini dell'espletamento delle funzioni e dei servizi dell'Università.

7.10 E' fatto divieto di divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica. In merito a tali informazioni, infatti, gli utenti sono tenuti al "segreto professionale" in ottemperanza agli obblighi di correttezza nei confronti del datore di lavoro.

7.11 Il personale dell'Ufficio IT, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 1.5.

7.12 Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, è raccomandabile che i *messaggi contengano l' avvertimento standardizzato*, sotto riportato, quale "firma mail in uscita". Il testo di tale messaggio non dovrà essere disattivato dall'utente:

Le informazioni contenute nella presente comunicazione e i relativi allegati possono essere riservate e sono, comunque, destinate esclusivamente alle persone o all'Ente sopraindicati e non sono da considerarsi comunicazioni personali, quindi eventuali risposte potranno essere conosciute da persone appartenenti all'Ente. La diffusione, distribuzione e/o copiatura del documento trasmesso da parte di qualsiasi soggetto diverso dal destinatario è proibita ai sensi dell'art. 616 c.p.. I dati forniti verranno utilizzati ai sensi dell'art. 13 del Reg EU 679/16 (normativa sulla privacy), anche tramite soggetti esterni, al fine di permettere l'espletamento degli adempimenti informativi, amministrativi e contabili connessi al rapporto contrattuale. Copia integrale dell'informativa potrà essere visionata presso le nostre sedi. Per non ricevere più comunicazioni di natura promozionale e newsletter sarà sufficiente scrivere in qualsiasi momento una e-mail all'indirizzo mail privacy@iulm.it con oggetto "cancellazione" e non sarà più disturbato.

Libera Università di Lingue e Comunicazione IULM - C.F. 80071270153 – P.IVA 07699170960

7.13. In caso di cessazione del rapporto con l'utente, l'indirizzo/gli indirizzi di posta elettronica assegnato/assegnati verranno immediatamente disabilitati. La conservazione delle email inviate e ricevute tramite la casella di posta elettronica avverrà nel rispetto dei principi di proporzionalità, necessità e limitazione della conservazione, secondo le tempistiche descritte dalla *Data Retention Policy* adottata dall'Ateneo, tenuto conto della funzione/mansione ricoperta in azienda e nel rispetto normativa vigente in tema di obblighi di conservazione della documentazione aziendale.

7.14 La conservazione delle mail inviate e ricevute da indirizzi email attivi avverrà nel rispetto dei principi di proporzionalità, necessità e limitazione della conservazione, secondo le tempistiche descritte dalla *Data Retention Policy* adottata dall'Ateneo, tenuto conto della funzione/mansione ricoperta in Università e nel rispetto della normativa vigente in tema di obblighi di conservazione della documentazione in accordo con il Manuale della Conservazione di Ateneo.

8. Navigazione Internet

8.1 Gli incaricati possono utilizzare la strumentazione informatica connessa ad Internet anche per la navigazione in rete, ove la funzione lo preveda e sotto la propria responsabilità. La navigazione deve comunque avvenire nel rispetto della legge, dell'ordine pubblico, del buon costume e delle norme di prudenza e cautela atte ad evitare problemi di sicurezza al sistema informativo dell'Ateneo.

8.2 A titolo puramente esemplificativo, l'utente **non potrà utilizzare** Internet per:

- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e/o musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale dell'Ufficio IT);
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione o

eventualmente dal Responsabile d'ufficio e/o dell'Ufficio IT e comunque nel rispetto delle normali procedure di acquisto;

- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio e dalla Direzione;
- accessi a connessioni anonime o connessioni cifrate che, non permettono l'identificazione dell'indirizzo di navigazione, o comunque a connessioni che esulano quelle autorizzate dal sistema.

9. Controlli

Gli eventuali controlli, compiuti dal personale incaricato dell'Ufficio IT (anche esterno) per la verifica di condotte illecite o anomalie di sistema, ai sensi del precedente punto 1.5, potranno avvenire attraverso sistemi (quali ad esempio firewall che consentono, oltreché la creazione di black list, blocchi e filtri, anche il monitoraggio della navigazione web effettuata da ciascun utente), e anche mediante verifica dei file log. Il trattamento sarà svolto in forma automatizzata e manuale, con modalità e strumenti volti a garantire la massima sicurezza e riservatezza, ad opera di soggetti appositamente incaricati a tali attività.

Sarà facoltà del Titolare, solo in caso di effettiva necessità, tramite il personale IT o tramite addetti esterni alla manutenzione dei sistemi informatici, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici lavorativi e ai documenti ivi contenuti.

Ai sensi e per gli effetti di cui all'art. 4 comma 3, L. n. 300/1970, l'Ateneo informa che il personale incaricato del servizio IT, ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC, ovvero dei Notebook, come anche di visualizzare le singole cartelle contenute sui predetti dispositivi e i relativi file, assieme alla cronologia della navigazione internet ed i messaggi di posta elettronica.

Il controllo con i sistemi sopra descritti non è continuativo ed è effettuato solo da personale appositamente incaricato per il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda. Sarà in ogni caso applicato il principio di liceità, proporzionalità e limitazione del trattamento.

10. Social Media Policy

L'Università IULM riconosce i benefici apportati dai social media, tuttavia, pur dichiarandosi favorevole al loro utilizzo, ritiene che l'utilizzo di questi canali di comunicazione possa presentare alcuni rischi.

Per tale motivo, con il presente Regolamento, si forniscono alcune indicazioni per un utilizzo responsabile degli stessi:

- è vietato l'utilizzo dei social network di natura personale e non lavorativa, durante l'orario di lavoro;

- sui social e nel web, non è consentito intervenire in qualità di portavoce ufficiale dell'Università IULM, qualora non si rivesta tale ruolo;
- non è consentita la pubblicazione di contenuti o materiali: coperti da riservatezza o segreto, offensivi, illegali, vessatori, diffamanti, , minacciosi, volgari, osceni, che ledano diritti di terzi e/o che incoraggino condotte contrarie alle vigenti normative, ai codici di condotta o simili.

Qualora ci si imbatta in commenti sul conto dell'Università IULM:

- se i commenti sono positivi: è consentito interagire liberamente, purché nel pieno rispetto delle regole sopra elencate;
- se i commenti sono negativi: evitare di rispondere e contattare il proprio superiore gerarchico;
- se i commenti hanno ad oggetto argomenti che richiedono competenze specifiche: evitare di rispondere e contattare il proprio superiore gerarchico;
- in caso di dubbio, non pubblicare e contattare il proprio superiore gerarchico.

11. Protezione antivirus

11.1 Il sistema informatico della IULM è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

11.2 **Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare prontamente l'accaduto al personale dell'Ufficio IT.**

11.3 Ogni dispositivo di provenienza esterna all'Università viene verificato dal programma antivirus prima del suo utilizzo se collegato al sistema. Inoltre, nel caso venga rilevato un virus, il dispositivo corrotto dovrà essere prontamente consegnato al personale del Ufficio IT.

11.4 Tutti i file contenenti software o eseguibili (inclusi file di testo e volantini) devono essere sottoposti ad un controllo antivirus e contrassegnati come esenti da virus, prima di essere consegnati a terze parti.

12. Utilizzo di telefoni fissi, Smartphone, Mobile Device ed equiparati, fax e fotocopiatrici

12.1 Il telefono fisso affidato all'utente è uno strumento di lavoro. Salvo esplicita autorizzazione, ne viene concesso l'uso esclusivamente ai fini dello svolgimento dell'attività lavorativa; non sono quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza.

12.2 Qualora venisse assegnato un Mobile Device aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al Mobile Device si applicano le medesime regole: in particolare, salvo esplicita autorizzazione, è vietato l'utilizzo messo a disposizione per inviare o ricevere SMS e/o MMS di

natura personale o comunque non pertinenti allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) è possibile soltanto in presenza di preventiva autorizzazione scritta ed in conformità delle istruzioni impartite dalla Direzione al riguardo.

12.3 È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile d'ufficio.

12.4 È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile d'ufficio.

12.5 Gli eventuali controlli, compiuti dal personale incaricato ai sensi del precedente punto 1.5 potranno avvenire mediante sistemi tecnologici e/o fatturazione del traffico telefonico e/o dati, in grado di verificare in particolare il chiamante, i tempi di conversazione e il numero chiamato.

13. Utilizzo del Servizio wireless dell'Università IULM

Per quanto attiene l'utilizzo del Servizio wireless dell'Università IULM si rimanda alle "Condizioni e norme di utilizzo del Servizio Wireless dell'Università IULM" pubblicate sul Portale dell'Ateneo.

14. Accesso ai dati trattati dall'utente

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/ sostituzione/ implementazione di programmi, manutenzione hardware, ecc.) o per finalità di verifica e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, ecc.), comunque estranei a finalità di controllo dell'attività lavorativa, è facoltà della Direzione tramite il personale dell'Ufficio IT o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali ed ai documenti ivi contenuti, nonché mediante sistemi tecnologici e/o fatturazione del traffico telefonico e/o dati.

15. Sistemi tecnologici e controlli

15.1 Il Datore di lavoro, considerato il divieto di utilizzo di strumenti tecnologici *preordinati* al controllo dell'attività lavorativa del dipendente, garantisce che tali strumenti saranno installati, se del caso, esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro, per la tutela del patrimonio aziendale , previa idonea informativa all'interessato (vedi punto 20).

15.2 Di seguito la tipologia dei controlli che potranno essere effettuati:

- controllo difensivo: in presenza di seri indizi, il personale incaricato potrà effettuare, attraverso i predetti sistemi tecnologici, controlli rivolti ad accertare condotte illecite del lavoratore (c.d. controllo difensivo del datore di lavoro), anche mediante verifica dei file log presenti sulla strumentazione informatica, qualora, con dette modalità, non si pregiudichi la sicurezza del sistema e del trattamento dati;

- controllo graduale: in caso di anomalie o malfunzionamenti, il personale incaricato effettuerà, mediante l'ausilio dei Sistemi installati, controlli anonimi che si concluderanno con avvisi generalizzati diretti agli incaricati dell'area o del settore in cui è stata rilevata l'anomalia. In tali avvisi sarà evidenziato l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite. In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

15. 3 Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie e ove ricorra una o più delle seguenti ipotesi:

- quando venga presentata una specifica richiesta di informazioni da parte dell'Autorità giudiziaria;
- quando si verifichi un evento dannoso o una situazione di pericolo che richiedano un immediato e necessario intervento.

15.4 dati raccolti dai predetti controlli potranno essere utilizzati per tutte le finalità connesse al rapporto di lavoro, nel rispetto della normativa privacy e statuto dei lavoratori vigente.

15.5 Sono presenti i seguenti strumenti tecnologici con potenziale controllo attività lavorativa art. 4 legge 300/70:

A. Firewall Proxy server e Antispam: sistemi di monitoraggio / tracciatura navigazione internet e della posta elettronica (Antispam). Il sistema Proxy potrà raccogliere tutti i dati personali, anche eventualmente particolari, presenti nella cronologia di navigazione internet effettuata tramite gli strumenti aziendali. Il sistema Antispam potrà permettere l'accesso alle seguenti tipologie di informazioni relativi alla casella di posta elettronica aziendale: mittente, data e ora ricevimento / invio email, oggetto.
B. Sistemi di telefonia fissa, mobile e sistemi VoIP che sono comprensivi di:
   - una piattaforma di gestione delle utenze telefoniche usata per la configurazione di nuove utenze, con l'attribuzione dei servizi di telefonia decisi per ciascuna tipologia di utente;
   - un secondo sistema grazie al quale l'Ateneo effettua il trattamento dei dati di traffico generati dalle centrali telefoniche nel quale gli stessi sono conservati ed ai quali è possibile accedere attraverso un sistema di analisi e controllo del traffico telefonico tramite il quale sono visualizzati i dettagli delle chiamate in uscita che il sistema provvede a memorizzare per un intervallo temporale di almeno 6 mesi.

15.6 Si veda l'informativa ex art. 13 Regolamento (UE) 2016/679 (punto 20) per i dettagli circa le modalità e le finalità del trattamento di dati e le altre informazioni previste.

16. Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti

del personale dipendente con provvedimenti disciplinari previsti dal vigente Contratto di lavoro del personale tecnico-amministrativo, nonché con tutte le azioni civili e penali consentite.

17. Aggiornamento e revisione

17.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento.

17.2 Il presente Regolamento è soggetto a revisione periodica, almeno triennale.

18. Entrata in vigore del Regolamento e pubblicità

18.1 Il nuovo Regolamento entrerà in vigore a partire dalla data di pubblicità dello stesso al personale.

18.2 Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

18.3 Il presente Regolamento, oltre ad essere affisso nella bacheca aziendale, e pubblicato.

19. Campo di applicazione del Regolamento

19. 1 Il presente Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Università a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.).

19.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, tirocinante, etc.) in possesso di specifiche credenziali di autenticazione.

20. Informativa Privacy ai sensi e per gli effetti di cui all'articolo 13, Reg. (UE) 2016/679

Con la presente siamo a fornire le dovute informazioni in ordine al trattamento dei dati personali, ai sensi dell'**art. 13 del Regolamento (UE) 2016/679** del Parlamento Europeo e del Consiglio del 27 aprile 2016 – Regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

1. IL TITOLARE DEL TRATTAMENTO, ai sensi dell'articolo 24 del Regolamento (UE) 2016/679 è la Libera Università di Lingue e Comunicazione IULM (di seguito anche "Università IULM") con sede in Milano, via Carlo Bo n. 1, nella persona del legale rappresentante pro-tempore.
L'Ateneo ha provveduto a nominare, ai sensi degli artt. 37 – 39 del Reg. UE 2016/679, il Responsabile della Protezione dei Dati (RPD/DPO-Data Protection Officer), reperibile al seguente indirizzo email: dpo.iulm@dpoprofessionalservice.it.

2.TIPOLOGIA DI DATI TRATTABILI
Dati personali relativi all'utilizzo del sistema informativo e strumenti aziendali.

3.FINALITÀ DEL TRATTAMENTO
I dati personali, ed eventualmente sensibili, saranno oggetto di trattamento per le seguenti finalità:

- esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali;
- sicurezza e tutela del patrimonio, compreso del sistema informativo aziendale e prevenzione dei reati

Le informazioni raccolte attraverso questi sistemi saranno utilizzabili a tutti i fini connessi al rapporto di lavoro, come da art. 4 legge 300/70

4. MODALITÀ DEL TRATTAMENTO – CONSERVAZIONE
Il trattamento sarà svolto in forma automatizzata e manuale, con modalità e strumenti volti a garantire la massima sicurezza e riservatezza, ad opera di soggetti di ciò appositamente incaricati in ottemperanza a quanto previsto dagli artt. 32 e ss. del Regolamento (UE) 2016/679.
I dati verranno o conservati per il tempo indispensabile per il corretto perseguimento delle finalità sopra elencate. Sarà in ogni caso seguito il principio di necessità, proporzionalità e limitazione del trattamento (art. 6 del Regolamento) in modo che la tenuta dei dati sia effettivamente congrua e giustificabile alla luce delle esigenze tecniche di gestione del sistema informatico.

5. AMBITO DI COMUNICAZIONE E DIFFUSIONE
I dati potranno essere comunicati a società contrattualmente legate alla Libera Università di Lingue e Comunicazione IULM al fine di ottemperare ai contratti o finalità connesse. I dati saranno trattati da incaricati, cioè da persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile. I dati potranno essere comunicati a terzi appartenenti alle seguenti categorie: - eventuali soggetti terzi e consulenti del lavoro ai fini di gestione del personale, nell'ambito di rapporti di assistenza e consulenza;- soggetti esterni alla amministrazione del sistema informativo e/o manutenzione occasionale del sistema informativo, quali: incaricati, responsabili informatici esterni e società che abbiano in outsourcing la tenuta dei dati informatici o la manutenzione hardware e software, in caso di necessità guasto o malfunzionamento; - soggetti che forniscono servizi per la gestione del sistema informativo usato dal titolare e delle reti di telecomunicazioni; - autorità competenti per adempimenti di obblighi di leggi e/o di disposizioni di organi pubblici, su richiesta. I soggetti appartenenti alle categorie suddette svolgono la funzione di Responsabile del trattamento dei dati, oppure operano in totale autonomia come distinti Titolari del trattamento. L'elenco dei responsabili è costantemente aggiornato e disponibile presso la sede del titolare.

6. NATURA DEL CONFERIMENTO E RIFIUTO Il conferimento dei dati è necessario per l'utilizzo dei sistema informativo e degli strumenti tecnologici del Titolare, in mancanza del conferimento, l'Università IULM potrà tuttavia trovarsi nell'impossibilità di farle utilizzare gli strumenti informatici aziendali.

7. DIRITTI DEGLI INTERESSATI

Lei potrà far valere i propri diritti come espressi dagli artt. 15, 16, 17, 18, 19, 20, 21, 22 del Regolamento UE 2016/679, rivolgendosi al Titolare al seguente contatto privacy@iulm.it. Lei ha il diritto, in qualunque momento, di chiedere al Titolare del trattamento l'accesso ai Suoi dati personali, la rettifica, la cancellazione degli stessi, la limitazione del trattamento. Inoltre, ha il diritto di opporsi, in qualsiasi momento, al trattamento dei suoi dati (compresi i trattamenti automatizzati, es. la profilazione) nonché alla portabilità dei suoi dati. Fatto salvo ogni altro ricorso amministrativo e giurisdizionale, se ritiene che il trattamento dei dati che la riguardano, violi quanto previsto dal Reg. UE 2016/679, ai sensi dell'art. 15 lettera f) del succitato Reg. UE 2016/679, Lei ha il diritto di proporre reclamo al Garante per la protezione dei dati personali e, con riferimento all'art. 6 paragrafo 1, lettera a) e art. 9, paragrafo 2, lettera a), ha il diritto di revocare in qualsiasi momento il consenso prestato. Nel caso di richiesta di portabilità del dato il Titolare del trattamento Le fornirà in un formato strutturato, di uso comune e leggibile, da dispositivo automatico, i dati personali che la riguardano, fatto salvo i commi 3 e 4 dell'art. 20 del Reg. UE 2016/679.

Data di aggiornamento informativa: 2 ottobre 2018