CONSIGLIO NAZIONALE DELL'ECONOMIA E DEL LAVORO

REGOLAMENTO SULL'UTILIZZO DELLE RISORSE INFORMATICHE E TELEFONICHE DEL CONSIGLIO NAZIONALE DELL'ECONOMIA E DEL LAVORO

**Ufficio Risorse umane, formazione,
transizione al digitale e sistemi informativi**

REGOLAMENTO
sull'utilizzo delle risorse informatiche e telefoniche del Consiglio Nazionale dell'Economia e del Lavoro

Prefazione

Estensori del Documento:

- Ufficio III - Gestione delle Risorse Umane e la formazione; per la transizione digitale e dei sistemi informativi; per la revisione delle procedure, dei modelli di lavoro e per la realizzazione del fascicolo informatico
- Data Protection Officer

Informazioni Privacy

Nel presente documento vengono illustrate procedure interne al CNEL, dove possono essere riportate informazioni di natura sensibile. In particolare, nomi degli utenti, username, numeri telefonici ed indirizzi mail.

Data	Versione	Autore	Note
25-08-2022	0.1	Ufficio III e DPO	Prima Stesura

SOMMARIO

Art. 1 - Finalità

1.1 Il presente Regolamento è volto a promuovere fra tutto il personale dipendente e nei collaboratori a qualunque titolo il corretto utilizzo degli strumenti informatici messi a disposizione del personale dall'Ente ed il pieno rispetto delle norme e regolamenti vigenti, in particolare di quelle contenute nel GDPR.

1.2 La presente regolamentazione non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro, ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali. È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. UE 679/2016.

1.3 Si vogliono fornire le indicazioni necessarie con l'obiettivo principale di evitare il verificarsi di qualsiasi abuso o uso non conforme, in un'ottica di prevenzione del rischio da perdita di informazioni e dati non solo personali.

Art. 2 - Definizioni

Backup: copia di riserva di un disco, di una parte del disco o di uno o più file su supporti di memorizzazione diversi da quello in uso.

Chat: servizio offerto da Internet, che permette mediante apposito software una 'conversazione' fra più interlocutori costituita da uno scambio di messaggi scritti che appaiono in tempo reale sul monitor di ciascun partecipante.

Chiave USB o **unità flash USB** o **penna USB** (anche in inglese USB flash drive, o pendrive): è una memoria di massa portatile di dimensioni molto contenute che si collega al computer mediante la porta USB.

Client: Computer o programma collegato ad un altro (computer o programma) a cui inoltra le richieste dell'incaricato.

Dati: l'insieme di informazioni di cui un dipendente o un collaboratore (a prescindere dal rapporto contrattuale con l'Ente) può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge.

Dati personali: 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 (art. 4 GDPR).

Dipendente: personale dell'ente assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio.

Dos (Denial of Service): è un attacco informatico che non consente agli utenti di accedere ai servizi offerti dalla rete o alle risorse del computer.

GDPR: General Data Protection Regulation - Regolamento Generale sulla Protezione dei Dati - Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

Incaricato: ogni dipendente, come sopra identificato, ed ogni consulente esterno che, nell'ambito dell'attività assegnatagli, tratta dati (nell'accezione di quanto in premessa) riferiti all'Ente ed è autorizzato dal titolare o dal Responsabile al trattamento dei dati personali.

LAN: è l'acronimo del termine inglese Local Area Network, in italiano rete locale.

Identifica una rete costituita da computer collegati tra loro, dalle interconnessioni e dalle periferiche condivise in un ambito fisico delimitato.

Malware: abbreviazione per malicious software (che significa letteralmente software malintenzionato, ma di solito tradotto come software dannoso), indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata.

Postazione di lavoro: luogo attrezzato per svolgere un'attività lavorativa dotato di personal computer ed eventuali altre unità hardware.

Proxy: server che funge da intermediario per le richieste da parte degli utenti che ricercano risorse su altri server.

Phishing: tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione mail.

NAS (Network Attached Storage): dispositivo che permette di memorizzare e condividere dati attraverso una rete Wi-Fi o cablata con altri dispositivi.

Repository: In un repository sono raccolti dati e informazioni in formato digitale, valorizzati e archiviati sulla base di metadati che ne permettono la rapida individuazione, anche grazie alla creazione di tabelle relazionali. Grazie alla sua peculiare architettura, un repository consente di gestire in modo ottimale anche grandi volumi di dati.

Rete locale: una Local Area Network (LAN) (in italiano rete locale) è una rete informatica di collegamento tra più computer, estendibile anche a dispositivi

periferici condivisi, che copre un'area limitata, come un'abitazione, una scuola, un'azienda o un complesso di edifici adiacenti.

Server: computer o programma a cui altri (computer o programmi) si collegano per l'elaborazione delle richieste dell'incaricato.

Strumenti Informatici: tutte le risorse informatiche utilizzate dal lavoratore, intendendo con ciò PC, notebook, tablet, smartphone, risorse, e-mail ed altri strumenti con relativi software e applicativi messi a disposizione dall'Ente per rendere la prestazione lavorativa;

Autorizzato: ogni incaricato, come sopra identificato che, nell'ambito dell'attività assegnatagli, utilizza credenziali di accesso a strumenti informatici per il trattamento di dati.

Utente: ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata come "incaricato del trattamento".

Virus: programma appartenente alla categoria dei malware che, una volta eseguito, infetta dei file in modo da arrecare danni al sistema, rallentando o rendendo inutilizzabile il dispositivo infetto.

Art. 3 - Principi generali

3.1 Il presente Regolamento intende fornire ai dipendenti e collaboratori, denominati anche incaricati o utenti, le indicazioni per una corretta e adeguata gestione delle informazioni, in particolare attraverso l'uso di strumenti informatici dell'Ente. Nell'utilizzo degli strumenti informatici e del patrimonio informativo dell'Ente il dipendente è tenuto ad usare la massima diligenza, nel rispetto

degli obblighi di cui agli articoli 2104 e 2105 del codice civile. Gli strumenti, le reti e le banche dati possono essere utilizzati esclusivamente per ragioni di servizio. Comportamenti difformi, potendo causare gravi rischi alla sicurezza ed alla integrità dei sistemi informativi, sono suscettibili di valutazione ai sensi del codice disciplinare di cui all'art.62 del CCNL - comparto Funzioni Centrali del 12.02.2018, e possono assumere rilevanza anche sotto il profilo penale.

3.2 L' Ente garantisce un adeguato aggiornamento in merito ai rischi, alle procedure operative, alla prevenzione dei danni e, più in generale, alle problematiche relative alla sicurezza in materia di trattamento dei dati. Ogni dipendente e collaboratore è tenuto a rispettare il Regolamento, che è reso disponibile tramite le modalità specificate all'art.16.

3.3 I dati personali e le altre informazioni dell'utente registrati negli strumenti informatici o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio. Per tutela del patrimonio si intende altresì la sicurezza informatica e la sicurezza delle informazioni. Tali informazioni sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, visto che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal GDPR.

3.4 È riconosciuto al datore di lavoro il potere di effettuare attività di monitoraggio, che nella fattispecie saranno svolte solo dall'Amministratore di Sistema o dal personale delegato dall'Amministratore di Sistema, sempre nel rispetto dei seguenti principi:

a) **il principio di necessità**, secondo cui i sistemi informativi e i programmi i nformatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e

6 del GDPR);

b) **principio di pertinenza e non eccedenza** secondo cui Il Titolare del trattamento deve trattare i dati personali "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza".

3.5 L'utente si attiene alle seguenti regole di trattamento:

a) non comunica a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, elementi e informazioni dei quali il dipendente /collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile del trattamento dell'Ufficio di appartenenza.

b) non estrae originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro.

c) non lascia incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni quando il dipendente/collaboratore si allontana dalla postazione di lavoro.

Art. 4 - Campo di applicazione

Il presente regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o di livello, nonché a tutti i collaboratori dell'Ente a prescindere dal rapporto contrattuale con lo stesso intrattenuto.

Art. 5 - Credenziali di accesso alle risorse informatiche

5.1 Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dall'Amministratore di Sistema, previa formale richiesta del Dirigente dell'ufficio nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori esterni la richiesta dovrà essere inoltrata direttamente dal Dirigente dell'Ufficio con il quale il collaboratore si coordina nell'espletamento del proprio incarico. La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell'utente ed elenco dei sistemi informativi per i quali deve essere abilitato l'accesso. Ogni successiva variazione delle abilitazioni di accesso ai sistemi informativi dovrà essere richiesta formalmente all'Amministratore di Sistema dal Dirigente di riferimento.

5.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (altresì nominati username, nome utente o userid), assegnato dall'Amministratore di Sistema, ed una relativa password. La password è personale e riservata e dovrà essere conservata e custodita dall'utente con la massima diligenza senza divulgarla.

5.3 La password deve essere di adeguata robustezza: deve essere composta da almeno 8 caratteri, formata da lettere maiuscole, minuscole, numeri e caratteri speciali. Non deve contenere riferimenti agevolmente riconducibili all'utente (username, nomi o date relative alla persona o ad un familiare).

5.4 È necessario procedere alla modifica della password a cura dell'utente al primo accesso e, successivamente, almeno ogni tre mesi.

5.5 Nel caso di cessazione del rapporto con il dipendente/collaboratore, il Dirigente dell'Ufficio di riferimento dovrà comunicare formalmente e preventivamente all'Amministratore di Sistema la data effettiva a partire dalla quale le credenziali saranno disabilitate.

Art. 6 - Utilizzo della infrastruttura di rete

6.1 Per l'accesso agli strumenti informatici dell'Ente attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo quanto previsto dall'art. 5.

6.2 È assolutamente proibito accedere alla rete ed ai sistemi informativi utilizzando credenziali di altre persone.

6.3 L'accesso alla rete garantisce all'utente la disponibilità di condivisione di rete (cartelle su server) nelle quali vanno inseriti e salvati i files di lavoro, organizzati per Ufficio o per diversi criteri o per obiettivi specifici di lavoro. Gli strumenti Informatici e tutte le cartelle di rete possono ospitare esclusivamente contenuti professionali. Pertanto, non è consentito il salvataggio sui server dell'Ente, ovvero sugli strumenti informatici, di documenti non inerenti all'attività lavorativa. Ogni materiale personale rilevato dall'Amministratore di Sistema a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche sugli strumenti informatici viene rimosso secondo le regole previste dal presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare.

6.4 Tutte le risorse di memorizzazione, diverse da quelle citate al punto precedente, non sono sottoposte al controllo regolare dell'Amministratore di Sistema e non sono oggetto di backup periodici. A titolo meramente esemplificativo e non esaustivo si citano: il disco C: o altri dischi locali dei singoli PC, la cartella "Documenti" o "Desktop" dell'utente, gli eventuali dispositivi di memorizzazione locali o nella disponibilità personale come hard disk portatili o NAS ad uso esclusivo. Pertanto, la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.

6.5 A meno di espressa autorizzazione e per ragioni di servizio da parte del

Dirigente dell'Ufficio di appartenenza, non è consentito trasferire documenti elettronici dai sistemi informativi e strumenti dell'Ente a device esterni (hard disk, chiavi USB, CD, DVD e altri supporti).

6.6 Senza il consenso dell'Amministratore di Sistema è vietato salvare documenti elettronici dell'Ente (ad esempio pervenuti via mail o salvati sul Server o sullo strumento informatico in dotazione) su repository esterne (quali ad esempio Dropbox, Google Drive, OneDrive, WeTransfer, ecc.) ovvero inviandoli a terzi via posta elettronica o con altri sistemi. In caso di necessità l'Ente dovrà mettere a disposizione modalità in linea con le presenti direttive.

6.7 Con regolare periodicità (almeno una volta al mese), ciascun utente provvede alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6.8 All'interno delle sedi lavorative è resa disponibile anche una rete senza fili, c.d. "WiFi". Tali reti consentono l'accesso alle risorse e ad internet per i dispositivi non connessi alla rete LAN mediante cavo. L'accesso mediante rete WiFi viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente ed in occasione di convegni a relatori e partecipanti che necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari dell'Ente che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse. L'impostazione della connessione WiFi sarà effettuata dall'Amministratore di Sistema.

6.9 L'Amministratore di Sistema si riserva la facoltà di negare o interrompere l'accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la

sicurezza informatica.

Art. 7 - Utilizzo degli strumenti informatici

L'utente è consapevole che gli strumenti informatici forniti sono di proprietà dell'Ente e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa. Ogni dipendente/collaboratore è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Ciascun utente si deve quindi attenere alle seguenti regole di utilizzo degli strumenti informatici:

a) l'accesso agli strumenti informatici è protetto da password; per l'accesso devono essere utilizzati Username e password assegnate dall'Amministratore di Sistema. A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza.

b) Gli strumenti informatici devono essere custoditi con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente all'Amministratore di Sistema ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione della password di accensione (BIOS), senza preventiva autorizzazione da parte dell'Amministratore di Sistema.

c) Non è consentito all'utente modificare le caratteristiche hardware e software impostate sugli Strumenti assegnati, salvo preventiva autorizzazione da parte dell'Amministratore di Sistema.

d) L'utente è tenuto a scollegarsi dal sistema e a bloccare l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la postazione di lavoro (PC) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima.

e) Non è consentita l'installazione di programmi diversi da quelli autorizzati dall'Amministratore di Sistema.

f) È obbligatorio consentire l'installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC sempre protetto.

g) Non è consentito utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione di opere protette da copyright.

h) Non è consentito l'utilizzo di supporti di memoria (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli strumenti, salvo che il supporto utilizzato sia stato fornito dall'Amministratore di Sistema. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative.

i) Non è consentito connettere al PC qualsiasi periferica non autorizzata preventivamente dall'Amministratore di Sistema (ad esempio, ma non limitatamente a, smartphone, fotocamere, webcam, stampanti).

j) Non è consentito connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, stampanti, etc.) non autorizzato preventivamente dall'Amministratore di Sistema.

k) Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, l'utente è tenuto a comunicarlo tempestivamente all'Amministratore di Sistema.

l) Salvo che la postazione di lavoro non debba essere utilizzata da remoto per scopi lavorativi e non sia possibile successivamente procedere alla sua accensione in tempo utile per il suo utilizzo da remoto, la stessa postazione di lavoro deve essere sempre spenta prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. È fatto divieto di disabilitare in tutte le postazioni le funzionalità di "stand-by" e/o di autospegnimento. L'operazione è consentita limitatamente all'unità centrale per i computer fissi ed esclusivamente nella stessa casistica di cui al punto precedente.

Art. 8 - Utilizzo di internet

8.1 Ciascun dipendente /collaboratore si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi:

a) è ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa, ad es. i siti istituzionali delle PP.AA., di fornitori e partners. L'accesso è regolato dal proxy con le sue policy di sicurezza debitamente implementate e aggiornate.

b) Non è consentito compiere azioni che siano potenzialmente in grado di arrecare danno all'Ente, ad esempio, il download o l'upload di file audio e/o video, l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa.

c) Non è consentito il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dagli Amministratori di Sistema.

d) Non è consentito l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dal Titolare e dall'Amministratore di Sistema, con il rispetto delle normali procedure di acquisto.

e) Non è consentito la partecipazione a Forum non professionali, ai Social Network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

8.2 L'Ente si riserva di bloccare l'accesso a siti "a rischio" attraverso l'utilizzo di blacklists pubbliche in continuo aggiornamento e di predisporre filtri, basati su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri, suscettibili di agevolare attacchi DOS o di scaricare malware. In caso di blocco accidentale di siti di interesse, potrà contattare l'Amministratore di Sistema per uno sblocco selettivo.

8.3 Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri, è necessario richiedere lo sblocco mediante una mail indirizzata all'Amministratore di Sistema, ed in copia al Titolare del trattamento, nella

quale siano indicati chiaramente: motivo della richiesta, utente e postazione da cui effettuare la navigazione libera, intervallo di tempo richiesto per completare l'attività. Al termine dell'attività l'Amministratore di Sistema ripristinerà i filtri alla situazione iniziale.

8.4 È consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati dall'Amministratore di Sistema. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche ed e-mail. È consentito un utilizzo legato esclusivamente a scopi professionali.

8.5 Per motivi tecnici e di corretto funzionamento del sistema informatico è buona norma, salvo comprovata necessità, non accedere a risorse web che impegnino in modo rilevante banda, come a titolo esemplificativo: filmati o web radio, in quanto possono limitare e/o compromettere l'uso della rete da parte degli altri utenti.

Art. 9 - Utilizzo della posta elettronica

Ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo dell'indirizzo di Posta elettronica:

a) ad ogni utente viene fornito un account e-mail nominativo, coerente con il modello (**ncognome@cnel.it**). L'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi lavorativi, ed è assolutamente vietato ogni utilizzo di tipo privato. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa;

b) l'iscrizione a mailing-list o newsletter esterne con l'indirizzo ricevuto è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio;

c) allo scopo di garantire sicurezza alla rete, evitare di aprire messaggi di posta

in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito, oppure che contengano allegati di tipo ***.exe**, ***.com**, ***.vbs**, ***.htm**, ***.scr**, ***.bat**, ***.js** e ***.pif**. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi informatiche. In qualunque situazione di incertezza è necessario contattare l'Amministratore di Sistema per una valutazione dei singoli casi;

d) non è consentito l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo;

e) nel caso fosse necessario inviare allegati "pesanti" (fino a 10MB) è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti. Nel caso di allegati ancora più voluminosi è necessario rivolgersi all'Amministratore di Sistema.

f) Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittografia con apposito software (archiviazione e compressione con password). La password di cifratura deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati. Tutte le informazioni, i dati personali e/o sensibili di competenza possono essere inviati soltanto a destinatari - persone o Enti – qualificati e competenti;

g) non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, è raccomandabile utilizzare un messaggio "Out of Office" facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo preferibilmente di tipo collettivo, rivolgersi all'Amministratore di Sistema per tale eventualità;

h) in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione auto-reply o l'inoltro automatico su altre caselle e si debba conoscere il

contenuto dei messaggi di posta elettronica, il titolare della casella di posta ha la facoltà di delegare un altro dipendente (fiduciario) per verificare il contenuto di messaggi e per inoltrare al Titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del Dirigente assicurarsi che sia redatto un verbale attestante quanto avvenuto e che si sia informato il lavoratore interessato alla prima occasione utile;

i) la diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti al servizio, su autorizzazione del Dirigente competente. Per evitare che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo ed indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn) se la tipologia del messaggio lo consente;

j) la casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell'allegato sulle condivisioni;

k) i messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l'eliminazione dello spam. I messaggi che dovessero contenere virus vengono eliminati dal sistema e il mittente/destinatario viene avvisato mediante messaggio specifico.

Art. 10 - Utilizzo dei telefoni, cellulari, fax, fotocopiatrici, scanner e stampanti

10.1 Il dipendente è consapevole che gli strumenti di stampa, così come anche il telefono, i cellulari assegnati sono di proprietà dell'Ente e sono resi disponibili all'utente per rendere la prestazione lavorativa ed esclusivamente per tale fine.

10.2 Il telefono e/o il cellulare assegnato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavora-

tiva e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti all'attività lavorativa stessa a meno dell'esistenza di contratti del tipo "*dual billings*". La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza.

10.3 Qualora venisse assegnato un cellulare all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone si applicano le medesime regole sopra previste per gli altri dispositivi informatici. Per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica è raccomandato il rispetto delle regole per una corretta navigazione in Internet di cui all'art.8 del presente regolamento, se consentita.

10.4 Per gli smartphone è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate dall'Amministratore di Sistema.

10.5 Non è consentito l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, fatta salva esplicita autorizzazione da parte del Dirigente dell'Ufficio di appartenenza.

10.6 Non è consentito l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Dirigente dell'Ufficio di appartenenza.

10.7 Per quanto concerne l'uso delle stampanti, gli utenti sono tenuti a:

a) stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative;

b) prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili);

c) prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi.

d) nel caso in cui si rendesse necessaria la stampa di informazioni riservate l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni a persone terze non autorizzate.

Art. 11 - Assistenza agli utenti

11.1 L'Amministratore di Sistema può accedere ai dispositivi informatici sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

- verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale.
- verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete.
- richieste di aggiornamento software e manutenzione preventiva hardware e software.

11.2 Gli interventi tecnici possono avvenire previo consenso dell'utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, l'Amministratore di Sistema è autorizzato ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

11.3 L'accesso in teleassistenza sui PC della rete richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Amministratore di Sistema, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.

11.4 Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o l'Amministratore di Sistema devono presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al

presente regolamento.

Art. 12 - Controllo sugli strumenti informatici

12.1 L'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. Il Titolare del trattamento, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2, L. 300/1970), di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinino un trattamento di dati personali riferiti o riferibili ai lavoratori. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. I controlli devono essere effettuati nel rispetto dei principi di cui all'art. 3 del presente regolamento.

12.2 L'uso degli strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite dell'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.).

Gli interventi di controllo, di seguito descritti, possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli strumenti in dotazione:

a) ***Controlli per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi***

(ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, ecc.) - Qualora risulti necessario l'accesso agli Strumenti informatici ed alle informazioni ivi contenute, il Responsabile del trattamento dei dati personali per il tramite dell'Amministratore di Sistema, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo:

- avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento;
- successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare il personale addetto al controllo a rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP, dell'utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite;
- qualora il rischio di compromissione del sistema informativo sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali sopra descritti, il Responsabile del Trattamento, unitamente all'Amministratore di Sistema, potrà intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia prendendo tutte le misure tecnicamente necessarie alla soluzione del problema.

b) ***Controlli per esigenze produttive e di organizzazione.***

Per esigenze produttive e di organizzazione si intendono – fra le altre – l'urgente ed improrogabile necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un Utente (quali file salvati, posta elettronica, chat, SMS, ecc) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato. Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni il

Responsabile del trattamento dei dati personali, per il tramite dell'Amministratore di Sistema, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo):

- redazione di un atto da parte del Dirigente dell'Ufficio competente che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
- incarico all'Amministratore di sistema di accedere alla risorsa con credenziali di Amministratore oppure tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'Utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.
- redazione di un verbale che riassuma i passaggi precedenti.

In ogni caso, l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro. Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal GDPR.

Art. 13 - Conservazione dei dati

13.1 In riferimento agli articoli 5 e 6 del GDPR e in applicazione dei principi di diritto di accesso, legittimità, proporzionalità, sicurezza, accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet e dal traffico telematico (log di sistema e del server proxy), la cui conservazione non sia necessaria, sono cancellati entro al massimo 365 giorni dalla loro produzione.

13.2 In casi eccezionali, quali ad esempio per esigenze tecniche o di sicurezza, per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o all'obbligo di custodire o consegnare i dati per ottemperare

ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria, è consentito il prolungamento dei tempi di conservazione, limitatamente al soddisfacimento delle esigenze sopra esplicitate.

13.3 L'Ente si impegna ad applicare le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal vigente quadro normativo.

Art. 14 - Partecipazione a Social Media

14.1 L'utilizzo a fini promozionali e commerciali di Facebook, Twitter, Linkedin, dei blog e dei forum, anche professionali, (ed altri siti o social media) è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

14.2 Fermo restando il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro.

14.3 La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni considerate dall'Ente riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in svolgimento presso gli uffici. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'Ente. L'utente, nelle proprie comunicazioni, non potrà quindi

inserire il nominativo e il logo dell'Ente, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione del Titolare.

14.4 L'utente deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali di colleghi e in genere di collaboratori, se non con il preventivo personale consenso di questi, e comunque non potrà postare nei social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro, se non con il preventivo consenso del Responsabile al trattamento dei dati personali.

14.5 Qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Ente, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ente.

Art. 15 - Norme finali

La pubblicazione del presente Regolamento, avverrà nelle seguenti forme: trasmissione per posta elettronica interna a tutti i Dirigenti, a tutti i dipendenti, mediante affissione nei luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 della L. 300/1970 (c.d. Statuto dei lavoratori).

Francesco
Tufarelli
24.04.2023
10:00:09
GMT+00:00

Francesco TUFARELLI
Segretario Generale


REPUBBLICA ITALIANA
CNEL
CONSIGLIO NAZIONALE ECONOMIA E LAVORO