



**FEDERAZIONE NAZIONALE
DEGLI ORDINI
DEI CHIMICI E DEI FISICI**



**DISCIPLINARE
PER L'UTILIZZO
DI
PERSONAL COMPUTER, DISPOSITIVI
ELETTRONICI, POSTA
ELETTRONICA E INTERNET**

SOMMARIO

Introduzione, definizioni e finalità

1. Principi generali
2. Ambito di applicazione
3. Interessi e rischi
4. Responsabilità personale dell'Utente
5. Nomina dell'Amministratore di sistema
6. Regole relative all'utilizzo della postazione di lavoro (PC), dei personal computer portatili, telefoni
7. Utilizzo dei supporti magnetici
8. Utilizzo della stampante/scanner e altre apparecchiature
9. Utilizzo della rete informatica
10. Protezione antivirus
11. Regole applicabili all'utilizzo di posta elettronica
12. Gestione della casella di Posta Elettronica di un Lavoratore cessato dal servizio. Disattivazione dell'account.
13. I controlli
14. II controlli non autorizzati
15. Informativa agli Utenti
16. Responsabilità e sanzioni
17. Norme finali
18. Aggiornamento e revisione del Disciplinare

ALLEGATO A

CONTROLLI EFFETTUATI

1. Internet
2. Posta elettronica

Introduzione, definizioni e finalità

L'esigenza della Federazione Nazionale degli Ordini dei Chimici e dei Fisici di adottare un Disciplinare per l'utilizzo dei personal computer fissi e portatili, dei dispositivi elettronici in generale (quali a titolo esemplificativo ma non esaustivo fax, fotocopiatrici, scanner, masterizzatori, telefoni fissi, *pen drive* e supporti di memoria), della posta elettronica e internet nasce dal ricorso sempre più frequente dell'utilizzo di tali strumenti nell'organizzazione e nell'espletamento dell'attività lavorativa. L'utilizzo di tali indispensabili risorse deve avvenire nell'ambito del generale contesto di diligenza, fedeltà e correttezza che caratterizza il rapporto lavorativo tra l'Ente e i propri dipendenti e adottando tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose che un utilizzo non avveduto di tali strumenti può condurre, anche in considerazione della difficoltà di tracciare una netta linea di confine tra l'attività lavorativa e la sfera personale e la vita privata del lavoratore e dei terzi che interagiscono con quest'ultimo.

Il presente Disciplinare, è stato predisposto sulla base e secondo le indicazioni contenute nella circolare AGID del 18/04/2017 (disposizioni in materia di sicurezza informatica), nel Regolamento UE 2016/679 del 27/04/2016 (GDPR - regolamento generale sulla protezione dei dati), nel D.lgs. n. 196/2003 come modificato ed integrato dal D.lgs. n. 101/2018, nelle "Linee guida del Garante per la Protezione dei Dati personali per posta elettronica e internet" (Deliberazione n. 13 del 1° marzo 2007). Ha per oggetto i criteri e le modalità di utilizzo del servizio di posta elettronica ed internet e, più in generale, delle dotazioni informatiche dell'Ente da parte dei propri dipendenti, collaboratori e consiglieri che, a vario titolo, svolgono un'attività per conto della Federazione accedendo al suddetto sistema informatico (di seguito, "utenti").

L'insieme delle norme comportamentali ivi incluse, pertanto, è volto a conformare l'Ente ai principi di diligenza, informazione e correttezza nell'ambito dei rapporti di lavoro, con l'ulteriore finalità di prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano.

A tal fine, pertanto, si rileva che gli eventuali controlli ivi previsti escludono finalità di monitoraggio sistematico, diretto ed intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al Decreto Legislativo n. 196/2003, modificato dal D.lgs. n. 101/2018 (in seguito "**Codice Privacy**"), alla Legge n. 300/1970 (in seguito "**Statuto dei Lavoratori**") e s.m.i. ed ai provvedimenti appositamente emanati dall'Autorità Garante per la Protezione dei Dati Personali (si veda in particolare Provv. 1° marzo 2007 e 1° febbraio 2018) e al Regolamento Europeo n. 679 del 2016 (in seguito "**GDPR**").

Il presente regolamento, è stato adottato, previa delibera n. X0004_18 del 19 dicembre 2018 dal Consiglio della Federazione Nazionale degli Ordini dei Chimici e dei Fisici, e disciplina le modalità di accesso e di uso delle strumentazioni, della rete informatica, telematica e dei servizi che, tramite la rete stessa, è possibile ricevere o offrire all'interno e all'esterno per dare il supporto informativo documentario alla ricerca, alla didattica, all'aggiornamento e alle attività collaborative tra Ordini territoriali, nonché per tutti gli adempimenti amministrativi di legge.

I dipendenti e i consiglieri della Federazione Nazionale degli Ordini dei Chimici e dei Fisici saranno informati tramite apposita circolare e il Regolamento sarà reso disponibile anche sul sito intranet della Federazione.

Il Disciplinare potrà essere aggiornato ogniqualvolta se ne presenti l'opportunità e di tali revisioni sarà data tempestiva comunicazione ai dipendenti. È responsabilità di tutti i soggetti che utilizzano PC ed altri dispositivi elettronici, la posta elettronica e internet messi a disposizione della Federazione, applicare e rispettare puntualmente il presente Disciplinare.

1. Principi generali

Il Disciplinare è adottato per assicurare la funzionalità e il corretto impiego dei personal computer fissi e portatili, dei dispositivi elettronici, della posta elettronica e di internet da parte dei lavoratori: a tal fine, definisce le modalità d'uso di tali strumenti nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali. Il luogo di lavoro è una formazione sociale nella quale è 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.

La Federazione prevede l'utilizzo delle strumentazioni informatiche, della rete internet e della posta elettronica quali strumenti utili a perseguire le proprie finalità istituzionali e prevede che lo stesso si conformi ai seguenti principi:

- principio di necessità e minimizzazione: i sistemi informativi e i programmi informatici vengono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;
- principio di correttezza: le caratteristiche essenziali dei trattamenti sono rese note agli utenti;
- principio di pertinenza e non eccedenza: i trattamenti sono effettuati per finalità determinate;
- Principio di trasparenza: si accompagna ed è coerente con quanto previsto dall'art 4 dello Statuto dei Lavoratori.

2. Ambito di applicazione

La rete informatica della Federazione è costituita dall'insieme delle risorse informatiche, cioè:

- dalle componenti hardware/software e dagli apparati elettronici collegati alla rete informatica della Federazione,
- dall'insieme delle banche dati in formato digitale ed in generale di tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

Il presente Disciplinare si applica a tutti i Lavoratori:

- a) dipendenti, responsabili e consiglieri, a qualsiasi titolo inseriti nell'organizzazione e nello statuto dell'Ente, senza distinzione di ruolo e/o mansione.
- b) collaboratori dell'Ente a prescindere dal rapporto contrattuale intrattenuto con la stessa.

3. Interessi e rischi

Le risorse informatiche e telematiche, messe a disposizione dall'Ente, devono essere utilizzate in modo responsabile e ispirato ai principi di diligenza e correttezza.

Per l'Ente l'utilizzo improprio, da parte del Lavoratore di Posta Elettronica, Fax, mail, Internet e telefoni, può pregiudicare il regolare funzionamento delle installazioni tecniche o altri beni o interessi meritevoli di tutela e/o giuridicamente protetti, fra cui:

- a) economie dei costi;
- b) la capacità di memoria utilizzabile dei server o l'ampiezza di banda disponibile per il collegamento in rete;

- c) sicurezza delle applicazioni e dei dati (disponibilità, integrità, confidenzialità);
- d) produttività sul lavoro;
- e) la reputazione o l'immagine dell'Amministrazione;

Per il Lavoratore, i rischi derivanti dall'utilizzo di Posta Elettronica, Fax, mail, Internet e telefoni riguardano:

- a) la protezione dei dati personali, propri e di terzi, poiché i predetti strumenti lasciano "tracce" del loro uso;
- b) la possibilità che la Federazione, in fase di eventuale legittimo controllo, venga a conoscenza di dati od opinioni personali del Lavoratore;
- c) relativamente all'uso di Posta Elettronica e di Internet, l'introduzione di virus, worm, o installazioni di programmi estranei nel computer utilizzato dal Lavoratore, con conseguente perdita di tutti o parte dei file salvati sul medesimo computer.

4. Responsabilità personale dell'utente

Ogni utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dalla Federazione nonché dei relativi dati trattati per finalità aziendali.

A tal fine ogni utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con la Federazione, è tenuto a tutelare (per quanto di propria competenza) il patrimonio "informatico" da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse.

Ogni utente, pertanto, è tenuto, in relazioni al proprio ruolo e alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica, riportando al Presidente e senza ritardo, eventuali rischi di cui è a conoscenza ovvero violazioni del presente Regolamento interno.

5. Nomina dell'Amministratore di sistema

La Federazione conferisce all'Amministratore di sistema il compito di sovrintendere alle risorse informatiche della Federazione assegnandogli in maniera esclusiva le seguenti attività:

- a) gestione dell'hardware e del software (installazione, aggiornamento, rimozione) di tutte le strutture tecniche informatiche dell'istituto, siano esse collegate in rete o meno;
- b) configurazione dei servizi di accesso alla rete interna, ad internet e a quelli di posta con creazione, attivazione e disattivazione dei relativi account;

- c) attivazione della password di accensione;
- d) controllo del corretto utilizzo delle risorse di rete, dei computer e degli applicativi, durante le normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- e) rimozione sia sui PC degli incaricati sia sulle unità di rete, di ogni tipo di file o applicazione che può essere pericoloso per la sicurezza o costituisce violazione del presente regolamento;
- f) distruzione delle unità di memoria interne alla macchina (hard - disk, memorie allo stato solido) ogni qualvolta si procederà alla dismissione di un PC e dei supporti removibili consegnati a tale scopo dagli utenti;
- h) utilizzo delle credenziali di amministrazione del sistema per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di indispensabile ed indifferibile necessità di intervento per prolungata assenza, irrintracciabilità o impedimento dello stesso, solo per il tempo necessario al compimento di attività indifferibili e solo su richiesta del Titolare del trattamento.

L'Amministratore di sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, ha facoltà di accedere in qualunque momento, anche da remoto, e dopo aver richiesto l'autorizzazione all'utente interessato, al PC di ciascun utente.

Le attività di gestione e manutenzione dei Personal Computer dell'Ente fanno capo all' Amministratore di Sistema e non è permesso agli utenti di intervenire personalmente sulle apparecchiature informatiche.

6. Regole relative all'utilizzo della postazione di lavoro (PC) e dei personal computer portatili

Gli utenti utilizzano per il proprio lavoro soltanto computer di proprietà della Federazione di cui sono responsabili, salvo eccezioni autorizzate dal datore di lavoro e dall'Amministratore di sistema.

Sono tenuti a:

- applicare al PC portatile le regole di utilizzo previste per i PC connessi in rete,
- custodirlo con diligenza e in luogo protetto durante gli spostamenti,
- rimuovere gli eventuali file elaborati sullo stesso prima della sua riconsegna,
- non disattivare sul PC lo screen saver e la relativa password,
- conservare la password nella massima riservatezza e con la massima diligenza,

- non modificare la configurazione hardware e software del PC se non esplicitamente autorizzati dall'amministratore di sistema,
- non rimuovere, danneggiare o asportare componenti hardware,
- nel caso il software antivirus rilevi la presenza di un virus, sospendere immediatamente ogni elaborazione in corso, senza spegnere il PC e segnalare prontamente l'accaduto al personale incaricato dell'assistenza tecnica,
- permettere l'autoaggiornamento del PC, prestare la massima attenzione ai supporti di origine esterna (es. pendrive), verificando preventivamente, tramite il programma antivirus, ogni file acquisito attraverso qualsiasi supporto e avvertendo immediatamente l'Amministratore di sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti,
- non lasciare incustodita e accessibile la propria postazione una volta eseguita la connessione al sistema con le proprie credenziali di autenticazione,
- non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a persone non autorizzate, in particolar modo per quanto riguarda l'accesso ad internet e ai servizi di posta elettronica,
- spegnere il PC al termine del lavoro o in caso di assenze prolungate dalla propria postazione.

7. Utilizzo di supporti magnetici

Gli utenti devono trattare con particolare cura i supporti magnetici (dischetti, nastri, DAT, chiavi USB, CD riscrivibili,) in particolar modo quelli riutilizzabili, per evitare che persone non autorizzate possano accedere ai dati ivi contenuti. Di conseguenza le azioni da compiere obbligatoriamente sono le seguenti:

- a) porre attenzione nell'utilizzo dei supporti rimovibili personali,
- b) custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto (presso il custode delle password),
- c) consegnare i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili, ...) obsoleti all'Amministratore di sistema per l'opportuna distruzione onde evitare che il loro contenuto possa essere, successivamente alla cancellazione, recuperato.

8. Utilizzo della stampante/scanner e altre apparecchiature

Stampanti e materiali di consumo in genere (carta, inchiostro, toner, supporti digitali come CD e DVD) possono essere usati esclusivamente per compiti di natura strettamente istituzionale, evitando in ogni modo sprechi e utilizzi eccessivi.

Gli utenti devono effettuare la stampa dei dati solo se strettamente necessaria e ritirare prontamente dai vassoi delle stampanti comuni i fogli per impedire a persone non autorizzate di accedere alle stampe di documenti riservati, distruggere personalmente e sistematicamente le stampe che non servono più.

La ricezione o l'effettuazione di telefonate personali sono consentite solo nel caso di comprovata necessità ed urgenza, mediante il telefono fisso a disposizione. È vietato l'utilizzo del fax e delle fotocopiatrici per fini personali.

9. Utilizzo della rete informatica

La stazione di lavoro assegnata al singolo utente ed abilitata alla navigazione in Internet costituisce uno strumento dell'Ente utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo quanto in di seguito specificato. In questo senso, 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 (es.: filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà essere a tal fine contattato il personale del Servizio ICT);
- 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;
- Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa la Federazione rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevenano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una *black list*.

È tuttavia consentito ai dipendenti di poter accedere per finalità personali a siti di informazione (Giornali e quotidiani) e/o di altro genere (es. siti prenotazione treni/aerei/home banking) purché per un periodo di tempo assai limitato e solo per

eventuali necessità ed urgenze. Tale navigazione per finalità personali deve essere comunque improntata a criteri di buona fede e correttezza e non può in alcun caso pregiudicare il disbrigo assiduo e diligente delle mansioni assegnate. Gli eventuali controlli, compiuti dal personale incaricato del Servizio ICT, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 30 giorni, ossia il tempo indispensabile per il corretto perseguimento delle finalità di sicurezza dell'Ente.

- E' consentito l'utilizzo di soluzioni di Instant Messenger e/o chat esclusivamente per scopi professionali ed attraverso gli strumenti ed i software messi a disposizione dalla Federazione.

- Non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo.

- Non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell'Ente in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata approvata espressamente.

Violazioni della sicurezza o interruzioni della comunicazione di rete sono da considerarsi vietate. Violazioni della sicurezza includono accesso a dati dei quali il lavoratore non è un destinatario, o accesso ad un server o account al quale il dipendente non sia espressamente autorizzato ad accedere, a meno ciò non rientri nei propri compiti.

10. Protezione antivirus

Il sistema informatico della Federazione è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo (evitando, quindi, di compiere quei comportamenti vietati dal presente regolamento e già menzionati: es. navigazione su siti non sicuri, download di file non autorizzati, etc.). È fatto assoluto divieto a ciascun utente di modificare le impostazioni del software antivirus. Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso nonché segnalare prontamente l'accaduto al personale del Servizio ICT. Ogni dispositivo magnetico di provenienza esterna all'Ente dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Servizio ICT.

11. Regole applicabili all'utilizzo di posta elettronica

La Federazione mette a disposizione dei lavoratori indirizzi di posta elettronica individuali in dominio istituzionale @chimici.it (servizio di posta interno all'ente) che consentono:

- di inviare e ricevere comunicazioni attinenti allo svolgimento dell'attività lavorativa;
- di partecipare a gruppi di lavoro in condivisione e collaborazione, attinenti allo svolgimento dell'attività lavorativa.

Tramite la posta istituzionale con dominio **@chimicifisici.it** possono essere trasmesse le seguenti comunicazioni:

- comunicazioni agli iscritti e ai singoli Ordini territoriali;
- convocazioni riunioni;
- comunicazioni ai fornitori di servizi in *outsourcing*;
- comunicazioni di servizio anche dirette al singolo dipendente;
- materiale preparatorio alle riunioni collegiali;
- circolari;
- copia elettronica di documenti redatti su supporti cartacei (purché in formati e dimensioni opportune).

Ogni utente assegnatario di una casella di posta elettronica istituzionale è responsabile del corretto utilizzo della stessa ed è tenuto a utilizzarla in modo conforme a quanto stabilito dal presente regolamento, quindi deve:

- a) conservare la password nella massima riservatezza e con la massima diligenza,
- b) mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti,
- c) utilizzare l'account per l'invio di comunicazioni attinenti all'attività lavorativa,
- d) inviare preferibilmente file in formato PDF,
- e) al termine delle operazioni effettuare il logout dall'account.

Agli utenti è fatto divieto di qualsiasi uso della posta elettronica che possa in qualche modo recare danno all'istituto o a terzi e quindi di:

- a) prendere visione della posta altrui,
- b) simulare l'identità di un altro utente, ovvero utilizzare per l'invio di messaggi credenziali di posta non proprie, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza,

- c) utilizzare strumenti software o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'istituto,
- d) trasmettere a mezzo posta elettronica dati *sensibili*, personali o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento della protezione dei dati,
- e) utilizzare il servizio di posta elettronica per inoltrare giochi, appelli e petizioni, messaggi tipo "catene" e altre e-mail che non siano di lavoro.

I messaggi di posta elettronica devono contenere un avvertimento ai destinatari del seguente tenore letterale: *"Il presente messaggio contiene informazioni di natura professionale attinente all'attività istituzionale della Federazione Nazionale degli Ordini dei Chimici e dei Fisici. Ai fini dello svolgimento dell'attività lavorativa le eventuali risposte potranno essere conosciute da altri soggetti nell'ambito dell'organizzazione del mittente. Questo messaggio di posta elettronica e il suo contenuto sono riservati e confidenziali e destinati esclusivamente al soggetto indicato nell'indirizzo. Se per errore ricevete questo messaggio o non siete il soggetto destinatario o delegato dal destinatario alla lettura, Vi preghiamo di darcene immediatamente notizia e quindi di cancellare definitivamente il messaggio di posta elettronica"*.

Al fine di garantire la continuità all'accesso dei messaggi da parte dei soggetti adibiti ad attività lavorative che richiedono la condivisione di una serie di documenti si consiglia e si incoraggia l'utilizzo abituale di caselle di posta elettronica condivise tra più lavoratori o delle caselle di posta istituzionali dell'Ente eventualmente affiancandoli a quelli individuali.

In caso di assenza prolungata programmata del dipendente, si consiglia e si raccomanda al dipendente di attivare il sistema di risposta automatica ai messaggi di posta elettronica ricevuti indicando, nel messaggio di accompagnamento, le coordinate di un collega o della struttura di riferimento che può essere contattata in sua assenza e/o altre modalità utili di contatto della struttura organizzativa.

12. Gestione della casella di Posta Elettronica di un Lavoratore cessato dal servizio. Disattivazione dell'account riconducibile a persona identificata o identificabile.

La Federazione, quale datore di lavoro, pur avendo la facoltà di verificare l'esatto adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di

lavoro da parte dei dipendenti, deve in ogni caso salvaguardarne la libertà e la dignità. Con riferimento ai trattamenti effettuati sulla posta elettronica dopo la cessazione del rapporto di lavoro (ex dipendente), in conformità ai principi in materia di protezione dei dati personali, gli account riconducibili a persone identificate o identificabili vengono rimossi previa disattivazione entro 3 (tre) giorni lavorativi e contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del titolare del trattamento. L'interesse della Federazione ad accedere alle informazioni necessarie all'efficiente gestione della propria attività, pertanto, è contemperato con la legittima aspettativa di riservatezza sulla corrispondenza da parte dei dipendenti nonché dei terzi.

Si prende altresì atto che la disattivazione è realizzata "secondo modalità tali da inibire in via definitiva la ricezione in entrata di messaggi diretti al predetto account, nonché la conservazione degli stessi su server dell'Ente".

13. I CONTROLLI

La Federazione, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, Statuto dei Lavoratori), esclude la configurabilità di forme di controllo aziendali aventi direttamente ad oggetto l'attività lavorativa del dipendente.

Ciononostante, non si esclude che, per ragioni organizzative e produttive ovvero per esigenze dettate dalla sicurezza del lavoro e di tutela del patrimonio dell'Ente, si utilizzino sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori.

I controlli posti in essere, pertanto, saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati. Tali controlli saranno effettuati secondo il principio della "gradualità".

Secondo questo principio:

- i controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura aziendale ovvero a singole aree lavorative;
- nel caso in cui si dovessero riscontrare violazioni del presente Regolamento interno, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, verrà diffuso un avviso generalizzato, o circoscritto all'area o struttura lavorativa interessata, relativo all'uso anomalo degli strumenti informatici aziendali, con conseguente invito ad attenersi scrupolosamente alle istruzioni ivi impartite.

In caso siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale;

- Traccia dei log di tutte le attività svolte come da normativa.

14. I controlli non autorizzati

In ogni caso la Federazione non può in alcun modo utilizzare sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività del lavoratore.

Per tali s'intendono, a titolo meramente esemplificativo e non esaustivo:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica stesso;
- la lettura sistematica delle pagine internet visualizzate da ciascun utente, dei contenuti ivi presenti, e del tempo di permanenza sulle stesse;

Per i dettagli sulle modalità dei controlli posti in essere dalla Federazione, si rimanda all'Allegato A.

15. Informativa agli utenti

Il presente regolamento è messo a disposizione degli utenti, per la consultazione, sui mezzi di comunicazione interna utilizzati dall'Ente (circolare, sito) e quindi portato a conoscenza di ciascun dipendente. L'utente qualora l'Ente decidesse di perseguire, per fini legati alla sicurezza dell'intero

sistema informativo, il controllo della posta elettronica e della navigazione in internet, viene informato degli strumenti e dei modi di trattamento effettuati prime che questo sia iniziato.

16. Responsabilità e sanzioni

L'utente delle risorse informatiche della Federazione che abbia violato il presente disciplinare o la normativa ivi richiamata, potrà essere soggetto ad azione disciplinare in conformità a quanto stabilito dai contratti collettivi e dagli artt. 54 e seguenti del D.lgs. n. 165/2001 nonché dal Codice disciplinare e di comportamento, fatta salva la possibilità per l'Ente di esercitare le opportune azioni giudiziarie nelle sedi competenti, a tutela dei propri diritti giuridicamente tutelati. In caso di danno, la violazione espone altresì l'utente responsabile ad azioni legali di carattere civile o penale da parte dei danneggiati e a richieste di risarcimento anche da parte della Federazione.

17. Norme finali

Le disposizioni del presente regolamento si applicano, per quanto compatibili, anche alle ipotesi di collegamento alla rete aziendale da postazioni esterne all'ufficio (ad esempio: collegamento da casa);

18. Aggiornamento e revisione del Disciplinare

Il presente Disciplinare viene consegnato ai Consiglieri, dipendenti, consulenti, società, partners e tutti gli utenti che ne sottoscrivono la consegna per ricevuta e comunque all'atto dell'assunzione e/o al momento dell'assegnazione di un account utente. Il presente Disciplinare è soggetto a revisione con frequenza annuale e ogni qualvolta sia necessario un aggiornamento alla luce dell'esperienza, di nuove normative e dell'innovazione tecnologica.

Tutti gli utenti possono proporre quando ritenuto necessario, integrazioni al presente regolamento e le proposte saranno esaminate dal Titolare del trattamento in collaborazione con l'Amministratore di sistema.

ALLEGATO A

CONTROLLI EFFETTUATI

Il presente allegato ha la finalità di informare i lavoratori sull'eventuale possibilità di forme di controllo indirette della loro attività lavorativa – richieste da esigenze organizzative, produttive e di sicurezza del lavoro e sicurezza informatica – nonché quella di disciplinare le modalità operative di utilizzo dei sistemi adoperati (ex art. 4 comma 2 L. 300/1970).

Si precisa che, nonostante l'utilizzo di tali sistemi, la Federazione valuterà attentamente l'impatto sui diritti dei lavoratori (prima dell'installazione di apparecchiature suscettibili di consentire il controllo a distanza e dell'eventuale trattamento) e riterrà vietati controlli costanti, prolungati e indiscriminati.

1. INTERNET

La Federazione, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o estranee all'attività lavorativa), ha adottato misure restrittive che impediscono ad origine.

In particolare, la Federazione adotterà le seguenti misure di concerto con il fornitore dei servizi Internet:

- 1) individuazione di categorie di siti e dei software considerati non conformi con lo svolgimento della prestazione lavorativa.
- 2) configurazione di sistemi di filtraggio che prevengano determinate operazioni reputate incoerenti con l'attività lavorativa – quali l'upload o l'accesso a determinati siti e/o il download di file o software aventi particolari caratteristiche.
- 3) conservazione e registrazione nel tempo di dati (quali file di log) a cura del fornitore del servizio di connessione a internet. I dati personali contenuti e registrati nei file di log possono essere trattati nelle ipotesi di seguito riportate:
 - per corrispondere ad eventuali richieste dell'autorità giudiziaria. Si osserva che il trattamento dei dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose, non astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti.

- quando si verifichi un evento dannoso o una situazione di pericolo che richiede un immediato intervento.

- in caso di utilizzo anomalo degli strumenti da parte degli utenti.

Il controllo, in ogni caso, avverrà in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai file di log riferiti al traffico web).

2. POSTA ELETTRONICA

Il fornitore del servizio di Posta Elettronica procederà periodicamente ad un controllo quantitativo - aggregato e non identificativo - della posta elettronica per verificarne un uso equilibrato e coerente con l'attività istituzionale dell'Ente.

Comunque il monitoraggio non è finalizzato al controllo delle attività degli utenti. Le informazioni raccolte consentono un controllo dell'efficienza e dell'utilizzo corretto delle risorse informatiche.

Si esclude, pertanto, ogni forma di lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail e/o per evadere richieste dovute a esigenze organizzative, produttive o di sicurezza.