**Cooperativa Sociale**
**Coopselios**
Società Cooperativa
C.F. e P.I. 01164310359
www.coopselios.com

Iscrizione registro imprese
RE n. 01164310359
REA RE n. 167007
Iscrizione albo società
cooperative n. A101139

# PROCEDURA AZIENDALE

# UTILIZZO DEI SISTEMI INFORMATICI: Personal computer - Posta Elettronica - Rete Internet

| Revisione | Data | Redazione | Approvazione |
|---|---|---|---|
| 1 | 01/07/22 | Servizio ICT | Direzione Genale |
| 2 | 12/09/22 | Servizio ICT | Direzione Genale |
| 3 | 23/11/22 | Servizio ICT | Direzione Genale |
| 4 | 4/11/2024 | DPO | |
| | | | |
| | | | |

# Sommario

## 1. Premessa

Il presente regolamento disciplina le modalità di utilizzo degli strumenti informatici aziendali, internet e posta elettronica, anche in ottemperanza a quanto previsto dal Regolamento Europeo 679/2016, dal D.Lgs. 196/2003 e s.i.m. "Codice in materia di protezione dei dati personali", dalla Deliberazione n. 13 del 01/03/2007 del Garante per la protezione dei dati personali "Linee guida del Garante per posta elettronica e internet" e, in via analogica, dalla Direttiva n. 2/09 del 26/05/2009 della Presidenza del Consiglio dei Ministri "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro" nelle quali sono fornite indicazioni in merito all'uso corretto degli strumenti informatici da parte dei lavoratori ed alle modalità di controllo da parte dei datori di lavoro, al fine di evitare abusi, pur mantenendo il diritto del lavoratore ad una sfera di riservatezza anche nelle relazioni professionali.

## 2. Definizioni

| | |
|---|---|
| **SI (SistemiInformativi):** | insieme di elementi che raccolgono, elaborano, memorizzano e distribuiscono dati e informazioni a supporto delle attività aziendali |
| **ICT (Information& CommunicationTecnology):** | servizio che si occupa di tutti i processi connessi alla trasmissione, ricezione ed elaborazione dei dati e delle informazioni automatizzando ed ottimizzando i flussi relativi ai Sistemi Informativi |
| **LOG:** | Registrazione cronologica delle operazioni e il file su cui tali registrazioni sono memorizzate |
| **Rete Interna:** | Insieme delle risorse di rete che consentono il collegamento informatico e telematico tra le diverse sedi |
| **Utente:** | Soggetto con diritto di accesso ai servizi informatici e di rete, in accordo con il proprio profilo di appartenenza e il presente regolamento |
| **Profilo utente:** | Tipologia di Utente con accesso ad un numero predefinito di servizi informatici e di rete |
| **Account istituzionale:** | Account fornito da Coopselios a ciascun utente per accedere ai servizi informatici e di rete in accordo con il relativo "Profilo Utente" |
| **File Server:** | Server di rete sul quale gli utenti possono archiviare/condividere i propri file |
| **BIOS:** | insieme piú o meno complesso di routines Software che collegano l'Hardware della mainboard o di una scheda dotata di processore con il sistema operativo |
| **Virus:** | programma o **una** sezione di codice caricato nel computer senza che **il** proprietario ne sia **a** conoscenza o lo abbia autorizzato. Alcuni **virus** causano solo fastidi, mentre la |

| | |
|---|---|
| | maggior parte è dannosa e ideata per infettare e prendere **il** controllo dei sistemi vulnerabili |
| **Spyware:** | Software scaricato, spesso in maniera inconsapevole, durante la navigazione in Internet o l'installazione di un software gratuito, programmato per registrare e trasmettere a terzi dati personali e informazioni sull'attività online di un utente |
| **Malware:** | Programma, documento o messaggio di posta elettronica in grado di apportare danni a un sistema informatico |
| **Bitlocker:** | funzionalità di protezione dei dati integrata nei sistemi operativi Microsoft che permette di crittografare l'intera partizione del sistema operativo. |
| **Browser:** | programma per navigare in Internet che inoltra la richiesta di un documento alla rete e ne consente la visualizzazione una volta arrivato |
| **Onedrive:** | servizio di Microsoft che **c**onsente di archiviare e condividere i file con altri utenti e di accedervi da qualsiasi dispositivo. |
| **VPN(Rete virtuale privata):** | connessione di rete privata creata tra dispositivi attraverso la rete Internet. Le VPN sono utilizzate per trasmettere dati sulle reti pubbliche in modo anonimo e sicuro. |

## 3. Revisione

Modifiche al presente regolamento vengono elaborate in accordo o su indicazione della Direzione Generale, sulla base dell'evoluzione tecnologica nel settore o comunque ogni qualvolta si riscontrino evidenti e documentabili esigenze tecniche o funzionali.

## 4. Campo di applicazione

Il regolamento deve essere osservato da tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché da tutti i collaboratori dell'Azienda, a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.).

## 5. Il trattamento dei dati con i sistemi informatici

Il (sostanziale) titolare del trattamento dei dati in Cooperativa è il Presidente.
Una persona fisica, un dipendente, che materialmente svolge operazioni sui dati personali di altre persone deve essere autorizzato al trattamento (o incaricato) dal titolare del trattamento. L'autorizzato opera quindi in subordinazione al titolare del trattamento.
Tutti gli autorizzati potrebbero essere nominati con diversi livelli di delega.

**Cooperativa Sociale**
**Coopselios**
Società Cooperativa
C.F. e P.I. 01164310359
www.coopselios.com

Iscrizione registro imprese
RE n. 01164310359
REA RE n. 167007
Iscrizione albo società
cooperative n. A101139

Vedi allegato 2 di questo documento per le istruzioni operative di Coopselios

## 6. Utilizzo del Personal Computer

**II Personal Computer (PC) sia fisso che portatile, affidato al dipendente**, è uno strumento aziendale e non personale, pertanto vi devono essere archiviati dati relativi all'attività svolta e non dati propri. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

**I dipendenti che ricevono in consegna PC di proprietà di Coopselios sono denominati "consegnatari" del bene ricevuto ed hanno obbligo di vigilanza e custodia.**

**Le impostazioni dei PC e dei relativi programmi, hardware e software, sono predisposte dagli addetti ICT sulla base di criteri e profili decisi dall'Azienda,** in funzione della qualifica del dipendente, delle mansioni a cui questo è adibito, nonché dalle decisioni e della politica di utilizzo di tali strumenti stabilita dall'Azienda stessa. Il dipendente non può modificarle autonomamente, eventuali variazioni necessarie possono essere effettuate solo dal personale ICT, comprese quelle di carattere straordinario che a giudizio del diretto responsabile sono indispensabili per l'espletamento di peculiari attività istituzionali assegnate (installazione di software dedicato, accessi). In particolare:

- Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale ICT, non è altresì consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.
- Solo il personale incaricato, che opera presso l'ICT, è autorizzato a compiere interventi nel sistema informatico aziendale 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.).
- L'inosservanza della presente disposizione espone inoltre la Cooperativa a gravi responsabilità civili; si evidenzia che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.
- Non è consentita l'attivazione della password all'accensione del PC (BIOS), senza preventiva autorizzazione da parte dell'ICT.

**Il personale ICT ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC, 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, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

**I file dati elaborati dal dipendente**

- Per tutti i dati di interesse lavorativo, per cui si renda necessaria la garanzia della conservazione e relativi backup, deve essere utilizzata l'area condivisa sul File Server

aziendale riservata all'utente o, comunque, su tale area i dati devono essere copiati periodicamente.

- Nel caso in cui tale suggerimento non fosse seguito non se ne garantisce la conservazione ed il recupero dei dati in caso di cancellazione o compromissione
- Le cartelle presenti all'interno del server aziendale sono da intendersi quali aree di condivisione di informazioni strettamente professionali e, dunque, non possono essere utilizzate per scopi differenti, fatte salve specifiche autorizzazioni da parte di COOPSELIOS; pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità, fatte salve particolari ed eccezionali ipotesi.
- Particolare attenzione deve essere prestata alla duplicazione dei dati: è infatti assolutamente da evitare un'archiviazione ridondante.
- Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili.

**I supporti rimovibili (es. USB key, hard disk esterni),** contenenti informazioni aziendali di qualsivoglia natura ovvero costituenti il know how (materiale/immateriale) aziendale o di terzi soggetti, devono essere trattati con particolare cautela, onde evitare che il loro contenuto possa essere trafugato, alterato, distrutto o conosciuto da soggetti non autorizzati.
**Smart card / token per la firma digitale: n**el caso in cui il dipendente sia in possesso di smart card / token per la firma digitale la stessa non deve essere abbandonata e deve essere rimossa dall'apposito alloggiamento nel caso di allontanamento del dipendente dalla postazione di lavoro.

- L'utente assegnatario di un supporto rimovibile o Smart card / token per la firma digitale è tenuto a comunicare, senza ingiustificato ritardo, a COOPSELIOS l'eventuale furto, smarrimento ovvero guasto di esso.

**Il Buon uso del Personal Computer**

- Il PC deve essere spento ogni sera prima di lasciare gli uffici, in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo.
- L'utente è tenuto a scollegarsi dal sistema/rete ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima attraverso il blocco del PC con CTRL+ALT+CANC→BLOCCO al fine di evitare che persone estranee effettuino accessi non permessi.
- Su ogni PC è comunque configurato lo screen sever con password che si attiva dopo 10 min. di inattività
- Ai PC portatili si applicano le regole di utilizzo previste per i Pc fissi connessi in rete, con particolare attenzione ai seguenti punti:
  - conservare lo strumento in un luogo sicuro alla fine della giornata lavorativa;
  - non lasciare mai incustodito l'elaboratore in caso di utilizzo in ambito esterno all'azienda;

- essere sempre ben consapevole delle informazioni archiviate sul portatile il quale è maggiormente soggetto a furto e smarrimento rispetto alla postazione fissa;
- operare sempre nella massima riservatezza quando si utilizza il PC portatile in pubblico: i dati, ed in particolare le password, potrebbero essere intercettati da osservatori indiscreti.
- Su ogni PC portatile è installato BitLocker un sistema di cifratura del file system, che non permette, in caso di furto o smarrimento, l'accesso ai dati se non attraverso la conoscenza della password.

## 7. Gestione credenziali di autenticazione e password

**A chi è autorizzato all'uso del PC viene assegnato un "Account istituzionale"**

- L'utilizzo del computer e delle procedure informatiche è protetto da credenziali di accesso (username e password) che costituiscono l' "Account istituzionale".
- L'assegnazione viene fatta dal personale ICT, a seguito di formale richiesta del diretto Responsabile del servizio nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.
- La verifica delle credenziali "autorizza" l'utente ad accedere all'uso dei servizi di rete, collegamento alla rete Intranet, Internet, posta elettronica e applicativi vari messe a disposizione per la tipologia di "Profilo Utente" definito nell'ambito della creazione dell'Account.
- Le credenziali vengono revocate alla chiusura del rapporto tra Utente e Coopselios.
- Le credenziali di accesso sono nominali cioè riconducibili ad un unico soggetto, associati ad una parola chiave (password).
- Tutte le attività informatiche effettuate a seguito di autenticazione sono ricondotte alla persona fisica a cui sono state rilasciate le credenziali.
- Alle credenziali di accesso è associata una parola chiave (password).
- Al primo accesso effettuato sul sistema e/o procedura informatica, il dipendente ha la responsabilità di cambiare la password assegnatagli dall'ICT.
- La password deve essere composta da almeno dodici caratteri e formata da lettere (maiuscole o minuscole), e numeri (almeno 1 carattere maiuscolo, 1 carattere minuscolo e 1 numero) e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
- Il sistema richiede il cambio della password ogni 90 giorni in base al profilo utente.

## 8. Protezione antivirus

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacchi al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo. Ad esempio: non aprire mail e/o relativi allegati sospetti, non navigare su siti non professionali ecc.
Coopselios è inoltre dotata di sistemi di protezione contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale.

Ogni utente è tenuto a controllare la presenza ed il regolare funzionamento del software antivirus aziendale. Nel caso in cui il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente sospendere ogni elaborazione in corso – staccando il cavo di rete senza spegnere il computer - e segnalare l'accaduto all'ICT.
Ogni dispositivo magnetico di provenienza esterna all'Azienda o i supporti di memorizzazione utilizzati dovranno essere verificati mediante il programma antivirus prima del loro utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, non dovranno essere utilizzati.
In sintesi sulla base delle indicazioni sin qui riportate, gli utilizzatori di un PC fisso/portatile di Coopselios si devono attenere alle seguenti regole:

**Decalogo per il buon uso del PC**

I. Non è consentito l'utilizzo di programmi differenti da quelli installati da COOPSELIOS;
II. Lunghezza minima password: 12 caratteri (minuscole + maiuscole + numero);
III. La password è **riservata** e non và ceduta a nessuno;
IV. Ogni volta che ci si allontana dal PC si deve bloccare il PC;
V. Prestare molta attenzione ai supporti rimovibili;
VI. Spegnere il PC prima di andare via;
VII. Pulire periodicamente il PC;
VIII. Controllare il regolare funzionamento dell'Antivirus;
IX. Utilizzare il File Server solo per scopi lavorativi e non privati;
X. custodire adeguatamente i PC Portatili e la password di BitLocker.

## 9. Uso della posta elettronica e indicazioni

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro finalizzato allo scambio di informazioni nell'ambito dell'attività lavorativa. Poiché le caselle sul dominio "coopselios.com" sono di proprietà dell'Azienda, che ne concede l'uso ai dipendenti secondo le norme indicate nel presente regolamento, i dipendenti assegnatari sono responsabili del corretto utilizzo delle stesse. Gli assegnatari si impegnano inoltre a rispettare le regole di "Netiquette"[1] di Coopselios contenute al punto 9.1 di questa Procedura.

[1] La netiquette è una parola inglese che unisce il vocabolo inglese network (rete) e quello francese etiquette (buona educazione). È un insieme di regole informali che disciplinano il buon comportamento di un utente sul web di Internet, specie nel rapportarsi agli altri utenti attraverso risorse come newsgroup, mailing list, forum, blog, reti sociali o e-mail in genere

Le comunicazioni via posta elettronica devono avere un contenuto espresso in maniera professionale e corretta, nel rispetto della normativa vigente.

**Le comunicazioni in uscita, devono essere 'firmate'**

La firma contiene il proprio nome e cognome, il proprio ruolo, il Servizio/ Ufficio di appartenenza, nome dell'Azienda, recapito telefonico dell'ufficio e del cellulare di servizio, indirizzo e-mail

**I messaggi di posta elettronica (sotto la firma) contengono un avvertimento (Disclaimer) ai destinatari del seguente tenore letterale:**

**Disclaimer:**

> Qualora il messaggio Le fosse pervenuto per errore, La preghiamo di cancellarlo immediatamente senza visionarne il contenuto e, se possibile, di darcene cortesemente notizia.
> Avvertenza: la presente casella e-mail, i messaggi e gli allegati da essa derivanti, sono di esclusivo utilizzo aziendale/lavorativo e mai personale.
> Risposte al presente messaggio: si avvisa il destinatario che eventuali Sue risposte potranno essere lette dall'intera azienda/ufficio/servizio di appartenenza del mittente.
> Informativa Privacy: ai sensi dell'art. 13 Regolamento UE 2016/679, informiamo che i dati sono trattati sia con modalita` informatiche che cartacee da persone appositamente autorizzate.
> I dati non saranno diffusi e verranno utilizzati per dar corso ai rapporti in essere ed adempimenti connessi. Informiamo inoltre che potra` essere richiesta la rettifica, il blocco, la cancellazione e la portabilita` dei dati, inviando un'e-mail o fax al Titolare del trattamento.
>
> Nota: l'informativa di sintesi, e` integrata da ulteriore informativa articolata ed estesa presente sul sito web.

Il Disclaimer rappresenta una misura di sicurezza per il mittente che può rammentare al destinatario di una e-mail le leggi vigenti in materia di privacy e di violazione della corrispondenza, avvertendolo dei rischi in cui incorre se adotta comportamenti vietati.
Il Disclaimer viene impostato automaticamente dal server di posta per le mail verso destinatari esterni all'organizzazione.

**L'accesso alla casella di posta elettronica e la sua password**

L'accesso alla casella di posta elettronica avviene attraverso il nome account ed una password provvisoria che vengono comunicate dal servicio ICT; Al primo accesso il dipendente ha la responsabilità di cambiare la password assegnatagli inserendone una con i seguenti requisiti di complessità:

- Lunghezza minima: 12 caratteri
- Complessità minima: Minuscole + maiuscole + numero (almeno uno per tipo)

Per ricordarsi più facilmente le password si possono usare anche delle frasi (es: ilmiocanesichiamaPippo1)

Si ricorda che una password lunga ma meno complessa è più sicura di una password corta ma più complessa.
Si ricorda di NON SCRIVERE le password su fogli da tenere a portata di mano e di non usare la stessa password su sistemi esterni a Coopselios es: Amazon, Ebay etc…

La password è **riservata** e non và ceduta a nessuno ne tantomeno scritta su post-it o fogli volanti sulla scrivania e non va salvata nel browser.
Si ricorda che siamo responsabili di quello che scriviamo ed inviamo e se qualcuno invia materiale non adeguato a nostra insaputa toccherà a noi dimostrare di non esserne responsabili.
La password ha una durata di 90 gg poi il sistema chiederà di cambiarla.
**caselle di posta elettronica condivise:** 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 l'utilizzo abituale di caselle di posta elettronica condivise tra più lavoratori (es. ICT@coopselios.com). Tali caselle sono accessibili all'interno della mail del dipendente.
Ogni assegnatario deve consultare la propria casella con frequenza giornaliera, salvo casi di assenza dal lavoro; tale casella può, comunque, essere consultabile dal dipendente titolare della stessa tramite accesso pubblico al di fuori della rete aziendale.
**Nel caso di assenza dal lavoro prolungata e programmata**
Nel caso di assenza dal lavoro prolungata e programmata, il dipendente deve attivare il sistema di risposta automatica ai messaggi di posta elettronica ricevuti indicando, nel messaggio di accompagnamento, ogni riferimento utile per contattare la struttura organizzativa competente.
Nei casi di assenza non programmata o impossibilità, temporanea o protratta nel tempo, se non è possibile attivare la procedura sopra citata, per garantire l'ordinaria operatività aziendale, il dipendente deve delegare ad un collega a sua scelta ("fiduciario") il compito di verificare il contenuto di messaggi e di inoltrare al diretto Responsabile quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.
Qualora il dipendente non abbia delegato un collega (fiduciario), il suo diretto Responsabile può richiedere alla ICT di accedere alla casella di posta elettronica del dipendente assente, in modo da prendere visione dei messaggi di posta. In questo caso il Responsabile deve informare il dipendente appena possibile, fornendo adeguata spiegazione e riportando l'evento su apposito verbale.
La stessa procedura deve essere attuata qualora, per garantire l'ordinaria operatività aziendale, sia necessario accedere a informazioni o documenti di lavoro presenti sul PC del dipendente assente.
**Nel caso in cui si debba inviare un documento o dati sensibili all'esterno dell' Azienda**
Nel caso in cui si debba inviare un documento all'esterno dell' Azienda è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat *.pdf). Tale software specifico è fornito dall' ICT su tutte le postazioni di lavoro. Nel caso di invio di allegati "pesanti" utilizzare i formati compressi (*.zip, *.7z, *.rar).
Laddove sia invece necessario inviare documento contenente dati sensibili è obbligatoria la creazione di un file protetto da password (nel caso di più documenti creare una cartella compressa sempre protetta da password contenete). La password deve essere comunicata con un altro strumento (per es. Sms, WhatsApp, dettata al telefono, ecc).
**Nel caso di mittenti sconosciuti o link sconosciuti**

Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus, occorrerà cancellare i messaggi senza aprirli. Analogamente, messaggi provenienti da mittenti conosciuti che contengono allegati con estensioni sospetti o sconosciuti non devono essere aperti.
Evitare di cliccare su link sconosciuti e/o ambigui all'interno dei messaggi di posta elettronica e non comunicare credenziali personali (banca ed altro) alle richieste pervenute con email apparentemente inviati da mittenti conosciute cestinando immediatamente tali messaggi;
Va evitata la diffusione incontrollata di sistemi per propagare messaggi a diffusione capillare e moltiplicata che inducono il destinatario a produrne molteplici copie da spedire, a propria volta a nuovi destinatari, in quanto limitano l'efficienza del sistema di posta.
**L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali**. Prima di iscriversi occorre verificare in anticipo se il sito è affidabile.
**È invece vietato l'utilizzo dell'indirizzo mail aziendale per l'iscrizione a qualsiasi servizio on line** (social network, gruppi di discussione, servizi telefonici, bancari, assicurativi di tipo personale etc.) che non sia strettamente correlato alla propria attività istituzionale.

**La manutenzione della casella di posta**

Lo spazio a disposizione di ogni casella di posta elettronica è 50 GB monitorabile dal punto di menu "spazio di archiviazione" della casella stessa.
Per ogni utente è inoltre disponibile 1 TB all'interno di OneDrive che è uno spazio Cloud che gli utenti possono utilizzare per l'archiviazione di file.
La casella di posta elettronica deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti o salvandoli in una apposita cartella di servizio creata sul proprio PC o sul file server: il dipendente ha il dovere di verificare periodicamente (settimanalmente) lo spazio a disposizione nella casella di posta propria, evitando così di non ricevere messaggi per mancanza di spazio disponibile.
Per la trasmissione di file attraverso la posta elettronica bisogna prestare attenzione alla dimensione degli allegati che non devono mai superare i 5 MB quando i file superano tale dimensione si consiglia di come collegamento a OneDrive in modo da non appesantire la propria casella di posta elettronica e quella del destinatario andando ad erodere i 50 GB disponibili.

Sulla base delle indicazioni sin qui riportate, gli utilizzatori di una casella pubblica di posta sul dominio @coopselios.com devono attenersi alle seguenti regole:

**Decalogo per il buon uso delle Mail**

I. conservare le password al sicuro e impostare la lunghezza minima password a 12 caratteri (minuscole + maiuscole + numero);
II. non utilizzare l'indirizzo mail aziendale per comunicazioni personali;
III. l'iscrizione a "mailing list" esterne è concessa solo per motivi professionali;
IV. le comunicazioni in uscita verso "esterni", devono essere 'firmate';
V. nel caso di assenza dal lavoro prolungata e programmata, il dipendente deve attivare il sistema di risposta automatica ai messaggi o inoltro verso collega;
VI. rispondere all'eventuale richiesta del mittente di conferma di lettura del messaggio;
VII. non inviare messaggi che possano danneggiare la reputazione e l'immagine dell'Azienda;

VIII. non inviare comunicazioni che siano diffamatorie, oscene, pornografiche, offensive, tali da recare danno o che possano essere considerate da altri fonti di molestie o discriminazione religiosa, sessuale, razziale, politica o sindacale;

IX. evitare di mettere in rete documenti che danneggino la privacy di qualcuno e, se proprio si deve, crittografare prima il file;

X. evitare di allegare file di grosse dimensioni.

## 9.1 Regole di Netiquette in Coopselios

Al fine di utilizzare in modo corretto ed efficace le comunicazioni tramite mail La cooperativa Coopselios si dota di regole di "netiquette":

a) **Chi scrive (il mittente) deve essere facilmente riconoscibile e contattabile**: Nei programmi di posta elettronica (come Outlook) esiste la possibilità di inserire automaticamente in chiusura della email un testo che comprenda "la firma" dello scrivente (utilizzare nel menu impostazioni l'inserimento automatico della firma)

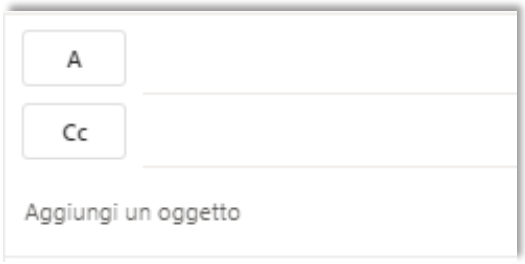
Sotto la firma inserire il messaggio per la riservatezza e trattamento dei dati personali e di privacy

**Esempio di firma:**

Claudio Fevola
Responsabile ICT – Sistemi Informativi
cfevola@coopselios.com
Cooperativa sociale Coopselios
via A. Gramsci 54/s 42124 Reggio Emilia
https://www.coopselios.com

Uff. 0522378711
Cell.: 3393792326

b) **Campo "A" : inviamo a chi ha la "Competenza di rispondere" è il destinatario o destinatari del messaggio**.




E' il destinatario (o i destinatari) che ha pieno titolo a trattare una certa materia o è direttamente coinvolto in una attività come titolare o come facente parte di un team.
**Tutti i destinatari in "A" sono formalmente obbligati a dare una risposta.**

**Campo "CC": invio per "conoscenza " sono** il destinatario (o i destinatari) che è necessario informare pubblicamente dei contenuti dell'email.
**Il destinatario in "CC" può interagire con il mittente e i destinatari, ma non è formalmente obbligato a rispondere**.

Utilizzando queste due campi "A" e "CC" campo tutti i destinatari della email visualizzeranno, oltre all'indirizzo del mittente, tutti gli indirizzi degli altri destinatari.
Quindi usare questi campi va bene se l'email è rivolta a tutte le persone senza distinzioni (personale interno, colleghi) e se tutti i destinatari si conoscono tra loro.
Se la mail avesse come destinatari degli esterni (ad esempio un messaggio ai genitori di bimbi di un nostro asilo), non dobbiamo consentire, per motivi di privacy, che i destinatari vedano i reciproci indirizzi. Dovremo usare una diversa modalità: il campo CCN (come spiegato al punto d)

c) **inserire sempre un oggetto nella mail**. L'oggetto altro non è che il titolo dell'email. E' la sintesi del messaggio quindi uno dei principali elementi che determina l'apertura di una mail, insieme al mittente. Il testo contenuto in questo campo deve essere ben esplicativo: con poche parole si deve identificare l'intero contenuto del messaggio di posta elettronica.

d) **L'uso corretto del campo "CCN"**. Questa modalità di spedizione posta elettronica va utilizzata se si ha la necessità di mantenere la privacy tra i destinatari della tua corrispondenza. I normali campi per gli indirizzi 'A' e 'Cc' (copia conoscenza) rendono visibili gli indirizzi di posta elettronica a tutti i destinatari del messaggio. Se le persone a cui si invii il messaggio non si conoscono personalmente, potrebbe risultare spiacevole ed oggetto di denuncia. Utilizzare la copia conoscenza nascosta non rispetta la privacy dei destinatari. Inoltre si eviterà anche quello spiacevole scambio di e-mail con in copia tutti i destinatari originari (uso del rispondi a tutti). Infine eviterà inoltre che gli indirizzi possano essere utilizzati da sprovveduti perditempo per alimentare lo spam. Recentemente all' Ospedale San Raffaele di Milano l'aver utilizzato il campo cc (copia per conoscenza), al posto del campo CCN (copia per conoscenza nascosta), per l'invio di due newsletter è stato valutato atto di violazione dei dati di una certa gravità, che il Garante per le protezione dei dati personali ha punito con la sanzione amministrativa pecuniaria di 70 mila Euro[2].
Se, ad esempio, vuoi spedire una e-mail ai tuoi colleghi che lavorano con te ad un determinato progetto, per tenere aggiornati colleghi appartenenti ad altre aree di lavoro e, in modo invisibile mantenere aggiornata la dirigenza aziendale sullo stato di avanzamento del progetto, puoi inserire gli indirizzi e-mail del tuo team di lavoro nel campo destinatari 'A', i destinatari di altre aree di lavoro nel campo copia conoscenza 'Cc'. Puoi eventualmente includere anche te in questo ultimo campo per inviarti una copia della e-mail che stai scrivendo.
Quindi Inserire tutti i destinatari nel campo Ccn è il modo migliore per mantenere la privacy quando si invia una comunicazione via e-mail ad una lista numerosa di persone esterne a Coopselios (clienti o fornitori).

---

- [2] Garante Privacy 28 aprile 2022: Ordinanza ingiunzione nei confronti di Società Ospedale San Raffaele... - https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9779057

Usi del campo "CCN" con finalità diverse da quelle della tutale della privacy dei destinatari sono sconsigliate.

e) **Rispondere alle mail se si è i destinatari.** Quando qualcuno ti parla di solito rispondi, anche solo per buona educazione – a maggior ragione sul posto di lavoro. Fai lo stesso per iscritto: è un modo semplice di coltivare delle buone relazioni e, a volte, la risposta è necessaria per fare proseguire gli altri nelle attività.
La programmazione del lavoro quotidiano deve prevedere un tempo opportuno per leggere la posta (in funzione della quantità di mail che di solito si ricevono). Se la risposta ad una mail richiede tempo, può essere utile scrivere che si è ricevuto il messaggio e che si darà una risposta entro … .

f) **Come usare la funzione "Rispondi a tutti":** Chi riceve il messaggio di posta elettronica come destinatario principale dovrà agire in merito e rispondere tenendo in copia tutti i destinatari; mentre chi riceve la mail in "copia conoscenza" viene solo informato e non è chiamato a rispondere. Qualora volesse apportare ulteriori informazioni alla corrispondenza è sempre bene che usi con cautela l'opzione "Rispondi a tutti": può infatti decidere di rispondere solo al mittente o alle persone più indicate. Chi riceve il messaggio di posta elettronica come destinatario principale dovrà agire in merito e rispondere tenendo in copia tutti i destinatari; mentre chi riceve la mail in "copia conoscenza" viene solo informato e non è chiamato a rispondere. Qualora volesse apportare ulteriori informazioni alla corrispondenza è sempre bene che usi con cautela l'opzione "Rispondi a tutti": può infatti decidere di rispondere solo al mittente o alle persone più indicate.

g) **Essere chiari nel messaggio e nel layout:** Curare il layout, aiuta a fare chiarezza e facilita la fruizione della mail. Alcuni spunti:
- dalla sintesi al dettaglio: la mail segue un filo logico? È chiara? Dà tutte le informazioni necessarie per capire di cosa stai parlando o c'è bisogno di aggiornare il destinatario su qualcosa, prima di passare all'argomento principale?
- Le maiuscole sono importanti (nomi propri, luoghi geografici, parole dopo i punti), ricordare però che il testo tutto in maiuscolo è assolutamente sconsigliato: in Internet equivale ad urlare e così viene inteso dagli utenti.
- Poco spazio dà un senso di soffocamento. Lasciamo una riga tra un argomento e l'altro. Lo spazio è gratis nelle mail.
- Andare a capo dà enfasi a una frase o introduce un nuovo discorso
- Se la mail è lunga e complessa, usare il grassetto per evidenziare le parole chiave (non tutto, se no è inutile!).

h) **Le formule di apertura e chiusura**: Per la redazione del testo dell'e-mail formale è possibile iniziare con formule introduttive – Alla cortese attenzione di… - o l'aggettivo di circostanza - Egregio, Gentile o Caro - avendo cura di scegliere il più adatto alla circostanza.

Successivamente si potrà iniziare a comporre il messaggio con i consueti saluti - buongiorno, buonasera, salve - evitando di adoperare il "ciao" che è invece più indicato per le e-mail informali. Le opportune formule di commiato – ad esempio "In attesa di un suo cortese riscontro…" - andranno inserite anche alla fine del testo prima di chiudere l'email formale con i saluti - "Distinti Saluti" o "Cordiali Saluti".

i) **Attenzione al contenuto delle Mail ed ai suoi inoltri. Il contenuto delle email inviate dal computer aziendale non va considerato privato**: per questo occorre fare sempre attenzione a quanto si scrive, per evitare che in futuro il messaggio possa danneggiare lo stesso mittente. Anche lavorando di fretta e sotto pressione, per non incorrere in vere e proprie gaffe e scongiurare guai più seri in ufficio, occorre evitare di inoltrare mail con contenuto sensibile al destinatario sbagliato. Va prestata la massima attenzione: un clic di troppo ed informazioni sensibili e non divulgabili potrebbero diventare di pubblico dominio.

j) **No agli allegati troppo pesanti**: Si deve tener presente che è sconsigliato inviare allegati troppo pesanti, evitando di intasare sia la propria mailbox che quella del destinatario. Ormai la maggior parte degli utenti utilizza la posta su smartphone e tablet e ricevere allegati di grandi dimensioni può essere scomodo. Outlook 365 consente l'uso di allegati all'interno dello spazio OneDrive dove ogni utente Coopselios ha a disposizione 1 TB .

k) **Per le comunicazioni interne (colleghi) impara il gergo "asap":** Gli acronimi all'inizio possono sucitare ilarità, ma quando si inizia ad usarli si comprende quanto siano. Di seguito una lista di quelli più comuni.
FYI – Acronimo di "For Your Information", in italiano sarebbe "Per tua informazione". Si usa quando si inoltra a qualcuno uno scambio di mail per metterlo al corrente di quanto è stato detto, anzichè riassumerlo o parafrasarlo.
ASAP – Acronimo di "As Soon As Possible", significa "Il più presto possibile". Si usa per segnalare un contenuto urgente e chiedere al destinatario una risposta immediata.
RSVP – Sta per "Répondez s'il vous plaît" , cioè "Rispondete per favore". È una formula di cortesia per sollecitare una risposta, spesso riguardo alla partecipazione ad un evento o ad un meeting (sarebbe come dire "Fammi sapere se ci sarai").
TBC-TBD – Significa "To Be Confirmed – To Be Decided", cioè "Da confermare". Serve a sottolineare che un elemento è ancora in sospeso.

l) **Non rischiare:** Se si inizia una nuova conversazione o nelle mail con l'esterno, prima scrivere il testo e poi inserire il destinatario: così si evita di rischiare di spedire un testo prima di averlo finito o di averlo riletto.
Rileggere più volte e verificare che non ci siano errori ortografici, grammaticali e sintattici. Controllare anche che le correzioni automatiche siano precise (alle volte specie nei messaggi il correttore cambia il senso delle parole). Gli errori comunicano poca cura e professionalità e non sempre siamo giustificati dalla fretta.

Se la comunicazione è importante la posta deve servire solo per l'invio di un documento. Preparare la comunicazione in Word (usufruendo delle sue funzionalità e degli schemi di lettera e comunicazione predisposti), valutare se protocollare la comunicazione. Stampare il documento in PDF. Inviare la versione PDF ed archiviare la versione Word.

m) **Buona regola è quella di usare il meno possibile la posta elettronica per le comunicazioni interne**. Le comunicazione di decisioni importanti vanno prese e comunicate, se possibile, in riunione, la successiva mail potrà eventualmente inoltrare il promemoria delle decisioni prese in riunione e le documentazioni necessarie.
Inoltre può essere opportuno valutare come far diventare il lavoro di ufficio più efficace limitando interruzioni per false urgenze. Spesso chi si interrompe per leggere sistematicamente e costantemente i messaggi perde inevitabilmente la concentrazione sul lavoro programmato aumentando tempi e probabilità di errore. Le urgenze a cui si deve dare risposta immediata (incidenti, catastrofi) sono, dato il nostro lavoro, poche e non devono usare il canale mail. Per le comunicazioni urgenti va preferita una telefonata o le sirene d'allarme(es. antincendio).
In riunione è ineducato leggere la posta e la messaggistica mentre qualcuno sta parlando con noi.

## 10. Uso della rete Internet e dei relativi servizi

**La rete Internet può e deve essere utilizzata dal dipendente a supporto dell'attività lavorativa**, favorendo la comunicazione verso l'esterno e per il reperimento e la divulgazione di informazioni utili per lo svolgimento della propria professione.
**L'abilitazione ad Internet deve essere preceduta da richiesta** del diretto Responsabile al servizio ICT.
Il collegamento ad Internet dai PC aziendali dovrà avvenire **esclusivamente tramite la rete aziendale** attraverso collegamento in sede o via VPN. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, è stato attivato uno specifico sistema di filtro automatico che impedisce determinate operazioni quali lo scarico di programmi o l'accesso a determinati siti inseriti in una black-list.
L'accesso alle risorse del sistema intranet dall'esterno (ad esempio da casa) è consentito esclusivamente tramite un collegamento che necessita di autenticazione VPN (Virtual Private Network) ovvero solo gli utenti autorizzati vi possano accedere. L'abilitazione e le credenziali di accesso vengono forniti dall'ICT, previa richiesta formale con assunzione di responsabilità, verificati i requisiti di sicurezza.

**Per l'utilizzo della rete Internet possono essere impiegati esclusivamente gli applicativi "browser" (es. Microsoft EDGE, Mozilla Firefox, Chrome, ecc.) installati sulle postazioni di lavoro dal personale ICT**. Non è consentito agli operatori effettuare sulle postazioni l'installazione di qualsiasi altro applicativo per l'accesso alla rete pubblica, anche quando tale installazione risultasse tecnicamente possibile.
**E' fatto divieto all'utente lo scarico di software gratuito** (freeware) e software gratuito per un certo periodo di prova (shareware) prelevato da siti Internet, se non espressamente autorizzato dal servizio

ICT e l'uso di Internet per lo scarico di files o programmi per la fruizione di contenuto audio/video non legati ad un uso d'ufficio.
**E' fatto divieto all'utente accedere a siti che offrano contenuti audio/video tramite streaming** (stazioni radio – televisione on line, ecc.) se non espressamente autorizzati dietro richiesta del dipendente al servizio ICT.
**E' vietata 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).
**Ai dipendenti non è consentito l'impiego di Internet per attività che non rientrano tra i compiti istituzionali.** Ne è però ammesso l'utilizzo per assolvere proprie incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (ad esempio per effettuare adempimenti on line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari ed assicurativi). Tale modalità di utilizzazione di Internet deve essere contenuta nei tempi strettamente necessari allo svolgimento delle transazioni/comunicazioni e privilegiando, quando possibile, l'utilizzo delle pause di lavoro. Il fine è quello di contribuire a ridurre gli spostamenti della persone e gli oneri logistici e di personale a carico dell'amministrazione che eroga il servizio, favorendo, altresì, la dematerializzazione dei processi produttivi.

## 11. Monitoraggio e controlli

**Le attività sull'uso del servizio di accesso a internet sono automaticamente registrate in files di LOG, che riportano i dettagli della navigazione, i siti e i documenti consultati.**
Il trattamento dei dati contenuti nei LOG può avvenire esclusivamente in forma anonima e/o aggregata.
I file di LOG verranno conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza.
I dati anonimi e/o aggregati sono disponibili agli Amministratori di sistema ICT e/o dai fornitori esterni che svolgono l'attività per la Cooperativa.
I dati personali contenuti nei LOG possono essere trattati esclusivamente nei seguenti casi:

- per rispondere ad eventuali richieste dell'autorità giudiziaria o della polizia giudiziaria;
- su richiesta della Direzione Generale qualora si verifichi un evento dannoso o di pericolo che richieda un immediato intervento;
- su richiesta della Direzione Generale qualora si verifichi un utilizzo anomalo degli strumenti da parte degli utenti di una specifica Struttura;
- qualora vi sia l'evidenza o comunque il fondato sospetto che sia in corso o sia stato posto in essere un illecito.

Qualora le misure tecniche preventive non siano sufficienti ad evitare eventi dannosi o situazioni di pericolo, l'Azienda effettua con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti fasi:

- analisi aggregata del traffico di rete riferito all'intera Azienda o a sue Strutture e rilevazione della tipologia di utilizzo (e-mail, file audio, accesso a risorse estranee alle mansioni);

- emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti al settore in cui è stata rilevata l'anomalia;
- in caso di successivo permanere di una situazione non conforme, è possibile effettuare controlli circoscritti su singole postazioni di lavoro o su base individuale.
- L'utente è direttamente e totalmente responsabile dell'uso di Internet, delle informazioni che immette, delle modalità con cui opera, dei siti web o pagine internet ai quali abbia stabilito collegamento tramite link.

Con la stessa gradualità vengono effettuati controlli sull'occupazione dello spazio di memorizzazione sui server aziendali attraverso le seguenti fasi:

- analisi aggregata dei dati memorizzati sui server a livello di intera struttura lavorativa (reparto, servizio, ecc.) e rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato ) e relativa pertinenza con l'attività lavorativa;
- emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti il settore in cui è stata rilevata l'anomalia;
- in caso di successivo permanere di una situazione non conforme, è possibile procedere con un analisi puntuale ed una eventuale eliminazione del materiale non conforme anche sulle singole postazioni di lavoro.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

## 12. Non osservanza della normativa aziendale

Le disposizioni di cui al presente regolamento rivestono carattere di obbligatorietà e la loro non osservanza costituisce illecito che, quando rilevato, può portare all'instaurazione di procedimenti disciplinari a carico dell'utilizzatore che lo ha posto in essere e, ricorrendone gli estremi, alla segnalazione dello stesso alle autorità competenti.

**Cooperativa Sociale**
**Coopselios**
Società Cooperativa
C.F. e P.I. 01164310359
www.coopselios.com

Iscrizione registro imprese
RE n. 01164310359
REA RE n. 167007
Iscrizione albo società
cooperative n. A101139

# Allegato 1 DISCIPLINARE SULL'UTILIZZO DEI SISTEMI INFORMATIVI

## DISCIPLINARE INTERNO AVENTE AD OGGETTO LE REGOLE SULL'UTILIZZO DEI SISTEMI INFORMATIVI

E DI OGNI STRUMENTO DI LAVORO (IVI INCLUSO, QUALSIVOGLIA BENEFITS CD. AZIENDALE) MESSO A DISPOSIZIONE DALL'AZIENDA PER LO SVOLGIMENTO DELLA PROPRIA PRESTAZIONE LAVORATIVA E/O CARICA SOCIETARIA

**Premesse.**

**Posto che l'utilizzo, per scopi di lavoro[3] , dei sistemi informativi**[4] e di ogni strumento di lavoro ex art. 4 comma 2)[5] della Legge n. 300/1970 (Statuto dei Lavoratori) ed ex art. 173 del D.Lgs. n. 81/2008 (T.U. sulla sicurezza sul lavoro), ivi incluso qualsivoglia benefits cd. aziendale, **deve ispirarsi ai principi di buona fede, di diligenza, di correttezza[6] , di liceità, di necessità[7] , di trasparenza e di proporzionalità, COOPSELIOS** Cooperativa Sociale S.C., (C. f. e P. IVA: 01164310359) (infra "COOPSELIOS"), in persona del suo legale rappresentante pro tempore, con sede legale in Reggio Emilia (RE), via A. Gramsci, 54/S, **ha deciso di adottare**, anche nel rispetto del Provvedimento del Garante Privacy italiano n. 13 del 1.3.2007 (intitolato "Lavoro: le linee guida del

[3] Raccomandazione CM/Rec (2015)5 del Comitato dei Ministri agli Stati Membri "sul trattamento dei dati personali nel contesto occupazionale", art. 2 ("per "scopi di lavoro" si intendono i rapporti tra dipendenti [n.d.r.: o similari, quali, ad esempio, collaboratori o membri di un organo societario] e datori di lavoro per quanto riguarda l'assunzione, l'esecuzione del contratto di lavoro [n.d.r.: o similare, qual è la collaborazione o un incarico societario], la gestione, compreso l'adempimento di obblighi derivanti dalla legge o da contratti collettivi, nonché la pianificazione ed efficiente gestione di un ente e la cessazione del rapporto di lavoro [n.d.r., o di collaborazione o societario]"), art. 3 ("Nel trattamento di dati personali per scopi di lavoro dovrebbero essere garantiti il rispetto della vita privata e la protezione dei dati personali, segnatamente al fine di consentire il libero sviluppo della personalità del dipendente ed opportunità di rapporti personali e sociali sul luogo di lavoro"), art. 7 ("…si possono comunicare dati personali ai rappresentanti dei dipendenti esclusivamente nella misura in cui tali dati siano necessari per permettere a questi ultimi di rappresentare adeguatamente gli interessi dei dipendenti ovvero qualora i dati in questione siano necessari per l'adempimento ed il controllo degli obblighi fissati in contratti collettivi") ed art. 8 ("I dati personali raccolti per scopi di lavoro dovrebbero essere comunicati esclusivamente a soggetti pubblici nell'esercizio delle rispettive funzioni ufficiali ed al fine dello svolgimento di tali funzioni, ed esclusivamente nei limiti degli obblighi legali del datore di lavoro ovvero conformemente ad altre disposizioni del diritto interno"). Cfr., altresì, paragrafo 1.3.) della Raccomandazione n. R (89) 2 sull'uso dei dati personali per scopi di lavoro, adottata il 18.1.1989 dal Consiglio d'Europa: "L'espressione "per scopi di lavoro" si riferisce ai rapporti tra dipendenti e datori di lavoro per quanto riguarda il reclutamento dei dipendenti, l'esecuzione del contratto di lavoro, la gestione, compresi gli obblighi derivanti dalla legge o da contratti collettivi, e la pianificazione e l'organizzazione del lavoro".

[4] Art. 2 della Raccomandazione CM/Rec (2015)5 del Comitato dei Ministri agli Stati Membri "sul trattamento dei dati personali nel contesto occupazionale": "per "sistemi informativi" si intende qualsiasi dispositivo o gruppo di dispositivi interconnessi o correlati, dei quali uno o più di uno svolga, in base ad un programma, trattamenti automatizzati di dati informatici nonché di dati informatici memorizzati, ottenuti o trasmessi da tali dispositivi ai fini del loro funzionamento o utilizzo, della loro protezione o manutenzione".

[5] In merito, giova rilevare come sussista, ad oggi, un orientamento ondivago: (i) Garante della Protezione dei dati personali italiano, Provvedimento n. 303 del 13.7.2016 [doc. web.: 5408460]: "In tale nozione, infatti – e con riferimento agli strumenti oggetto del presente provvedimento, vale a dire servizio di posta elettronica e navigazione web – è da ritenere che possano ricomprendersi solo servizi, software o applicativi strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza. Da questo punto di vista e a titolo esemplificativo, possono essere considerati "strumenti di lavoro" alla stregua della normativa sopra citata il servizio di posta elettronica offerto ai dipendenti (mediante attribuzione di un account personale) e gli altri servizi della rete aziendale, fra cui anche il collegamento a siti internet. Costituiscono parte integrante di questi strumenti anche i sistemi e le misure che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore (ad esempio: sistemi di logging per il corretto esercizio del servizio di posta elettronica, con conservazione dei soli dati esteriori, contenuti nella cosiddetta "envelope" del messaggio, per una breve durata non superiore comunque ai sette giorni; sistemi di filtraggio anti-virus che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui server per l'erogazione dei servizi di rete; sistemi di inibizione automatica della consultazione di contenuti in rete inconferenti rispetto alle competenze istituzionali, senza registrazione del tentativo di accesso. Altri strumenti pure utili al conseguimento di una elevata sicurezza della rete aziendale, invece, non possono normalmente consentire controllo sull'attività lavorativa, non comportando un trattamento di dati personali dei dipendenti, e di conseguenza non sono assoggettati alla disciplina di cui all'art. 4 Stat. Lav. (ad es. sistemi di protezione perimetrale – firewall – in funzione di antintrusione e sistemi di prevenzione e rilevamento d'intrusione – IPS/IDS – agenti su base statistica o con il ricorso a sorgenti informative esterne. […] Anche su tale aspetto si è soffermato il Garante nelle menzionate audizioni chiarendo che i principi di necessità e proporzionalità impongono di privilegiare misure preventive ed, in ogni caso, gradualità nell'ampiezza del monitoraggio "che renda assolutamente residuali i controlli più invasivi, legittimandoli solo a fronte della rilevazione di specifiche anomalie" quali, ad esempio, la riscontrata presenza di virus e "comunque all'esito dell'esperimento di misure preventive meno limitative dei diritti dei lavoratori"; (ii) Circolare n. 2 del 7.11.2016 dell'INL: "…l'interpretazione letterale del disposto normativo [n.d.r.: art. 4 comma 2) dello Statuto del Lavoratori] porta a considerare quali strumenti di lavoro quegli apparecchi, dispositivi, apparati e congegni che costituiscono il mezzo indispensabile al lavoratore per adempiere la prestazione lavorativa dedotta in contratto, e che per tale finalità siano stati posti in uso e messi a sua disposizione"; (iii) Tribunale Ordinario di La Spezia, Sezione Lavoro, sentenza del 25.11.2016: "…si ritiene che gli strumenti richiamati dal comma 2 non siano […] esclusivamente gli strumenti indispensabili per svolgere la prestazione (tra i quali pacificamente non rientra la tessera Viacard, trattandosi di un mezzo, alternativo al denaro contante, per il pagamento dei pedaggi autostradali), bensì qualsiasi strumento utilizzato dal lavoratore nel rendere la propria prestazione. Pertanto, possono rientrare nel campo di applicazione del comma 2 anche strumenti, quali la tessera in questione, non imprescindibili, ma comunque utilizzati dai lavoratori come ausilio allo svolgimento della propria prestazione, con conseguente esclusione degli oneri di cui al comma 1".
Cfr., altresì, volume "Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro", Giuffrè, 2022, capitolo 12) paragrafo 3) ("…l'unico, testuale, elemento distintivo tra la categoria generale (di cui al primo comma) e quella circoscritta (di cui al secondo comma) è che quest'ultima si riferisce esclusivamente agli strumenti che sono direttamente "utilizzati dal lavoratore per rendere la prestazione lavorativa. E' strumento di lavoro, quindi, lo strumento assegnato al lavoratore e che sia utile per lo svolgimento della sua prestazione; non è, invece, strumento di lavoro il dispositivo o il programma applicativo che, pur essendo assegnato al lavoratore, non sia funzionale all'esecuzione della prestazione lavorativa ed abbia esclusivamente finalità di controllo […] Non convincente è altresì la tesi secondo cui lo strumento di cui trattasi debba essere "necessario", e non semplicemente "utile", ai fini dell'esecuzione della prestazione), e capitolo 16) paragrafo 3) ("…occorre pur sempre che vi sia una relazione dello "strumento" con la prestazione lavorativa […] la specificazione, "per rendere la prestazione", per non essere tautologica o ridonante, deve esprimere un significato precettivo ulteriore, che consiste appunto nel distinguere, tra tutte le funzioni "incorporate" nello strumento, quelle che attengono alla prestazione lavorativa […] la locuzione "per rendere la prestazione lavorativa" non si deve intendere in senso naturalistico ma giuridico […] Alla luce della suddetta nozione di prestazione lavorativa, si può concludere che gli strumenti di lavoro, il cui impiego non necessita di accordo sindacale o di autorizzazione, le cui informazioni sono utilizzabili ai fini del rapporto di lavoro, una volta assolti gli oneri previsti dal comma 3, sono tutti quelli che servono al lavoratore per adempiere esattamente a tutti gli obblighi derivanti dal contratto di lavoro […] Questo significa che sono strumenti di lavoro anche tutte le apparecchiature che il datore insindacabilmente ritenga servano per rendere più efficiente quantitativamente e qualitativamente la prestazione lavorativa dovuta, con i limiti, ovvi, posti dall'art. 2087 c.c. e dal motivo illecito").

[6] Cfr. Provvedimento n. 136 del 15.4.2021 [doc. web n.: 9586936] a firma del Garante Privacy italiano: "Nell'ambito del rapporto di lavoro l'obbligo di informare il dipendente è altresì espressione del principio generale di correttezza dei trattamenti, contenuto nell'art. 5, par. 1, lett. a) del Regolamento" (cfr. anche il Provvedimento n. 234 del 10.6.2021 [doc. web n. 9675440] sempre a firma del Garante Privacy italiano).

7 Cfr. Corte di giustizia dell'UE, sentenza del 9.11.2010 (nei procedimenti riuniti C-92/09 e C-93/09), passaggio 77): "…le deroghe e le limitazioni alla protezione dei dati personali devono operare entro i limiti dello stretto necessario (sentenza Satukunnan Markkinaporssi e Satamedia, cit., punto 56)".

Garante per posta elettronica e internet")[8] , **la presente policy interna**[9] (infra "Policy") **al fine di illustrare**, in un ottica di (massima) trasparenza e correttezza, **le regole circa l'utilizzo dei sistemi informativi** e di ogni strumento di lavoro o similare (es. rete internet; posta elettronica aziendale), in ossequio alle prescrizioni normative (e di soft law) comunitarie e nazionali applicabili in materia.

**1. Ambito di applicazione e pubblicità/conoscenza/accessibilità.**
1.1. **La Policy si applica a tutto il personale dipendente** e similare di COOPSELIOS, senza alcuna distinzione di ruolo, di livello e d'inquadramento, **nonché ai collaboratori di COOPSELIOS**[10] e/o, in via analogica, a tutti i soggetti che rivestono una carica societaria in COOPSELIOS, ove pertinente (infra "utente").
**La presente Policy viene consegnata, da parte di COOPSELIOS, all'atto di assunzione e/o di instaurazione di un rapporto di lavoro/collaborazione ovvero viene pubblicata nella propria intranet aziendale o in un luogo similare**.

**2. Scopo.**
2.1. La precipua finalità della Policy è quella di rendere edotto ogni utente in merito alle corrette ed idonee modalità di utilizzo di qualsivoglia sistema informativo e/o strumento di lavoro messo a disposizione, da parte di COOPSELIOS, al fine di espletare l'attività lavorativa/ruolo (anche societario) assegnata/o (infra "attività lavorativa").

**3. Personal computer.**
3.1. Il personal computer, affidato da COOPSELIOS all'utente, **è uno strumento di lavoro: pertanto, ogni utilizzo non inerente all'attività lavorativa è vietato**, in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza; tale strumento deve essere **custodito con cura e diligenza** sia all'interno del proprio luogo di lavoro sia nel caso in cui venga utilizzato nel corso di trasferte lavorative ovvero in caso di smart working.
3.2. COOPSELIOS rende noto a ciascun utente della propria facoltà di compiere, anche per il tramite di apposito personale debitamente autorizzato, interventi nel sistema informativo aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (es. aggiornamento/sostituzione/implementazione di programmi): in tal caso, COOPSELIOS si impegna a darne preventiva (o successiva, laddove l'intervento in questione rivesta carattere di improrogabile urgenza) comunicazione all'utente.
3.3. **Non è consentito l'utilizzo di programmi differenti da quelli installati da COOPSELIOS** ovvero da quest'ultima autorizzati, a meno che non siano necessariamente funzionali all'esecuzione della propria attività lavorativa.

---

8 Cfr. sul punto: "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 [...] Grava quindi sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli [...] Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse a seconda delle dimensioni della struttura, tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative. In questo quadro, può risultare opportuno adottare un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori, ecc.) e da sottoporre ad aggiornamento periodico".
9 In merito, Tribunale di Vicenza, Sezione Lavoro, sentenza del 28.10.2019: "...il comma 3 [n.d.r., dell'art. 4 dello Statuto dei Lavoratori] prevede che dev'essere fornita al lavoratore una informazione adeguata, nel senso che lo stesso deve essere portato a conoscenza della possibilità di essere assoggettato ai controlli, anche tecnologici, da parte del datore di lavoro. Questa informazione deve inoltre riguardare anche le modalità e i limiti con cui vengono posti in essere. L'informativa si considera adeguata se determina la consapevolezza in capo al lavoratore circa il fatto che gli strumenti che utilizza per svolgere la propria attività lavorativa producono delle informazioni che possono essere conosciute e utilizzate dal datore di lavoro a fini disciplinari"; cfr., altresì, Tribunale di Venezia, sentenza del 6.8.2021, in base al quale è sufficiente l'affissione della Policy nell'intranet aziendale (in una apposita cartella di rete) ovvero, in subordine, accanto al distributore automatico del caffè; cfr. anche il Documento di lavoro n. 55 del 29.5.2002 del WP Art. 29 (ora, EDPB): "...il fatto che il datore di lavoro fornisca ad un dipendente informazioni adeguate al proposito può ridurre le legittime aspettative di riservatezza di quest'ultimo".
10 Fatte salve alcune limitazioni circa la cogente applicazione delle tutele prescritte dall'art. 3 dello Statuto dei Lavoratori, potenzialmente non usufruibili dai lavoratori ex art. 409 comma 1) n. 3) c.p.c. e dai lavoratori ex art. 2 comma 2) del D.Lgs. n. 81/2015, così come modificato dal D.L. n. 101/2019: sul punto, volume "Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro", Giuffrè, 2022, capitolo 27) paragrafo 4): "...l'art. 4 può essere considerato una delle "punte di diamante" del diritto del lavoro italiano, nonostante sia stato comprensibilmente al centro di un intenso dibattito dottrinale sia prima che dopo le modifiche subite nell'ambito della riforma del mercato del lavoro complessivamente nota come Jobs Act. [...] inevitabile interrogarsi in merito alle possibilità di applicare l'art. 4 anche oltre i confini della subordinazione, ossia ai rapporti di lavoro parasubordinato e, più nello specifico, alle tante tribolate collaborazioni etero-organizzate di cui all'art. 2, d.lgs. n. 81/2015 [...] Tali considerazioni preliminari non possono che trovare la loro fonte nell'individuazione della finalità della norma, che risulta di grande rilievo per la particolare commistione di interessi coinvolti. E difatti, se da un lato essi attengono ad elementi di natura prettamente economica e imprenditoriale (pur tutelati a livello costituzionale dall'art. 41), dall'altro lato si scontrano con le necessità di tutela della persona in quanto tale e in quanto soggetto che, proprio attraverso il lavoro, si inoltra nel percorso di emancipazione individuale e sociale costruito dal combinato disposto dei primi quattro articoli della Carta Costituzionale, non a caso contenenti i "principi fondamentali" sui quali si fonda la Repubblica italiana. E' proprio in considerazione del "lavoro" inteso quale "principe dei diritti sociali" e quale strumento primario di sviluppo della personalità, nella sua componente individuale e collettiva, tutelato in "tutte le sue forme e applicazioni" dall'art. 35 della Costituzione, che occorre interrogarsi circa la legittimità di escludere un'intera categoria di lavoratori dalla protezione da ingerenze altrui nella sfera di riservatezza personale, solo in ragione dell'assenza del potere direttivo tipico del rapporto di lavoro subordinato [...] può applicarsi la disciplina appena tratteggiata anche a categorie di lavoratori non subordinati che pure, per le modalità di realizzazione dell'attività di coordinamento (più o meno accentuato) con l'organizzazione produttiva della controparte negoziale, si trovino in una situazione di sottoposizione all'altrui raccolta, utilizzo e archiviazione di dati equiparabile in una parola alla para subordinazione? [...] il tentativo di risposta non può prescindere dalla distinzione del lavoro para subordinato in due species: da un lato, le collaborazioni di cui all'art. 409, co. 1, n. 3, c.p.c., ovvero quelle collaborazioni che ci concretano in una prestazione d'opera coordinata e continuativa, prevalentemente personale, anche se a carattere non subordinato; dall'altro lato, le collaborazioni organizzate dal committente di cui al primo comma dell'art. 2, d.lgs. n. 81/2015, così come modificate per effetto del d.l. n. 101/2019, ovvero quelle collaborazioni che si concretano in "prestazioni di lavoro prevalentemente personali, continuative e le cui modalità di esecuzione sono organizzate dal committente [...] Se così è, sembrerebbe pacifico sostenere la necessità di applicare l'art. 4, con l'intera disciplina dei controlli da remoto in essa contenuta, anche alle collaborazioni organizzate dal committente [...] Più complessa risulta la soluzione della questione con riferimento alle altre tipologie di lavoro parasubordinato e, segnatamente, alle collaborazioni coordinate e continuative ex art. 409 c.p.c. e alle collaborazioni, anche organizzate dal committente, rientranti nell'ambito di applicazione del secondo comma del citato art. 2. In tali ipotesi, difatti, non è prevista l'estensione dello statuto protettivo del lavoro subordinato, di tal che, dato il superamento delle regole sul lavoro a progetto e fermo il rispetto delle specifiche norme di tutela che sono state nel tempo elaborate dal Legislatore, la disciplina della collaborazione è rimessa all'autonomia individuale o collettiva. Mancando un "appiglio normativo" e in assenza di un chiaro pronunciamento del Garante in tal senso, la strada dell'applicazione estensiva dell'art. 4 anche a tali tipologie di lavoratori parasubordinati risulta irta di ostacoli ed assai difficoltosa".

3.4. E' assolutamente vietato l'utilizzo di personal computer privato a scopo aziendale, questo infatti, se non opportunamente protetto, potrebbe essere veicolo di Virus ed altri programmi malevoli.

**4. Rete aziendale (intranet).**
4.1. Ai fini dell'accesso alla rete interna aziendale (intranet), COOPSELIOS si impegna, ove necessario, a fornire all'utente le specifiche credenziali di autenticazione; di conseguenza, **è vietato accedere alla rete aziendale mediante un codice d'identificazione utente differente da quello assegnato,** a meno che vi siano comprovate (anche urgenti) esigenze lavorative.
4.2. Le cartelle presenti all'interno del server aziendale sono da intendersi quali aree di condivisione di informazioni strettamente professionali e, dunque, non possono essere utilizzate per scopi differenti, fatte salve specifiche autorizzazioni da parte di COOPSELIOS; pertanto, **qualunque file che non sia legato all'attività lavorativa non può essere dislocato**, nemmeno per brevi periodi, in queste unità, fatte salve particolari ed eccezionali ipotesi.

**5. Supporti rimovibili.**
5.1. I supporti rimovibili (es. USB key), contenenti informazioni aziendali di qualsivoglia natura ovvero costituenti il know how (materiale/immateriale) aziendale o di terzi soggetti, devono essere trattati con particolare cautela, onde evitare che il loro contenuto possa essere trafugato, alterato, distrutto o conosciuto da soggetti cd. terzi non autorizzati.
L'utente assegnatario di un supporto rimovibile è tenuto a comunicare, senza ingiustificato ritardo, a COOPSELIOS l'eventuale furto, smarrimento ovvero guasto di esso.
5.2. E' assolutamente vietato l'utilizzo di supporti rimovibili privati a scopo aziendale, questi infatti, se non opportunamente protetti, potrebbero essere veicolo di Virus ed altri programmi malevoli.

**6. Posta elettronica.**
6.1. **La casella di posta elettronica[11] , assegnata all'utente da parte di COOPSELIOS, è uno strumento di lavoro.**
E', pertanto, vietato utilizzarla per motivi differenti da quelli strettamente legati all'attività lavorativa, fatte salve le specifiche ipotesi autorizzate da COOPSELIOS: di conseguenza, eventuali messaggi di posta elettronica ricevuti da terzi soggetti non direttamente o indirettamente connessi all'attività lavorativa da espletare in nome e per conto di COOPSELIOS dovranno essere immediatamente cancellati, previo eventuale inoltro ad un proprio (ed extra lavorativo) indirizzo di posta elettronica.
6.2. **In caso di definitiva cessazione del rapporto di lavoro/ruolo, l'utente è tenuto, da un lato, ad eliminare tutti i messaggi e documenti non pertinenti all'attività lavorativa e non utili alle esigenze aziendali, mantenendo, tuttavia, integra tutta la corrispondenza e la documentazione inerente all'attività lavorativa espletata e da eseguire pro futuro**; dall'altro lato, l'utente è tenuto, in tal caso, ad eliminare qualsivoglia documento/link/abbonamento (anche gratuito)/iscrizione effettuata, per motivi extra lavorativi, tramite l'ausilio della posta elettronica aziendale.
Laddove ricorra l'ipotesi in questione, COOPSELIOS precisa che, nel rispetto del consolidato pensiero giurisprudenziale in materia nonché nel rispetto della normativa (comunitaria e nazionale) sulla protezione dei dati personali[12] , il proprio account di posta elettronica aziendale (es. nome.cognome@azienda.it) verrà rimosso, immediatamente o comunque entro un termine ragionevole (commisurato ai tempi tecnici di predisposizione delle necessarie misure)[13] , al termine del rapporto di lavoro/ruolo, previa disattivazione dello stesso (mediante l'implementazione di un messaggio automatico di cd. mancato recapito) e contestuale adozione di un sistema (automatico) volto ad informare terzi ed a fornire a quest'ultimi indirizzi di posta elettronica alternativi riferiti all'attività imprenditoriale di COOPSELIOS.
Oltre a ciò, COOPSELIOS comunica all'utente che, in caso di definitiva cessazione del rapporto di lavoro/ruolo, quest'ultimo provvederà a conservare i messaggi di posta elettronica racchiusi all'interno del relativo indirizzo (ed utili e pertinenti per il proseguo dell'attività lavorativa e delle esigenze aziendali) per un termine (medio) di 2 anni (periodo temporale soggetto ad una eventuale riduzione o estensione, a seconda dello specifico ruolo (anche societario) rivestito dall'(ex) utente), decorrenti dall'effettiva cessazione del relativo rapporto di lavoro/ruolo[14]: tale termine è da considerarsi mediamente proporzionato/congruo, al fine così d'individuare un

[11] Cfr. Provvedimento n. 13 del 1.3.2007 a firma del Garante Privacy italiano: "Il contenuto dei messaggi di posta elettronica – come pure i dati esteriori delle comunicazioni e i file allegati – riguardano forme di corrispondenza assiste da garanzie di segretezza tutelate anche costituzionalmente, la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale). Tuttavia con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa. La mancata esplicitazione di una policy al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione. Tali incertezze si riverberano sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro che intenda apprendere il contenuto dei messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore (posta "in entrata") o di quelli inviati da quest'ultimo (posta "in uscita")".
[12] Cfr. in ambito comunitario: art. 8 della Convenzione europea dei diritti dell'uomo; pronunzie della Corte europea dei diritti dell'uomo: Niemietz c. Allemagne 16.12.1992 (ric. n. 13710/88), spec. par. 29; Copland v. UK, 3.4.2007 (ric. n. 62617/00), spec. par. 41; Barbulescu v. Romania, 5.9.2017 (ric. n. 61496/08), spec. par. 70-73; Antovi and Mirkovi v. Montenegro, 28.11.2017 (ric. n. 70838/13), spec. par. 41-42. In ambito nazionale, inter alia: artt. 2 e 41 comma 2) della Costituzione; Provvedimento del Garante Privacy n. 115 del 2.7.2020, n. 216 del 4.12.2019, n. 53 del 1.2.2018, n. 547 del 22.12.2016, n. 136 del 5.3.2015, n. 551 del 27.11.2014 e n. 58 del 10.3.2007.
[13] Cfr. Provvedimento n. 216 del 4.12.2019 [doc. web n. 9215890], n. 53 del 1.2.2018 [doc. web n. 8159221] e n. 136 del 5.3.2015 [doc. web n. 3985524] a firma del Garante Privacy italiano.
[14] Cfr. Provvedimento n. 472 del 17.7.2024 [doc. web n. 10053224] del Garante Privacy.

giusto equilibro tra gli interessi dei soggetti coinvolti, ossia l'interesse economico/imprenditoriale di COOPSELIOS teso a consentire il normale proseguo/continuità dell'attività d'impresa[15] e l'interesse alla riservatezza dell'ex utente.
Nel corso di tale termine, COOPSELIOS si riserva la facoltà di accedere soltanto a quelle comunicazioni, racchiuse all'interno della casella di posta elettronica del relativo ex utente, che sono state valutate come strettamente necessarie al fine di garantire la continuità aziendale, fatte salve specifiche e comprovate esigenze di far valere e tutelare un diritto, anche in sede giudiziale.
Una volta decorso tale termine, COOPSELIOS si impegna, invece, a cancellare, distruggere o anonimizzazione l'integrale contenuto racchiuso all'interno della casella di posta elettronica aziendale del relativo ex utente.
6.3. Nell'ipotesi in cui all'utente venga assegnato, da parte di COOPSELIOS, un indirizzo di posta elettronica descritto al precedente art. 6.2. ovvero un indirizzo di posta elettronica cd. funzionale (es. area@azienda.it), quest'ultima si impegna, ove necessario, a mettere a disposizione dell'utente apposite funzionalità di sistema (e di agevole utilizzo) che consentano di inviare automaticamente, in caso di assenza programmata e/o non programmata, messaggi di risposta contenenti le "coordinate" (elettroniche e/o telefoniche) di un altro utente o altre utili modalità di contatto dell'azienda.
Inoltre, in caso di eventuali assenze programmate e/o non programmate, COOPSELIOS si riserva, altresì, la facoltà, ove ritenuto necessario al fine di garantire la continuità aziendale, di disporre, in modo autonomo, l'attivazione della sopra descritta funzionalità di sistema ovvero di delegare un altro lavoratore (cd. fiduciario) alla verifica (e conseguente eventuale risposta e/o inoltro) del contenuto dei messaggi di posta elettronica ritenuti rilevanti per lo svolgimento dell'attività imprenditoriale racchiusi all'interno del citato indirizzo di posta elettronica, previo (o successivo, in caso di improrogabile urgenza) avvertimento all'utente interessato: a tal riguardo, COOPSELIOS precisa che quest'ultima ipotesi (ossia, di delega al cd. fiduciario) è eventualmente esercitabile anche, in modo diretto, da parte dell'utente interessato, laddove si registri un assenza dello stesso e nel caso in cui sussista, a parere insindacabile di COOPSELIOS, la necessità di garantire la continuità aziendale[16] .

**7. Navigazione in internet.**
7.1. **Il personal computer, assegnato al singolo utente ed abilitato alla navigazione in internet, costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa**. E', quindi, proibita la navigazione in Internet per motivi differenti da quelli legati all'attività lavorativa, fatta salva l'eventuale autorizzazione da parte di COOPSELIOS ovvero per particolari ed eccezionali ipotesi.
Al fine di evitare la navigazione in siti internet non pertinenti all'attività lavorativa, COOPSELIOS comunica che può eventualmente adottare, a sua discrezione, un sistema di blocco o filtro automatico teso a prevenire determinate operazioni quali l'upload o l'accesso a determinati siti internet inseriti in una eventuale black list.
7.2. Al tal riguardo, COOPSELIOS comunica, in via generale, all'utente che: i) non è consentito visitare siti internet non inerenti e/o non necessari per lo svolgimento delle mansioni lavorative affidate, né tantomeno siti internet aventi ad oggetto contenuti contrari all'etica comune ovvero a qualsivoglia disposizione normativa; ii) non è consentita alcuna forma di registrazione a siti internet non necessari direttamente e/o indirettamente allo svolgimento della mansione lavorativa assegnata; iii) non è consentito installare prodotti e/o programmi elettronici in violazione della normativa sul diritto d'autore o altra normativa applicabile in materia.

**8. Utilizzo del telefono/cellulare/sistema di messaggistica/chat aziendale.**
8.1. **Il telefono** (e/o cellulare)[17] , ivi inclusa l'eventuale applicazione di messaggistica istantanea/chat aziendale installata o da installare (es. whatsapp), affidato all'utente **è uno strumento di lavoro** [18] ; pertanto, ne viene concesso l'uso esclusivamente per lo svolgimento

[15] Cfr. volume "Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro", Giuffrè, 2022, capitolo 3) paragrafo 2): "La libertà d'impresa è, come noto, l'essenza stessa del Trattato di Roma e del mercato unico. Il concetto di libertà d'impresa, nel sistema del diritto dell'UE, è molto ampio e ricomprende l'esercizio di ogni attività economica sia su base individuale che su base collettiva. L'art. 16 della Carta precisa, tuttavia, che l'esercizio della libertà d'impresa deve avvenire in conformità al diritto dell'Unione e delle legislazioni e prassi nazionali ed è, dunque, nel diritto dell'Unione che devono, innanzitutto, essere ricercate le garanzie e i limiti all'esercizio dell'attività di impresa. E' noto, altresì, che, ai sensi dell'art. 52, par. 3, della Carta, nel caso di corrispondenza dei diritti da questa previsti con quelli della Convenzione europea dei diritti dell'uomo e dei relativi Protocolli, significato e portata sono definiti da quest'ultima. Quest'ultimo passaggio è centrale perché consente di porre al centro dell'analisi giuridica del rapporto tra libertà d'impresa e dignità del lavoratore (nella prospettiva della sua riservatezza), il sistema della Convenzione europea dei diritti dell'uomo [...] L'art. 88 del Regolamento UE 2016/679 presuppone un criterio di bilanciamento mobile che deve rispettare i criteri di proporzionalità, necessità e finalità come ricostruiti dalla giurisprudenza della Corte di Giustizia e della Corte europea dei diritti dell'uomo. Tutto ciò, del resto, è stato ribadito dal punto 10 c del "European Social Pillar" approvato al Vertice sociale di Goteborg il 16 novembre 2017 [...] Si noti che la centralità della persona e della tutela della sua riservatezza va ben oltre il ristretto ambito del lavoro subordinato in quanto, nella prospettiva della Convenzione europea dei diritti dell'uomo, del Regolamento 2016/679 e della Carta, non rileva la qualificazione giuridica del rapporto che lega datore di lavoro e lavoratore, ma la, più semplice, relazione tra "titolare" e "interessato"".
[16] Cfr. Raccomandazione CM/Rec (2015)5 del Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazione, paragrafo 14.3.): "Il datore di lavoro può accedere alle comunicazioni elettroniche di natura professionale dei dipendenti, informati preventivamente dell'esistenza di tale possibilità, soltanto se ciò risulti necessario per finalità di sicurezza o per altre finalità comunque legittime. In caso di assenza del dipendente, il datore di lavoro dovrebbe prendere le misure necessarie e prevedere idonee procedure al fine di consentire l'accesso a comunicazioni elettroniche di natura professionale soltanto se tale accesso rappresenti una necessità di ordine professionale. L'accesso dovrebbe avvenire nel modo meno intrusivo possibile e solo previa informazione del dipendente interessato".
[17] Cfr. sul punto: Provvedimento del Garante Privacy italiano del 13.3.2008 [doc. web n. 1522362] circa la possibilità di ottenere, ove richiesto, l'indicazione in "chiaro" delle ultime tre cifre delle bollette telefoniche, in deroga rispetto a quanto disposto dall'art. 124 comma 4) del novellato D.Lgs. n. 196/2003 (Codice Privacy); Provvedimento del Garante Privacy italiano n. 3 del 1.1.2018 [doc. web n.: 7554790] circa la (potenziale) sussistenza, in capo ad un datore di lavoro, dell'interesse legittimo teso a controllare, previo rispetto delle prescrizioni racchiuse all'interno dell'art. 4 della Legge n. 300/1970, la fatturazione e l'andamento dei consumi, al fine di valutare, ove necessario, l'adeguatezza del contratto sottoscritto con il relativo fornitore di un servizio di comunicazione elettronica.
[18] Cfr. Tribunale Ordinario di Milano, Sezione Lavoro, sentenza 24.10.2017: "Il vincolo di strumentalità con lo svolgimento della prestazione lavorativa, previsto dalla norma, deve sussistere con riguardo a tutta la vasta categoria degli "strumenti" potenzialmente idonei al controllo. Ove vengano in rilievo apparati per l'informatica e le telecomunicazioni, occorre allora distinguere tra componenti hardware e componenti software e verificare, in relazione a ciascuna di esse (da considerarsi quale distinto "strumento" ai sensi della norma in esame), se sia ravvisabile il nesso di funzionalizzazione allo svolgimento della prestazione lavorativa [...] Lo smart phone, infatti, non può essere considerato, ai fini che qui interessano, come strumento unitario ed inscindibile; esso è formato da una pluralità di componenti hardware (apparato telefonico, GPS, CPU etc.) e sofware (sistema operativo, programmi e applicazioni, tra cui whatsapp). Ognuna di tali componenti va considerata come autonomo "strumento" di lavoro e di potenziale controllo".

dell'attività lavorativa, **non essendo quindi consentite comunicazioni a carattere personale** o comunque non strettamente inerenti l'attività lavorativa stessa, fatti salvi i casi di comprovata necessità e/o urgenza ovvero i casi di preventiva autorizzazione da parte di COOPSELIOS.
L'eventuale uso cd. promiscuo di uno o più di tali strumenti è possibile soltanto in presenza di una preventiva autorizzazione da parte di COOPSELIOS. Infine, il relativo utente assegnatario è tenuto a comunicare, senza ingiustificato ritardo, a COOPSELIOS l'eventuale furto, smarrimento ovvero guasto di esso.

**9. Utilizzo di carte di credito, fuel card, viacard e autoveicolo (eventualmente dotato di telepass).**
9.1. COOPSELIOS ricorda all'utente assegnatario di uno o più dei benefits in questione che gli stessi dovranno essere inderogabilmente ed **esclusivamente utilizzati per l'espletamento della mansione lavorativa assegnata**, fatte salve specifiche autorizzazioni ad opera di COOPSELIOS; altresì, COOPSELIOS ricorda che il lavoratore assegnatario di uno o più dei descritti benefits è tenuto a comunicare, senza ingiustificato ritardo, a quest'ultima l'eventuale furto, smarrimento ovvero guasto di essi.

**10. Sistema di controlli.**
10.1. **COOPSELIOS** – consapevole del fatto che il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità del soggetto interessato, garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore ed una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (cfr. artt. 2 e 41 comma 2 della Costituzione; art. 2 comma 5) del D.Lgs. n. 82 del 7.3.2005; art. 8 comma 1) della Convenzione Europea dei Diritti dell'Uomo) – **comunica che l'utilizzo degli strumenti aziendali sopra descritti producono delle informazioni**[19] **che possono essere conosciute ed utilizzate da COOPSELIOS per l'esecuzione delle tipologie di controlli**[20] (difensivi)[21] sotto illustrati, eseguibili da apposito personale (anche esterno) previamente autorizzato da COOPSELIOS.

[19] In particolar modo, costituite dai dati personali ex art. 4 n. 1) del GDPR.
[20] La relativa base giuridica del trattamento si rinviene, in particolare, nelle seguenti disposizioni normative: art. 6 paragrafo 1) lettera f) del GDPR (cfr. Parere n. 6/2014 del WP Art. 29); art. 9 paragrafo 2) lettera f) del GDPR.
[21] Volume "Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro", Giuffrè, 2022, capitolo 15) paragrafo 1): "La formula "controlli difensivi" individua nell'uso comune la species delle verifiche disposte dal datore di lavoro per accertare comportamenti illeciti dei propri dipendenti lesivi del patrimonio aziendale".

A tal fine, **COOPSELIOS si riserva la facoltà di effettuare un "controllo cd. difensivo ex post"**[22] laddove ne sussistano i relativi presupposti ovvero **un controllo volto a verificare eventuali eventi anomali[23] , lesivi o pericolosi del patrimonio[24] , del business** e/o della sicurezza aziendale riguardanti, anche in modo congiunto tra di loro, gli strumenti ex art. 4 comma 2) dello Statuto dei Lavoratori, e i sistemi informativi, **gli archivi automatizzati, parzialmente automatizzati ovvero non automatizzati**, nel rispetto, inter alia, dei principi di pertinenza, di non eccedenza, di necessità, di proporzionalità, di buona fede, di correttezza e di ragionevolezza.

[22] In merito, i giudici di legittimità hanno affermato che esulano dal campo di applicazione dell'art. 4 dello Statuto dei Lavoratori (e, dunque, non richiedono l'osservanza delle garanzie ivi previste) i controlli difensivi da parte del datore di lavoro se diretti ad accertare comportamenti illeciti e lesivi del patrimonio e dell'immagine aziendale, tanto più quando sono effettuati ex post, ossia dopo l'attuazione del comportamento in addebito, così da prescindere dalla mera sorveglianza sull'esecuzione della prestazione lavorativa (cfr. Corte di Cassazione, sentenze n. 13226/2018 e n. 22662/2016). La ratio di tale principio risiede nel presupposto che "l'interpretazione della disposizione (L. n. 300 del 1970, art. 4) va ispirata ad un equo e ragionevole bilanciamento fra le disposizioni costituzionali che garantiscono il diritto alla dignità e libertà del lavoratore nell'esercizio delle sue prestazioni oltre al diritto del cittadino al rispetto della propria persona (artt. 1, 3, 35 e 38 Cost.), ed il libero esercizio dell'attività imprenditoriale (art. 41 Cost.), con l'ulteriore considerazione che non risponderebbe ad alcun criterio logico-sistematico garantire al lavoratore – in presenza di condotte illeciti sanzionabili penalmente o con la sanzione espulsiva – una tutela della sua "persona" maggiore di quella riconosciuta ai terzi estranei all'impresa (così, testualmente, in motivazione, Corte di Cassazione n. 10636/2017). Cfr., altresì, Corte di Cassazione sez. lavoro n. 10955 del 27.5.2015: "…può trarsi il principio della tendenziale ammissibilità dei controlli difensivi "occulti", anche ad opera di personale estraneo all'organizzazione aziendale, in quanto diretti all'accertamento di comportamenti illeciti diversi dal mero inadempimento della prestazione lavorativa, sotto il profilo quantitativo e qualitativo, ferma comunque restando la necessaria esplicazione delle attività di accertamento mediante modalità non eccessivamente invasive e rispettose delle garanzie di libertà e dignità dei dipendenti, con le quali l'interesse del datore di lavoro al controllo ed alla difesa ed alla difesa della organizzazione produttiva aziendale deve contemperarsi, e, in ogni caso, sempre secondo i canoni generali della correttezza e buona fede contrattuale". Sul punto, cfr. altresì Corte di Cassazione, Sezione Lavoro, sentenza n. 25732 del 22.9.2021: "La giurisprudenza di questa Corte ha quindi elaborato, onde consentire al datore di lavoro di contrastare comportamenti illeciti del personale, la categoria dei cd. "controlli difensivi". Secondo l'indirizzo giurisprudenziale più recente e più evoluto, "esulano dall'ambito di applicazione dell'art. 4, comma 2, St. lav. (nel testo anteriore alle modifiche di cui all'art. 23, comma 1, del d.lgs. n. 151 del 2015) e non richiedono l'osservanza delle garanzie ivi previste, i "controlli difensivi" da parte del datore se diretti ad accertare comportamenti illeciti e lesivi del patrimonio e dell'immagine aziendale, tanto più se disposti ex post, ossia dopo l'attuazione del comportamento in addebito, così da prescindere dalla mera sorveglianza sull'esecuzione della prestazione lavorativa […]. In altri termini, i controlli datoriali a distanza, detti "difensivi", non erano assoggettati ai presupposti di legittimità stabiliti dal previgente art. 4, secondo comma, St. lav. in presenza di due condizioni necessarie e di una eventuale. Era in primo luogo indispensabile che l'iniziativa datoriale avesse la finalità specifica di accertare determinati comportamenti illeciti del lavoratore. […] L'altro presupposto necessario era che gli illeciti da accertare fossero lesivi del patrimonio o dell'immagine aziendale. […] Il terzo presupposto era che i controlli fossero stati disposti ex post, ossia dopo l'attuazione del comportamento in addebito, così da prescindere dalla mera sorveglianza sull'esecuzione della prestazione lavorativa. […] Sebbene i "controlli difensivi" fossero sottratti all'area di operatività dell'originaria versione dell'art. 4, comma 2, St. lav., era chiaro nella giurisprudenza che essi non potevano comunque essere esercitati liberamente dal datore di lavoro al di fuori di regole di civiltà e di criteri ragionevoli volti a garantire, con l'impiego di determinati accorgimenti e cautele, un adeguato bilanciamento tra le esigenze di salvaguardia della dignità e riservatezza del dipendente e quelle di protezione, da parte del datore di lavoro, dei beni (in senso lato) aziendali. Sicché la disciplina dei controlli in questione è stata ricostruita mediante il richiamo ai principi di buona fede e correttezza. […] Ritiene la Corte che possa soccorrere in questo contesto la distinzione tra i "controlli difensivi" in senso lato e quelli in senso stretto. […] Occorre perciò distinguere tra i controlli a difesa del patrimonio aziendale che riguardano tutti i dipendenti (o gruppi di dipendenti) nello svolgimento della loro prestazione di lavoro che li pone a contatto con tale patrimonio, controlli che dovranno essere necessariamente realizzati nel rispetto delle previsioni dell'art. 4 novellati in tutti i suoi aspetti e "controlli" difensivi" in senso stretto, diretti ad accertare specificamente condotte ascrivibili – in base a concreti indizi – a singoli dipendenti, anche se questi si verifica durante la prestazione di lavoro. Si può ritenere che questi ultimi controlli, anche se effettuati con strumenti tecnologici, non avendo ad oggetto la normale attività del lavoratore, si situino, anche oggi, all'esterno del perimetro applicativo dell'art. 4. […] Può, quindi, in buona sostanza, parlarsi di controllo ex post solo ove, a seguito del fondato sospetto del datore circa la commissione di illeciti ad opera del lavoratore, il datore stesso provveda, da quel momento, alla raccolta delle informazioni. […] seguente principio di diritto: "Sono consentiti i controlli anche tecnologici posti in essere dal datore di lavoro finalizzati alla tutela dei beni estranei al rapporto di lavoro o ad evitare comportamenti illeciti, in presenza di un fondato sospetto circa la commissione di un illecito, purché sia assicurato un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore, sempre che il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto". Cfr. Corte di Cassazione, sez. lavoro, sentenza n. 4375 del 23.2.2010: "insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti non può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore".

[23] Cfr. Tribunale Ordinario di La Spezia, Sezione Lavoro, sentenza del 25. 11.2016: "…l'interpretazione della norma non può spingersi sino al punto di ritenere l'applicabilità della stessa e, dunque, la necessità dell'informativa, anche nel caso in cui il controllo sia finalizzato all'accertamento di illeciti completamente avulsi dalla prestazione lavorativa. Milita in questo senso la stessa formulazione letterale della nuova disposizione: l'art. 4 novellato, infatti, richiama le esigenze organizzative e produttive, la sicurezza del lavoro e la tutela del patrimonio come esclusive finalità in funzione delle quali possono essere installati strumenti che consentano il controllo a distanza dell'attività dei lavoratori. Pertanto, l'informativa che va data è relativa alla possibilità che sia controllata l'attività lavorativa, per ragioni, tra le altre, di tutela del patrimonio aziendale. Non si ritiene invece necessario dover informare il lavoratore che lo strumento dal quale derivi la possibilità di controllo, se verrà utilizzato al di fuori dell'orario di lavoro o comunque per finalità estranee allo svolgimento della prestazione, potrà essere utilizzato per contestare illeciti che, per l'appunto, non hanno alcuna connessione, neppure indiretta, con l'attività lavorativa. Riportando dunque tale astratta distinzione alla concrete tipologie di controlli, si ritiene che il datore di lavoro debba dare l'informativa preventiva di cui al comma 3 per poter utilizzare le informazioni raccolte al fine di contestare illeciti che, anche se non hanno direttamente ad oggetto l'esatto adempimento dello svolgimento della prestazione lavorativa, sono comunque ad essa connessi, quantomeno dal punto di vista temporale. Si pensi, tra i casi scrutinati dalla giurisprudenza intervenuta sul previgente art. 4, all'ipotesi del lavoratore sanzionato perché sorpreso a conversare oppure al caso della mancata registrazione della vendita da parte dell'addetto alla cassa di un esercizio commerciale, con appropriazione delle somme incassate (Cass., n. 18821/2008), o, ancora, l'effettuazione di telefonate ingiustificate durante l'orario di lavoro (Cass., n. 4746/2002). Dovrebbero, invece, ad avviso di chi scrive, esulare dal campo di applicazione dell'art. 4, anche nella sua formulazione novellata, i controlli che hanno ad oggetto illeciti estranei allo svolgimento della prestazione lavorativa, quali, ad esempio, la trasmissione a terzi di informazioni riservate acquisite in ragione del servizio…" (ex multis, Tribunale di Torino, sentenza n. 1664 del 19.9.2018: "esulano dal campo di applicazione di tale norma i controlli che hanno ad oggetto illeciti estranei allo svolgimento della prestazione lavorativa ovvero riguardano la tutela dei beni estranei al rapporto stesso").

[24] Volume "Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro", Giuffrè, 2022, capitolo 15) paragrafo 2): "…nel "patrimonio aziendale" possiamo annoverare, non solo eventuali beni materiali e immateriali dell'impresa, ivi compresi brevetti, diritti di esclusiva, informazioni riservate, ecc., ma anche l'"immagine esterna" dell'impresa "così come accreditata presso il pubblico. E finanche dare protezione al riconoscibile posizionamento e avviamento sul mercato dell'impresa datore di lavoro" (cfr. Corte di Cassazione, sentenze n. 2722 del 23.2.2012 e n. 9904 del 13.5.2016).

Al di là della fattispecie del "controllo cd. difensivo ex post", i controlli poc'anzi annunziati[25] possono essere eseguiti[26] , da parte di COOPSELIOS, a "tutti i fini connessi al rapporto di lavoro" ex art. 4 comma 3) dello Statuto dei Lavoratori [27] (ivi inclusi, dunque, quelli disciplinari ovvero per svolgere investigazioni difensive (anche nei confronti di comportamenti illeciti/abusivi/anomali/pericolosi del patrimonio, dell'immagine, della reputazione, del posizionamento sul mercato, del business (anche potenziale), della sicurezza, dell'integrità (anche fisica/tecnica/organizzativa/commerciale/imprenditoriale) del patrimonio, del business e della sicurezza aziendale) ovvero per far valere o difendere un diritto di COOPSELIOS, anche in sede giudiziaria[28] ), preferibilmente mediante l'utilizzo delle seguenti modalità, da scegliere a seconda delle specifiche circostanze: (i) controlli in forma aggregata ed anonima: COOPSELIOS provvederà ad effettuare controlli preliminari sui dati aggregati riferiti all'intera struttura lavorativa ovvero ad una o più aree della stessa; tali controlli (i quali si svolgeranno in forma anonima) si concluderanno con un avviso generalizzato (ovvero circoscritto al personale afferente all'area o settore in cui è stata individuata l'anomalia) circa un rilevato utilizzo anomalo di uno o più strumenti aziendali, sistemi informativi, archivi automatizzati, parzialmente automatizzati ovvero non automatizzati ovvero circa un rilevato comportamento anomalo/illecito/abusivo, e con l'invito ad attenersi scrupolosamente alle mansioni e/o al ruolo assegnate/o oltre che alla Policy[29] , oltre che alla normativa applicabile in materia; (ii) controlli in forma individuale[30] : nel caso in cui l'utilizzo anomalo di uno o più strumenti ex art. 4 comma 2) dello Statuto dei Lavoratori ovvero nel caso in cui un'anomalia riguardi uno o più sistemi informativi, archivi automatizzati, parzialmente automatizzati ovvero non automatizzati ovvero nel caso di un comportamento anomalo/illecito/abusivo sia grave, rilevante o comunque degno di attenzione, COOPSELIOS si riserva il diritto di procedere ad effettuare controlli su base individuale.

---

[25] Cfr. Tribunale di Venezia, sentenza del 6.8.2021: "Costituisce, infatti, dato acquisito a far data dalla Novella dell'art. 4 SL, che le informazioni ottenute per il tramite degli strumenti utilizzati per la prestazione lavorativa, ben possono essere utilizzate a prescindere dalla loro natura/finalità difensiva, ma tale utilizzabilità necessita che siano soddisfatti gli adempimenti e i requisiti di cui al 3° comma. In base alla nuova formulazione della norma il datore può, infatti, trarre informazioni dagli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, con possibilità dunque di controllo a distanza, e può farlo a tutti i fini connessi al rapporto di lavoro (dunque, per quanto qui interessa, anche a fini disciplinari), a condizione, tuttavia, ex comma 3, 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". Sul punto la recente pronuncia della Cassazione n. 4871 del 24 febbraio 2020 afferma che – ai sensi dell'art. 4, comma 3, L. 300/1970, come sostituito dall'art. 23 D.Lgs. n. 151/2015 – il datore di lavoro può utilizzare per fini connessi al rapporto di lavoro le informazioni raccolte mediante le apparecchiature utilizzate dai dipendenti, se sussistono i requisiti espressi dai commi 1 e 2 del predetto art. 4 dello Statuto dei Lavoratori: condizione essenziale, a tal fine, è che venga fornita idonea notizia ai dipendenti circa le modalità di uso degli strumenti di lavoro e di effettuazione dei controlli cd. difensivi".

[26] Peraltro, in modo corretto, necessario, adeguato, appropriato, pertinente, commisurato, temporaneo, equo (dunque, non eccessivo/eccedente), commisurato, assolutamente indispensabile, eccezionale, per uno scopo determinato e legittimo, ed al fine di arrecare la minore intrusione nei confronti del relativo soggetto interessato (cfr., ex multis: Documento di Lavoro n. 55 del 29.5.2002 del WP Art. 29; CEDU, sentenza del 17.10.2019, causa "Lopez Ribalda e altri c. Spagna"; CEDU, sentenza del 5.9.2017, causa "Barbulescu c. Romania", paragrafo 49): "Il controllo della corrispondenza di un lavoratore o del suo impiego dell'Internet può ritenersi necessario unicamente in circostanza eccezionali. Il controllo della posta elettronica di un lavoratore può ad esempio risultare necessario per ottenere conferma o prova del fatto che esso abbia compiuto determinate azioni, tra le quali rientrerebbe un'eventuale attività criminosa del lavoratore, se ed in quanto ciò risulta indispensabile al datore di lavoro per difendere i propri interessi come ad esempio nel caso in cui abbia una responsabilità subordinata per le azioni del lavoratore. Tra le attività lecite rientrerebbe altresì la rilevazione della presenza di virus informatici e più generalmente qualsiasi attività del datore di lavoro mirante a garantire la sicurezza del sistema. Giova ricordare che l'apertura della posta elettronica di un dipendente può rendersi necessaria anche per motivi diversi dal controllo e dalla vigilanza, come quello di mantenere lo scambio di corrispondenza nel caso in cui il dipendente sia assente (ad esempio, per malattia o per ferie) e non vi sia altro modo (come la funzione di risposta automatica o l'inoltro automatico) per ottenere tale risultato"; Convenzione 108+, art. 5 paragrafo 1): "Il trattamento dei dati deve essere proporzionato allo scopo legittimo perseguito e riflettere in tutte le fasi del trattamento un giusto equilibrio tra tutti gli interessi coinvolti, pubblici o privati, e i diritti e le libertà in gioco"; volume "Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro", Giuffrè, 2022, capitolo 15), paragrafo 7): "…la travaglia esperienza giurisprudenziale dei controlli difensivi, anche alla luce del nuovo campo di applicazione del riformato art. 4, co. 1, St. lav., va allora ricondotta all'interno della sua naturale collocazione di diritto comune, ossia nell'ambito della categoria generalissima della legittima difesa avverso gli "atti di aggressione contro l'altrui diritto". Ovvero, nell'ambito della nozione civilistica di legittima difesa nei rapporti inter-privati, che la dottrina di diritto civile ricostruisce sul combinato disposto degli artt. 2044 c.c. e 52 c.p. […] Orbene, la legittima difesa civilistica può essere realizzata anche per il tramite della "predisposizione di uomini e strumenti, onde evitare che il pericolo preventivato dell'altrui aggressione possa realizzarsi". Dunque appare compatibile anche con la predisposizione occasionale di strumenti tecnologici di controllo a distanza […] Ricondurre i controlli difensivi nell'ambito della legittima difesa civilistica significa peraltro emanciparli del tutto dal campo di applicazione dell'art. 4 cit., per cui non avrebbe alcun senso limitarli alle offese della sfera patrimoniale. Ciò significa che del tutto legittimamente il datore di lavoro potrebbe disporre anche un controllo occulto ed a distanza per registrare, in ipotesi, una probabile aggressione fisica o verbale alla persona di un suo dirigente o dipendente, ancorché la condotta non abbia una diretta incidenza sul patrimonio aziendale […] L'art. 52 c.p., cui fa diretto rinvio l'art. 2044 c.c., riguarda indifferentemente la "necessità di difendere un diritto proprio od altrui […] bilanciamento dei valori costituzionali in giuoco (artt. 1, 3, 35 Cost. da un lato, art. 41 Cost. dall'altro)").

[27] Art. 4 comma 3) dello Statuto dei Lavoratori: "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".
Cfr. volume "Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro", Giuffrè, 2022, capitolo 12) paragrafo 7): "La funzione dell'informazione prevista dal terzo comma dell'art. 4 è, infatti, più puntuale e specifica, ed è quella, tipica del contratto di lavoro, di consentire al lavoratore la conoscenza ex ante degli adempimenti dovuti (per poterne valutare anche la eventuale rilevanza sul piano disciplinare), e, nello stesso tempo, di mantenere un divieto di controlli "occulti", sia pure dando di questi ultimi una configurazione "aggiornata" rispetto a quella desunta dal testo originario dello Statuto".

[28] Cfr. Provvedimento n. 512 del 19.12.2018 (intitolato "Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101") a firma del Garante Privacy italiano [doc. web n. 9069653]: paragrafo 1) ("Le presenti regole deontologiche devono essere rispettate nel trattamento di dati personali per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria, sia nel corso di un procedimento, anche in sede amministrativa, di arbitrato o di conciliazione, sia nella fase propedeutica all'instaurazione di un eventuale giudizio, sia nella fase successiva alla sua definizione…"); paragrafo 2) comma 5) ("Se i dati sono trattati per esercitare il diritto di difesa in sede giurisdizionale, ciò può avvenire anche prima della pendenza di un procedimento, sempreché i dati medesimi risultino strettamente funzionali all'esercizio del diritto di difesa").
In tal caso, può applicarsi la limitazione di cui all'art. 2 undecies comma 1) lettera e) del novellato D.Lgs. n. 196/2003 (Codice Privacy) ("I diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto: allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria.

[29] Cfr. Raccomandazione CM/Rec (2015)5 del Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazionale, paragrafo 14.2.: "In particolare, qualora il trattamento riguardi dati personali relativi a pagine dell'Internet o di un'Intranet alle quali abbia acceduto il dipendente, si dovrebbe privilegiare l'adozione di misure preventive, quali filtri atti a impedire determinate operazioni, e di un approccio scalare all'eventuale sorveglianza dei dati personali, dando preferenza a controlli casuali e non individualizzati su dati anonimi o comunque aggregati".

[30] Cfr. Corte di Cassazione, Sezione Lavoro, sentenza n. 266682 del 10.112017: "Sul punto di controllo da parte del datore di lavoro sull'utilizzo dello strumento presente sul luogo di lavoro e uso del lavoratore per lo svolgimento della prestazione poi questa Corte, premesso che la materia esula dai controlli a distanza disciplinati dalla L. n. 300 del 1970, art. 4, ha precisato che il datore di lavoro può effettuare dei controlli mirati (direttamente o attraverso la propria struttura) al fine di verificare il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 c.c.), tra cui i p.c. aziendali, purché rispetti la libertà e la dignità dei lavoratori, nonché, con specifico riferimento alla disciplina in materia di protezione dei dati personali dettata dal D.Lgs. n. 196 del 2003, i principi di correttezza, di pertinenza e di non eccedenza…"; cfr., altresì, paragrafo 14.3.) della Raccomandazione CM/Rec (2015)5 del Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazionale: "Il datore di lavoro può accedere alle comunicazioni elettroniche di natura professionale dei dipendenti, informati preventivamente dell'esistenza di tale possibilità, soltanto se ciò risulti necessario per finalità di sicurezza o per altre finalità comunque legittime. In caso di assenza del dipendente, il datore di lavoro dovrebbe prendere le misure necessarie e prevedere idonee procedure al fine di consentire l'accesso a comunicazioni elettroniche di natura professionale soltanto se tale accesso rappresenti una necessità di ordine professionale. L'accesso dovrebbe avvenire nel modo meno intrusivo possibile e solo previa informazione del dipendente interessato".

10.2. **In aggiunta a quanto prescritto al precedente art. 10.1., COOPSELIOS si riserva il diritto di accedere alle informazioni contenute ed archiviate all'interno dei sistemi informativi e di ogni strumento di lavoro messo a disposizione di ciascun utente nel caso in cui tale attività risulti strettamente necessaria, proporzionata ed indispensabile per accertare, far valere ovvero difendere un diritto anche in sede giudiziale , anche laddove il relativo rapporto tra l'utente e COOPSELIOS sia già cessato per qualsivoglia ragione:** in tal caso, l'accesso in parola verrà effettuato in ossequio al principio di minimizzazione e di proporzionalità, ossia unicamente in relazione alle informazioni tese a consentire di valutare la sussistenza dei presupposti per procedere a tutelare i propri diritti e/o interessi aziendali in un eventuale contenzioso o precontenzioso.
10.3. **In caso di accertato mancato rispetto**, da parte dell'utente, **delle disposizioni contenute nella Policy, COOPSELIOS si riserva il diritto di agire**, nei confronti del relativo utente inadempiente, esercitando i poteri ad essa assegnati in ossequio all'art. 4 comma 3) della Legge n. 300/1970 ovvero in base a qualsivoglia altra disposizione normativa applicabile.
10.4. Per quanto concerne i residuali aspetti relativi alla rispetto della normativa comunitaria e nazionale sulla protezione dei dati personali, **si rimanda, in modo integrale, alla relativa informativa** ex art. 13 del GDPR di COOPSELIOS, consegnata all'atto dell'assunzione e/o instaurazione di un rapporto di lavoro/collaborazione similare ovvero resa, **sempre, agevolmente disponibile all'interno della propria intranet aziendale o in un luogo similare**.

Reggio Emilia, lì 4.11.2024 (data di ultimo aggiornamento).

**COOPSELIOS Cooperativa Sociale S.C.**
(in persona del suo legale rappresentante pro tempore)

---

MODULO PER PRESA VISIONE
– **DA FAR FIRMARE PER PRESA VISIONE E CONSEGNA** –

Io sottoscritto/a ……, dichiaro di aver ricevuto, da parte di COOPSELIOS, la Policy di sopra e, di conseguenza, di aver preso visione del relativo contenuto.
Firma: ……

---

# Allegato 2 ISTRUZIONI OPERATIVE per la persona autorizzata al trattamento dei dati personali

## ISTRUZIONI OPERATIVE E NOTE COMPORTAMENTALI PER IL SOGGETTO CD. AUTORIZZATO AL TRATTAMENTO EX ARTT. 4 N. 10), 29 E 32 PARAGRAFO 4) DEL REGOLAMENTO UE N. 2016/679

**1. Scopo.**

1.1. Il presente documento **ha lo scopo di fornire a ciascun soggetto cd. autorizzato al trattamento** ex artt. 4 n. 10), 29 e 32 paragrafo 4) del Regolamento UE n. 2016/679 (GDPR) (infra "soggetto cd. autorizzato") **le necessarie informazioni ed istruzioni volte a garantire che il trattamento dei dati personali**31 oggetto di autorizzazione **siano effettuati nel rispetto della normativa** nazionale e comunitaria vigente in materia, ivi inclusi i connessi atti di soft law ed orientamenti giurisprudenziali.

A tal riguardo, si comunica che il mancato rispetto delle presenti istruzioni, da considerarsi vincolanti ed inderogabili per ciascun soggetto cd. autorizzato, può comportare eventualmente, in capo al singolo soggetto, l'insorgere di una responsabilità di qualsivoglia natura.

**2. Ambito.**

2.1. **Il trattamento dei dati** – di cui COOPSELIOS Cooperativa Sociale S.C., (C. f. e P. IVA: 01164310359) (infra "COOPSELIOS"), in persona del suo legale rappresentante pro tempore, con sede legale in Reggio Emilia (RE), via A. Gramsci, 54/S, riveste un ruolo "privacy" cd. attivo (es. Titolare; co-Titolare; Responsabile o sub Responsabile del trattamento) – oggetto di autorizzazione, ad opera di quest'ultima, in favore del relativo soggetto cd. autorizzato – **è consentito al solo ed unico fine di espletare, in modo diretto o indiretto, le attività connesse all'esecuzione dell'incarico/mansione lavorativa** e/o ruolo, anche societario, assegnato al singolo soggetto cd. autorizzato.

**3. Trattamenti con strumenti elettronici e/o telematici.**

3.1. **Il trattamento di dati personali mediante strumenti elettronici, informatici e/o telematici è consentito al soggetto cd. autorizzato laddove questi sia dotato di apposite credenziali di autenticazione (username)** che gli consentono il superamento di una procedura di autenticazione relativa ad uno specifico trattamento ovvero ad un insieme di trattamenti. Il processo di autenticazione informatica, tramite il quale un sistema elettronico/telematico verifica l'identità dichiarata dal soggetto cd. autorizzato, presuppone l'assegnazione, in favore di quest'ultimo, delle relative credenziali di autenticazione (consegnate dalla scrivente società) che consistono in un codice per l'identificazione del soggetto cd. autorizzato associato ad una parola chiave riservata (password) conosciuta unicamente da quest'ultimo.

3.2. **Il soggetto cd. autorizzato è tenuto a non modificare**, senza alcuna motivazione e fatta salva l'eventuale preventiva autorizzazione da parte della scrivente società, **l'username assegnato**. Invece, in merito alla password da associare al relativo username, si evidenzia come la stessa deve possedere, in modo inderogabile, le seguenti caratteristiche: i) deve essere costituita da almeno otto caratteri alfanumerici; ii) deve essere segreta e personale, e non può essere conosciuta da parte di soggetti terzi; iii) deve essere digitata in condizioni di riservatezza; iv) non deve essere composta con riferimenti agevolmente riconducibili al relativo soggetto cd. autorizzato; v) deve essere modificata almeno ogni tre mesi.

Con riferimento alla parola chiave riservata, si illustrano le seguenti prescrizioni comportamentali che devono essere applicate da parte del soggetto cd. autorizzato: è vietato comunicarla a terzi soggetti, ancorché gli stessi rivestano la medesima qualifica di soggetto cd. autorizzato da parte di COOPSELIOS; è vietato conservarla in un luogo facilmente accessibile da parte di soggetti terzi; è vietato comporla in presenza di altri soggetti, ancorché colleghi o appartenenti al medesimo organo societario.

3.3. I dispositivi cd. di autenticazione informatica, eventualmente consegnati da COOPSELIOS al soggetto cd. autorizzato, sono da considerare strettamente personali e, di conseguenza, devono essere utilizzati solo ed esclusivamente dal soggetto cd. autorizzato che li ha ricevuti; in caso di furto, perdita anche accidentale del riferito dispositivo, il soggetto cd. autorizzato è tenuto ad informare prontamente e per iscritto il COOPSELIOS.

3.4. Ogni volta in cui il soggetto cd. autorizzato abbia la possibilità di accedere ad una rete informatica esterna è tenuto ad accertarsi che lo strumento elettronico in sua dotazione mediante il quale effettua tale accesso sia idoneamente ed adeguatamente protetto; il soggetto cd. autorizzato è tenuto, altresì, ad accertare che lo strumento elettronico in sua dotazione sia costantemente ed idoneamente protetto con un apposito programma antivirus.

**4. Trattamenti senza l'ausilio di strumenti elettronici e/o telematici.**

4.1. **Il soggetto cd. autorizzato è tenuto a custodire diligentemente gli atti ed i documenti contenenti i dati personali dei soggetti interessati, affinché siano preservati da danneggiamenti ovvero smarrimenti. Al fine di evitare accessi non autorizzati è richiesto che:** i) i documenti contenenti i dati personali **siano custoditi in archivi** non automatizzati adeguatamente protetti, al fine di evitare la lettura ovvero l'estrazione non autorizzata dei documenti, garantendo quindi la riservatezza e l'integrità dei dati personali ivi contenuti; ii) **le chiavi degli spazi in cui sono custoditi i documenti devono essere riposte in un luogo sicuro**; iii) i documenti contenenti i dati personali, una volta prelevati dai relativi archivi, devono essere riposti a fine giornata all'interno degli stessi; iv) **i documenti contenenti i dati personali non devono rimanere incustoditi in luoghi accessibili al pubblico;** v) i documenti contenenti i dati personali non devono essere condivisi, comunicati ovvero inviati a persone che non ne necessitano per lo svolgimento delle relative mansioni, ancorché le stesse rivestano la qualifica di soggetto cd. autorizzato.

[31] Tale definizione è da intendersi in senso lato, giacché potenzialmente ricomprendente – a seconda delle circostanze determinate dai margini di operatività e di trattamento modulati e parametrati in ragione del ruolo lavorativo (e conseguenti compiti) svolti dallo specifico soggetto cd. autorizzato in nome e per conto di COOPSELIOS – i dati personali ex art. 4 n. 1) del GDPR, i dati personali cd. particolari ex art. 9 paragrafo 1) del GDPR e i dati personali cd. giudiziari ex art. 10 del GDPR.

**5. Formazione.**
5.1. Ciascun soggetto cd. autorizzato è tenuto a frequentare uno o più corsi di formazione o di aggiornamento in relazione alla normativa sulla protezione dei dati personali, organizzati da COOPSELIOS.

Reggio Emilia, lì 4.11.2024 (data di ultimo aggiornamento).

**COOPSELIOS Cooperativa Sociale S.C.**
(in persona del suo legale rappresentante pro tempore)

---

**MODULO PER PRESA VISIONE**
**– DA FAR FIRMARE PER PRESA VISIONE E CONSEGNA –**

Io sottoscritto/a ……., dichiaro di aver ricevuto, da parte di COOPSELIOS, le "Istruzioni Operative e Note Comportamentali" di sopra e, di conseguenza, di aver preso visione del relativo contenuto.
Firma: ……

---