NOMINA AD INCARICATO DEL TRATTAMENTO

(per tirocinanti/studenti in alternanza scuola lavoro/collaboratori a qualsiasi titolo)

In attuazione della normativa privacy, la Aliante Cooperativa Sociale con sede in Via Gaetano Salvemini 12 – 41123 Modena – nella persona del legale rappresentante pro tempore, nella qualità di Titolare del trattamento

DESIGNA

il/la sig./sig.ra _____ che svolge attività di _____ presso _____ soggetto Incaricato esterno al **trattamento delle informazioni e dei dati che attengono alle banche dati della Aliante Cooperativa Sociale a cui lo stesso/a accede per lo svolgimento delle proprie mansioni**

OBBLIGA

il suddetto alla riservatezza su notizie connesse all'attività svolta ed alla osservanza in modo scrupoloso di quanto previsto dalla normativa vigente in materia di privacy nonché alle istruzioni impartite secondo l'Allegato A.

Luogo e data _____

L'Incaricato al trattamento (firma per accettazione) _____

Per ricevuta del REGOLAMENTO RECANTE ISTRUZIONI PER I TIROCINANTI/STUDENTI IN ALTERNANZA SCUOLA LAVORO/COLLABORATORI A QUALSIASI TITOLO

Luogo e data _____

Il Tirocinante/collaboratore_____

Allegato A (da consegnare al tirocinante)

REGOLAMENTO RECANTE ISTRUZIONI PER I TIROCINANTI/STUDENTI IN ALTERNANZA SCUOLA LAVORO/COLLABORATORI A QUALSIASI TITOLO

***

Di seguito sono riportate le istruzioni impartite ai tirocinanti/studenti in alternanza scuola lavoro/collaboratori a qualsiasi titolo per il trattamento dei dati personali effettuato nell'ambito delle mansioni svolte presso le strutture di Aliante Cooperativa Sociale
Alla fine del presente documento è inoltre riportato un Glossario ad uso dei medesimi incaricati con la spiegazione del significato di alcuni termini più ricorrenti, così come definiti dal Regolamento EU 679/2016.
Ognuno dei suddetti soggetti è tenuto a:

- effettuare operazioni di trattamento di dati personali soltanto per le **finalità** e con le **modalità** strettamente correlate allo svolgimento delle attività affidate e secondo le prassi seguite in ambito societario;
- accedere solo ai dati personali, ivi compresi le categorie particolari di dati ai sensi dell'art. 9 del Regolamento EU 679/2016, strettamente necessari all'esecuzione delle predette attività;
- verificare che i dati acquisiti dagli interessati siano esatti e completi e, che siano utilizzati in modo pertinente e non eccedente rispetto alle attività svolte e ai compiti assegnati;
- mantenere la riservatezza sui dati personali, anche per particolari categorie di dati ai sensi dell'art. 9 del Regolamento EU, di cui venga a conoscenza o in possesso per le attività svolte, senza divulgarli a terzi al di fuori dei casi connessi allo svolgimento delle stesse attività, secondo le prassi seguite in ambito societario od in base alle istruzioni ricevute dal Titolare;
- astenersi, in caso di cessazione dell'attività, dall'effettuare operazioni di trattamento dei dati personali di cui sia venuto a conoscenza durante lo svolgimento dell'incarico ed, in particolare, dal conservarli, duplicarli, comunicarli, o cederli a terzi;
- **informare prontamente il Titolare del trattamento su ogni questione rilevante in relazione al trattamento di dati personali effettuato o su eventuali richieste ricevute dalle persone cui si riferiscono i dati.**

***

Inoltre, deve inoltre attenersi a tutte le prescrizioni e misure di sicurezza che vengono qui di seguito riportate:

1 PROCEDURE E REGOLE PER IL TRATTAMENTO DEI DATI PERSONALI

Al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento, ciascun soggetto deve osservare le seguenti regole di ordinaria diligenza, nonché ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa in ambito privacy:

- **tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire la massima riservatezza delle informazioni di cui si viene in possesso, considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;**
- le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali gli stessi dati sono stati raccolti;
- in caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro si devono porre in essere tutte le misure necessarie (es. blocco del pc) affinché soggetti terzi, anche se dipendenti, non possano accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, cartaceo o automatizzato;

Quanto sopra descritto impone, in altri termini, di operare con la massima attenzione in tutte le fasi di trattamento, dall'acquisizione dei dati, al loro aggiornamento, alla conservazione ed eventuale distruzione.

*

a) POSTAZIONE DI LAVORO

La postazione di lavoro (computer fisso o laptop) degli autorizzati al trattamento deve essere:

- utilizzata solo per scopi legati alla propria attività lavorativa;
- utilizzata in modo esclusivo da un solo utente o, in alternativa, configurato in maniera tale che ciascun utente possa accedere mediante le proprie credenziali;
- protetta, evitando che terzi possano accedere ai dati che si stanno trattando.

Occorre, inoltre, precisare che è dovere di ciascun autorizzato:

- non lasciare sulla scrivania informazioni riservate su qualunque supporto esse siano archiviate (fogli di carta, post-it, CD-ROM, chiavette USB, ecc.);
- impostare lo screen saver con password, in modo che si attivi dopo massimo 6 minuti di inattività o in caso di abbandono momentaneo del proprio PC;

- **non lasciare lavori incompiuti sullo schermo, chiudere sempre il programma quando ci si allontana dalla postazione di lavoro, si consiglia in aggiunta al bloccaschermo automatico di bloccare manualmente il computer con i tasti**;
- non lasciare il computer portatile incustodito sul posto di lavoro (es. al termine dell'orario lavorativo, durante le pause di lavoro, o durante riunioni lontane dalla propria postazione);
- non lasciare incustoditi telefoni cellulari e tablet;
- non utilizzare fax e/o telefono per trasmettere informazioni riservate se non si è assolutamente certi dell'identità dell'interlocutore o del destinatario, e se esso non è legittimato a riceverle.

*

b) GESTIONE DELLE PASSWORD

Per una corretta gestione delle password, ciascun Incaricato deve aver cura di:

- in caso di accesso alle risorse di rete e agli applicativi del Titolare: comporla utilizzando almeno **8 caratteri alfanumerici** (devono contenere lettere, numeri e almeno una maiuscola);
- in caso di trattamento di dati su pc non collegato alla rete informatica del Titolare: salvare i files con password di protezione di **almeno 8 caratteri alfanumerici** (devono contenere lettere, numeri e almeno una maiuscola);

Occorre, inoltre, per ciascun autorizzato:

- **non basare la scelta su informazioni facilmente deducibili quali, ad esempio, il proprio nome, il nome dei propri familiari, le date di nascita, i codici fiscali, ecc. o in qualche misura riconducibili all'attività lavorativa** (es. Aliante00);
- adottare le necessarie cautele per mantenerla riservata e non divulgarla a terzi, ogni utente è responsabile diretto della propria password;
- non permettere ad altri utenti (es. colleghi) di operare con il proprio identificativo utente;
- non trascriverla su supporti (es. fogli, post-it) facilmente accessibili a terzi, meglio tenerla nel portafoglio, oppure su un file PC obbligatoriamente protetto da password complessa;
- non comunicarla mai per telefono, salvo gravi necessità;
- cambiarla almeno ogni 6 mesi, o 3 mesi in caso di dati particolari (o immediatamente nei casi in cui sia compromessa).

*

c) ANTIVIRUS

I Personal Computer (PC)/Portatili in dotazione al personale della Cooperativa, pur protetti contro gli attacchi dei virus informatici mediante appositi programmi, rimangono potenzialmente esposti ad aggressioni di virus non conosciuti. Per ridurre le probabilità che si verifichino tali attacchi è necessario che vengano osservate le seguenti regole:

- controllare che il programma antivirus installato sia aggiornato periodicamente;
- non utilizzare nelle strutture e presso le postazioni della Società risorse informatiche e/o supporti elettronici private o di provenienza incerta (PC o altre periferiche, chiavette USB, Token, CD-ROM, lettori MP3 ecc.);
- in ogni caso, qualora fosse necessario l'utilizzo dei suddetti dispositivi per lo svolgimento dell'attività lavorativa, verificare con l'ausilio del programma antivirus in dotazione ogni supporto magnetico contenente dati (es. CD-ROM), prima dell'esecuzione dei file in esso contenuti;
- non installare alcuna applicazione/software che non siano state preventivamente approvate ed autorizzate dal Titolare (es. free software scaricabili dalla rete o privi di regolare licenza d'uso);
- usare correttamente e solo per esigenze di lavoro i servizi di posta elettronica e di Internet;
- non modificare le configurazioni impostate sul proprio PC;
- spegnere il PC al termine della giornata di lavoro.

Occorre, inoltre, per ciascun interessato:

- chiudere correttamente i programmi in uso (es. utilizzando le funzioni di log-out);
- non aprire, se si lavora in rete, file sospetti e di dubbia provenienza;
- porre la necessaria attenzione sui risultati delle elaborazioni effettuate e sulle eventuali segnalazioni anomale inviate dal PC;

Alla verifica di un malfunzionamento del PC, che può far sospettare la presenza di un virus, è bene che l'autorizzato:

- sospenda ogni operazione sul PC evitando di lavorare con il sistema infetto;
- chiuda il sistema e le relative applicazioni.

- contatti immediatamente l'Amministratore di sistema (nel caso di accesso alle risorse di rete e agli applicativi del Titolare);

*

d) INTERNET E POSTA ELETTRONICA

Gli strumenti di comunicazione telematica (Internet e Posta elettronica) devono essere utilizzati solo ed esclusivamente per finalità lavorative. Sono vietati comportamenti che possano arrecare danno alla Cooperativa. In particolare, l'utente - in caso di accesso alle risorse di rete e agli applicativi del Titolare - dovrà osservare le seguenti regole:

- è consentita la navigazione internet solo in siti attinenti e necessari per lo svolgimento delle mansioni assegnate;
- **è consentito solo l'utilizzo dei programmi ufficialmente installati dall'Amministratore di sistema**;
- non è consentito scaricare software gratuiti (freeware o shareware) da siti Internet;
- non è consentita la registrazione a siti internet o partecipare a forum di discussione se questo non è strettamente necessario per lo svolgimento della propria attività lavorativa;
- non è consentito l'utilizzo funzioni di Instant Messaging, Skype, e Chat a meno che non siano state preventivamente autorizzate dal Titolare;
- è vietato aprire e-mail e file allegati di origine sconosciuta o che presentino degli aspetti anomali (quali ad esempio, un oggetto non chiaro) o che vengano riconosciuti come spam;
- non è consentito rispondere a messaggi provenienti da un mittente sconosciuto o di dubbio contenuto;
- è vietato l'utilizzo della posta elettronica per comunicare informazioni riservate, dati personali o dati critici, senza garantirne l'opportuna protezione;
- occorre sempre accertarsi che i destinatari della corrispondenza per posta elettronica siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare;
- occorre sempre essere consapevoli che posta elettronica e navigazione internet sono veicoli per l'introduzione sulla propria macchina (e quindi nelle strutture della Società) di virus e altri elementi potenzialmente dannosi;
- è vietato modificare le caratteristiche impostate sulle dotazioni od installare dispositivi di memorizzazione, comunicazione o altro (ad esempio masterizzatori, modem), o collegare alla rete aziendale qualsiasi apparecchiatura di origine esterna (ad es. switch, hub, apparati di memorizzazione di rete, ecc.), in autonomia, e senza preventiva autorizzazione da parte del proprio diretto responsabile.

<u>Nell'utilizzo della posta elettronica la società formula inoltre le seguenti regole di comportamento a cui gli utenti devono attenersi:</u>

a. conservare le comunicazioni inviate o ricevute, in particolare quelle dalle quali si possano desumere impegni e/o indicazioni operative provenienti dalla Committenza pubblica;
b. prestare attenzione ai messaggi di posta elettronica ed ai file, programmi e oggetti allegati, ricevuti da mittenti sconosciuti, con testo del messaggio non comprensibile o comunque avulso dal proprio contesto lavorativo. In tali casi gli utenti devono in particolare:
   - una volta aperto il messaggio, evitare di aprire gli allegati o cliccare sui "link" eventualmente presenti,
   - cancellare il messaggio e svuotare il "cestino" della posta,
   - segnalare l'accaduto all'Amministratore di Sistema.
c. evitare di cliccare sui collegamenti ipertestuali dubbi presenti nei messaggi di posta: in caso di necessità, accedere ai siti segnalati digitando il nome del sito da visitare direttamente nella barra degli indirizzi nei consueti strumenti di navigazione;
d. in caso di iscrizione a servizi informativi accessibili via internet ovvero a servizi di editoria on line, veicolati attraverso lo strumento di posta elettronica:
   - adoperare estrema cautela ed essere selettivi nella scelta della società che fornisce il servizio;
   - in particolare l'adesione dovrà avvenire in funzione dell'attinenza del servizio con la propria attività lavorativa,
   - utilizzare il servizio solo per acquisire informazioni inerenti finalità aziendali, facendo attenzione alle informazioni fornite a terzi;
e. in caso di errore nella spedizione o ricezione, contattare rispettivamente il destinatario cui è stata trasmessa per errore la comunicazione o il mittente che, per errore, l'ha spedita, eliminando quanto ricevuto (compresi allegati) senza effettuare copia;
f. evitare di predisporre messaggi che contengano materiali che violino la legge sul diritto d'autore, o altri diritti di proprietà intellettuale o industriale.

e) TRASMISSIONE E RIPRODUZIONE DEI DOCUMENTI

Al fine di prevenire eventuali accessi ai dati aziendali da parte di soggetti terzi non autorizzati, occorre adottare delle cautele nella trasmissione e riproduzione dei documenti contenenti dati personali.

Quando le informazioni devono essere trasmesse telefonicamente occorre essere assolutamente certi dell'identità dell'interlocutore e verificare che esso sia legittimato ad ottenere quanto domandato.

In particolare, nel caso di richieste da parte di terzi può essere necessario, a seconda della natura dei dati oggetto della richiesta, procedere nel seguente modo:

- chiedere il nome della persona che ha chiamato, la motivazione della richiesta e il numero di telefono dal quale sta effettuando la chiamata;
- verificare che il numero dichiarato corrisponda a quello riportato sul monitor del telefono;
- procedere immediatamente a richiamare la persona che ha richiesto l'informazione, in modo da accertarsi della identità dichiarata in precedenza.

Quando il dato deve essere inviato a mezzo fax, posta elettronica, SMS, ecc. e, in particolar modo, nel caso in cui vengano inviati documenti contenenti dati particolari, occorre:

- prestare la massima attenzione affinché il numero telefonico o l'indirizzo e-mail immesso siano corretti;
- verificare che non vi siano inceppamenti di carta o che dalla macchina non siano stati presi più fogli;
- nel caso di documenti inviati per fax, attendere sempre il rapporto di trasmissione per un ulteriore verifica del numero del destinatario e della quantità di pagine inviate;
- in caso di trasmissione di dati particolarmente delicati è opportuno anticipare l'invio chiamando il destinatario della comunicazione al fine di assicurare il ricevimento nelle mani del medesimo, evitando che terzi estranei o non autorizzati conoscano il contenuto della documentazione inviata;
- nel caso di documenti inviati per posta elettronica, accertarsi, prima di confermare l'invio, di avere allegato il file giusto.

Tutti coloro che provvedono alla duplicazione di documenti con stampanti, macchine fotocopiatrici o altre apparecchiature, in caso di copia erronea o non leggibile correttamente, da cui potrebbero essere desunti dati personali, sono tenuti a distruggere il documento in maniera tale da rendere impossibile la ricostruzione e in modo da escludere qualunque possibilità, da parte di estranei, di venire a conoscenza dei dati medesimi.

*

f) ARCHIVI CARTACEI

Tutto il materiale cartaceo contenente dati personali non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, deve essere riposto in un luogo sicuro.

Inoltre, occorre usare la medesima perizia nello svolgimento delle normali quotidiane operazioni di lavoro, per evitare che il materiale risulti facilmente visibile a persone terze o, comunque, ai non autorizzati al trattamento.

In caso di trattamento di dati particolari (condizione di salute, dati giudiziari, ecc.), tutta la documentazione cartacea deve essere conservata in armadi/cassetti chiusi a chiave o stanze chiuse a chiave in caso di allontanamento, anche temporaneo, dalla postazione di lavoro.

L'accesso a tutti i locali della Cooperativa e ai locali dislocati sul territorio ove si svolgono i servizi deve essere consentito solo a personale preventivamente autorizzato.

***

2 CONTROLLI DA PARTE DELLA TITOLARITÀ

La Cooperativa, tramite i suoi addetti ovvero consulenti autorizzati ha la possibilità di effettuare controlli sulle proprie apparecchiature tecnologiche al fine di preservare la sicurezza informatica dei dati personali in esse contenuti.

Nel rispetto dei principi di pertinenza e non eccedenza, le verifiche sugli strumenti informatici potranno essere realizzati dalla Cooperativa nel pieno rispetto dei diritti e delle libertà fondamentali del personale, e dei contenuti riportati nel presente Regolamento.

In caso di anomalie, la Cooperativa, privilegerà preliminari controlli anonimi e quindi riferiti a dati aggregati nell'ambito di intere strutture lavorative nelle quali si è verificata l'anomalia.

In tali casi, il controllo si concluderà con un avviso al Responsabile/Coordinatore della struttura interessata in cui è stato rilevato l'utilizzo anomalo degli strumenti aziendali, affinché lo stesso inviti le strutture da lui dipendenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

In caso di successive, perduranti anomalie, ovvero ravvisandone comunque la necessità, la Società si riserva di effettuare verifiche anche su base individuale, comunque finalizzate esclusivamente alla individuazione di eventuali condotte illecite.

In nessun caso verranno realizzate verifiche prolungate, costanti o indiscriminate, fatte salve le verifiche atte a tutelare i legittimi interessi del Titolare.

***

Alla fine del periodo di tirocinio/collaborazione il soggetto interessato deve darne comunicazione all'Amministratore di Sistema che provvederà a disabilitare l'utente per impedire accessi oltre il termine del periodo autorizzato;
Si ricorda, infine, che la violazione degli obblighi previsti dal Regolamento EU 679/2016 può esporre la Cooperativa quale Titolare, i relativi esponenti ed anche i singoli Responsabili e/o Incaricati del trattamento a rischi sul piano delle responsabilità e delle sanzioni previste per legge a livello civile, amministrativo ed anche penale.

Il Titolare del trattamento: Aliante Cooperativa Sociale

Glossario privacy

- **trattamento:** *qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;*
- **dato personale***: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;*
- **categorie particolari di dati:** *dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.*
- **dati genetici:** *i dati personali relativi alle caratteristiche genetiche ereditarie o acqui- site di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;*
- **dati biometrici:** *i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;*
- **dati relativi alla salute:** *i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;*
- **archivio***: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;*
- **titolare del trattamento***: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.*
- **responsabile del trattamento***: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;*
- **terzo:** *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;*
- **interessati:** *persone fisiche cui si riferiscono i dati personali;*
- **consenso dell'interessato**: *qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*;
- **destinatario:** *la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi (le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari);*
- **amministratore di sistema:** *soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione.*