Al Sig. _____

Mansione/i _____

Servizio/i _____

Consegna a mano

Autorizzazione al trattamento dei dati personali degli utenti

Ai sensi dell'art. 29 del Regolamento Europeo 679/2016

La Cooperativa Sociale Il Brutto Anatroccolo ONLUS con sede legale in Roma, via Pian di SCO n° 60 – C.F. 05853410586 e P.IVA 01456901006, in persona del suo legale rappresentante Enrico Fratini nato a Roma il 13/07/1961 ed ivi residente in via Nomentum n° 41 , C.F. FRTNRC61L13H501L

Premesso che

1. In data 25 maggio 2018 è entrato vigore il Regolamento Europeo n.679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e risulta quindi necessario, in base alle nuove norme, autorizzare gli addetti al trattamento dei dati personali
2. Che l'art. 29 del suddetto Regolamento prescrive che solo le persone autorizzate ed appositamente istruite abbiano la possibilità di trattare dati personali
3. Che il committente, Titolare del trattamento, ha individuato la Cooperativa come Responsabile del trattamento
4. Che per ragioni organizzative è possibile che lei debba contattare i colleghi e/o i coordinatori dei servizi in cui lei stesso opera
5. Che nello svolgimento delle Sue mansioni Ella viene a conoscenza e svolge il trattamento dei dati personali e particolari, relativi allo stato di salute, degli utenti dei servizi in cui opera

LA AUTORIZZA

Al trattamento dei dati personali di contatto dei colleghi

finalizzato alle comunicazioni relative all'organizzazione del servizio

Al trattamento dei dati personali e dei dati particolari degli utenti dei servizi in cui opera

finalizzato alla gestione ed allo svolgimento delle sue attività

I dati che lei potrà trattare sono i seguenti:

- Dati di contatto dei colleghi (nome, cognome, numero di telefono ed email) del suo servizio.
- Dati anagrafici ed identificativi degli utenti (ad esempio: nome e cognome, indirizzo, dati anagrafici ecc... che lei assiste
- Dati particolari relativi allo stato di salute (ad esempio: tipo di disabilità o di disagio, diagnosi, prescrizioni mediche, terapie, certificati medici ecc...) degli utenti che lei assiste.

L'elenco è da considerarsi indicativo e non esaustivo.

Allo scopo, Le precisiamo che Ella dovrà:

1. rispettare le istruzioni impartite dalla Cooperativa
2. **garantire l'assoluta riservatezza dei dati personali di cui può venire a conoscenza durante lo svolgimento della sua attività e non divulgare alcuna informazione relativa all'interessato al di fuori delle situazioni previste per la corretta gestione delle sue attività**
3. **Non riprendere fotografie o video in cui siano presenti gli utenti e in ogni caso non divulgare tali immagini né su social network né su messaggistica istantanea (WHATSAPP).**
4. non accedere a dati personali per motivi differenti da quelli espressamente autorizzati
5. trattare i dati personali nella misura necessaria e sufficiente alle finalità proprie e specifiche con gli strumenti messi a disposizione dalla Cooperativa

6. adottare, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate, oggi o in futuro, dal Responsabile. In particolare, se utilizza Computer dovrà quanto di seguito precisato:
    - utilizzare sempre le proprie credenziali di autenticazione, evitando di lasciare aperto il sistema operativo in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
    - trattare i soli dati la cui conoscenza sia necessaria, sufficiente e non ridondante per lo svolgimento delle operazioni da effettuare;
7. segnalare alla Cooperativa circostanze che rendano necessario od opportuno l'aggiornamento delle misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
8. svolgere, in ogni caso, il trattamento dei dati personali per le finalità e secondo le modalità stabilite, anche in futuro, dalla Cooperativa e, comunque, in modo lecito e secondo assoluta correttezza;
9. in generale, prestare la più ampia e completa collaborazione alla Cooperativa al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

Qualsiasi trasgressione delle istruzioni impartite potrà comportare sanzioni disciplinari di gravità commisurata alla violazione.

Cooperativa Sociale ONLUS
Il Brutto Anatroccolo
Via Pian di Scò, 60 - 00139 Roma
P.IVA 01456901006

Roma _____ Per Il Brutto Anatroccolo Società cooperativa sociale ONLUS

Il Presidente del CdA

Enrico Fratini

Il Sig._____ dichiara di aver ricevuto e recepito le istruzioni per garantire la sicurezza dei dati e sottoscrive la presente in data _____per ricevuta dell'originale e per integrale accettazione di quanto in essa espresso.

FIRMA PER RICEVUTA, ACCETTAZIONE E PRESA VISIONE DELLA CLAUSOLA DI RISERVATEZZA E DELLE ISTRUZIONI ALLEGATE

_____

CLAUSOLA DI RISERVATEZZA

Il Lavoratore si impegna a mantenere la massima riservatezza, nella vigenza del rapporto di lavoro e successivamente alla sua cessazione per qualsiasi causa, su qualsiasi informazione, dato e/o esperienza relativa all'organizzazione, all'attività della Cooperativa, alle strategie operative e di sviluppo ed alle conoscenze tecniche dello stesso e, in generale, su qualsiasi informazione, dato e/o esperienza relativa alla Cooperativa e/o a suoi committenti e/o utenti, dei quali sia venuto a conoscenza durante lo svolgimento del proprio incarico. Il Lavoratore si impegna altresì a non diffondere o comunicare a terzi, in mancanza di preventiva autorizzazione scritta della Cooperativa, alcuna informazione o dato riguardante l'attività svolta in favore di questa e dei suoi committenti e/o utenti nonché i risultati della stessa.

Il Lavoratore si impegna, altresì, a restituire e/o consegnare immediatamente alla Cooperativa al momento della cessazione del rapporto di lavoro/collaborazione, per qualsiasi causa, ogni documento in suo possesso riguardante direttamente o indirettamente l'attività della Cooperativa e/o l'attività svolta in favore della stessa, compreso il cartellino identificativo.

Il Lavoratore si impegna al rispetto di tutti gli obblighi di segreto, di riservatezza e di protezione dei dati e delle informazioni di cui possa venire a conoscenza nel corso delle sue attività. Si impegna altresì a non eseguire attività in violazione alle regole e alle istruzioni relative alla sicurezza dei dati.

Il Lavoratore è tenuto ad utilizzare le attrezzature informatiche della struttura esclusivamente per lo svolgimento delle funzioni lavorative comunque correlate alle mansioni assegnate. Tutti gli strumenti che la Cooperativa fornisce (telefono, PC, scanner, fotocopiatrice, ecc.), dovranno essere utilizzati per il raggiungimento dei fini istituzionali e non per scopi personali.

Sistema sanzionatorio

L'inosservanza di quanto sopra, costituisce violazione del dovere di diligenza e fedeltà del lavoratore e può comportare l'irrogazione di sanzioni disciplinari commisurate alla gravità della violazione, come regolamentato e previsto dal Contratto Collettivo Nazionale di lavoro applicato.

Data Firma del Lavoratore

ISTRUZIONI PER IL TRATTAMENTO DEI DATI

In ottemperanza al Regolamento Europeo 679/2016 (GDPR) in materia di privacy, l'autorizzato dovrà effettuare i trattamenti di dati personali di propria competenza e pertinenza, attenendosi scrupolosamente a quanto stabilito nell'atto autorizzativo, nelle seguenti istruzioni (consegnate previa illustrazione orale del contenuto delle stesse) e ad ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal Titolare o dal Responsabile del trattamento.

1. PRINCIPI GENERALI

I dati personali devono essere:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

2. DEFINIZIONI

«dati personali»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica,culturale o sociale;

«dati particolari»: sono i dati che possono rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

«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;

«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;

«incaricato del trattamento»: il soggetto autorizzato dal Titolare o dal Responsabile a compiere operazioni di trattamento dei dati.

3. SICUREZZA DEI DATI E DELLE INFORMAZIONI

IL BRUTTO ANATROCCOLO considera i dati e le informazioni gestite, per il particolare rilievo che assumono per il perseguimento dei propri fini sociali, parte integrante del proprio patrimonio. E' obiettivo di assoluta priorità salvaguardare la sicurezza del proprio sistema informativo e tutelare la riservatezza, l'integrità e la disponibilità delle informazioni prodotte, raccolte o comunque trattate, da ogni minaccia intenzionale o accidentale, interna o esterna.

In tale contesto si intende per:

- **Riservatezza** la garanzia che una determinata informazione sia preservata da accessi impropri e sia utilizzata esclusivamente dai soggetti autorizzati.
- **Integrità** la garanzia che ogni informazione sia realmente quella originariamente inserita nel sistema informatico e sia stata modificata in modo legittimo da soggetti autorizzati.
- **Disponibilità** la garanzia di reperibilità dell'informazione in relazione alle esigenze di continuità di erogazione del servizio e di rispetto delle norme che ne impongono la conservazione sicura.
- **Autenticità** la garanzia che l'informazione ricevuta corrisponda a quella generata dal soggetto o entità che l'ha trasmessa.

4. TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.

4.1 Custodia

- I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento
- I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti alla fine dell'uso.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro, in particolar modo se all'esterno della sede della cooperativa.
- L'utilizzo dei documenti contenenti dati degli utenti è strettamente limitato ai soli incaricati autorizzati. Durante la fase di utilizzo i documenti devono essere conservati in modo da non permettere la consultazione da parte di altri e da non permetterne il danneggiamento o la distruzione, anche accidentale.

4.2 Comunicazione

- L'utilizzo dei dati personali deve avvenire in base al "principio di necessità" e cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento).
- I dati non devono essere comunicati all'esterno e comunque a soggetti terzi, salvo il caso in cui ciò sia necessario per lo svolgimento degli incarichi affidati e con previa autorizzazione della Cooperativa..
- É espressamente vietato, al di fuori delle occasioni previste dal servizio (riunioni o verifiche), condividere coi colleghi o divulgare ad altro personale della Cooperativa dati personali o particolari degli utenti o dei loro familiari di cui si sia a conoscenza per motivi di servizio.

4.3 Distruzione

- Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

5. TRATTAMENTI CON STRUMENTI ELETTRONICI

La consapevolezza che non è possibile ottenere, in ambito informatico, una condizione di sicurezza assoluta, comporta la necessità di gestire il rischio ad un livello accettabile attraverso procedure e prassi consolidate.

5.1 Gestione delle credenziali di autenticazione

L'accesso alle procedure informatiche che trattano dati personali è consentito a chi è in possesso di "credenziali di autenticazione" che permettono il superamento di una procedura di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato (*user-id*) associato ad una parola chiave riservata (*password).*

Gli Incaricati devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni:

- Gli strumenti di autenticazione (le *password*) che consentono l'accesso alle applicazioni devono essere mantenute riservate. Essi non vanno mai condivisi con altri utenti (anche se Incaricati del trattamento)
- Le *password* devono essere sostituite al primo utilizzo e successivamente nei tempi indicati a seconda della tipologia di dati trattati
- Le *password* devono essere composte da almeno otto caratteri. Le *password* non devono contenere riferimenti agevolmente riconducibili all'Incaricato (es. nomi propri e di parenti; date di nascita, nomi o cognomi propri o di parenti; matricola o user- id).
- Custodire le *password* sempre in un luogo sicuro e non accessibile a terzi.
- Non divulgare le *password* a terzi; non condividerla con colleghi o esterni.

5.2 Protezione del PC e dei dati

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

- Tutti i PC devono essere dotati di password.
- Tutti i PC devono essere dotati di software antivirus aggiornato costantemente.
- Sui PC devono essere installati esclusivamente software necessari all'attività lavorativa, dotati di licenza e forniti dalle strutture di appartenenza. Sono vietati i software scaricati da Internet o acquisiti autonomamente.

- I PC devono essere spenti ogni sera prima di lasciare gli uffici. In caso di assenza temporanea dal posto di lavoro, è necessario usare il comando WINDOWS-L (premere il tasto con la finestra e tasto L in contemporanea) in modo da eliminare la possibilità di accessi indesiderati: lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.
- Sui PC devono essere installati, appena vengono resi disponibili tutti gli aggiornamenti software necessari a prevenirne vulnerabilità e correggerne i difetti.
- Non è consentito modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita dell'Amministratore di Sistema.
- In caso di PC portatile l'utilizzatore ne è responsabile. Deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro ed è obbligatoria una password complessa.
- Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
- I PC portatili utilizzati all'esterno delle strutture della cooperativa devono essere custoditi in un luogo protetto.

5.3 Uso dei supporti rimovibili

- È vietato l'uso di dispositivi USB o di altri supporti di memorizzazione salvo che non siano adeguatamente protetti da possibili accessi abusivi. La protezione può essere effettuata mediante criptazione dei supporti con BITLOCKER, app di crittografia presente in WINDOWS 10 oppure proteggendo le cartelle contenenti dati e/o i documenti con password robuste in modo da rendere impossibile l'accesso a estranei in caso di smarrimento o custodia impropria.

5.4 Uso dei dati in formato digitale

- Le immagini degli utenti sono DATI e come tali vanno trattate: è fatto assoluto divieto di diffondere immagini (fotografie o video) degli utenti su qualsiasi sito web o social network o app di messaggistica, anche personale.
- I dati personali archiviati su supporti di tipo magnetico devono essere protetti con le stesse misure di sicurezza previste per i supporti cartacei.

5.5 Backup dei dati

- Gli incaricati che trattano i dati sui PC non collegati in rete, o per i quali non sono previsti back-up centralizzati, devono provvedere al back-up dei dati almeno settimanalmente.
- I supporti di back-up devono essere custoditi in luogo sicuro e ad accesso controllato.
- In occasione di ogni back-up, deve preliminarmente accertarsi l'esito positivo della procedura.

5.6 Uso dispositivi personali

- È consentito l'uso di dispositivi personali (PC portatili, tablet o smartphone) di proprietà del lavoratore a condizione che siano protetti con le stesse misure di sicurezza di quelli della Cooperativa (vedi punti precedenti). Ogni lavoratore si assume la completa responsabilità del proprio dispositivo ed è quindi responsabile in caso di usi impropri o di perdita/violazione dei dati personali in esso contenuti.

6. ISTRUZIONI DI CARATTERE GENERALE

6.1 La postazione di lavoro

Sulla PDL devono essere presenti esclusivamente gli strumenti di lavoro messi a disposizione dalla Cooperativa. Quando l'addetto abbandona la PDL deve bloccare il computer (comando WINDOWS-L). E' vietato l'uso delle apparecchiature audio/video all'interno dell'ambiente di lavoro (es.: videocamere o smartphone) per effettuare riprese o fotografie.

6.2 Come gestire la Posta elettronica

La casella di posta elettronica è uno **strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

- Non aprire messaggi con allegati di cui non si conosce l'origine, possono contenere virus o programmi maliziosi in grado di danneggiare seriamente il computer e la rete aziendale prima di essere neutralizzati.
- Se nonostante le indicazioni, succede di aprire un file o un messaggio che si sospetta possa contenere un virus o un codice malizioso, scollegare il PC dalla rete, spegnerlo e fare avvertire immediatamente l'Amministratore di sistema.
- È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
- Non dare mai la propria password di accesso alla casella di posta elettronica ad altri, né comunicarla in base a richieste – di solito false – di controllo

- Se possibile utilizzare WEB mail (gmail o altre) e non memorizzare i messaggi ricevuti e inviati sul dispositivo

6.3 Uso di WHATSAPP

Whatsapp è un comodissimo strumento di messaggistica istantanea, ma dobbiamo ricordare che i dati identificativi (ad es. indirizzo email e numero telefonico) del mittente e dei destinatari sono condivisi con il gruppo di aziende di Facebook e con terze parti ed occorrono quindi molte accortezze nel suo utilizzo.

I messaggi scambiati di Whatsapp sono ragionevolmente sicuri: il programma utilizza una chiave crittografica, cioè solo i destinatari possono leggere o vedere ciò che è stato inviato, ma i messaggi rimangono sul dispositivo, che deve quindi essere protetto (vedi punti 5). Nei gruppi l'Amministratore è responsabile della netiquette del gruppo, che deve essere chiaramente scritta a sua cura nel riquadro <descrizione del gruppo>.

Le regole generali da applicare per l'uso di Whatsapp sono le seguenti:

- Salvo autorizzazione specifica da parte della Cooperativa non possono essere inviate immagini o video di utenti né fra singoli lavoratori né sui gruppi.
- Relazioni o documenti contenenti dati personali e particolari non devono essere inviate né fra singoli lavoratori né sui gruppi.
- I gruppi possono servire per scambiare informazioni organizzative, ma non per scambiare informazioni e dati personali relativi ad utenti.

6.4 Come usare correttamente Internet

Un dispositivo (PC, tablet o smartphone) abilitato alla navigazione in Internet costituisce uno strumento spesso necessario allo svolgimento della propria attività lavorativa, ma anche in questo caso sono necessarie precauzioni per evitare violazioni dei dati.

È assolutamente proibita, con i dispositivi aziendali, la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

- Evitare di scaricare dalla rete file e software di uso non direttamente riferibile all'attività di lavoro, in quanto questo può essere pericoloso per i dati, per la rete aziendale e per il dispositivo stesso
- È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
- È da evitare ogni forma di navigazione in siti non sicuri o ambigui (controllare che sia presente nella striscia del browser il lucchetto e la scritta HTTPS)
- Impostare il proprio browser con l'opzione di rifiuto dei cookie, per evitare il tracciamento e la profilazione

7. SANZIONI PER INOSSERVANZA DELLE NORME

Le presenti istruzioni sono impartite ai sensi delle normative vigenti in materia di privacy; l'inosservanza delle quali da parte dell'Incaricato può comportare sanzioni ai sensi degli artt. 83 e 84 del Regolamento Europeo Violazioni specifiche nell'ambito della riservatezza dei dati personali possono comportare per l'incaricato sanzioni disciplinari commisurate alla gravità della violazione stessa.