DISCIPLINARE INTERNO RELATIVO ALL'UTILIZZO DEI DATI

E

ORGANIZZAZIONE INTERNA SISTEMI INFORMATICI

(REVISIONE 01)

LABIRINTO
cooperativa sociale

Labirinto Cooperativa Sociale

Via Milazzo n. 28 (61122) PESARO
tel. 0721. 456415 - fax 0721.456502
mail: info@labirinto.coop - pec: segreteria.labirinto@pcert.it

1. SEZIONE I – AMBITO GENERALE

1.1 Definizioni

Titolare del trattamento: la persona fisica, l'impresa, l'ente, l'associazione, ecc. cui fa capo effettivamente il trattamento di dati personali e spetta assumere le decisioni fondamentali sugli scopi e sulle modalità del trattamento medesimo.
Responsabile del trattamento dei dati: la persona, la società, l'ente, l'associazione o l'organismo cui il titolare affida, anche all'esterno, per la particolare esperienza o capacità, compiti di gestione e controllo del trattamento dei dati.
DPO: Responsabile della protezione dei dati: soggetto designato dal titolare o dal responsabile del trattamento dei dati, per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del regolamento medesimo
RSGI: Responsabile sistemi di gestione integrati
RFN: Resp fornitori
Dipendente: personale dell'azienda assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio.
Incaricato: ogni soggetto che, nell'ambito dell'attività assegnatagli, tratta dati riferiti alla Cooperativa.
Interessato: la persona fisica cui si riferiscono i dati personali.
Trattamento (di dati personali): un'operazione o un complesso di operazioni che hanno per oggetto dati personali.
NDA: non-disclosure agreement, ovvero accordo di non divulgazione, è un negozio giuridico di natura sinallagmatica che designa informazioni confidenziali e con il quale le parti si impegnano a mantenerle segrete, pena la violazione dell'accordo stesso e il decorso di specifiche clausole penali in esso contenute.
Device: dispositivo
Dato personale: qualsiasi informazione che riguardi persone fisiche identificate o che possono essere identificate anche attraverso altre informazioni, ad esempio, attraverso un numero o un codice identificativo. Sono, ad esempio, dati personali: il nome e cognome o denominazione; l'indirizzo, il codice fiscale; ma anche un'immagine, la registrazione della voce di una persona, la sua impronta digitale, i dati sanitari, i dati bancari, ecc.
Dato particolare: un dato personale che, per la sua natura, richiede particolari cautele, ad esempio quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'adesione a partiti, sindacati o associazioni, lo stato di salute e la vita sessuale delle persone, i dati biometrici e i dati genetici.
Dato giudiziario: i dati personali che rivelano l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (quali, ad es., i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione). Rientrano in questa categoria anche la qualità di imputato o di indagato.
Misure di sicurezza: tutti gli accorgimenti tecnici ed organizzativi, i dispositivi elettronici o i programmi informatici utilizzati per garantire che i dati non vadano distrutti o persi anche in modo accidentale, che solo le persone autorizzate possano avere accesso ai dati e che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti.

1.2 Premessa

L'ambito lavorativo porta la nostra Cooperativa a gestire una serie di informazioni, proprie e di terzi, per poter erogare i servizi che gli vengono contrattualmente richiesti.
Tali informazioni sono dati personali quando sono riferiti a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che la Cooperativa adotti una serie di misure idonee previste dalle norme.
Altre informazioni, pur non essendo dati personali ai sensi di legge, sono in tutto e per tutto informazioni riservate, ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali la Cooperativa è chiamata a garantire la riservatezza, o per NDA, o per una più ampia tutela del patrimonio aziendale.

Ai fini di questo disciplinare si specifica, pertanto, che con il termine dati deve intendersi l'insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i dati personali intesi a norma di legge.
Inoltre, nell'ambito della sua attività, la Cooperativa tratta dati cartacei ovvero informazioni su supporto cartaceo e dati digitali ovvero informazioni che vengono memorizzate, elaborate o semplicemente transitano attraverso apparecchiature digitali.
In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui l'incaricato viene a conoscenza, nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con la Cooperativa stessa) salvo specifica autorizzazione esplicita della Cooperativa.
Labirinto gestisce prioritariamente servizi per l'ente committente, in tali casi il trasferimento dei dati può avvenire solo seguendo quanto indicato dai capitolati, regolamenti o le istruzioni/procedure indicate dall'ente stesso nell'incarico a Labirinto come Responsabile.
Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta.
La progressiva diffusione delle nuove tecnologie informatiche ed in particolare l'accesso alla rete internet dal computer aziendale espone la Cooperativa a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine della Cooperativa stesso, nonché danni patrimoniali.
Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, la Cooperativa ha adottato il presente Disciplinare Interno diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali.

1.3 Esclusione all'uso degli strumenti informatici

All'inizio del rapporto lavorativo o di consulenza, la Cooperativa valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari device aziendali, di internet e della posta elettronica da parte degli incaricati.
Successivamente e periodicamente la Cooperativa valuta la permanenza dei presupposti per l'utilizzo dei device aziendali, di internet e della posta elettronica.
È fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici aziendali.
I casi di esclusione possono riguardare:
1. L'utilizzo del COMPUTER o di altri DEVICE;
2. L'utilizzo della posta elettronica;
3. L'accesso a internet.

Le eventuali esclusioni sono strettamente connesse al principio della natura aziendale e lavorativa degli strumenti informatici nonché al principio di necessità di cui alla normativa vigente. Più specificatamente hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo gli incaricati che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno.
I casi in cui le esclusioni dovranno risultare operative in forza di tali motivazioni verranno comunicati individualmente.

1.4 Titolarità dei device e dei dati

La Cooperativa è esclusiva titolare e proprietaria dei Device messi a disposizione degli Incaricati ai soli fini dell'attività lavorativa.
La Cooperativa è l'unica esclusiva titolare e proprietaria di tutte le informazioni (che non costituiscono dati personali), le registrazioni ed i dati contenuti e/o trattati mediante i propri device digitali o archiviati in modo cartaceo nei propri locali.
L'incaricato non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei device aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i files di filmati o altre tipologie di files) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere copiati, comunicati o diffusi senza l'autorizzazione della Cooperativa.

1.5 Finalità nell'utilizzo dei device

I device assegnati sono uno strumento lavorativo nelle disponibilità dell'Incaricato e per tale motivo dovranno esclusivamente essere utilizzati per tale fine. I device, quindi, non devono essere usati per finalità private e diverse da quelle aziendali, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare.
Qualsiasi eventuale tolleranza da parte di questa Cooperativa, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Disciplinare.

1.6 Restituzione dei device

A seguito di una cessazione del rapporto di collaborazione con la Cooperativa o, comunque, al venir meno, ad insindacabile giudizio della Cooperativa, della permanenza dei presupposti per l'utilizzo dei device aziendali, gli incaricati hanno i seguenti obblighi:
1. Procedere immediatamente alla restituzione dei device in uso al RFN;
2. Divieto assoluto di formattare o alterare o manomettere o distruggere i device assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.

1.7 Restituzione dei dati cartacei

A seguito di una cessazione del rapporto di collaborazione con la Cooperativa o, comunque, al venir meno, ad insindacabile giudizio della Cooperativa, della permanenza dei presupposti per l'utilizzo di dati cartacei aziendali, gli incaricati hanno i seguenti obblighi:
1. Procedere immediatamente alla restituzione dei dati cartacei in loro possesso al Responsabile o Coordinatore/Referente del servizio;
2. Divieto assoluto di alterare o manomettere o distruggere i dati cartacei assegnati o renderli inintelligibili tramite qualsiasi processo.

2. SEZIONE II – PASSWORD

2.1 Le Password

Le password possono essere un metodo di autenticazione assegnato dalla Cooperativa per garantire l'accesso protetto ad uno strumento hardware oppure ad un applicativo software.
La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e della Cooperativa nel suo complesso. Nel tempo anche la password più sicura perde la sua segretezza. Per questo motivo la password va cambiata entro e non oltre i 3 mesi.
Non memorizzare la password in quanto il miglior luogo in cui conservare una password è la propria memoria.
Le password che non vengono utilizzate da parte degli incaricati per un periodo superiore ai sei mesi verranno disattivate dall'ente.
In qualsiasi momento la Cooperativa si riserva il diritto di revocare all'Incaricato il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

2.2 Regole per la corretta gestione delle password

L'Incaricato, da parte sua, per una corretta e sicura gestione delle proprie password deve rispettare le regole seguenti:
1. Le password sono assolutamente personali e non vanno mai comunicate ad altri;
2. Occorre cambiare immediatamente una password non appena si abbia alcun dubbio che sia diventata poco "sicura";
3. Le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali e numeri;

4. Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
5. Le password devono essere sostituite almeno ogni tre mesi, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password.
6. Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti della Cooperativa.

In alcuni casi, sono implementati meccanismi che consentono all'Incaricato fino ad un numero limitato di tentativi errati di inserimento della password oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene bloccato per alcuni minuti. In caso di necessità contattare il Titolare.

2.3 Divieto di uso

Al fine di una corretta gestione delle password, la Cooperativa stabilisce il divieto di utilizzare come propria password:

1. Nome, cognome e loro parti;
2. Lo username assegnato;
3. Un indirizzo di posta elettronica (e-mail);
4. Parole comuni (in Inglese e in Italiano);
5. Date, mesi dell'anno e giorni della settimana, anche in lingua straniera;
6. Parole banali e/o di facile intuizione, ad es. pippo, security e palindromi (simmetria: radar);
7. Ripetizioni di sequenze di caratteri (es. abcabcabc);
8. Una password già impiegata in precedenza.

2.4 Alcuni esempi di password non ammesse

La password ideale deve essere complessa, senza alcun riferimento, ma facile da ricordare. Una possibile tecnica è usare sequenze di caratteri prive di senso evidente, ma con singoli caratteri che formano una frase facile da memorizzare (es.: "NIMzz5DICmm!", Nel Mezzo Del Cammin, più il carattere 5 e il punto esclamativo). Decifrare una parola come questa può richiedere giorni, una come "radar" meno di dieci secondi. Alcuni esempi di password assolutamente da evitare:

1. Se Username = "mariorossi", password = "mario", o ancora peggio, password = "mariorossi";
2. Il nome della moglie/marito, fidanzato/a, figli, ecc. anche a rovescio!;
3. La propria data di nascita, quella del coniuge, ecc.;
4. Targa della propria auto;
5. Numero di telefono proprio, del coniuge, ecc.;
6. Parole comuni tipo "Kilimangiaro", “Password”, “Qwerty”, “12345678” (troppo facili);
7. Qualsiasi parola del vocabolario (di qualsiasi lingua diffusa, come inglese, italiano, ecc.).

2.5 La password nei sistemi

Ogni Incaricato può variare la propria password di accesso a qualsiasi sistema aziendale in modo autonomo, qualora il sistema in questione metta a disposizione degli Utenti una funzionalità di questo tipo (Change password), oppure facendone richiesta al Titolare. La password può essere sostituita dal Titolare, anche qualora l'Utente l'abbia dimenticata.

2.6 Audit delle password

Nell'ambito delle attività riguardanti la tutela della sicurezza della infrastruttura tecnologica, la Cooperativa potrebbe effettuare analisi periodiche sulle password degli Incaricati al fine di verificarne la solidità, le policy di gestione e la durata, informandone preventivamente gli Incaricati stessi.

Nel caso in cui l'audit abbia, tra gli esiti possibili, la decodifica della password, questa viene bloccata e all'Incaricato richiesto di cambiarla.

3. SEZIONE III – OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO

In questa sezione vengono trattate le operazioni a carico dell'Incaricato e il quadro di riferimento generale per l'esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell'integrità del patrimonio aziendale

3.1 Login e logout

Il "Login" è l'operazione con la quale l'Incaricato si connette al sistema informativo aziendale o ad una parte di esso, dichiarando il proprio Username e Password (ossia l'Account), aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet), ognuno dei quali richiede un username e una password.
In questi casi, sebbene sia preferibile che ogni utente abbia un suo specifico user name e password, la Cooperativa potrà assegnare un univoco user name e password per gruppi di incaricati per l'accesso alla macchina fisica, mentre rimarranno separati ed univoci per l'accesso agli applicativi che contengono dati.
Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.
È necessario impostare il "blocco del computer" per evitare l'accesso alla sessione di lavoro (tastiera e schermo disattivati) da soggetti non autorizzati.

3.2 Obblighi

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale.
L'incaricato deve quindi eseguire le operazioni seguenti:
1. Se si allontana dalla propria postazione dovrà mettere in protezione il suo device affinché persone non autorizzate non abbiano accesso ai dati protetti.
2. Bloccare il suo device prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
3. Chiudere la sessione (Logout) a fine giornata;
4. Spegnere il PC dopo il Logout;
5. Controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo device.

4. SEZIONE IV – USO DEL PERSONAL COMPUTER

4.1 Modalità d'uso del computer aziendale

I files creati, elaborati o modificati sul computer assegnato devono essere poi sempre salvati a fine giornata sul sistema di repository documentale centralizzato.
Il computer consegnato all'incaricato è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza, ed è dunque vietato.
L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Il computer che viene consegnato contiene tutti i software necessari a svolgere le attività affidate dalla Cooperativa. Per necessità dovrà rivolgersi al Titolare che demanderà la risoluzione a persona qualificata ad esempio eventuali amministratori di sistema utilizzando la propria login con privilegi di amministratore e la password dell'amministratore, potranno accedere, con le regole indicate nel presente documento, sia alla memoria di massa locali di rete (repository e backup) che ai server aziendali nonché, previa comunicazione al dipendente, accedere al computer, anche in remoto.

In particolare l'Incaricato deve adottare le seguenti misure:
1. Utilizzare solo ed esclusivamente le aree di memoria della rete dalla Cooperativa ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri files fuori dalle unità di rete;
2. Spegnere il computer, o curarsi di effettuare il Logout, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché 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;
3. Mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), disposti dalla Cooperativa;
4. Non dare accesso al proprio computer ad altri utenti, a meno che siano incaricati con cui condividono l'utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo.

4.2 Divieti espressi sull'utilizzo del computer

All'incaricato è vietato:
1. La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni dei suoi dati personali o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere.
2. Modificare le configurazioni già impostate sul personal computer.
3. Installare alcun software di cui la Cooperativa non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l'espressa autorizzazione della Cooperativa. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale.
5. Caricare sul disco fisso del computer o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.
6. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa della Cooperativa.
7. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico della Cooperativa, quali per esempio virus, trojan horses ecc.
8. Accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.
9. Effettuare in proprio attività manutentive.
10. Permettere attività manutentive da parte dei soggetti non espressamente autorizzati dalla Cooperativa.
11. Per i Pc utilizzati nei servizi scollegati dalla rete si ricorda che è VIETATO conservare al loro interno ***dati particolari***, giudiziari o comuni organizzati in aggregazioni di dati, es nome + cognome + foto, o nome cognome e indirizzo o numero di telefono, ecc. Si consiglia obbligatoriamente l'uso di acronimi o codici identificativi. In caso fosse strettamente necessario gestire ***dati particolari***, giudiziari o comuni trattati in forma elettronica e salvati su personal computer staccato dalla rete o su supporti hardware esterni (comprese chiavette USB) ***questi devono essere backappati con periodicità minima di 1gg***. su altro supporto (altro hardware esterno), conservato in luogo sicuro (es. in altro luogo diverso da quello abituale) non accessibile a terzi (es. sotto chiave o in cassaforte) e cancellati dalle chiavette USB.

4.3 Antivirus

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, ecc.
La Cooperativa impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana.
L'incaricato, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer, e, in particolare, deve rispettare le regole seguenti:
1. Comunicare alla Cooperativa ogni anomalia o malfunzionamento del sistema antivirus;

2. Comunicare alla Cooperativa eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, all'incaricato:
1. È vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione;
2. È vietato ostacolare l'azione dell'antivirus aziendale;
3. È vietato disattivare l'antivirus senza l'autorizzazione espressa della Cooperativa anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer;
4. È vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani.

Contattare il Resp informatico prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra. Nel caso il software antivirus rilevi la presenza di un virus, l'operatore deve immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al Resp Informatico.

5 SEZIONE V – INTERNET

5.1 Internet è uno strumento di lavoro

La connessione alla rete internet dal device avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. L'utilizzo per scopi personali non è consentito. **In particolare si vieta l'utilizzo dei social network**, se non espressamente autorizzati e con esclusivo riferimento a pagine aziendali.
Labirinto ha attivato il sito internet www.labirinto.coop, una pagina Facebook (https://www.facebook.com/LabirintoCoopSociale) e un canale YuoTube, ove vengono pubblicate notizie relative a servizi di Labirinto, incontri, convegni, ecc: Si occupa di tale attività l'ufficio comunicazione.

a) Se per ragioni di servizio si riscontrasse la necessità di aprire altre pagine facebook queste devono essere autorizzate dal Datore di Lavoro, informando i Resp di settore e il Responsabile della comunicazione integrata, le stesse devono essere collegate al sito della Cooperativa: www.labirinto.coop;
b) Non sono ammesse altre tipologie di pubblicazione su supporti di navigazione Internet;
c) È fatto assoluto divieto di pubblicare foto di dipendenti, tirocinanti, volontari, utenti, clienti, familiari, ecc non espressamente autorizzati, tramite moduli di consenso/autorizzazione foto/video. Le uniche figure autorizzate alla pubblicazione sono, per i servizi (progetti di documentazione attività) i Coordinatori/Referenti nominati nei moduli di consenso/autorizzazione foto/video, per la Cooperativa (attività di partecipazione) il Responsabile della comunicazione integrata.

5.2 Misure preventive per ridurre navigazione illecite

La Cooperativa potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.

5.3 Divieti espressi concernenti internet

1. È vietata la navigazione sui siti non autorizzati o non necessari per l'espletamento delle mansioni lavorative.
2. È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Titolare e con il rispetto delle normali procedure di acquisto.
3. È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
4. È vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a

mailing list spendendo il marchio o la denominazione della Cooperativa, salvo specifica autorizzazione della Cooperativa stessa.
5. È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
6. È vietato all'Incaricato di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale.
7. È vietato accedere dall'esterno alla rete interna delle Cooperativa salvo con le specifiche procedure previste dalla Cooperativa stessa.
8. È vietato, infine, creare siti web personali sui sistemi della Cooperativa nonché acquistare beni o servizi su Internet a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.
Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali e sensibili è posta sotto la personale responsabilità dell'Incaricato inadempiente.

5.4 Divieti di sabotaggio

È vietato accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dalla Cooperativa per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

5.5 Diritto d'autore

È vietato utilizzare l'accesso ad internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, …) se non espressamente autorizzato dalla Cooperativa.

6 SEZIONE VI – POSTA ELETTRONICA/WHATSAPP/MESSAGGI TELEFONICI

6.1 La Posta Elettronica è uno strumento di lavoro

L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa.
L'uso per motivi personali è vietato.
L'identificativo della casella di posta elettronica è composto con il seguente schema: ***inizialenome.cognome@labirinto.coop,***(in caso di omonimia: inizialenomeN°.cognome@labirinto.coop; in caso di nome doppio: entrambi le iniziali del nome)
Nello spazio firma della propria mail è obbligatorio inserire il seguente testo:

Questa email è stata inviata in conformità alle norme vigenti in materia di tutela dei dati personali (D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018, e Regolamento europeo 679/2016 – GDPR).
Il titolare del trattamento è la Labirinto Cooperativa Sociale - Soc. Coop p.a. (P.I. 01204530412 – tel. 0721. 456415 - fax 0721.456502 – mail info@labirinto.coop) con sede in Via Milazzo 28 – 61122 – PESARO.
Se avete ricevuto questo messaggio per errore, Vi preghiamo di distruggerlo e di informarci immediatamente per fax allo 0721.456502 o inviando un messaggio all'indirizzo e-mail: info@labirinto.coop.
Ricordiamo che la diffusione, distribuzione e/o copiatura del documento trasmesso da parte di qualsiasi soggetto diverso dal destinatario è proibita, sia ai sensi dell'art. 616 c.p., che ai sensi degli artt. 22 e 32 del GDPR – Regolamento generale sulla protezione dei dati (UE/2016/679).
Se non desiderate più ricevere comunicazioni, e comunque per esercitare anche tutti gli altri diritti previsti dal GDPR n. 679/16 in materia di protezione dei dati personali, scrivete a info@labirinto.coop
Rispettate l'ambiente, evitate di stampare questa mail.

Gli Incaricati assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

6.2 Divieti espressi in merito alla posta elettronica

1. È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio della Cooperativa per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta della Cooperativa, nonché utilizzare il dominio della Cooperativa per scopi personali.
2. È vietato redigere messaggi di posta elettronica utilizzando l'indirizzo aziendale, diretti a destinatari non collegati alla Cooperativa.
3. È vietato creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale.
4. È vietato trasmettere messaggi a gruppi numerosi di persone (es. a tutto un ufficio o ad un'intera divisione) senza l'autorizzazione necessaria o, in alternativa, è auspicabile l'utilizzo della funzione CCN (copia nascosta).
5. È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.
6. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni della Cooperativa informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.

6.3 Posta elettronica in caso di assenze programmate ed assenze non programmate

Nel caso di assenza prolungata sarebbe buona norma attivare il servizio di risposta automatica (Auto-reply).

In alternativa e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività aziendale, l'Incaricato deve nominare un collega fiduciario con lettera scritta che in caso di assenza inoltri i files necessari a chi ne abbia urgenza.

Qualora l'Incaricato non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, la Cooperativa, mediante personale appositamente incaricato, potrà verificare il contenuto dei messaggi di posta elettronica dell'incaricato, informandone l'incaricato stesso e redigendo apposito verbale.

6.4 Utilizzo illecito di Posta Elettronica

- È vietato inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.
- È vietato inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
- Qualora l'Incaricato riceva messaggi aventi tale contenuto, deve darne comunicazione al titolare.

6.5 Utilizzo illecito di Whatsapp

Whatsapp è stata creata come un'app di messaggistica privata quindi non ha una configurazione tale da permettere la protezione di dati aziendali, per tale ragione l'utilizzo ci espone a forti rischi se vengono trattati dati relativi a dipendenti o utenti: in tali casi è vietato utilizzarlo e va data preferenza oltre che alle chiamate telefoniche, agli incontri diretti e all'uso di e-mail.

WhatsApp purtroppo non dà accesso ad un sistema centrale che raccoglie tutte le informazioni inerenti le operazioni svolte e quindi non si possono monitorare realmente le attività.

Allo stesso tempo ogni comunicazione svolta può essere copiata, inoltrata, modificata dalla persona che la riceve e utilizzata come prova documentale. Ancor più se viene condivisa con altre persone all'interno di una chat.

Per tale ragione quando scriviamo ad un collaboratore i suoi orari, trattamenti ecc se non siamo sicuri di scrivere qualcosa di estremamente corretto, è sconsigliabile utilizzare questo strumento.
Inoltre non è autorizzato l'utilizzo del proprio smartphone per comunicare fotografie del foglio delle presenze, dei luoghi di lavoro, delle note spese, ecc Questo modo di lavorare può sembrare comodo perché viene fatto con il proprio smartphone ma è molto limitante e non facilita affatto il lavoro amministrativo e di rendicontazione perché in realtà si crea un groviglio di informazioni che vanno selezionate, assemblate e riscritte manualmente nel sistema gestionale o di fatturazione aziendale.
Infine è vietato l'utilizzo di chat di equipe, ad eccezione di messaggi per dare appuntamenti urgenti, avvisare di richiamare, ecc cioè di estrema semplicità e senza particolari contenuti.

Ove non sia possibile l'uso della mail possono essere utilizzati i messaggi telefonici (no WhatsApp) con l'uso obbligatorio di pin telefonico, possibile anonimizzazione dai dati (es. iniziali o codice identificativo utente), successiva cancellazione dei messaggi, ecc.).

7 SEZIONE VII – USO DI ALTRI DEVICE (PERSONAL COMPUTER PORTATILE, TABLET, CELLULARE, SMARTPHONE E DI ALTRI DISPOSITIVI ELTTRONICI)

7.1 L'utilizzo del notebook, tablet o smartphone

Il computer portatile, il tablet e il cellulare (di seguito generalizzati in "device mobile") possono venire concessi in uso dalla Cooperativa agli Incaricati che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete della Cooperativa.
L'Incaricato è responsabile dei device mobili assegnatigli dalla Cooperativa e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai device mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare i files creati o modificati sui device mobili devono essere trasferiti sulle memorie di massa aziendali al primo rientro in ufficio e cancellati in modo definitivo dai device mobili (Wiping). Sui device mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dalla Cooperativa. Ai device va applicata la procedura di protezione (PIN) e, in particolare se utilizzati all'esterno (convegni, visite in azienda, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto. ***In caso di perdita o furto dei device mobili deve far seguito la denuncia alle autorità competenti.*** Allo scopo si deve avvisare immediatamente la Cooperativa tramite la segreteria e il RSGI che provvederà – se del caso – ad occuparsi delle procedure connesse alla protezione dei dati. La perdita e il furto dei device mobili, contenenti dati della Cooperativa, comporta un data breach (ossia una violazione dei dati). Per maggiore informazioni in merito, leggere attentamente la SEZIONE XV denominata DATA BREACH: VIOLAZIONE DEI DATI.
Anche di giorno, durante l'orario di lavoro, all'Incaricato non è consentito lasciare incustoditi i device mobili.
All'Incaricato è vietato lasciare i device mobili incustoditi e a vista dentro l'auto o in una stanza d'albergo o nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.

7.2 Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ecc.)

Agli Incaricati può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, …) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, …).
Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

7.3 Device personali.

Ai dipendenti non è permesso svolgere la loro attività su PC fissi, portatili, device personali.

Ai dipendenti, se espressamente autorizzati dalla Cooperativa, è permesso solo l'utilizzo della posta elettronica aziendale sui loro device personali.
In tal caso è necessario che il device abbia password di sicurezza stringenti approvate dalla Cooperativa e l'eventuale furto o smarrimento del device deve essere immediatamente segnalato anche alla Cooperativa per eventuali provvedimenti di sicurezza.
Al collaboratore è vietato l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, cd-rom, DVD, macchine fotografiche, videocamere, tablet, …).
Gli Incaricati non dipendenti (collaboratori esterni), possono utilizzare i propri device personali per memorizzare dati della Cooperativa solo se espressamente autorizzati dallo stesso e assumendone formalmente e personalmente l'intera responsabilità del trattamento.
Tali device dovranno essere preventivamente valutati dalla Cooperativa, per la verifica della sussistenza di misure minime ed idonee di sicurezza.

7.4 Distruzione dei Device

Ogni Device ed ogni memoria esterna affidati agli incaricati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti alla Cooperativa che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento.
In particolare la Cooperativa provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

8 SEZIONE VIII – SISTEMI IN CLOUD

8.1 Cloud Computing

In informatica con il termine inglese cloud computing (in italiano nuvola informatica) si indica un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità on demand attraverso Internet a partire da un insieme di risorse preesistenti e configurabili.
Le risorse non vengono pienamente configurate e messe in opera dal fornitore apposta per l'utente, ma gli sono assegnate, rapidamente e convenientemente, grazie a procedure automatizzate, a partire da un insieme di risorse condivise con altri utenti lasciando all'utente parte dell'onere della configurazione. Quando l'utente rilascia la risorsa, essa viene similmente riconfigurata nello stato iniziale e rimessa a disposizione nel pool condiviso delle risorse, con altrettanta velocità ed economia per il fornitore.
Utilizzare un servizio di cloud computing per memorizzare dati personali o sensibili, espone la Cooperativa a potenziali problemi di violazione della privacy. I dati personali vengono memorizzati nel server farms di aziende che spesso risiedono in uno stato diverso da quello della Cooperativa. Il cloud provider, in caso di comportamento scorretto o malevolo, potrebbe accedere ai dati personali per eseguire ricerche di mercato e profilazione degli utenti.
Con i collegamenti wireless, il rischio sicurezza aumenta e si è maggiormente esposti ai casi di pirateria informatica a causa della minore sicurezza offerta dalle reti senza fili. In presenza di atti illegali, come appropriazione indebita o illegale di dati personali, il danno potrebbe essere molto grave per la Cooperativa, con difficoltà di raggiungere soluzioni giuridiche e/o rimborsi se il fornitore risiede in uno stato diverso da paese dell'utente.
Nel caso di industrie o aziende, tutti i dati memorizzati nelle memorie esterne sono seriamente esposti a eventuali casi di spionaggio industriale.

8.2 Utilizzo di sistemi cloud

È vietato agli incaricati l'utilizzo di sistemi cloud non espressamente approvati dalla Cooperativa.
Per essere approvati i sistemi cloud devono rispondere ad almeno i seguenti requisiti:

- Essere sistemi cloud esclusivi e non condivisi;
- Essere sistemi cloud posizionati fisicamente in Italia o all'interno dell'Unione Europea;
- L'azienda che fornisce il sistema in cloud deve essere preventivamente nominata Responsabile del Trattamento dei dati da parte dell'ente;

- L'azienda che fornisce il sistema in cloud deve comunicare alla Cooperativa, almeno una volta all'anno, i nominativi degli amministratori di sistema utilizzati.
- Dovranno essere verificate tutte le indicazioni e prescrizioni previste dalla normativa vigente.

9 SEZIONE IX – GESTIONE DEI DATI CARTACEI

9.1 Clear Desk Policy

Gli Incaricati sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.
Gli Incaricati sono invitati dalla Cooperativa ad adottare una "politica della scrivania pulita". Ovvero si richiede agli incaricati di trattare dati cartacei solo se necessario, privilegiando l'utilizzo degli strumenti digitali messi a disposizione dalla Cooperativa.
I principali benefici di una politica della scrivania pulita sono:
1) Una buona impressione a clienti e fornitori che visitano la nostra Cooperativa;
2) La riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle;
3) La riduzione che documenti confidenziali possano essere sottratti alla Cooperativa.

In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.
Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) sarà cura degli Incaricati riporre in luogo sicuro (armadio, cassettiera, archivio, …) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti nella Cooperativa.
A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra.
Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica.
Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archiviarli digitalmente.
È necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.
Ove possibile, è buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti.
Si ricorda che è consigliato, in particolare presso i servizi, l'uso di acronimi o codici identificativi.

10 SEZIONE X – NOTE ESPLICATIVE IN MERITO ALLA PUBBLICAZIONE ON LINE O DIFFUSIONE, A MEZZO STAMPA, DI FOTO E VIDEO (NONCHE' AL RILASCIO DI INTERVISTE)

10.1 Inquadramento normativo (Art. 96 e 97 legge 633/1941)

Il ritratto di una persona non può essere esposto, riprodotto o messo in commercio senza il consenso di questa, salve le disposizioni dell'articolo seguente.
Non occorre il consenso della persona ritrattata quando la riproduzione dell'immagine è giustificata dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali, o quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico. Il ritratto non può tuttavia essere esposto o messo in commercio, quando l'esposizione o messa in commercio rechi pregiudizio all'onore, alla reputazione od anche al decoro della persona ritrattata.

10.2 In merito alla possibilità di pubblicare o diffondere foto che ritraggano altre persone

Inoltre, il fatto che un soggetto abbia dato il proprio consenso alla foto significa solamente che acconsente allo scatto dell'immagine e, acconsentire allo scatto, partecipare alla foto, addirittura il mettersi in posa non implica alcuna autorizzazione alla pubblicazione. Pertanto, il soggetto ritratto deve dare il proprio consenso sia per la foto, che per la sua pubblicazione.

10.3 In merito alla possibilità di pubblicare o diffondere foto che ritraggano minori

Nel caso di minorenni, il consenso deve essere rilasciato da entrambi i genitori esercenti la potestà genitoriale (la firma di un solo genitore non è sufficiente). Quindi ogni altro soggetto, compreso il minore, non può fornire un valido consenso. Di conseguenza, nel caso in cui le liberatorie non siano state firmate o non siano state firmate correttamente, non solo non si potrebbero scattare le foto, ma non si potrebbero, a maggior ragione, utilizzare (sia per quanto riguarda il mondo online, che per quanto concerne l'offline e quindi volantini, cartelloni, articoli di giornale etc.).

10.4 Autorizzazione ad effettuare foto/video

- **Il Dipendente, Volontario, Tirocinante, Collaboratore nel modulo di CONSENSO/AUTORIZZAZIONE ALLA PUBBLICAZIONE DI FOTO, VIDEO E UTILIZZO DEI DATI, autorizza** a titolo gratuito, anche ai sensi degli artt. 10 e 320 cod. civ. e degli artt. 96 e 97 della legge n. 633/41 sul diritto d'autore, **l'utilizzo delle foto scattate e/o dei video girati,** a titolo esemplificativo e non esaustivo durante le seguenti occasioni: attività presso le sedi o i servizi gestiti dalla cooperativa; attività di partecipazione alla vita sociale della cooperativa (es. assemblee, convegni, seminari, corsi di formazione, riunioni di equipe, incontri, cene, ecc.), saranno **gestiti esclusivamente dal sig. SIMONE BUCCHI, Responsabile della comunicazione integrata**, incaricato/a da Labirinto Cooperativa Sociale - Soc Coop p.a. al trattamento delle foto e dei video di cui sopra, come da nomina sottoscritta in data _07.09.18_;
- **L'Utente nel modulo di CONSENSO/AUTORIZZAZIONE ALLA PUBBLICAZIONE DI FOTO, VIDEO E UTILIZZO DEI DATI,** a titolo gratuito, anche ai sensi degli artt. 10 e 320 cod. civ. e degli artt. 96 e 97 della legge n. 633/41 sul diritto d'autore, **l'utilizzo delle foto scattate e/o dei video girati:**
  - Dal/dalla sig./sig.ra …**NOMINATIVO COORDINATORE/REFERENTE DEL SERVIZIO**…., incaricato/a da Labirinto Cooperativa Sociale - Soc Coop p.a. al trattamento delle foto e dei video di cui sopra, come da nomina sottoscritta in data …**DATA DI NOMINA**….;
  - Per il progetto denominato …**INSERIRE TITOLO PROGETTO E EVIDENZIARE: COME, DOVE, QUANDO VERRANNO TRATTATE LE FOTO SCATTATE E/O DEI VIDEO GIRATI……;**

La presente autorizzazione potrà essere revocata in ogni tempo ai sensi degli artt. da 15 a 22 e dell'art. 34 del GDPR con comunicazione scritta da inviare a Labirinto Cooperativa Sociale - Soc Coop p.a., fermo restando che il trattamento sino ad allora effettuato sarà da intendersi in ogni caso lecito.

10.5 In merito alla conservazione delle foto/video

La conservazione delle foto/video può avvenire solo in virtù del principio di liceità, dopo che sia stata acquista l'autorizzazione dall'interessato (o chi ne fa le veci) tramite gli appositi moduli dedicati. Le foto/i video per le/i quali si è ottenuta autorizzazione potranno essere conservati fino ai tre anni successivi dalla fine del servizio/attività in questione.

11 SEZIONE XI – APPLICAZIONE E CONTROLLO

11.1 Il controllo

La Cooperativa, in qualità di Titolare degli strumenti informatici e dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

1. Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati.
2. Evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo.
3. Verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire anche con audit e vulnerability assessment del sistema informatico. Per tali controlli la Cooperativa si riserva di avvalersi di soggetti esterni.
Si precisa, in ogni caso, che la Cooperativa non adotta "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (ex art. 4, primo comma, l. n. 300/1970 – Statuto dei Lavoratori).

11.2 Modalità di verifica

In applicazione del principio di necessità, la Cooperativa promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili agli Incaricati e allo scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici.
La Cooperativa informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.
In particolare eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte degli Incaricati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.
Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (es. scarico di files pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) si effettuerà un avvertimento in modo generalizzato con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

11.3 Modalità di conservazione

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione:
1. Ad esigenze tecniche o di sicurezza del tutto particolari;
2. All'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
3. All'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme della Cooperativa strettamente correlate agli obblighi, compiti e finalità già esplicitati.

12 SEZIONE XII – SOGGETTI PREPOSTI AL TRATTAMENTO, INCARICATI E RESPONSABILI

12.1 Individuazione dei soggetti autorizzati

La Cooperativa può designare un Responsabile del trattamento cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità.
Per quanto riguarda i soggetti preposti al connesso trattamento dei dati (in particolare, gli incaricati della manutenzione) sono stati appositamente incaricati di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità di sicurezza informatica, senza realizzare attività di controllo a distanza, neanche di propria iniziativa.
I soggetti che operano quali amministratori di sistema o le figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, svolgono un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

13 SEZIONE XIII – ORGANIZZAZIONE INTERNA SISTEMI INFORMATICI

13.1 Consegna del pc fisso/personal computer/chiavetta usb

1. Il PC fisso o personal computer e/o chiavetta USB, viene richiesto/a dall'operatore che necessita di tale/i strumento/i operativo/i al **Responsabile di riferimento** di settore (per i servizi) o di funzione (per gli uffici). Quest'ultimo valutata la reale necessità di tale/i strumento/i indispensabile/i all'attività lavorativa, inoltrano la richiesta scritta al RFN.
2. Al momento della consegna dello strumento operativo all'operatore verrà fatta firmare dal RFN (o da chi per lui demandato), una lista di distribuzione da sottoscrivere che evidenzi i seguenti dati: NOMINATIVO OPERATORE, RUOLO, ACCESSO ARCHIVIO (SI/NO), IDENTIFICATIVO DEL PC, TIPO PC, SISTEMA OPERATIVO, SOFTWERE UTILIZZATO/I, SISTEMA ANTIVIRUS, UTILIZZO CHIAVETTA USB (SI/NO); Le liste di distribuzione raccolte durante l'anno da RFN, serviranno per modificare l'apposito registro da inviare annualmente al RSGI, in occasione della redazione del All2 - Doc integrativo al registro dei trattamenti ex DPS;
3. RSGI in corrispondenza al ruolo del nuovo possessore di PC, modificherà la nomina dell'operatore indicando la variazione delle banche dati utilizzate per la firma della stessa;

13.2 Aggiornamento All2 - Doc integrativo al registro dei trattamenti ex DPS

1. L'RFN aggiornerà l'apposito registro (inviato annualmente da RSGI), rispetto a tutti i cambiamenti inerenti a nuove consegne (sostituzioni, cambiamenti sui personal computer, PC fissi o penne internet e nominativi utenti) e invierà l'elenco aggiornato a RSGI
1. L'RSGI in collaborazione con il Direttore, aggiornerà l'All2 - Doc integrativo al registro dei trattamenti ex DPS con i dati utili.

13.3 Gestione e manutenzione del pc fisso/personal computer

1. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal Responsabile Informatico per conto di LABIRINTO né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone LABIRINTO stessa a gravi responsabilità civili; si evidenzia inoltre 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, sono sanzionate anche penalmente.
2. Salvo preventiva espressa autorizzazione dal Direttore, non è consentito all'operatore modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, etc.).
3. Ogni operatore deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente al Responsabile Informatico nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo articolo relativo alle procedure di protezione antivirus e articolo relativo alle manutenzioni.

13.4 Organizzazione rispetto alle manutenzioni:

Tutte le chiamate riguardanti i problemi informatici devono passare attraverso la RFN per la registrazione degli interventi richiesti, a tal fine le richieste devono pervenire in forma scritta, evidenziando il problema riscontrato e l'urgenza di intervento: in caso di urgenze riguardanti la connessione internet (sono considerate urgenze i lavori che non possono essere fermati o in scadenza), l'operatore può chiamare direttamente il fornitore indicato dal RFN;

13.5 Sostituzioni strumenti informatici

In caso di perdite o furto del computer portatile, la possibilità di ritrovarlo sono scarsissime ma le conseguenze, in termini di perdita della privacy, potrebbero essere molto elevate. Per questo sarà obbligatorio NON LASCIARE MAI IL COMPUTER PORTATILE IN MACCHINA O INCUSTODITO ed

evitare per quanto possibile di usare il computer portatile come un archivio, affidando invece i file ad altri sistemi di archiviazione (vedi paragrafo 4.2 Divieti espressi sull'utilizzo del computer).
In caso di perdite, sottrazioni, avvertire la RFN per poter attivare la sostituzione dello strumento informatico) e il RSGI per attivare in collaborazione con il DPO le attività legate alla comunicazione della violazione al Garante.

14 SEZIONE XIV – PROVVEDIMENTI DISCIPLINARI

14.1 Violazioni

Il mancato rispetto o la violazione delle regole nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

14.2 Conseguenze delle infrazioni disciplinari

Le infrazioni disciplinari alle norme del presente Disciplinare Interno potranno essere punite, a seconda della gravità delle mancanze, in conformità alle disposizioni di legge e/o del Contratto Collettivo Nazionale del Lavoro applicato, tra cui:

1. Il biasimo inflitto verbalmente;
2. Lettera di richiamo inflitto per iscritto;
3. Multa;
4. La sospensione dalla retribuzione e dal servizio;
5. Il licenziamento disciplinare e con le altre conseguenze di ragioni e di legge;

14.3 Modalità di esercizi dei diritti

Il lavoratore interessato del trattamento dei dati effettuato mediante strumenti informatici ha diritto di accedere, ai sensi del Regolamento UE 679/2016, alle informazioni che lo riguardano scrivendo alla Cooperativa.

15 SEZIONE XV – DATA BREACH: VIOLAZIONE DEI DATI

15.1 Premessa

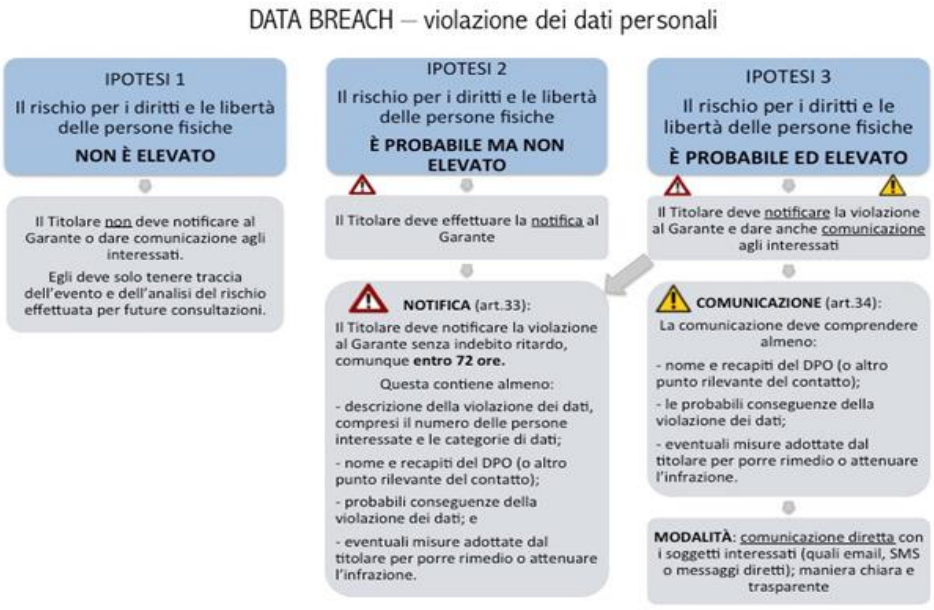
Il regolamento UE n. 679/16 prescrive specifici adempimenti nel caso di una violazione di dati personali, pertanto, è necessario che oltre il titolare, i responsabili e tutti gli incaricati del trattamento dei dati siano informati e formati in merito alle regole da adottare in caso di data breach.

15.2 Definizione di violazione dei dati

Per violazione dei dati personali si intende la divulgazione (intenzionale o non), la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati trattati da aziende o pubbliche amministrazioni. Un data breach, quindi, non è solo un attacco informatico, ma può essere anche un accesso abusivo, un incidente (es. un incendio o una calamità naturale), la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali (furto di un notebook di un dipendente).

15.3 Valutazione della Violazione dei dati

Spetta al responsabile del trattamento o all'incaricato avvertire il titolare dell'avvenuta violazione dei dati, se quest'ultimo non ne è ancora a conoscenza.



Il titolare dovrà, a quel punto, accertarsi della violazione e valutarne la gravità.

IPOTESI 1

Il titolare, dopo aver valutato che il rischio non è elevato, deve annotare l'evento nel registro delle violazioni, nonché le conseguenze, i provvedimenti adottati e monitorare le eventuali e/o successive violazioni.

Il titolare dovrebbe anche documentare nel registro le ragioni delle decisioni assunte, nei casi in cui non ha proceduto alla notifica, ha ritardato la notifica e nei casi in cui non ha comunicato la violazione agli interessati. Tale documentazione dovrà essere fornita al Garante in caso di accertamenti.

IPOTESI 2

Il titolare, dopo aver valutato che il rischio è probabile ma non elevato, ai sensi dell'art. 33 GDPR ha l'obbligo di notificare la violazione dei dati alle autorità di controllo. La notifica dovrà avvenire entro 72 ore e comunque "senza ingiustificato ritardo".

Contrattualmente titolare e responsabile possono pattuire che la notifica alle autorità spetti al responsabile, sempre per conto del titolare.

La notifica deve avere il contenuto previsto dall'art. 33 del GDPR:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

IPOTESI 3

Il titolare, dopo aver valutato che il rischio è probabile ed elevato, dovrà notificare la violazione all'autorità di controllo competente e comunicare con un linguaggio semplice e chiaro la violazione stessa anche gli interessati, sempre "senza ingiustificato ritardo".

Non è richiesta la comunicazione nei casi indicati dall'art. 34:

- il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

- il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Per valutare i fattori che determinano il rischio per le libertà e i diritti degli interessati, è possibile utilizzare i seguenti parametri:

- tipo di "breach": il tipo di violazione è un parametro per la valutazione del rischio. La violazione dei dati sanitari di tutti i pazienti di un ospedale è ben diversa dalla perdita dei dati sanitari di un singolo paziente;
- natura, numero e grado di sensibilità dei dati personali violati: l'accesso al nome e all'indirizzo dei genitori di un figlio rappresenta un rischio diverso rispetto all'accesso da parte dei genitori naturali del nome e dell'indirizzo dei genitori adottivi;
- facilità di associare i dati violati ad una persona fisica: può accadere che i dati violati non siano facilmente riconducibili ad una determinata persona fisica;
- gravità delle conseguenze per gli Interessati: quando il titolare del trattamento percepisce il rischio che i dati oggetto della violazione possono essere utilizzati immediatamente contro gli Interessati (es. sostituzione di persona);
- numero di Interessati esposti al rischio: un parametro è sicuramente quello del numero degli Interessati potenzialmente coinvolti;
- caratteristiche del titolare del trattamento: un attacco ad una struttura ospedaliera certamente è diverso dall'attacco ad una piccola azienda.

15.4 Sanzioni

In caso di mancato rispetto delle procedure di notifica della violazione si applica la sanzione amministrativa fino ad un importo di 10 milioni di euro oppure il 2% del fatturato dell'intera società. In caso di mancata notifica si configura anche l'assenza di adeguate misure di sicurezza, per cui si cumulano due distinte sanzioni.

15.5 Il Registro Data Breach

Il tracciamento dei casi di violazione dei dati personali, all'interno del registro, viene effettuato allo scopo di:

- individuare e tenere sotto controllo i fattori di rischio, ossia i fattori che determinano con più frequenza una violazione dei dati personali;
- misurare l'efficacia delle policy e delle procedure adottate;
- elaborare un piano di conformità che fissi gli obiettivi da raggiungere per essere "compliant" rispetto a leggi, best practices onde dimostrare la conformità in sede di audit di verifica/ispezioni/test.

16 SEZIONE XVI – VALIDITÀ, AGGIORNAMENTO ED AFFISSIONE

16.1 Aggiornamento

Il presente Disciplinare sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi della Cooperativa o in caso di mutazioni legislative.
Ogni variazione del presente Disciplinare sarà comunicata agli incaricati.

16.2 Affissione

Il presente Disciplinare verrà tenuto a disposizione di tutti i dipendenti, ai quali ne verrà in ogni caso fornita una copia all'atto del rilascio dell'informativa sul trattamento dei loro dati personali.

16.3 Entrata in vigore del regolamento

1. Il regolamento entra in vigore a seguito dell'approvazione da parte del CdA. Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

2. Sarà cura del Datore di lavoro, dopo l'approvazione del CdA, definire le modalità di consegna a ciascun operatore/utilizzatore di LABIRINTO, per l'opportuna conoscenza.
3. ***Tale regolamento sarà affisso nella bacheca aziendale di via Milazzo 28 e inserito in formato elettronico nella rete internet.***
4. Ogni Responsabile o Incaricato che abbia in custodia PC fissi o portatili deve conservarne una copia c/o il proprio ufficio/servizio.

16.4 Validità

Il presente Disciplinare ha validità a partire dal _12.06.2019__

Firma del Titolare del trattamento dei dati (LABIRINTO COOPERATIVA SOCIALE p.a.)

CONSEGNA INDIVIDUALE:

In data odierna _____il presente documento è stato consegnato a _____ (nome dipendente/incaricato), che dichiara di averlo ricevuto e di averne preso visione.

_____
Firma del dipendente/incaricato

CONSEGNA GRUPPO EQUIPE:

In data odierna _____il presente documento è stato consegnato c/o il servizio _____ (nome servizio), il Responsabile o Coordinatore/referente dovrà far firmare una lista di distribuzione del documento stesso ai dipendenti, collaboratori incaricati del proprio gruppo di lavoro.
La lista di distribuzione firmata da ogni dipendenti/tirocinanti/volontari del servizio viene conservata dal Responsabile o Coordinatore/referente.

_____
Firma del responsabile/coordinatore incaricato