CROCE ROSSA ITALIANA – COMITATO DI RAVENNA

REGOLAMENTO PER IL CORRETTO TRATTAMENTO DEI DATI

Adottato dal comitato in data: 15/07/2019

Ultima revisione: ___/___/_____

Parte prima - Premessa

Il comitato, nello svolgimento delle sue attività, gestisce una serie di informazioni, proprie e di terzi.
Tali informazioni possono essere considerate "dati personali", quando sono riferite a persone fisiche, secondo la definizione data dal Regolamento UE 2016/679, siano essi dati comuni che categorie particolari di dati (c.d. dati sensibili) e per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che il comitato adotti una serie di misure minime ed idonee previste dalle norme.
Sono poi gestite una serie di informazioni che, pur non essendo "dati personali" ai sensi di legge, sono a tutti gli effetti identificabili come informazioni riservate di cui l'organizzazione stessa è chiamata a garantire la riservatezza.
Nel presente regolamento sarà adottato il termine "dati" per intendere l'insieme ampio di informazioni comprendenti sia i dati personali che le informazioni riservate, cui un dipendente o un collaboratore o un socio può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza; in linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui il soggetto autorizzato viene a conoscenza, nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato, salvo comunicazioni obbligatorie previste dalla legge o oggetto della mansione affidata, o diffuso a nessuno (anche una volta concluso il rapporto lavorativo con il comitato stessa) salvo specifica autorizzazione esplicita del comitato.
Di seguito vengono esposte regole minime comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo, furti di dati ed informazioni riservate, danneggiamenti al sistema informativo e all'immagine del comitato stesso.
Il comitato di Ravenna è esclusivo Titolare e proprietario dei PC, dei software, delle caselle di posta elettronica e di ogni altro supporto cartaceo o telematico messo a disposizione dei soggetti autorizzati ai soli fini dell'attività lavorativa, salvo specifica autorizzazione del Titolare.
Il comitato è l'unica esclusiva titolare e proprietaria di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri device digitali o archiviati in modo cartaceo nei propri locali.
Il soggetto autorizzato non può presumere o ritenere che tutte 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 da lui copiati, comunicati o diffusi senza l'autorizzazione dell'organizzazione.

Le dotazioni aziendali assegnate sono uno strumento lavorativo nelle disponibilità del soggetto autorizzato esclusivamente per un fine di carattere lavorativo. I device e gli strumenti utilizzati per finalità proprie dell'attività del comitato, quindi, non devono essere utilizzati per finalità private e diverse da quelle aziendali. Qualsiasi eventuale tolleranza da parte del comitato, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni impartite nel presente Regolamento.
Il comitato, in accordo con quanto previsto sia dalla normativa in materia di protezione dei dati, sia dai Provvedimenti in materia emanati dal Garante per la protezione dei dati personali, ed in ossequio al divieto di controllo a distanza dei lavoratori previsto dalla l.300/1970 (c.d Statuto dei lavoratori), non effettua un controllo preventivo (ex ante) né dei device affidati ai soggetti autorizzati, né del contenuto dei device stessi e delle casella di posta elettronica né dei file di log di accesso al sistema informativo. Tuttavia il comitato si riserva il diritto di effettuare controlli ed accessi ex post (successivi) in caso di prolungata assenza o impedimento del dipendente o del socio che renda indispensabile e indifferibile intervenire per esclusive necessità operative, di sicurezza del sistema, per tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati, per evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo, per il fondato sospetto di attività illecite o illegali e per verificare la funzionalità del sistema e degli strumenti informatici. In questo caso ai dipendenti saranno fornite idonee informazioni e le procedure di accesso e controllo saranno svolte nel rispetto dei principi e delle prescrizioni delle norme sopracitate.
Sono destinatari del presente regolamento tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché tutti i collaboratori, a prescindere dal rapporto contrattuale con la stessa intrattenuto (collaboratore a progetto, in stage, consulente, tirocinante ecc.) e tutti i soci del comitato.

Parte seconda - Riservatezza

I dati sono da considerarsi quali informazioni riservate del Titolare. Su questa base:

- Lei non potrà in alcun caso comunicare i dati a terzi, a meno che ciò sia necessario per l'assolvimento di un obbligo derivante da una legge;
- nel caso in cui Lei riceva richiesta o intimazione di comunicare informazioni personali o particolari del processo di trattamento di dati da parte di una pubblica autorità o da parte dell'autorità giudiziaria, dovrà provvedere a dare di ciò pronta notizia al Titolare e si impegna a seguirne le istruzioni;
- non deve in alcun modo trasferire dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il fornitore. In tal caso, informa il Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

Parte terza – Definizioni

Dato personale: qualunque informazione concernente una persona fisica, identificata o identificabile («interessato»); si considera identificabile la persona che può essere indentificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati

relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

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

Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni uniche 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 rilevano informazioni relative al suo stato di salute.

Titolare: 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

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;

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. Tuttavia, 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; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità 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

Data Protection Officer (DPO): Il Responsabile della protezione dei dati

Autorizzato: persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Parte quarta - Utilizzo del PC, dei device aziendali e della rete interna

PC: Il PC affidato all'utente permette l'accesso alla rete aziendale solo attraverso specifiche credenziali di autenticazione, come meglio descritto successivamente nella sezione "Password".

In caso di perdita o furto dei PC e degli altri dispositivi elettronici l'utente deve avvisare immediatamente il titolare o il proprio diretto responsabile, che provvederà ad occuparsi delle procedure connesse alla privacy e successivamente della eventuale denuncia alle Autorità competenti (procedura data breach).
Anche di giorno durante l'orario di lavoro il collaboratore deve adottare le dovute precauzioni per non minacciare la sicurezza delle informazioni trattate durante l'attività.
Qualora avvenga un uso privato concordato con la Direzione o accidentale degli strumenti aziendali è fatto d'obbligo l'immediata cancellazione dei dati contenuti nello strumento e comunque prima della riconsegna dello stesso per manutenzioni ed al termine del rapporto di lavoro.
È necessario 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.
Ogni PC è dotato di un dispositivo salvaschermo che deve essere attivato in caso di assenza temporanea prolungata nell'arco della giornata lavorativa (premendo la combinazione di tasti Windows + L).
È espressamente vietato: effettuare attività manutentive in proprio sul PC; permettere attività manutentive da parte di soggetti non autorizzati dal comitato; caricare sul disco fisso del computer alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.

Password: l'accesso al PC della propria postazione di lavoro è protetto da un sistema di autenticazione. La password preimpostata assegnata alla consegna del device deve essere sostituita con una personale, sostituita secondo le disposizioni aziendali.
La password deve essere formata da due parole combinate insieme o da una breve frase di senso compiuto o da una sequenza da tastiera non riconducibile ad una singola parola di senso compiuto (al fine di ridurre il rischio derivante da attacchi dictionary e bruteforce), di lunghezza almeno pari a 12 caratteri, non facilmente riferibile alla persona che la usa (nome e cognome del dipendente, nome di figli/moglie/parenti, nome dell'animale domestico, luogo di nascita, ecc...) e non facilmente riferibile al comitato, e al cui interno sia presente almeno un simbolo non alfanumerico, un numero ed una lettera maiuscola. È necessario inserire le lettere maiuscole non all'inizio della parola ma al suo interno e di sostituire alcune lettere con simboli non alfanumerici, ad esempio p!nc0P@LL1n018, fINEstr@sulC0rt!l317 (si chiede di non utilizzare queste passwords, ma di considerarle solo come esempio).
Le regole qui sopra descritte devono essere utilizzate anche per la formazione delle password della casella di posta elettronica e degli altri eventuali account aziendali.
Quando il collaboratore deve cambiare la password è necessario evitare modifiche ovvie, come la sostituzione della prima lettera della password oppure di aggiungere 1, 2 o ! alla fine della password. Queste modifiche sono le più usate.
Sono vietate password generiche quali "password", "123456789", "qwertyuiop", "admin" ecc..., password già utilizzate in altri account (anche personali) e/o utilizzate precedentemente. È vietato condividere la password

internamente e comunicarla all'esterno tramite canali telematici (e-mail, sms, messaggistica via web). È vietato dare indicazione in merito al formato ed alla lunghezza della parola chiave; è vietato inoltre tenere annotata la password su post-it o foglietti a vista (ad esempio attaccati allo schermo del PC, sotto la tastiera ecc...); salvare la parola chiave in un file del computer; nel caso in cui ci sia necessità di tenerla annotata essa va conservata in un posto sicuro conosciuto dal proprietario della stessa, non a vista.
Il dipendente deve prontamente avvisare il titolare ed il servizio IT nel caso qualcuno insista nel cercare di conoscere la propria password e in caso di dimenticanza e/o ripristino della password.

Antivirus: Il sistema informatico del comitato è protetto da software antivirus, attivato continuamente e aggiornato automaticamente con frequenza periodica.
Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.
Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso e segnalare prontamente l'accaduto al servizio IT.
È importante utilizzare questi software antivirus per controllare qualsiasi file di provenienza esterna al comitato, inoltre è vietato disattivare per qualsiasi motivo, anche temporaneamente, l'antivirus, salvo autorizzazione scritta del titolare dell comitato o del tecnico informatico.
Inoltre: è vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione; 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.
È bene ricordare che i virus informatici possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, via mail, ecc.

Spazi cloud: i software gestionali (Mambu e Gaia) sono forniti in soluzione cloud e contengono informazioni strettamente professionali, pertanto non possono essere utilizzati per scopi diversi, tra cui effettuare salvataggi di qualsiasi tipo di file o di dato non pertinente all'attività del comitato.
Al fine di ridurre l'efficacia di eventuali attacchi informatici ai danni del comitato (ransomware, cryptolocker, ecc...) si rammenta che deve essere privilegiato l'utilizzo dei gestionali sopra indicati, sia per quanto riguardo la gestione dei soci sia per quanto riguarda la gestione delle attività del comitato, limitando il salvataggio di file contenenti dati personali o informazioni ritenute importanti sui singoli PC in locale allo stretto indispensabile. Quando possibile è necessario salvare i file elaborati sui PC nei software forniti. Si fa inoltre divieto di salvare dati e file personali in locale.
In caso si evidenzino anomalie di funzionamento del computer è importante darne rapida segnalazione al titolare del comitato oppure, se non è possibile, al servizio IT.
È inoltre espressamente vietato: registrare file, software o archivi in uso al comitato su dispositivi personali; fare copia dei software installati per uso personale; creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'organizzazione, quali per esempio virus, trojan horses, keylogger, spyware, ecc.
È inoltre vietato installare qualsiasi software, anche in versione dimostrativa o gratuita, di cui il comitato non possegga la licenza, a qualsiasi titolo acquisito, senza autorizzazione da parte del titolare o del servizio IT.
Inoltre è vietato installare software privi di licenza o con licenza contraffatta e software la cui provenienza sia

sospetta. Nel caso si ricevano richieste di installazione da parte di soggetti non identificati o non conosciuti l'installazione non deve essere eseguita e deve essere avvisato il titolare del comitato oppure, se non è possibile, direttamente il servizio IT.

Parte quinta - Utilizzo servizi vari su internet

L'accesso ad Internet è fornito allo scopo di consentire l'acceso ad eventuali informazioni e contenuti necessari allo svolgimento dell'attività relativa alla propria mansione. Essendo uno strumento di lavoro, gli utenti cui si attribuisce l'accesso, sono responsabili del suo corretto utilizzo. 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 è permesso con moderazione e con gli accorgimenti di cui al presente documento.
L'utente s'impegna a non cedere, una volta superata la fase di autenticazione, l'uso del proprio dispositivo personale a soggetti non autorizzati, in particolar modo per quanto riguarda l'accesso a Internet e ai servizi di posta elettronica.
Al fine di non compromettere la sicurezza del sistema informatico del comitato e di prevenire conseguenze legali o di altro genere a carico della stessa, gli utenti dovranno in ogni caso adottare i seguenti comportamenti:

- Evitare il download di programmi software, anche gratuiti, se non per esigenze strettamente professionali e comunque solo in caso di esplicita autorizzazione.
- È vietata la partecipazione, non esplicitamente autorizzata, a Forum non professionali, a chat, a bacheche elettroniche e, più in generale, qualunque utilizzo di servizi Internet, attuali o futuri, non strettamente inerenti all'attività professionale
- Evitare di scaricare file da siti non sicuri (riconoscibili dall'assenza del lucchetto verde a sinistra dell'indirizzo web e dall'assenza di https:// prima dell'indirizzo web).
- 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 dalil comitato per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.
- Non utilizzare modem personali, o qualunque altro dispositivo "Internet-Key" con account personali.
- Evitare di entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato.
- Non effettuare copia non autorizzata di materiale coperto da copyright.
- Non accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
- Non memorizzare documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

- Non accedere dall'esterno alla rete interna dell'organizzazione, salvo con le specifiche procedure previste dall'ente stesso.
- Non eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati all'host dell'utente (sniffing), a meno che questa attività non faccia parte dei compiti dell'utente e quindi formalmente autorizzata dalla Direzione.
- Non condividere file in modalità peer-to-peer.
- Non scaricare materiale e programmi in violazione della legislazione sui diritti di autore, che siano essi appartenenti a persone o aziende, coperti da copyright, brevetto o proprietà intellettuale, ivi compresa l'installazione o la distribuzione di software che non sia specificatamente licenziato per essere utilizzato all'interno delil comitato

Parte sesta - Utilizzo del servizio di posta elettronica

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità del comitato ed in stretta connessione con l'effettiva attività e mansioni del soggetto dipendente o collaboratore che utilizza tale funzionalità.
La posta elettronica è quindi uno strumento esclusivamente lavorativo e pertanto non è possibile utilizzare tale servizio per finalità in contrasto con quelle aziendali, non pertinenti all'attività lavorativa o personali.
Gli utenti in possesso di una casella di posta elettronica aziendale personale sono i diretti responsabili del corretto utilizzo di quest'ultima.
Al fine di non compromettere la sicurezza del comitato e di prevenire conseguenze legali a carico del comitato stesso è necessario adottare le seguenti norme comportamentali:

Phishing: se nonostante i controlli preventivi antispamming e antivirus automatici, si ricevono messaggi da mittenti sconosciuti contenenti allegati file (in particolare programmi eseguibili o file di word processor e fogli di calcolo contenenti delle macro, file compressi) evitare di aprire tali e-mail e tali allegati e procedere alla loro immediata eliminazione; se nonostante i controlli preventivi antispamming e antivirus automatici, si ricevono messaggi da mittenti sconosciuti contenenti richieste di comunicazioni di dati o richieste di collegamento a link esterni, evitare di comunicare tali dati o di aprire il link e procedere alla loro immediata eliminazione; nel caso in cui i messaggi sopraindicati si ricevano da mittenti conosciuti ma che non siano concordati, è necessario verificare il mittente tramite telefono, chiamando il diretto interessato (mittente del messaggio).
Come riconoscerli: i messaggi di phishing sono progettati per ingannare e spesso utilizzano imitazioni realistiche dei loghi o addirittura delle pagine web ufficiali di banche, aziende ed enti. Tuttavia, capita spesso che contengano anche grossolani errori grammaticali, di formattazione o di traduzione da altre lingue. E' utile anche prestare attenzione al mittente (che potrebbe avere un nome vistosamente strano o eccentrico) o al suo indirizzo di posta elettronica (che spesso appare un'evidente imitazione di quelli reali, sono formati da una sequenza incomprensibile di lettere e numeri e spesso non hanno il prefisso https:// prima di www.). Meglio diffidare dei messaggi con toni intimidatori, che ad esempio contengono minacce di chiusura del

conto bancario o di sanzioni se non si risponde immediatamente: possono essere subdole strategie per spingere il destinatario a fornire informazioni personali.
Una piccola accortezza consigliata è quella di posizionare sempre il puntatore del mouse sui link prima di cliccare: in molti casi si potrà così leggere in basso a sinistra nel browser il vero nome del sito cui si verrà indirizzati.

Inoltre:

- È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o comunque non inerenti la propria attività lavorativa e per la partecipazione a dibattiti, forum o mailing list salvo diversa ed esplicita autorizzazione scritta.
- Aprire allegati di posta elettronica ambigui o di incerta provenienza (gli allegati possono, infatti, contenere virus o codici nascosti di natura dolosa che possono comportare la divulgazione di password o il danneggiamento di dati).
- La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.
- Il sistema di gestione della posta elettronica non deve essere in nessun modo usato per scrivere o per diffondere messaggi che possano nuocere all'immagine del comitato verso l'esterno: messaggi offensivi, satirici o politicamente definibili, catene di S. Antonio, scherzi, avvisi di pericolo per la diffusione di virus ecc.
- Non usare il servizio per scopi illegali, per inviare e ricevere materiale pornografico, osceno, volgare, diffamatorio, oltraggioso, discriminatorio, abusivo, pericoloso.
- Non effettuare ogni genere di comunicazione finanziaria a scopo personale, ivi comprese le operazioni di remote Banking, acquisti on-line e simili, salvo diversa ed esplicita autorizzazione aziendale.
- Non simulare l'identità di un altro utente, ovvero utilizzare credenziali di posta non proprie per l'invio di messaggi.
- Evitare di modificare la configurazione hardware e software del dispositivo assegnato; né utilizzare sistemi client di posta elettronica non conformi a quelli accettati dal comitato.
- 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. Qualora il collaboratore riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente.
- Prestare particolare attenzione ai destinatari e, in caso di debba inviare lo stesso messaggio a destinatari non appartenenti alla stessa azienda o che non si conoscono tra di loro, utilizzare il Ccn.

È necessario sempre indicare l'oggetto della e-mail nell'apposita riga; nel caso in cui si chieda ad un soggetto di inviare una mail ad una casella comune o ad un alias (ad esempio info@...., amministrazione@....) chiedere sempre di indicare nell'oggetto il destinatario del messaggio.
I messaggi inviati tramite posta elettronica aziendale (di servizio e/o nominativi) dovranno contenere un testo che si componga di firma specifica del soggetto a cui si riferisce, unitamente al disclaimer privacy (fornita come "Informativa e-mail").

Nel caso di assenza prolungata deve essere attivato dal singolo dipendente, prima di assentarsi, il servizio di risposta automatica (Auto-reply), pertanto in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) dovrà impostare la risposta automatica per informare coloro che lo contattano dell'indisponibilità a leggere la comunicazione.
Di seguito un esempio di testo da indicare come risposta automatica:

"Non sono in ufficio fino al ... , avrò un limitato accesso alle mail e non posso garantire una risposta.
Per urgenze potete scrivere a *INDIRIZZO EMAIL DI RIFERIMENTO* o telefonare allo 0000/000000.
Grazie per avermi contattato".

Tutti i messaggi ricevuti, spediti o salvati, potranno essere letti da un Amministratore di Sistema, dal Legale rappresentate o suo delegato o da un collega espressamente designato esclusivamente per i seguenti motivi:

1. in caso di assenza improvvisa o non programmata per garantire una regolare continuità dell'attività lavorativa;
2. in seguito a segnalazioni di malfunzionamenti da parte del singolo utente;
3. fatti illeciti lesivi al patrimonio e/o immagine riscontrati precedentemente alla verifica.

In tutti questi casi il dipendente verrà informato.

Parte settima - Data breach

L'art. 33 del GDPR prescrive al Titolare del trattamento l'obbligo di documentare qualsiasi violazione dei dati personali, comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Per questi motivi Croce Rossa Italiana – Comitato di Ravenna si è dotato di un Registro delle violazioni, conservato a cura del titolare stesso; inoltre il GDPR ha introdotto l'obbligo per tutti i Titolari del trattamento di notificare all'autorità di controllo competente (Garante per la protezione dei dati personali) la violazione di dati personali (data breach), senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche.
È pertanto importante che tutti gli autorizzati al trattamento che operano sotto l'autorità del Titolare del trattamento siano preparati a fronteggiare una tale eventualità;
Per violazione di dati personali o data breach si intende "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati" (art. 4 del Regolamento). Essa può comportare un insieme di effetti negativi per i diritti e le libertà degli interessati, il GDPR ne identifica alcuni:
- la perdita del controllo sui propri dati personali;
- la limitazione dei diritti degli interessati;
- la discriminazione;
- il furto di identità;
- la frode;
- la perdita finanziaria;

- la possibile identificazione di un soggetto pseudonimizzato;
- il danno alla reputazione;
- la perdita della riservatezza sui dati personali protetti da segreto professionale;
- ogni altra perdita economica o svantaggio sociale significativo per l'interessato;

Le violazioni di dati personali possono essere identificate attraverso i seguenti tre principi in materia di sicurezza:

a) **Violazione della riservatezza** – Quando vi è una divulgazione o un accesso non autorizzato o accidentale a dati personali
b) **Violazione dell'integrità** – Quando vi è un'alterazione non autorizzata o accidentale di dati personali
c) **Violazione della disponibilità** – Quando vi è l'impossibilità di accedere ai dati personali o è avvenuta, anche accidentalmente, la loro distruzione.

Occorre notare inoltre che - a seconda delle circostanze - è possibile che una violazione possa riguardare sia uno solo di questi principi come due o più di essi.

Una violazione di dati personali (data breach) può avvenire secondo diverse modalità, qui indichiamo quattro esempi:

- Dipendente o collaboratore o socio infedele che sottrae dati dai database;
- Errore umano che comporta una violazione della riservatezza, integrità o disponibilità;
- Virus o attacco informatico;
- Furto di un bene (ad esempio PC contenente dati personali o dotato di software che permette l'accesso al server aziendale).

Qualora un autorizzato al trattamento (sia esso un dipendente o un collaboratore che presta a qualsiasi titolo un'attività di trattamento di dati presso il titolare) ritenga che sia in corso o vi sia il concreto rischio che si verifichi (o si sia già verificata) una violazione dei dati personali, deve tempestivamente e senza ritardo coinvolgere il **Titolare del trattamento,** che agisce nella persona del **presidente,** oppure, se ciò non è possibile, i **dipendenti dell'ufficio amministrativo.** Il Titolare del trattamento, e nel caso i dipendenti dell'ufficio amministrativo dopo aver coinvolto il titolare, contattano senza ingiustificato ritardo e senza indugio **l'Amministratore di sistema** (se designato) oppure Il **servizio IT**, sia esso interno od esterno, il quale avrà il compito di effettuare una prima analisi dell'accaduto. Allo stesso tempo, il Titolare del trattamento o suo delegato contatta i **consulenti privacy** designati, i quali, unitamente al tecnico informatico e al titolare o suo delegato, effettuano un'analisi approfondita dell'accaduto secondo i seguenti criteri:

- Natura della violazione dei dati personali
- (Ove possibile) il numero - anche approssimativo - di interessati coinvolti
- (Ove possibile) le categorie ed il numero - anche approssimativo - di dati personali coinvolti
- Probabili conseguenze della violazione

A seguito di tale valutazione il **Titolare** e i soggetti coinvolti individuano e - se del caso - adottano le misure adeguate per porre rimedio alla violazione o per attenuarne i possibili effetti negativi e aggiornano il registro data breach.

Il **Titolare**, nel caso in cui la violazione presenti un rischio per i diritti e le libertà delle persone fisiche, la notifica al Garante secondo le procedure all'uopo disposte dall'Autorità e - se del caso - procede alla Notificazione agli interessati.

Parte ottava - Gestione dei documenti cartacei ed istruzioni operative

Documenti cartacei e divieti

Tutti i documenti contenenti dati personali che sono necessari per lo svolgimento del lavoro devono essere a disposizione degli addetti per il tempo strettamente necessario e quindi depositati in armadi o cassetti chiusi o in stanze chiuse e, comunque, sottratti alla visione di persone estranee che dovessero trovarsi all'interno degli uffici.

Gli ospiti devono essere accolti e fatti attendere in un luogo in cui non siano presenti documenti cartacei o device collegati alla rete informatica interna; in occasione di un colloquio o riunione con un ospite i documenti presenti sulle scrivanie o sul tavolo presso cui si svolge devono essere asportati.

La documentazione cartacea contenente dati particolari (c.d. sensibili) o informazioni considerate importanti deve essere protetta in appositi armadi dotati di chiavi oppure in scaffalature e/o armadi situati in stanze o archivi chiusi a chiave.

Tutti i documenti contenenti dati particolari (c.d. sensibili) o informazioni ritenute importanti che si ritiene debbano essere eliminati devono essere distrutti, utilizzando una macchina distruggi-documenti o servendosi di un servizio di trasporto e smaltimento rifiuti, e non semplicemente gettati nei cestini o riciclati.

Non si devono mai lasciare in vista i cedolini paga, così come i documenti relativi ai dipendenti (copie dei documenti d'identità, contratto di lavoro, lettere disciplinari ecc...) o i fascicoli contenenti i documenti relativi ai soci; questi devono essere conservati in un luogo separato ad accesso limitato al solo personale addetto alla gestione del personale e dei soci.

È vietato il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici, come per esempio corridoi o sale riunioni, così come è vietato lasciare memorie esterne, fogli e cartelle e quant'altro a disposizione di estranei.

Le schede utilizzate durante i trasporti, in occasione di interventi di soccorso ed i documenti che individuano gli utenti del centro di ascolto contengono particolari categorie di dati e pertanto devono essere trattati con particolare attenzione: è vietato effettuare fotografie dei predetti documenti e comunicarli a terzi o diffonderli; le schede ed i documenti sopra indicati sono ad esclusivo uso interno e possono essere comunicati solo ad enti sanitari (Ospedali, Pronto soccorso) per finalità funzionali alla prestazione di assistenza.

Terminata la giornata di lavoro e/o in periodi di assenza verificare di non lasciare visibili documenti e atti riservati con particolare riferimento a quelli contenenti dati e informazioni di natura sensibile e/o riservati. Pertanto si fa richiamo alla "politica della scrivania pulita". Si richiede agli autorizzati di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dell'ente.

Istruzioni operative e divieti

L'uso di strumenti elettronici finalizzati alla produzione di documenti cartacei, come fotocopiatori, fax, stampanti richiede particolare attenzione: gli stampati prodotti non vanno lasciati presso l'apparecchio, fogli

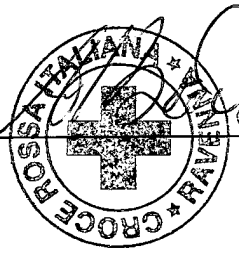
riportanti eventuali errori vanno strappati e gettati e non riciclati; nel caso di documenti riportanti dati particolari il fax va inviato solo dopo un accurato controllo dell'esattezza del numero di fax del destinatario.
Si può accedere ai soli dati, oggetto di trattamento, la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati e per le finalità di cui al provvedimento di autorizzazione.
Non fornire dati o informazioni di carattere personale per telefono, qualora non si abbia la certezza assoluta sull'identità dell'interlocutore. Qualora si abbia un sospetto sull'identità dell'interlocutore è necessario chiedere il nome ed in numero di telefono, avvisarlo che sarà richiamato, riagganciare e richiamare per accertare l'identità.
È espressamente vietato divulgare o comunicare a terzi non autorizzati, dati, informazioni, atti, documenti riservati (in qualunque forma) senza espressa autorizzazione del proprio Responsabile e/o della Direzione.
È espressamente vietato salvare dati personali e informazioni aziendali ritenute importanti o riservate in sistemi cloud (per esempio Dropbox, Google+, Evernote, ecc..) non autorizzati dal servizio IT e dalla Direzione o in sistemi cloud personali.
È generalmente vietato salvare dati e file su chiavette USB o HD destinati ad essere trasportati fuori dalil comitato, salvo che il salvataggio sia strettamente necessario all'attività aziendale e sia stato autorizzato dal titolare delil comitato.
È espressamente vietato pubblicare sul web (Social media, forum, chat, blog, siti internet) dati personali riferiti a clienti, fornitori, soci e dipendenti ed informazioni di carattere aziendale non autorizzate dal proprio Responsabile o dalla Direzione.

Videosorveglianza

La sede di via Gorizia è fornita di un sistema di videosorveglianza, composto da 4 telecamere le quali riprendono gli accessi esternamente e l'ingresso/uscita delle ambulanze internamente. Dal momento che le telecamere potrebbero riprendere persone, le immagini sono da considerarsi a tutti gli effetti dati personali e quindi è necessario adottare alcune norme comportamentali.
Le immagini sono visualizzabili dal monitor presente in sala operativa, la predetta sala è ad accesso riservato solo agli operatori autorizzati, pertanto nessun estraneo od ospite può essere autorizzato ad entrarci. La visualizzazione live delle immagini deve essere utilizzata per il riconoscimento degli ospiti.
Le immagini sono da considerarsi ad esclusivo uso interno, pertanto alle registrazioni può accedere solo il presidente e l'amministratore di rete e non possono essere comunicati a terzi estranei, eccezion fatta per gli organi di polizia giudiziaria e/o dell'autorità giudiziaria. È quindi vietato alla generalità dei soci, con eccezioni dei due soggetti sopra individuati, di accedere alle registrazioni, salvo autorizzazioni scritta dal parte del presidente, limitandosi quindi alla visualizzazione live delle immagini.
È fatto esplicito divieto di effettuare foto e video al monitor ed alle immagini visualizzabili da esso e di diffondere intenzionalmente le immagini.

Il presente Regolamento verrà consegnato a tutto il personale dipendente ed ai collaboratori tramite consegna cartacea e/o invio tramite e-mail, inoltre l'originale timbrato e firmato dal legale rappresentante sarà conservato presso la sede del comitato, a disposizione per eventuale consultazione. Le eventuali modifiche saranno rese note nella stessa maniera.

Timbro e firma del Titolare del trattamento



Informativa sul trattamento dei dati personali

(Art. 13 Regolamento UE 27 aprile 2016, n. 679 in materia di protezione dei dati personali *"GDPR"*)

In conformità con i requisiti posti dal Regolamento Generale in materia di protezione dei dati personali il Titolare del trattamento, **Croce Rossa Italiana – Comitato di Ravenna,** fornisce all'interessato le seguenti informazioni in relazione alla videosorveglianza effettuata presso la sede del comitato.

FINALITÀ E BASE GIURIDICA

Le riprese sono effettuate sulla base del legittimo interesse del Titolare del trattamento alla protezione e sicurezza della sede, delle persone al suo interno, della strumentazione e dei materiali utilizzati per gli interventi di assistenza e protezione civile presenti nelle apposite aree all'interno della sede. La finalità è pertanto quella di assicurare una maggior sicurezza della sede anche tramite il riconoscimento di ospiti ed intrusi.

MODALITÀ DEL TRATTAMENTO

La registrazione avviene tramite quattro telecamere, di cui tre esterne orientate verso gli accessi ed una interna alla rimessa ambulanze orientata verso l'ingresso/uscita delle stesse; le telecamere effettuano registrazione su HD conservato all'interno dell'armadio di rete. Gli operatori in centrale operativa sono autorizzati a visualizzare le immagini live tramite il monitor, mentre il presidente e l'amministratore di rete sono autorizzati anche ad accedere alle registrazioni.

DESTINATARI DEI DATI

Le immagini sono oggetto di trattamento interno e, in caso di eventi o tentati eventi criminosi, le immagini possono essere comunicate ad organi di polizia giudiziaria e all'autorità giudiziaria.

PERIODO DI CONSERVAZIONE

Le immagini sono conservate secondo i criteri previsti dalla normativa vigente. È inoltre attiva la sovrascrittura automatica delle immagini.

DIRITTI DELL'INTERESSATO

In relazione ai predetti trattamenti ed ai relativi dati esistenti presso i nostri archivi, **potranno essere esercitati i diritti di cui al Capo III, artt. Da 15 a 22 del Regolamento UE 2016/679**, nello specifico:

- Diritto di accesso (art.15);
- Diritto di rettifica (art.16);
- Diritto alla cancellazione (cd. diritto all'oblio, art.17);
- Diritto di limitazione del trattamento (art.18);
- Diritto di opposizione (art.21);

Lei inoltre potrà proporre reclamo ad un'autorità di controllo, ad esempio il Garante per la protezione dei dati personali.

TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento è **Croce Rossa Italiana - Comitato di Ravenna**, con sede in Ravenna (RA), via Gorizia 11, 48121, telefono **0544 38052**, e-mail **ravenna@cri.it**

Le richieste di esercizio dei diritti previsti dal GDPR a favore dell'interessato potranno essere rivolte al Titolare del trattamento.