REGOLAMENTO SULL'USO DELLE ATTREZZATURE INFORMATICHE E DEGLI IMPIANTI

Sulla base del Regolamento Europeo 679/2016 (GDPR)

e dalle successive integrazioni e indicazioni del Garante per la Privacy

Allegato 10

Al Regolamento aziendale in materia di protezione dei dati personali Rev. 1.0 del 20/09/2018

SOMMARIO

1. REVISIONI

Indice delle revisioni

Rev.	Data	Descrizione	Redatto	Verificato	Approvato
0.0	14/05/2018		✓	✓	✓
1.0	20/09/2018		✓	✓	✓

2. SCOPO

Il presente regolamento disciplina il trattamento dei dati personali contenuti nelle banche dati organizzate, gestite od utilizzate dall'Associazione Primavera Onlus, in relazione allo svolgimento delle proprie finalità istituzionali, in attuazione del D. Lgs. n. 196 del 30 Giugno 2003 così come modificato dal D.Lgs N. 101 del 10/08/2018 e del Regolamento Europeo 679/2016.

Per finalità istituzionali, ai fini del presente regolamento, si intendono le funzioni previste dalla legge, dallo Statuto, dai regolamenti, le funzioni svolte per mezzo di convenzioni, accordi, intese e mediante gli strumenti di programmazione negoziata previsti dalla legislazione vigente e le funzioni collegate all'accesso ed all'erogazione dei servizi resi dall'Associazione.

Ai fini del presente regolamento, per le definizioni di banca dati, di trattamento, di titolare, di responsabile, di incaricato, di interessato, di comunicazione, di diffusione, di dato anonimo, di blocco e di Garante si fa riferimento a quanto previsto dal D. Lgs. n. 196 del 30 Giugno 2003 così come modificato dal D.Lgs N. 101 del 10/08/2018.

Il presente regolamento si rivolge al personale dell'Associazione Primavera Onlus incaricato del trattamento dei dati suindicati e ne disciplina i comportamenti correlati.

Il presente regolamento deve servire per migliorare l'efficienza interna e i servizi forniti dall'Associazione.

3. CAMPO DI APPLICAZIONE

Il ***"*REGOLAMENTO INTERNO*"*** definisce regole e gli standard di comportamento nei confronti di tutti coloro che a qualsiasi titolo operano nei nostri uffici, dei collaboratori esterni e dei fornitori in genere.

Il ***"REGOLAMENTO INTERNO"*** riguarda tutti coloro che operano all'interno della nostra struttura ed in particolare:

- Il personale dipendente
- I collaboratori esterni
- Coloro che per motivi vari si trovano anche temporaneamente ad operare all'interno dei nostri locali.

Il ***"REGOLAMENTO INTERNO"*** deve essere conosciuto ed applicato da tutte le componenti della nostra attività.

A cura del Titolare, possono essere periodicamente attivati controlli, anche a campione, al fine di garantire la sicurezza delle banche-dati, e l'attendibilità dei dati inseriti e il rispetto delle norme e disposizioni previste dal presente regolamento.

4. RIFERIMENTI NORMATIVI

- Contratto nazionale di Lavoro
- Decreto legislativo 9 Aprile 2008 n. 81 "TESTO UNICO SULLA SALUTE E SICUREZZA SUL LAVORO"
- Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" così come modificato dal D.Lgs N. 101 del 10/08/2018
- Le linee guida del Garante per posta elettronica e internet pubblicato sulla Gazzetta Ufficiale n. 58 del 10 marzo 2007
- Garante per la Protezione dei Dati Personali con Provvedimento n. 456 del 30 luglio 2015
- Regolamento Europeo 679/2016

- Linee-guida del Garante sulla valutazione d'impatto della protezione dati (04/10/2017)

5. REGOLE GENERALI

5.1 ACCESSO AI LOCALI DELLA SEDE

I dipendenti, i collaboratori libero professionali esterni e i consulenti possono accedere ai locali degli uffici durante l'orario programmato con eccezione per le funzioni esplicitamente autorizzate dal Titolare.

5.2 ACCESSO AI LOCALI DELL'ASSOCIAZIONE

Gli utenti, gli assistiti e/o i loro familiari, i fornitori, etc. potranno accedere ai locali degli uffici durante l'orario di lavoro sia per prenotare appuntamenti o chiedere informazioni. **I sopradetti non possono avere accesso in punti in cui è possibile avere visuale degli schermi dei computer.**

5.3 ACCESSO ALLE SALE PER RIUNIONI, INCONTRI E CORSI

Le persone che devono partecipare a riunioni, incontri e corsi tenuti presso gli uffici, potranno accedere direttamente seguendo le indicazioni del personale addetto.

5.4 ACCETTAZIONE MERCE

I trasportatori e o Fornitori che consegnano merce hanno la possibilità di farlo esclusivamente durante l'orario di ufficio e avranno accesso solo all'ingresso. Per lo scarico merci direttamente all'ingresso degli uffici.

5.5 Ritiro Documenti

Tutti coloro che devono ritirare documenti possono presentarsi in nelle sedi delle Segreterie negli orari affissi.

6. UTILIZZO DELLE ATTREZZATURE E DEGLI IMPIANTI

6.1 SCRIVANIA E POSTI DI LAVORO

Ognuno è tenuto a conservare con la massima cura tutto il materiale che gli è stato affidato. Ogni incaricato deve tenere in ordine la propria scrivania e gli armadi evitando di tenere in vista bottiglie vuote, lattine, bicchieri usati, ecc.. e deve preoccuparsi di spegnere computer, stampanti, modem, fotocopiatrici, duplicatori, ecc… ogni qualvolta si lascia il posto di lavoro, in particolare durante l'intervallo di pranzo e la sera. Ognuno si deve preoccupare di controllare la chiusura delle finestre e delle persiane. Se per motivi di lavoro ci si sposta dal proprio posto di lavoro ad un altro per un periodo prolungato si deve comunicare al Responsabile dove ci si trova.

6.2 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.

(Vedi anche Procedura Operativa GDPR PO Pri -2.0 rev.0)

6.3 USO DEI PERSONAL COMPUTER, DELLE STAMPANTI E DELLE ATTREZZATURE

Il personal computer a disposizione per lavorare e le stampanti debbono essere tenute in uno stato di buona efficienza.

Se si riscontrano anomalie di funzionamento si deve far intervenire prontamente l'assistenza tecnica secondo la procedura prevista dal Responsabile (moduli, segnalazioni, etc.).

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.

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 dall'organizzazione. Per necessità aziendali, gli 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 alle 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 dell'ente 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 dall'organizzazione;

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.

All'incaricato è vietato:

1. La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali dell'incaricato 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. Utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta dell'ente.
4. Installare alcun software di cui l'ente 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 dell'organizzazione. 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 dell'organizzazione.
7. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'organizzazione, 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 dell'organizzazione.

(Vedi anche Procedura Operativa GDPR PO Pri – 2.1 rev.0)

6.4 SISTEMI ANTIVIRUS

Su tutti i personal computer interni **deve essere installato un sistema Antivirus**, conformemente alle indicazioni dell'Amministratore di Rete. Se si riscontrano anomalie di funzionamento si deve informare immediatamente l'Amministratore di Rete o il Responsabile.

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, via mail …

L'ente 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 all'ente ogni anomalia o malfunzionamento del sistema antivirus;

2. Comunicare all'ente 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. E' vietato ostacolare l'azione dell'antivirus aziendale;

3. E' vietato disattivare l'antivirus senza l'autorizzazione espressa dell'ente anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer;

4. E' 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 i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

(Vedi anche Procedura Operativa GDPRPO Pri – 2.2 rev.0)

6.5 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 dall'organizzazione agli Incaricati che durante gli spostamenti e/o per ragioni legati alla mansione svota necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'organizzazione.

L'Incaricato è responsabile dei device mobili assegnatigli dall'organizzazione 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 dall'ente. I device mobili 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 l'ente che provvederà – se del caso – ad occuparsi delle procedure connesse alla privacy. 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.

I device mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciti privi di PIN.

Laddove il device mobile sia accompagnato da un'utenza, l'Incaricato è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, …) e a rispettarli. Qualora esigenze lavorative richiedessero requirements differenti l'Incaricato è tenuto ad informare tempestivamente e preventivamente l'ente.

In relazione alle utenze mobili, salvo autorizzazione dell'organizzazione, è espressamente vietato ogni utilizzo all'estero e anche in caso di autorizzazione dell'organizzazione, gli utilizzi all'esterno devono essere preventivamente comunicati all'organizzazione per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

Il telefono è uno strumento di lavoro e va utilizzato esclusivamente per questo scopo. Le telefonate personali vanno limitate allo stretto necessario sia in numero che in durata. L'uso del telefono personale aziendale (cellulare), se in dotazione, è consentito per sole esigenze lavorative legate alla mansione svolta.

6.6 PRESCRIZIONI INTERNE SULLA SICUREZZA DEI DATI E DEI SISTEMI

Per i trattamenti di dati personali effettuato con l'ausilio di strumenti elettronici, gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

• Gli Incaricati del trattamento dei dati personali sono autorizzati ad effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito per iscritto e comunicato all'atto della designazione, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati comunali che contengono i predetti dati personali.

• Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate e, pertanto, in conformità alle informazioni comunicate agli interessati.

• L'Incaricato del trattamento dei dati personali deve prestare particolare attenzione all'esattezza dei dati trattati e, se sono inesatti o incompleti, deve provvedere ad aggiornarli tempestivamente.

• Ogni Incaricato del trattamento dei dati personali è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.

• Gli Incaricati del trattamento dei dati personali che hanno ricevuto le credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le componenti riservate delle credenziali di autenticazione (parole chiave) e i dispositivi di autenticazione in loro possesso e uso esclusivo.

• La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.

• La componente riservata delle credenziali di autenticazione (parola chiave) non deve contenere riferimenti agevolmente riconducibili all'incaricato.

• L'Incaricato del trattamento dei dati personali deve modificare la componente riservata delle credenziali di autenticazione (parola chiave) al primo utilizzo e, successivamente, almeno ogni sei mesi.

• In caso di trattamento di dati sensibili e di dati giudiziari la componente riservata delle credenziali di autenticazione (parola chiave) deve essere modificata almeno ogni tre mesi.

• Gli incaricati del trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali. Per i trattamenti di dati personali effettuato senza l'ausilio di strumenti elettronici gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali o negli armadi individuati per la loro conservazione se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.
- Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione o dagli armadi, l'incaricato del trattamento non dovrà lasciarli mai incustoditi.
- L'incaricato del trattamento deve inoltre controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici , composti da numerose pagine o più raccoglitori, siano sempre completi e integri.
- Al termine dell'orario di lavoro l'incaricato del trattamento deve riportare tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, nei locali individuati per la loro conservazione.
- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.
- Si deve adottare ogni cautela affinché ogni persona non autorizzata, non possa venire a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici.

- Per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche al minimo indispensabile.
- Particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro incaricato debitamente autorizzato;
- Documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura.
- E' inoltre tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tantomeno si possono utilizzare come carta per appunti.
- Quando i documenti devono essere trasportati essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, l'incaricato del trattamento deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti.
- L'incaricato del trattamento deve inoltre evitare che un soggetto terzo non autorizzato al trattamento possa esaminare, anche solo la copertina del documento in questione.
- E' proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un incaricato autorizzato a potere trattare i dati in questione.
- Si raccomanda vivamente non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente. Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico od aperto al pubblico.

6.7 UTILIZZO DI COLLEGAMENTI INTERNET

Per la tipologia di lavoro e per i vantaggi che derivano dall'utilizzo di INTERNET, sono messe a disposizione di tutto il personale le migliori tecnologie oggi disponibili. **Sono vietati comunque i collegamenti ad INTERNET per usi non strettamente collegati al lavoro da svolgere, e debbono essere evitate tutte le attività non strettamente necessarie (come ad esempio l'utilizzo di siti internet per ascoltare radio, download di film, canzoni, ecc....). Non è ammesso l'utilizzo di collegamenti per servizi o scopi personali, quali Servizi di Borsa, Prenotazione viaggi, ecc..** Si informa il personale che per effetto di copie di back up, della gestione tecnica della rete o di files di log sono conservate informazioni sulla navigazione degli utenti in forma centralizzata. Tale registrazione è obbligatoria e può essere esibita all'autorità giudiziaria in caso di richiesta di quest'ultima.

Divieti Espressi concernenti Internet

1. È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute dell'Incaricato poiché potenzialmente idonea a rivelare dati sensibili ai sensi del Codice Privacy.

2. È fatto divieto di 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.

3. È vietato all'Incaricato lo scarico di software (anche gratuito) prelevato da siti Internet, a meno che non sia preventivamente autorizzato per fini aziendali;

4. 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.

5. È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

6. 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 dell'organizzazione, salvo specifica autorizzazione dell'organizzazione stessa.

7. 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.

8. È vietato all'Incaricato di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale.

9. E' vietato accedere dall'esterno alla rete interna dell'organizzazione, salvo con le specifiche procedure previste dall'ente stesso.

10. È vietato, infine, creare siti web personali sui sistemi dell'organizzazione 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.

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 dall'ente per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

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 dall'organizzazione.

6.8 ACCESSO ALLA POSTA ELETTRONICA

L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa. L'uso per motivi personali deve essere moderato ed è tollerato esclusivamente ai sensi dell'articolo seguente.
Gli Incaricati possono avere in utilizzo indirizzi nominativi di posta elettronica.
Le caselle e-mail possono meglio essere assegnate con natura impersonale (tipo info, amministrazione, fornitori, direttore, direttore sanitario, consulenza, …) proprio per evitare ulteriormente che il destinatario delle mail possa considerare l'indirizzo assegnato al dipendente "privato", ai sensi dei suggerimenti del Garante a tal proposito.

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

Per fronteggiare le recenti minacce di software indesiderato in grado di modificare i dati aziendali (definito in vari modi tra i quali virus, ramsonware, cryptovirus, encryptor) stante le avvertenze della case produttrici di antivirus, antispyware e altri sistemi di sicurezza e prevenzione, e stabilito che l'origine più frequente delle infezioni virali di questo tipo di software avviene attraverso la posta elettronica, si diramano le seguenti direttive:

1. Chiunque adoperi software di posta elettronica (client) o consulti la posta elettronica attraverso un qualsiasi browser (webmail) deve prestare particolare attenzione al mittente ed all'oggetto ed astenersi anche solo dall'aprire il messaggio, se possibile, in caso di mittenti sconosciuti, di oggetto non coerente o palesemente erroneo, non conforme o vuoto.

2. Nei messaggi di posta elettronica prestare particolare attenzione ad eventuali collegamenti (link) contenuti nel testo del messaggio ed evitare di seguire il collegamento (clic sul link) se puntano ad indirizzi stranieri, a file di tipo eseguibile (.EXE) o file di programma (.JAR, . MSI, ecc)

3. Nei messaggi di posta elettronica prestare particolare attenzione ai file allegati ed evitare di scaricarli (download) se sospetti o sconosciuti.

4. Nel caso in cui sul proprio pc compaiono messaggi di richiesta di denaro (in italiano o in altra lingua) e appare impossibile aprire i propri file, è necessario staccare immediatamente il cavo di rete del pc e richiedere immediatamente l'intervento del proprio amministratore di rete

Tali disposizioni si applicano anche se l'utente consulta la posta elettronica personale: il Garante per la Protezione dei Dati Personali con Provvedimento n. 456 del 30 luglio 2015 ha stabilito che il datore di lavoro, pur non avendo il diritto di accedere ai contenuti specifici, ha il diritto di verificare l'utilizzo della posta elettronica aziendale al fine di prevenire infezioni virali e garantire la massima sicurezza possibile estendendo tale diritto a tutte le attività svolte dal dipendente con le attrezzature aziendali, ivi compresa la consultazione della posta elettronica personale se effettuata nelle ore di ufficio anche con mezzi propri (mobile, tablet, etc.) se commessi tramite la rete aziendale.

Divieti Espressi

1. È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio dell'organizzazione per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'organizzazione, nonché utilizzare il dominio dell'organizzazione per scopi personali.

2. È vietato redigere messaggi di posta elettronica utilizzando l'indirizzo aziendale, diretti a destinatari esterni dell'organizzazione, senza utilizzare il seguente disclaimer: «Le informazioni contenute in questo messaggio di posta elettronica e/o nel/i file/s allegato/i, sono da considerarsi strettamente riservate. Il loro utilizzo è consentito esclusivamente al destinatario del messaggio, per le finalità indicate nel messaggio stesso. Qualora riceveste questo messaggio senza esserne il destinatario, Vi preghiamo cortesemente di darcene notizia via e-mail e di procedere alla distruzione del messaggio stesso, cancellandolo dal vostro sistema; costituisce comportamento contrario ai principi

dettati dal Dlgs. 196/2003 e dal Reg. UE 679/2016 il trattenere il messaggio stesso, divulgarlo anche in parte, distribuirlo ad altri soggetti, copiarlo o utilizzarlo per finalità diverse. Un corretto comportamento da parte di tutti contribuirà a realizzare una società più civile. Grazie».

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 sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.

5. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'organizzazione informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.

6. È vietato utilizzare la posta elettronica per messaggi con allegati di grandi dimensioni.

Utilizzo Illecito di Posta Elettronica

1. È vietato inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.

2. 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.

3. Qualora l'Incaricato riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'organizzazione.

(Vedi anche Procedura Operativa GDPR PO Pri – 2.8 rev.0)

6.9 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.

I duplicatori di CD/DVD debbono essere utilizzati nel rispetto delle leggi sul Copyright.

6.10 DEVICE PERSONALI.

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

Al dipendenti, se espressamente autorizzati dall'ente, è permesso solo l'utilizzo della posta elettronica aziendale sui loro device personali.

In tali casi è necessario che il device abbia password di sicurezza stringenti approvate dall'ente e l'eventuale furto o smarrimento del device deve essere immediatamente segnalato anche all'ente 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 (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri device personali per memorizzare dati dell'ente solo se espressamente autorizzati dall'ente stesso e assumendone formalmente e personalmente l'intera responsabilità del trattamento e per la sussistenza delle misure minime ed idonee di sicurezza.

6.11 SISTEMI IN CLOUD

6.11.1 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 l'ente a potenziali problemi di violazione della privacy. I dati personali vengono memorizzati nelle server farms di aziende che spesso risiedono in uno stato diverso da quello dell'ente. 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 l'ente, 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.

6.11.2 UTILIZZO DI SISTEMI CLOUD

E' vietato agli incaricati l'utilizzo di sistemi cloud non espressamente approvati dall'ente. Per essere approvati i sistemi cloud devono rispondere ad almeno i seguenti requisiti:

- Essere sistemi cloud esclusivi e non condivisi;

- L'azienda che fornisce il sistema in cloud deve essere preventivamente nominata Responsabile al Trattamento dei dati da parte dell'ente;

- L'azienda che fornisce il sistema in cloud deve comunicare all'ente, almeno una volta all'anno, i nominativi degli amministratori di sistema utilizzati.

- Dovranno essere verificate tutte le indicazioni e prescrizioni previste dal Garante della Privacy nei suoi provvedimenti sugli Amministratori di Sistema e sul cloud.

7. PRELIEVO DI ATTREZZATURE

7.1 PRELIEVO DI DOCUMENTI

Di regola i documenti aziendali non si possono prendere e portare fuori della sede con la sola unica eccezione dei trasferimenti presso le autorità giudiziarie previa autorizzazione del Responsabile. In tutti i casi in cui si renda necessario, comunque, possono essere prelevati esclusivamente per gli scopi autorizzati e per il tempo strettamente necessario.

7.2 COMPUTER, STAMPANTI E SCANNER

L'utilizzo di computer (soprattutto dispositivi portatili), stampanti e scanner fuori dalla sede debbono essere autorizzati e deve esserne fatta richiesta scritta direttamente al Responsabile indicando:

Chi ne fa richiesta

Lo scopo

La destinazione

Quando il materiale verrà prelevato dalla sede.

Quando il materiale verrà riportato in sede.