REG. UE 679/2016
GDPR COMPLIANCE

REGOLAMENTO SUL CORRETTO UTILIZZO DEI DISPOSITIVI ELETTRONICI E DELL'ARCHIVIO CARTACEO

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO del 27 Aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

TITOLARE DEL TRATTAMENTO

NUOVA CARBINIA SRLU

TIMBRO E FIRMA

data emissione	numero rev.	CAUSALE
17.02.2019	1	Prima emissione

Sommario

DISCIPLINARE PER L'UTILIZZO DELLA RETE INTERNET E DELLA POSTA ELETTRONICA DA PARTE DEL PERSONALE

PREMESSA

Rispetto all'utilizzo interno delle strumentazioni informatiche, della rete internet e della posta elettronica da parte del personale dipendente, compete al datore di lavoro:

- assicurare la funzionalità delle dotazioni informatiche in dotazione ai dipendenti;
- adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati nonché per prevenire utilizzi indebiti
- adottare limiti e cautele per evitare la registrazione e la diffusione di fotografie e filmati in tempo reale anche utilizzando i terminali di nuova generazione applicati alla telefonia mobile
- indicare in modo particolareggiato quali siano gli strumenti messi a disposizione e le modalità di utilizzo degli strumenti messi a disposizione dei dipendenti ritenute corrette nell'organizzazione dell'attività lavorativa
- precisare in che misura e con quali modalità vengano effettuati i controlli
- tutelare i lavoratori interessati nel trattamento di dati per finalità di gestione del rapporto in ambito pubblico, adottando quelle misure che garantiscono un elevato standard di sicurezza e garanzia
- tener conto della normativa del presente disciplinare di seguito riportata che si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati del trattamento dati in attuazione del D. Lgs. 30/06/2003, n.°196 e del Disciplinare tecnico (Allegato B al citato decreto legislativo) e a cui devono attenersi tutti gli utilizzatori (d'ora in poi definiti utenti) delle strumentazioni informatiche, della rete internet e della posta elettronica.

FINALITÀ

Il presente Regolamento disciplina le modalità di accesso e di uso della Rete Informatica, telematica e dei servizi che, tramite la rete stessa, è possibile ricevere o offrire all'interno e all'esterno dell'azienda, nonché per tutti gli adempimenti amministrativi di legge.

AMBITO DI APPLICAZIONE

La rete aziendale è costituita dall'insieme delle Risorse informatiche, cioè:

- dalle componenti hardware/software e dagli apparati elettronici collegati alla rete;
- dall'insieme delle banche dati in formato digitale ed in generale di tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati

Il presente regolamento si applica, senza distinzione di ruolo e/o livello, a tutti i dipendenti autorizzati ad accedere alla rete aziendale nell'ambito della propria attività lavorativa ordinaria e straordinaria.

Analogamente il presente regolamento si applica alla ditta che effettua attività di manutenzione e agli altri eventuali soggetti esterni autorizzati all'accesso a specifiche banche dati e a tutti i collaboratori a prescindere dal rapporto contrattuale con gli stessi intrattenuto (es. soggetti in attività di stage, relatori e formatori per corsi di aggiornamento,..).

PRINCIPI GENERALI

L'azienda prevede l'utilizzo delle strumentazioni informatiche, della rete internet e della posta elettronica da parte degli utenti quali strumenti utili a perseguire le proprie finalità istituzionali e prevede che lo stesso si conformi ai seguenti principi:

- principio di necessità: i sistemi informativi e i programmi informatici vengono configuratiriducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;
- principio di correttezza: le caratteristiche essenziali dei trattamenti sono rese note ai lavoratori;
- principio di pertinenza e non eccedenza: i trattamenti sono effettuati per finalità determinate, esplicite e legittime e i dati sono trattati nella misura meno invasiva possibile.

VALUTAZIONE DEL RISCHIO

La Rete informatica, l'accesso alla rete internet e alla posta elettronica, il Pc affidato al dipendente sono strumenti di lavoro; su di essi vengono effettuate regolari attività di controllo, amministrazione e backup ed essi non possono in alcun modo essere utilizzati per scopi diversi perché ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

2. MISURE DI TIPO ORGANIZZATIVO

2.1. Assegnazione delle postazioni di lavoro.

Per ridurre il rischio di impieghi abusivi o dannosi, il datore di lavoro provvede a:

- individuare preventivamente le postazioni di lavoro e assegnarle personalmente a ciascun dipendente;
- individuare preventivamente gli utenti a cui è accordato l'utilizzo della posta elettronica e l'accesso a internet.

La strumentazione aziendale non è di esclusivo dominio del dipendente, ma rientra tra i beni a cui determinati soggetti possono comunque sempre accedere. L'eventuale accesso del datore di lavoro, qualora necessiti di informazioni contenute nei documenti residenti sul PC assegnato al dipendente, è legittimo.

2.2. Nomina dell'amministratore di sistema

Il datore di lavoro conferisce all'amministratore di sistema il compito di sovrintendere alle risorse informatiche aziendali assegnandogli in maniera esclusiva le seguenti attività:
gestione dell'hardware e del software (installazione, aggiornamento, rimozione) di tutte le strutture tecniche informatiche dell'azienda, siano esse collegate in rete o meno;

- configurazione dei servizi di accesso alla rete interna, ad internet e a quelli di posta elettronica con creazione, attivazione e disattivazione dei relativi account;
- attivazione della password di accensione (BIOS);
- creazione di un'area condivisa sul server per lo scambio dei dati tra i vari utenti, evitando condivisioni dei dischi o di altri supporti configurati nel PC che non siano strettamente necessarie perché sono un ottimo "aiuto" per i software che cercano di "minare" la sicurezza dell'intero sistema;
- controllo del corretto utilizzo delle risorse di rete, dei computer e degli applicativi, durante le normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- rimozione sia sui PC degli incaricati sia sulle unità di rete, di ogni tipo di file o applicazione che può essere pericoloso per la sicurezza o costituisce violazione del presente regolamento;
- distruzione delle unità di memoria interne alla macchina (hard - disk, memorie allo stato solido) ogni qualvolta si procederà alla dismissione di un PC e dei supporti removibili consegnati a tale scopo dagli utenti;
- utilizzo delle credenziali di amministrazione del sistema per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di indispensabile ed indifferibile necessità di intervento per prolungata assenza, irrintracciabilità o impedimento dello stesso, ma solo per il tempo necessario al compimento di attività indifferibili e solo su richiesta del Responsabile del trattamento

L'amministratore di sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, ha facoltà di accedere in qualunque momento, anche da remoto, e dopo aver richiesto l'autorizzazione all'utente interessato, al PC di ciascun utente.
L'amministratore di sistema può essere un consulente esterno con specifica nomina.

2.3. Utilizzo delle password

Per l'accesso alla strumentazione informatica aziendale ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione previste ed attribuite dall'incaricato della custodia delle password.
Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal custode delle password e consistono in un codice per l'identificazione dell'utente (user id), associato ad una

parola chiave (password) riservata che dovrà essere custodita dall'incaricato con la massima diligenza e non può essere divulgata.

2.4. Procedure di gestione delle credenziali di autenticazione

1. È necessario procedere alla modifica della parola chiave, a cura dell'incaricato, al primo utilizzo. Se l'utente non provvede autonomamente a variare la password entro i termini massimi, viene automaticamente disabilitato. Provvederà l'amministratore di sistema a riabilitare l'utente e ad assegnargli una password provvisoria che l'utente dovrà cambiare al primo accesso.
2. Per scegliere una parola chiave si devono seguire le seguenti istruzioni:
   - usare una parola chiave di almeno otto caratteri;
   - usare una combinazione di caratteri alfabetici e numerici (meglio inserire anche segni di interpunzione o un carattere speciale);
   - non usare mai il proprio nome o cognome, né quello di congiunti(le migliori password sono quelle facili da ricordare, ma allo stesso tempo difficili da indovinare, come quelle che si possono ottenere comprimendo frasi lunghe)
   - la password deve essere cambiata a intervalli regolari a cura dell'incaricato del trattamento d'intesa con il custode della password (ogni sei mesi)
3. la variazione delle password deve essere comunicata al custode delle password a cui dovrà essere consegnata in busta chiusa con data e firma dell'incaricato apposte sul lembo di chiusura, perché ne curi la conservazione;
4. È necessario curare la conservazione della propria parola chiave e bisogna evitare di comunicarla ad altri, di trascriverla su supporti(agenda, post-it,..) che siano accessibili ad altri o di consentire che qualcuno sbirci quello che si sta scrivendo sulla tastiera quando viene immessa la password;
5. Nel caso si sospetti che la password abbia perso la segretezza essa deve essere immediatamente sostituita, dandone comunicazione al custode delle password

2.5. Diritti e responsabilità dei dipendenti

Ogni utente è responsabile, sia sotto il profilo civile che penale, del corretto uso delle risorse informatiche, dei servizi e dei programmi ai quali ha accesso e dei dati che tratta.

2.6. Doveri di comportamento dei dipendenti

Le strumentazioni informatiche, la rete internet e la posta elettronica devono essere utilizzate dal personale e dagli studenti sotto il controllo dei loro docenti, come strumenti di lavoro e studio.

Ogni loro utilizzo non inerente l'attività lavorativa e di studio è vietato in quanto può comportare disservizi, costi di manutenzione e soprattutto minacce alla sicurezza.

In particolare non può essere dislocato nelle aree di condivisone della rete alcun file che non sia legato all'attività lavorativa, nemmeno per brevi periodi.

Agli utenti è severamente vietata la memorizzazione di documenti informatici di natura oltraggiosa o discriminatoria per sesso, lingua, religione, razza, origine etnica, condizioni di salute, opinioni, appartenenza sindacale politica.

Non è consentito scaricare, scambiare o utilizzare materiale coperto dal diritto d'autore.

3. MISURE DI TIPO TECNOLOGICO

3.1. Utilizzo della rete informatica

La rete informatica permette di salvare su server i files relativi alla produttività individuale. Le aree di condivisione in rete sono soggette a regolari attività di controllo, amministrazione e backup. L'accesso è regolamentato da policy di sicurezza che suddividono gli accessi fra gruppi e utenti. Periodicamente si provvede alla pulizia degli archivi, con cancellazione dei files obsoleti ed inutili

3.2. Utilizzo di internet

L'amministratore di sistema provvede alla configurazione di sistemi e all'utilizzo di filtri che prevengono determinate operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di file o software).

3.3. Utilizzo della posta elettronica

Sono previste apposite funzionalità di sistema che consentono:

- di inviare automaticamente in caso di assenze programmate, messaggi di risposta che contengano le coordinate di un altro soggetto o altri utili modalità di contatto del servizio presso il quale opera il lavoratore assente
- al lavoratore in caso di assenze improvvise o prolungate e per improrogabili necessità legate all'attività lavorativa, di delegare un collega (fiduciario) a verificare il contenuto di messaggi e a inoltrare al responsabile del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

3.4. Utilizzo dei personal computer

Gli utenti utilizzano per il proprio lavoro soltanto computer di proprietà dell'azienda, salvo espresse autorizzazioni contrarie dell'amministratore di sistema e sono tenuti a:

- attivare sul PC lo screen saver e la relativa password;
- conservare la password nella massima riservatezza e con la massima diligenza;
- non inserire password locali che non rendano accessibile il computer agli amministratori di rete se non esplicitamente autorizzato dal servizio informatico dell'azienda;
- non utilizzare cripto sistemi o qualsiasi altro programma di sicurezza crittografa non previsti esplicitamente dal servizio informatico dell'azienda;
- non modificare la configurazione hardware e software del proprio PC se non esplicitamente autorizzati dall'amministratore di sistema;
- non rimuovere, danneggiare o asportare componenti hardware;
- non installare sul proprio PC dispositivi hardware personali (modem, schede audio, masterizzatori, pendrive, dischi esterni, i-pood, telefoni, ecc.) salvo specifica autorizzazione;

In tal senso il titolare del personal computer deve provvedere a:

- non installare autonomamente programmi informatici, se non esplicitamente autorizzati dall'amministratore di sistema;
- non utilizzare programmi non autorizzati, con particolare riferimento ai videogiochi che sono portatori utilizzati per veicolare virus
- mantenere sempre aggiornati e attivi sulla propria postazione di lavoro i software antivirus con riferimento all'ultima versione disponibile
- nel caso il software antivirus rilevi la presenza di un virus, sospendere immediatamente ogni elaborazione in corso, senza spegnere il PC e segnalare prontamente l'accaduto al personale incaricato dell'assistenza tecnica.

- prestare la massima attenzione ai supporti di origine esterna (es. pendrive), verificando preventivamente tramite il programma antivirus ogni file acquisito attraverso qualsiasi supporto e avvertendo immediatamente l'amministratore di sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti
- non lasciare incustodita e accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione
- non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a persone non autorizzate, in particolar modo per quanto riguarda l'accesso ad internet e ai servizi di posta elettronica
- spegnere il PC al termine del lavoro o in caso di assenze prolungate dalla propria postazione.

3.5. Utilizzo della rete informatica

Gli utenti della rete informatica sono tenuti a utilizzare la rete in modo conforme a quanto stabilito dal presente regolamento e quindi:

- mantenere segrete e non comunicare a terzi, inclusi gli amministratori di sistema, le password d'ingresso alla rete ed ai programmi e non permettere ad alcuno di utilizzare il proprio accesso;
- provvedere periodicamente alla pulizia degli archivi con cancellazione dei file obsoleti o inutili ed evitare un'archiviazione ridondante;
- verificare preventivamente ogni archivio elettronico (file) acquisito attraverso qualsiasi supporto (es. pendrive) prima di trasferirlo su aree comuni della rete.

Agli utenti è fatto espresso divieto di influenzare negativamente la regolare operatività della rete, interferendo con la connettività altrui o con il funzionamento del sistema e quindi di utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files o software di altri utenti, utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber o keylogger), software di decodifica password (cracker) e più in generale:

- software rivolti alla violazione della sicurezza del sistema e delle privacy;
- sostituirsi a qualcuno nell'uso dei sistemi, cercare di catturare password altrui o forzare password o comunicazioni criptate;
- modificare le configurazioni impostate dall'amministratore di sistema;
- limitare o negare l'accesso al sistema a utenti legittimi;
- effettuare trasferimenti non autorizzati di informazioni (software, dati,..)
- distruggere o alterare dati altrui
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi.

3.6. Utilizzo di internet

L'accesso alla navigazione in internet deve essere effettuato esclusivamente a mezzo della rete di azienda e solo per fini lavorativi o di studio. È tassativamente vietato l'utilizzo di modem personali. Gli utenti sono tenuti ad utilizzare l'accesso ad internet in modo conforme a quanto stabilito dal presente regolamento e quindi devono:

- navigare in internet in siti attinenti allo svolgimento delle mansioni assegnate
- registrarsi solo a siti con contenuti legati all'attività lavorativa
- partecipare a forum o utilizzare chat solo per motivi strettamente attinenti l'attività
- lavorativa

Agli utenti è fatto espresso divieto di qualsiasi uso di internet che possa in qualche modo recare danno all'azienda o a terzi e quindi di

- fare conoscere ad altri la password del proprio accesso, inclusi gli amministratori di sistema
- usare internet per motivi personali
- servirsi dell'accesso internet per attività in violazione del diritto d'autore o di altri diritti
- tutelati dalla normativa vigente
- accedere a siti pornografici, di intrattenimento,..
- scaricare i software gratuiti dalla rete, salvo casi di comprovata utilità e previa
- autorizzazione in tal senso da parte del responsabile
- utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer
- (Napster, Emule, Winmx, e-Donkey,…)
- ascoltare la radio o guardare video o filmati utilizzando le risorse internet
- effettuare transazioni finanziarie, operazioni di remote bancking, acquisti on-line e simili, se
- non attinenti l'attività lavorativa o direttamente autorizzati dal responsabile del trattamento
- inviare fotografie, dati personali o di amici dalle postazioni internet

3.7. Utilizzo della posta elettronica

Gli utenti assegnatari di caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse e sono tenuti a utilizzarle in modo conforme a quanto stabilito dal presente regolamento, quindi devono:

- conservare la password nella massima riservatezza e con la massima diligenza
- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti
- utilizzare tecniche per l'invio di comunicazioni a liste di distribuzione solo se istituzionali
- inoltrare, a chi di riferimento nell'azienda, ogni comunicazione inviata o ricevuta che abbia
- contenuti rilevanti o contenga impegni contrattuali o precontrattuali con l'azienda e fare
- riferimento alle procedure in essere per la corrispondenza ordinaria
- utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta ricezione del messaggio da parte del destinatario
- prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura e, dove possibile, preferire l'utilizzo di cartelle di rete condivise
- inviare preferibilmente file in formato PDF
- accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i file attachment di posta elettronica prima del loro utilizzo
- rispondere a e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre
- chiamare link contenuti all'interno di messaggi solo quando vi sia la comprovata sicurezza sul contenuto dei siti richiamati
- indicare la persona autorizzata ad aprire la posta o la persona che riceverà la posta in caso di assenza

Agli utenti è fatto divieto di qualsiasi uso della posta elettronica che possa in qualche modo recare danno all'azienda e quindi di:

- prendere visione della posta altrui
- simulare l'identità di un altro utente, ovvero utilizzare per l'invio di messaggi credenziali di posta non proprie, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza;
- utilizzare strumenti software o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'azienda;

- trasmettere a mezzo posta elettronica dati sensibili, personali o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento della protezione dei dati;
- inviare tramite posta elettronica user-d, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici;
- utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing list salvo diversa ed esplicita autorizzazione;
- inviare o ricevere posta personale attraverso l'uso di un webmail;
- inviare o accettare messaggi in formato html;
- utilizzare il servizio di posta elettronica per inoltrare giochi, scherzi, barzellette, appelli e petizioni, messaggi tipo "catene" e altre e-mails che non siano di lavoro

3.8. Utilizzo di supporti magnetici

Gli utenti devono trattare con particolare cura i supporti magnetici (dischetti, nastri, DAT, chiavi USB, CD riscrivibili,..) in particolar modo quelli riutilizzabili, per evitare che persone non autorizzate possano accedere ai dati ivi contenuti e quindi devono:

- non utilizzare supporti rimovibili personali
- custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto
- consegnare i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili,..) obsoleti all'amministratore di sistema per l'opportuna distruzione onde evitare che il loro contenuto possa essere successivamente alla cancellazione, recuperato.

3.9. Utilizzo di PC portatili

L'utente è responsabile del PC portatile assegnatogli e deve:

- applicare al PC portatile le regole di utilizzo previste per i PC connessi in rete
- custodirlo con diligenza e in luogo protetto durante gli spostamenti
- rimuovere gli eventuali file elaborati sullo stesso prima della sua riconsegna

3.10. Utilizzo delle stampanti e dei materiali d'uso

Stampanti e materiali di consumo in genere (carta, inchiostro, toner, floppy disk, supporti digitali come CD e DVD) possono essere usati esclusivamente per compiti di natura strettamente istituzionale, evitando in ogni modo sprechi e utilizzi eccessivi.

Gli utenti devono effettuare la stampa dei dati solo se strettamente necessaria e ritirare prontamente dai vassoi delle stampanti comuni i fogli per impedire a persone non autorizzate di accedere alle stampe di documenti riservati

Distruggere personalmente e sistematicamente le stampe che non servono più.

3.11. Utilizzo di telefonini e altre apparecchiature di registrazione di immagini e suoni

E' fatto divieto assoluto di effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi, salvo:

- diversa disposizione esplicita del titolare del trattamento, da concordarsi di volta in volta e comunque sempre preventivamente al trattamento;
- informazione preventive degli interessati;
- acquisizione del loro libero consenso, preventivo ed informato.

4. CONTROLLI

Il datore di lavoro, per esigenze organizzative, per garantire la sicurezza sul lavoro, per evitare reiterati comportamenti dolosi illeciti può avvalersi legittimante, nel rispetto dell'art. 4 comma 2 dello statuto dei lavoratori, di sistemi che consentano un controllo a distanza e determinato di dati personali riferibili a singoli utenti.

Il datore di lavoro non può in alcun caso utilizzare detti sistemi per ricostruire l'attività del lavoratore tramite :

- lettura e registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio posta elettronica stesso;
- memorizzazione sistematica delle pagine web visualizzate;
- lettura e registrazione dei caratteri inseriti dai lavoratori tramite tastiera o dispositivi analoghi;
- analisi occulta dei dispositivi per l'accesso a internet o alla posta elettronica messi a disposizione dei dipendenti

Le attività sull'uso del servizio di accesso ad internet vengono automaticamente registrate attraverso il log di sistema ottenuti da un proxy server o da latro strumento di registrazione delle informazioni.

Analogamente sono allo stesso modo suscettibili di controllo i servizi di posta elettronica. Tali file possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente.

I dati contenuti nei log sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di verifica delle funzionalità dei sistemi di protezione e comunque non per più di un mese. Dopo tale periodo il sistema cancella automaticamente tali tracciati.

La riservatezza delle informazioni registrate è soggetta a quanto dettato dal D. lgs. n.° 196/2003, il trattamento dei dati avviene esclusivamente per fini istituzionali, per attività di monitoraggio e controllo e in forma anonima in modo tale da precludere l'identificazione degli utenti o delle loro attività. Le registrazioni possono essere utilizzate per fornire informazioni esclusivamente su:

- numero di utenti che visita ciascun sito o dominio, numero di pagine richieste e quantità
- dati scaricati
- numero di siti visitati da ciascun utente, quantità totale di dati scaricati, postazioni di lavoro
- utilizzate per la navigazione

I dati personali contenuti nei log possono essere utilizzati tassativamente solo nelle seguenti ipotesi:

- per corrispondere ad eventuali richieste dell'autorità giudiziaria e della polizia postale
- quando si verifiche un evento dannoso o una situazione di pericolo che richiede un
- immediato intervento
- in caso di utilizzo anomalo degli strumenti, da parte degli utenti, reiterato nonostante
- l'esplicito invito ad attenersi alle istruzioni impartite.

Qualora i controlli evidenzino un utilizzo anomalo degli strumenti informatici dell'azienda, il titolare del trattamento procede in forma graduata:

- in via preliminare si eseguono controlli su dati aggregati, in forma anonima e si provvede ad un avviso generalizzato agli utenti;
- se perdurano le anomalie si procede a controlli per tipologie di locali di utilizzo (uffici, aule,..) o tipologie di utenti (ata, docenti, studenti,..) e si procede con avvisi mirati alle categorie di utilizzatori;
- ripetendosi l'anomalia, sarà lecito il controllo su base individuale e si procederà all'invio di avvisi individuali
- in caso di verificato e reiterato uso non conforme delle risorse informatiche il titolare del trattamento attiva il procedimento disciplinare

I trattamenti in servizio proxy sono curati da personale tecnico incaricato del trattamento.

5. INFORMATIVA GLI UTENTI

Il presente regolamento è messo a disposizione degli utenti, per la consultazione, sui mezzi di comunicazione interna utilizzati dall'azienda (circolare, sito) e quindi portato a conoscenza di ciascun dipendente.
L'utente qualora l'azienda decidesse di perseguire, per fini legati alla sicurezza dell'intero sistema informativo, il controllo della posta elettronica e della navigazione in internet, viene informato degli strumenti e dei modo di trattamento effettuati prime che questo sia iniziato.

6. SANZIONI IN CASO DI MANCATO RISPETTO DEL REGOLAMENTO

La contravvenzione alle regole contenute nel presente regolamento da parte di un utente:

- può comportare l'immediata revoca delle autorizzazioni ad accedere alla rete informatica
- ed ai servizi/programmi autorizzati, fatte salve le sanzioni più gravi previste dalla enorme
- vigenti
- è perseguibile con provvedimenti disciplinari nelle forme e con le modalità previste dall'azienda,
- può portare alle azioni civili e penali consentite.

L'utilizzo dei servizi di accesso ad internet cessa o viene sospesa d'ufficio quando:

- non sussiste più la condizione di dipendente o l'autorizzazione al loro uso
- vi è il sospetto di manomissione dell'hardware o del software
- in caso di diffusione o comunicazione a terzi da parte del dipendente di password, codici di accesso ecc,..
- in caso di accesso doloso a file o servizi non rientranti tra quelli autorizzati
- ogni qual volta sussistano ragionevoli evidenze di una violazione degli obblighi dell'utente
- che mette a rischio il sistema

7. AGGIORNAMENTO E REVISIONE DEL REGOLAMENTO

Il presente regolamento è soggetto a revisione ogni qual volta sia necessario un aggiornamento alla luce dell'esperienza, di nuove normative e dell'innovazione tecnologica.

Tutti gli utenti possono proporre quando ritenuto necessario, integrazioni al presente regolamento e le proposte saranno esaminate dal responsabile del trattamento in collaborazione con l'amministratore di sistema.

La presente organizzazione, ai sensi di legge, prevede una serie di regole per trattare i dati con strumenti elettronici e per l'utilizzo degli strumenti elettronici stessi da parte dei suoi dipendenti.

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione (l'insieme degli strumenti elettronici, dei software e delle procedure atte a verificare l'identità) che consentono il superamento di una procedura di autenticazione relativa ad uno specifico trattamento o a un insieme di trattamenti

Le credenziali di autenticazione (i dati ed i dispositivi, in possesso di una persona da questi conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica) consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata ad un codice identificativo o a una parola chiave;

Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione;
Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato;
La robustezza delle password è il meccanismo più importante per la protezione dei dati. Un corretto utilizzo ed impiego delle password è a garanzia dell'utente. Le regole di seguito elencate sono vincolanti per tutti i sistemi, le workstation e gli altri device elettronici (server, postazioni PC Client, portatili, tablet, smartphone, etc…) tramite le quali si può accedere alla rete o alle banche dati contenenti i dati personali;
5. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri,
neppure in tempi diversi;
Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
Le credenziali sono disattivate anche in caso di perdita della qualità che consente al titolare l'accesso ai dati personali.

Sono impartite le seguenti istruzioni per non lasciare incustodito ed accessibile lo strumento elettronico durante una sessione di trattamento.
L'incaricato se si allontana dalla propria postazione dovrà mettere in protezione il suo sistema (PC Client o portatile) affinché persone non autorizzate non abbiano accesso ai dati protetti.
La responsabilità sull'efficacia di tale sistema è assegnata al responsabile dei servizi informativi.
Quando l'acceso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite le seguenti idonee a preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema:

Per ogni PC si è stabilito a seconda del suo sistema operativo la seguente procedura:

Se il sistema operativo non consente una gestione degli utenti differita tra amministratore del PC ed utilizzatore (o se il responsabile del sistema informatico non vuole renderle differenti). Il responsabile della gestione del sistema informatico affida l'incarico al trattamento della custodia delle password ad un addetto.
La responsabilità sull'efficacia di tale sistema è assegnata al responsabile della gestione del sistema informatico. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza ed individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incarico dell'intervento effettuato.
Ogni utente dovrà obbligatoriamente consegnare in busta chiusa la propria password alla persona incaricata alla custodia delle chiavi di accesso che gli sarà indicata dal responsabile al sistema informatico.
In caso di necessità il responsabile chiederà la busta contenete la password al custode per disporre della password di accesso al sistema. Al termine dei lavori comunicherà all'addetto della necessità di modificare la password. Per questo motivo ogni qualvolta per qualsiasi motivo un addetto modifica la sua password è **OBBLIGATO ALLA CONSEGNA IMMEDIATA DELLA BUSTA SIGILLATA CONTENENTE LA NUOVA PASSWORDAL CUSTODE**. La violazione di tale norma è grave e porta ad estreme conseguenze in quanto mette a repentaglio l'accesso ai dati da parte dell'organizzazione

in caso di necessità in tal caso i dati dovranno risiedere su di un server il cui acceso sarà limitato e vincolato al profilo della persona.

Se il sistema operativo consente una **gestione degli utenti differita tra amministratore del PC ed utilizzatore** si useranno profili differenti affinché sia sempre possibile l'accesso al PC in caso di necessità. Di tale possibiltà dovrà essere avvisato l'utilizzatore. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Quando agli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazioni. **I Profili di autorizzazione**, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
La normativa prevede che periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione, grazie ad un'apposita check-list verrà redatto un verbale di verifica semestrale.
Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito di trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione
La normativa prevede che i dati personali debbano essere protetti contro il rischio di intrusione e dell'azioni di programmi di cui all'art. 615- quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale grazie ad un'apposita check-list verrà redatto un verbale di verifica semestrale.
Allo scopo un gateway deve essere protetto. Un gateway è l'insieme di hardware, software e applicazioni che permettono l'interconnessione (Internet) o l'accesso remoto a sistemi esterni.
I Gateway devono consentire l'accesso remoto a sistemi esterni. I gateway devono consentire l'accesso alla rete interna solamente agli utenti autorizzati attraverso i sistemi di controllo specifici (Proxi/Firewall).
Pertanto tutta la Rete interna collegata verso internet è dotata di un sistema che impedisca gli accessi indesiderati. Tali sistemi anche se l'accesso è limitato nel tempo servono a prevenire l'accesso da parte di '' intrusi'' ai nostri sistemi di gestione dati. Tali sistemi sono denominati ''Firewall''.
La normativa prevede che gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti debbano essere effettuati almeno annualmente. ln caso di trattamento di dati sensibili o giudiziari la normativa prevede che tale aggiornamento almeno a livello semestrale. I sistemi sensibili ai virus informatici (sistemi operativi, programmi informatici, data base) devono essere protetti con opportuni programmi antivirus che devono essere aggiornati per garantire la loro efficacia.
Semestralmente dovrà essere verificato se il numero interno riportato da tutti i programmi antivirus è stato aggiornato al fine di verificare se il sistema di aggiornamento è funzionante grazie ad un'apposita check-list verrà redatto un verbale di verifica semestrale. Resta facoltà degli interessati procedere con un controllo più frequente. ln caso di mancato aggiornamento del software antivirus si dovrà provvedere a ripristinarne immediatamente il funzionamento.

Le cpu che ricevono le mail direttamente dall'esterno dovranno disporre di un Antivirus in grado di controllare le mail in arrivo e quelle in partenza, inoltre su tutte le cpu che contengono banche

dati o se quelle che hanno accesso ad Internet dovrà essere condotto un controllo settimanale con evidenza oggettiva.

In caso di segnali allarmanti (mail sospette, comportamenti della cpu imprevedibili) è necessario verificare immediatamente l'efficienza dell'antivirus ed il suo stato di aggiornamento.
La responsabilità sull'efficacia di tale sistema è assegnata al **responsabile dei servizi informativi**.
Le istruzioni riguardanti l'utilizzo del sistema antivirus e del relativo aggiornamento sono riportati nelle guide operative del prodotto.

La presente organizzazione si è dotata di opportuni antivirus che sono soggetti ad aggiornamenti periodici.

8. BACKUP:
Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Le modalità di backup implementate dall'organizzazione sono illustrate nell'allegato al presente documento ed aggiornate dal responsabile informatico

Al momento della stesura del presente documento, l'organizzazione non ha in essere sistemi di videosorveglianza o videocitofoni di propria proprietà. Non potendone escludere una futura installazione, però, l'organizzazione dichiara, nel caso, che, nel trattamento di dati tramite un sistema di videosorveglianza o con videocitofono o con telecamere in genere, anche senza registrazione di immagini, si seguiranno i seguenti principi generali e saranno svolti i seguenti adempimenti.

Principi generali

Principio di liceità, necessità e proporzionalità.
Il trattamento di dati attraverso il sistema di videosorveglianza è fondato sul presupposto di liceità che il Codice prevede espressamente per soggetti privati, sul principio di necessità e di proporzionalità.
Si segnala, inoltre, che non vengono effettuate intercettazioni di comunicazioni e conversazioni. Viene evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli.

Principio di finalità.
Il sistema di videosorveglianza è introdotto come misura complementare volta a migliorare la sicurezza (videocitofono o telecamera senza registrazione nell'area esterna di accesso o telecamera con registrazione per prevenzione di intrusioni non autorizzate).

Le finalità sono determinate e rese trasparenti, ossia direttamente conoscibili attraverso adeguate comunicazioni e/o cartelli di avvertimento al pubblico. Le finalità così individuate sono correttamente riportate nell'informativa.

Adempimenti

Informativa

Gli interessati sono informati che stanno per accedere o che si trovano in una zona videosorvegliata. L'informativa fornisce gli elementi previsti dal Codice (art. 13): - nell'area esterna è apposto il modello semplificato di informativa "minima":
nelle aree interne è presente con un avviso circostanziato che riporta gli elementi d' art. 13, con particolare riguardo alle finalità e all'eventuale conservazione;
Il supporto con l'informativa;

- è collocato nel luogo ripreso o nelle immediate vicinanze
- ha un formato ed un posizionamento tale da essere chiaramente visibile
- ingloba un simbolo o una stilizzazione di esplicita e immediata comprensione

Soggetti preposti e misure di sicurezza
Responsabili

Sono designati per iscritto i responsabili e gli incaricati del trattamento, autorizzati ad utilizzare gli impianti.

Tipologia	Responsabile	Incaricato
Rilevazione delle immagini	----------	----------

Il tecnico esterno che per scopi di manutenzione svolge prestazioni strumentali e subordinate alle scelte del titolare del trattamento e non visiona le immagini è :

Attività	Responsabile	Incaricato
Manutenzione al sistema di rilevazione delle immagini	----------	----------

Il Responsabile è istruito, attraverso periodici interventi di formazione, sui doveri, sulle garanzie e sulle responsabilità, sia all'atto dell'introduzione del sistema di videosorveglianza, sia in sede di modifiche delle modalità di utilizzo.

MISURE DI SICUREZZA
Le misure di sicurezza adottate sono le seguenti:

- Il Responsabile è nominato tramite lettera d'incarico;
- L'accesso al luogo in cui è sito il monitor del sistema di videosorveglianza è controllato;
- L'eventuale registrazione delle immagini può avvenire per un massimo di 24 ore e poi essere sovrascritte.

Consenso e Bilanciamento degli interessi
Il Titolare tratta dati personali in quanto il trattamento rientra nei presupposti di liceità previsti in alternativa al consenso. L'alternativa all'esplicito consenso è identificata nell'istituto del bilanciamento di interessi.

Le telecamere sono installate senza il consenso degli interessati, sulla base delle prescrizioni indicate dal Garante, in quanto il Titolare, che rileva le immagini, persegue un interesse legittimo a fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, prevenzione incendi, sicurezza del lavoro ecc.

Videocitofono

Al cancello d'accesso può essere installato, per identificare coloro che si accingono ad entrare, una videocamera che rileva immagini senza registrarle. Tale apparecchiatura è dislocata all'ingresso dell'edificio in corrispondenza del citofono, per finalità di controllo dei visitatori che si accingono ad entrare. L'esistenza della telecamera è conosciuta attraverso una informativa agevolmente rilevabile.

Installazione di appositi cartelli

Fac simile di cartello apposto vicino alla telecamera presente nei pressi dei punti in cui si effettua la rilevazione delle immagini.

Al fine di poter recuperare i dati a seguito di qualsiasi calamità si prevede di disporre SEMPRE UNA COPIA DEI DATI con frequenza giornaliera.

La copia potrà essere eseguita con qualsiasi idoneo mezzo (nastri magnetici, CD, DVD; altri supporti per la memorizzazione di massa).

BEST PRACTICE DI BACKUP SONO SEGUENTI:

Alternativa 1:

Copia dei dati con il sistema 5+5/6+6. Ovvero copia giornaliera di tutti dati, ogni giorno su un supporto digitale (nas, cassetta, cd-rom) diverso per sue settimane lavorative. In questo modo sono sempre in linea le ultime due settimane. Il supporto di fine mese viene trattenuto e tolto dal gruppo come backup di fine mese. In questo modo in un anno vengono sostituiti tutti i supporti (12) che saranno sempre in condizioni ottimali e si hanno anche i backup di ogni singola fine mese

Alternativa 2:

Copia dei dati (con metodologia precedente) su una memoria di massa esterna al sistema (hard disk esterno, chiave usb), da affidare a terzi per conservazione in luogo sicuro con attenzione alle modalità di trasporto dello stesso ed eventuale sua cifratura contenente dati sensibili.

Alternativa 3:

Copia dei dati (con la giusta periodicità) via internet su un server esterno, ospitato un una web farm sicura. Copia dei dati con trasferimento dei file in modalità criptata.

Nell'alternativa 1 e 2 le copie dovranno essere segregate in altri locali rispetto a quelli in cui sono dislocati i supporti di memorizzazione e conservati possibilmente in armadi ignifughi, al fine di preservarli in caso di furto o incendio. Dovranno essere custoditi a chiave ed affidati al responsabile della custodia dei dati secondo le disposizioni impartite nella lettera d'incarico. La responsabilità sull'efficacia di tale sistema è assegnata al responsabile della gestione del sistema informatico.