UNIONCAMERE
EMILIA-ROMAGNA

ESPOSTO ALL'ALBO
DIGITALE

DAL 9/1/2023
AL 15/1/2023

IL SEGRETARIO GENERALE
(Avv. Stefano Bellei)

Delibera n° 102/2022
in data 21/12/2022

Riunione del giorno 21/12/2022

Sono presenti:
Alberto Zambianchi, Presidente Unioncamere Emilia-Romagna;
Valerio Veronesi, Presidente Camera di commercio di Bologna (in collegamento MEET);
Paolo Govoni, Commissario straordinario della Camera di commercio di Ferrara (in collegamento MEET);
Giuseppe Molinari, Presidente della Camera di commercio di Modena (in collegamento MEET);
Andrea Zanlari, Commissario straordinario della Camera di commercio di Parma (in collegamento MEET);
Stefano Landi, Commissario straordinario della Camera di commercio di Reggio Emilia (in collegamento MEET);
Carlo Battistini, Presidente della Camera di commercio della Romagna (in collegamento MEET).

Per il Collegio dei Revisori dei Conti partecipano:
Rita Stati, Presidente;
Claudio Gandolfo, membro effettivo del Collegio;
Sante Trementozzi, membro effettivo del Collegio.

Assistono alla riunione della Giunta (in collegamento MEET):
Giada Grandi, Segretario Generale della Camera di commercio di Bologna;
Manuela Zilli, Segretario Generale della Camera di commercio di Parma;
Mauro Giannattasio, Segretario Generale Camere di Commercio di Ferrara e Ravenna;
Roberto Albonetti, Segretario Generale della Camera di commercio della Romagna.

Presiede Alberto Zambianchi, Presidente di Unioncamere Emilia-Romagna.

Segretario verbalizzante: Stefano Bellei, Segretario Generale di Unioncamere Emilia-Romagna, coadiuvato da Valentina Patano di Unioncamere Emilia-Romagna.

Oggetto: Approvazione del documento "Regolamento della Privacy per i dipendenti in Smart Working di Unioncamere Emilia Romagna", condiviso con le organizzazioni sindacali.

Il Presidente di Unioncamere Emilia-Romagna, Alberto Zambianchi, chiede al Segretario Generale Stefano Bellei di illustrare alla Giunta le motivazioni che hanno indotto a predisporre il documento "Regolamento della Privacy per i dipendenti in Smart Working di Unioncamere Emilia Romagna" **(allegato 8)**.

Bellei ricorda alla Giunta che l'accordo sullo Smart Working raggiunto il 29 novembre 2022 tra Unioncamere Emilia-Romagna e i rappresentanti della FILSCAMS CGIL, FISCAT CISL

UNIONCAMERE
EMILIA-ROMAGNA

ESPOSTO ALL'ALBO
DIGITALE

DAL 9/1/2023
AL 15/1/2023

IL SEGRETARIO GENERALE
(Avv. Stefano Bellei)

Delibera n° 102/2022
in data 21/12/2022

AMB e RSA, che ha stabilito che lo Smart working in questione è una modalità di svolgimento della prestazione lavorativa che si aggiunge alle modalità tradizionali, e prevede, all'art. 8 (riservatezza, privacy e salute/sicurezza), che l'Unione regionale provveda a redigere informative specifiche relative ai possibili rischi collegati all'attività di smart working, da consegnare sia alle RSA, sia alle OSS firmatarie del suddetto accordo.
E' stato, pertanto, preparato il documento "Regolamento della Privacy per i dipendenti in Smart Working di Unioncamere Emilia Romagna" il quale, tenuto conto delle conseguenze derivanti dall'applicazione sistematica dello Smart Working – o lavoro agile - sull'assetto organizzativo e sulla ripartizione dei compiti e delle responsabilità in materia di protezione dei dati personali, prevede raccomandazioni specifiche per tale modalità di svolgimento dell'attività lavorativa, che riguardano la sicurezza delle reti, le raccomandazioni e le prescrizioni per il lavoratore in lavoro agile a tutela della riservatezza dei dati e delle informazioni in suo possesso e/o disponibili sul sistema informativo, i trattamenti di dati svolti sia con strumenti elettronici o comunque automatizzati, sia con strumenti diversi da questi.

Tale regolamentazione è quanto mai opportuna ai fini dell'operatività in sicurezza dei lavoratori in smart working, sotto il profilo della tutela dei dati e della riservatezza e se ne propone l'approvazione.

La Giunta

- visto il Regolamento (UE) 2016/679 Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- visto il Decreto legislativo 30 giugno 2003, n. 196 come modificato dal decreto legislativo n. 101 del 10/08/2018
- verificato il documento e udito e condiviso quanto esposto dal relatore;

DELIBERA

- di approvare e adottare il "Regolamento della Privacy per i dipendenti in Smart Working di Unioncamere Emilia-Romagna", come da **allegato 8** a questo provvedimento (di cui costituisce parte integrante)";
- di approvare l'immediata eseguibilità della presente delibera.
- di prevedere la pubblicazione del documento nella sezione del sito camerale "Amministrazione trasparente".

IL SEGRETARIO
(Stefano Bellei)

IL PRESIDENTE
(Alberto Zambianchi)

REGOLAMENTO DELLA PRIVACY PER I DIPENDENTI IN SMART WORKING DI UNIONCAMERE EMILIA ROMAGNA

1) Raccomandazioni per la sicurezza delle reti

Le raccomandazioni sono le seguenti:

1. Seguire prioritariamente le policy e le raccomandazioni dettate dall'Amministratore di sistema.
2. Effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo (sia sugli strumenti aziendali, da remoto, attraverso l'amministratore di sistema, che su eventuali propri dispositivi).
3. Assicurarsi che i software di protezione del sistema operativo (Firewall, Antivirus, ecc.) siano abilitati e costantemente aggiornati (sia sugli strumenti aziendali, da remoto, attraverso l'amministratore di sistema, che su eventuali propri dispositivi).
4. Assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dall'Amministratore di sistema.
5. Non installare software proveniente da fonti/repository non ufficiali.
6. Bloccare l'accesso al sistema e/o configura la modalità di blocco automatico quando ci si allontana dalla postazione di lavoro.
7. Non cliccare su link o allegati contenuti in email sospette.
8. Utilizzare l'accesso a connessioni Wi-Fi adeguatamente protette.
9. Collegarsi a dispositivi mobili (pen-drive, hdd-esterno, etc.) di cui si conosce la provenienza (nuovi, già utilizzati, forniti dall'Amministratore di sistema).
10. Effettuare sempre la disconnessione dai servizi/portali utilizzati dopo che si è conclusa la sessione lavorativa.

2) Raccomandazioni per il lavoratore

Il dipendente in smart working è tenuto a:

- Custodire con diligenza la documentazione, i dati e le informazioni dell'Amministrazione utilizzati in connessione con la prestazione lavorativa;
- Al rispetto delle previsioni del Regolamento UE 679/2016 e del D.lgs. 196/2003 come modificato dal d.lgs. n. 101/2018 in materia di privacy e protezione dei dati personali;
- Nella qualità di "autorizzato" del trattamento dei dati personali, anche presso il proprio luogo di prestazione fuori sede, deve osservare tutte le istruzioni e misure tecniche ed organizzative previste:
    - Il dipendente è tenuto alla più assoluta riservatezza sui dati e sulle informazioni in suo possesso e/o disponibili sul sistema informativo;
    - Deve adottare, in relazione alla particolare modalità della sua prestazione, ogni provvedimento idoneo a garantire tale riservatezza (vedi cap.3 "Prescrizioni per lo Smart Worker"

In particolare, con riferimento alle modalità smart work, deve:

- Porre ogni cura per evitare che ai dati possano accedere persone non autorizzate presenti nel luogo di prestazione fuori sede;
- Procedere a bloccare l'elaboratore in dotazione in caso di allontanamento dalla postazione di lavoro, anche per un intervallo molto limitato di tempo;
- Qualora non si utilizzino dispositivi forniti dal titolare del trattamento il lavoratore dovrà dotarsi di un sistema adeguato a fronteggiare l'eventuale minaccia di virus informatici, ed effettuare un'accurata scansione preventiva

- Evitare l'uso dei social network non conforme agli scopi lavorativi o altre applicazioni social facilmente soggette alla pirateria informatica sugli strumenti aziendali, ed evitarne la contemporaneità di utilizzo sui propri dispositivi durante l'accesso ai sistemi informativi aziendali.
- Adoperare "misure di sicurezza" nell'utilizzo di pc o tablet come paraschermi (privacy-screen) che impediscano la visuale laterale del vicino, non tanto e solo per motivi di riservatezza, ma anche per la circolazione dei dati;
- Evitare di rivelare al telefono informazioni di carattere personale;
- Evitare il collegamento a reti non sicure o sulle quali non si abbiano adeguate garanzie;
- Alla conclusione della prestazione lavorativa giornaliera conservare e tutelare i documenti eventualmente stampati provvedendo alla loro eventuale distruzione solo una volta rientrato presso la Sua abituale sede di lavoro;
- Qualora, invece, al termine del lavoro risulti necessario trattenere presso il proprio domicilio materiale cartaceo contenente dati personali, lo stesso dovrà essere riposto in armadi, cassetti o altri contenitori muniti di serratura.

3) Le prescrizioni per lo Smart Worker

Schema esemplificativo di prescrizioni da seguire da parte dello Smart Worker in occasione dell'esecuzione della modalità lavorativa in Smart Working o "Lavoro Agile.

Ambiente di lavoro

Il/la dipendente deve aver cura di svolgere la prestazione lavorativa in ambienti tali da consentire comunicazioni stabili, efficienti e (possibilmente) non disturbate da rumori circostanti

Conversazioni

Le conversazioni tra il/la dipendente e gli altri interessati non devono essere oggetto di ascolto da parte di soggetti non autorizzati, i quali devono essere mantenuti ad una distanza che consenta di proteggere la confidenzialità; pertanto, è obbligo del/della dipendente:

- evitare di effettuare colloqui ad alta voce, di persona o per telefono, in presenza di soggetti non autorizzati a conoscere il contenuto della conversazione;
- utilizzare cuffie con microfono, in modo che nell'ambiente non sia diffusa la voce di chi è collegato;
- accertarsi che conviventi e compresenti non siano portati, anche involontariamente, a conoscenza di informazioni e processi attinenti all'attività lavorativa;
- non utilizzare familiari o terzi per veicolare informazioni, anche se ritenute "banali", afferenti all'attività lavorativa;
- nel caso di conversazioni telefoniche instaurate a seguito di chiamate inoltrate o ricevute, accertare, con cura, che l'interlocutore sia effettivamente un collega/cliente/fornitore legittimato e autorizzato a conoscere le informazioni oggetto della comunicazione.

Documentazione attività lavorativa

Unioncamere Emilia-Romagna, in qualità di Titolare, stabilisce che, ai sensi dell'art. 24 comma 1 del Regolamento U.E. 2016/679, la documentazione inerente all'attività lavorativa deve risiedere esclusivamente sulle cartelle di rete, poiché tale modalità operativa è ritenuta adeguata a garantire che il trattamento è effettuato conformemente al Regolamento.

Trasporto documenti

Il/La dipendente deve prestare particolare attenzione quando si trasportano da un locale all'altro, da uno stabile all'altro, da un luogo ad un altro (mediante mezzi pubblici o privati o anche a piedi) documenti contenenti dati personali.
Utilizzare cautele quali:

- Chiudere bene gli zaini o le borse con le quali si trasportano documenti cartacei o informatici;
- Questi ultimi devono essere spenti o resi inaccessibili senza password;
- Sorvegliare zaini, borse e dispositivi, non abbandonarli e averne cura durante il viaggio;
- Non dimenticarli sui mezzi di trasporto.

Conservazione dati personali

Per quanto riguarda la generica conservazione dei dati personali utilizzati dal/dalla dipendente in Smart Working, il Responsabile dell'unità organizzativa deve adottare soluzioni organizzative idonee a ridurre il più possibile i rischi di distruzione, perdita e accessi non consentiti ai dati anche in ambiente privato eletto dal/dalla dipendente; il lavoro in modalità Smart Working non deve essere effettuato al di fuori di ambienti privati protetti che garantiscano la necessaria riservatezza della prestazione.

Trasferimento di dati personali

Più in dettaglio, per quanto concerne l'utilizzo di documenti cartacei contenti dati personali e prelevati dagli archivi della Società, si sottolinea che il trasferimento di dati personali all'esterno deve essere giustificato da necessità strettamente correlate all'esercizio dell'attività lavorativa, agli obblighi di legge o alla difesa degli interessi della società; la circolazione dei dati personali cartacei, in situazione di mobilità deve essere ridotta al minimo indispensabile; i dati devono essere raccolti in porta documenti riportanti l'identificazione del/della dipendente utilizzatore, della Società e il suo recapito telefonico.

Utilizzo documenti cartacei

In particolare, i documenti cartacei:

- devono essere utilizzati solo per il tempo necessario allo svolgimento dei compiti assegnati e poi ripartiti negli archivi aziendali dedicati alla loro conservazione;
- non devono essere lasciati incustoditi; pertanto, nel caso di assenza, anche momentanea, dal luogo in cui si svolge lo Smart Working è necessario chiudere a chiave i locali che ospitano i dati ovvero riporli dentro un armadio/cassetto chiuso a chiave; non devono restare, senza ragione, applicati su supporti (lavagne o simili) che possono essere visionati da persone non autorizzate;
- devono essere resi illeggibili prima di essere cestinati, qualora siano destinati a divenire rifiuti (ad es. strappando più volte la carta in modo che i contenuti diventino non decifrabili/non ricostruibili).

Trattamento dati ed ausilio strumenti elettronici

Per quanto riguarda il trattamento di dati personali mediante l'ausilio di strumenti elettronici, si richiamano le indicazioni fornite dalla Società all'atto dell'autorizzazione al trattamento dei dati e si ribadisce quanto già prescritto dalle Policy della Società in materia di Privacy e in particolare:

- la password di accesso deve essere conservata con diligenza in modo che resti riservata, evitando sotto la responsabilità del/della dipendente, che altri ne vengano a conoscenza;
- il computer ed altri eventuali strumenti in dotazione e/o utilizzati per l'espletamento delle prestazioni in modalità Smart Working (P.C., smartphone, ecc.), non devono essere lasciati incustoditi ed accessibili a persone non autorizzate; in caso di allontanamento anche temporaneo dalla postazione di lavoro il/la dipendente è tenuto a disconnettere la sessione di lavoro bloccando l'operatività del computer ("ctrl-alt-canc") e/o l'accesso allo smartphone (password di blocco schermo);

- non devono essere utilizzati dispositivi di memorizzazione esterna (come sopra riportato la documentazione inerente all'attività lavorativa dovrà risiedere esclusivamente sulle cartelle di rete, poiché tale modalità operativa è ritenuta adeguata a garantire che il trattamento è effettuato conformemente al regolamento).

Trattamento dei dati soggetti a maggior tutela

Il dipendente dovrà, altresì, adottare le cautele previste per legge (diritto all'oscuramento e anonimato) nell'eventuale trattamento dei dati soggetti a maggior tutela ovvero dati particolarmente sensibili per i diritti e le libertà degli interessati.

Violazione dei dati personali

È fondamentale sottolineare che è severamente sanzionata dal Regolamento (UE) 2016/679 la violazione dei dati personali. Si tratta cioè della 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.

Tale violazione può afferire a una "violazione della riservatezza":

- in caso di divulgazione o accesso accidentale ai dati personali, alla "perdita della disponibilità" (comprese le ipotesi di sottrazione e/o furto),
- in caso di perdita o distruzione dei dati personali (accidentale o non autorizzata) e alla "violazione dell'integrità",
- in caso di alterazione non autorizzata o accidentale dei dati personali.

La violazione, in rapporto alla sua gravità, può comportare per l'UR la Notifica del Data Breach; cioè la comunicazione della violazione dei dati personali all'Autorità di Controllo (Garante per la protezione dei dati personali); nonché, qualora ne abbiano un danno, ai soggetti i cui dati sono stati violati.

Obbligo di segnalazione

Si ribadisce l'obbligo del/della dipendente di segnalare qualunque ipotesi di violazione dei dati personali. La segnalazione va fatta al Dirigente responsabile della struttura e al Responsabile della Protezione dei dati; tempestivamente e, comunque, nei termini previsti dalla normativa interna aziendale in materia. Anche al fine di consentire il rispetto dei ristretti termini di notifica all'Autorità di Controllo previsti dal Regolamento (UE) 2016/679, ove atto dovuto.

Allegato n. 1

Regolamento per i trattamenti di dati svolti sia con strumenti elettronici o comunque automatizzati, sia con strumenti diversi da questi

REGOLAMENTO PER I TRATTAMENTI DI DATI

SVOLTI SIA CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI, SIA CON STRUMENTI DIVERSI DA QUESTI

INDICE

1. NORME PER I TRATTAMENTI SVOLTI CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI

La presente Sezione del Regolamento Interno comprende le istruzioni operative generali relative a:

- Identificativo Personale e Password per l'accesso ai dati;
- Autonoma sostituzione della PW per l'accesso ai dati;
- Programma Antivirus e protezione da Software pericolosi;
- Riutilizzo controllato dei supporti di memorizzazione;
- Autorizzazioni per l'ingresso nei locali;
- Controllo dell'accesso ai locali;
- Trattamento per fini esclusivamente personali;
- Ripristino dei dati.

1.1) Identificativo Personale e Password per l'accesso ai dati

1.1.1) Il trattamento dei dati personali con strumenti elettronici è consentito al Personale Autorizzato dotati di "Credenziali di autenticazione", che consentono l'accesso ad uno specifico trattamento o ad un insieme di trattamenti. Le credenziali di autenticazione consistono in un codice per identificazione dell'Incaricato associato ad una parola chiave, conosciuta solamente dal medesimo. Il codice per l'identificazione non può essere assegnato ad altro Personale Autorizzato, neppure in tempi diversi.

La PW (parola chiave):

- Non deve essere divulgata e deve essere custodita con la massima diligenza;
- Deve essere modificata dall'assegnatario al primo utilizzo e, successivamente, al più tardi ogni sei mesi (tre mesi, per il Personale Autorizzato al trattamento di dati particolari);
- Deve essere composta da un numero di caratteri non inferiore ad otto, se il sistema lo consente, e non deve contenere riferimenti agevolmente riconducibili all'incaricato, come ad esempio nome-cognome, data di nascita.

Il nome utente (User ID) viene generato e comunicato all'inizio della presa di servizio.

Tassativamente esso non può essere mai utilizzato, neanche in momenti diversi, da altro Personale Autorizzato che non siano l'assegnatario. Ciò sta a significare, nella pratica, che nessun utilizzatore può connettersi ad un sistema informativo "presentandosi" come se fosse un'altra persona (usando l'User ID e la PW di un collega).

1.1.2) 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 inoltre disattivate in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali (ad es.: passaggio ad altre mansioni o trasferimento di ufficio, ecc.).

1.1.3) Qualora sull'Hard Disk del personal computer utilizzato in modalità non in rete (Stand Alone) siano registrati archivi di dati personali, è reso obbligatorio l'uso della PW all'atto della accensione del PC.

1.1.4) E' fatto obbligo, al fine di evitare che i dati personali possano essere letti da persone non autorizzate, di utilizzare la modalità dello "Screen Saver" con PW o disconnettere il PC dalla rete locale quando il computer non viene utilizzato dall'operatore (ad es., durante la pausa pranzo oppure quando l'incaricato si allontana dalla propria postazione di lavoro per un periodo di tempo significativo); sarà pertanto necessario reinserire la propria PW al momento del riavvio dell'attività.

Le apparecchiature devono essere spente ogni sera prima di lasciare gli uffici (salvo diverse disposizioni o in caso di particolare necessità), presidiando la postazione di lavoro fino al completo spegnimento del sistema.

Durante la pausa per il pranzo o in caso di altre assenze significative dal posto di lavoro ogni incaricato dovrà eseguire le seguenti operazioni:

- Salvataggio e chiusura di tutti i file ed applicazioni aperte, per non ostacolare eventuali attività di amministrazione;
- Blocco dello schermo con la combinazione dei tasti "CRTL-ALT-CANC" per evitare di lasciare incustodito l'accesso allo strumento.

L'operatore che dovrà effettuare la stampa dei dati è tenuto a ritirarla immediatamente dai vassoi delle stampanti comuni, per evitare accessi di persone non autorizzate.

1.1.5) E' fatto divieto assoluto di consentire a terzi (anche colleghi di altri uffici) l'accesso ai propri archivi mediante l'utilizzo della propria PW.

1.1.6) In caso di necessità improrogabile o di connessione al sistema informativo attraverso le credenziali di uno specifico Incaricato ed in concomitanza della irreperibilità di quest'ultimo, viene adottata la seguente procedura:

- L'Amministratore di Sistema modifica i parametri di accesso e provvede a rendere disponibile l'apparecchiatura;
- Al rientro dell'Incaricato, si provvederà ad informarlo dell'avvenuto intervento, disponendo che modifichi immediatamente la PW precedentemente usata.

1.2) Autonoma sostituzione della PW per l'accesso ai dati

1.2.1) La parola chiave (PW) è autonomamente determinata dal singolo Personale Autorizzato, secondo le regole più sopra riportate. Essa viene inserita dall'Incaricato nel sistema in sostituzione di quella temporaneamente assegnata dal Responsabile o dall'Amministratore di Sistema e, successivamente, viene modificata con cadenza semestrale o trimestrale, a seconda che si tratti di dati comuni o di dati particolari.

1.2.2) La PW, in ogni caso, non può essere comunicata ad altri soggetti per nessun motivo e non deve essere trascritta od annotata in maniera evidente o visibile da altri. Nella generazione della PW si dovranno adottare criteri di massima prudenza, al fine di evitare che la stessa possa essere individuata per tentativi. A tale scopo, è utile usare un proprio codice che preveda, oltre ai simboli alfanumerici, anche segni di interpunzione, così da produrre un PW estranea al linguaggio comune.

1.3) Antivirus e protezione da programmi pericolosi

1.3.1) Tutti i PC in uso presso gli uffici della Società connessi in rete sono dotati di programma atto alla rilevazione ed alla rimozione dei c.d. "virus informatici". Il programma antivirus è installato i-n modalità residente nella memoria dell'unità centrale; esso risulta perciò sempre attivo e viene aggiornato con cadenza periodica.

1.3.2) L'Amministratore di Sistema provvede agli aggiornamenti periodici, alla verifica frequente del prodotto utilizzato ed alla impostazione delle opzioni di controllo previste dal programma antivirus. Le opzioni stabilite dall'Amministratore di Sistema non possono essere modificate.

1.3.3) Devono essere aggiornati periodicamente, con cadenza almeno annuale, tutti i programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici ed a correggere eventuali difetti. In caso di trattamento di dati particolari l'aggiornamento deve avvenire al massimo ogni sei mesi.

Con l'occasione si ricorda che:

- In conformità alle disposizioni contenute nel D. Lgs. n. 518/1992 e successive modifiche ed integrazioni, è fatto assoluto divieto di installare arbitrariamente programmi Software non rilasciati ufficialmente dalla Società proprietaria del programma; è fatto altresì divieto di importare programmi dalla rete Internet se non per uso professionale e strettamente attinente alle funzioni svolte; non sono inoltre consentiti l'apertura e l'esecuzione di file in allegato ai messaggi E-Mail ricevuti da mittenti sconosciuti;
- È vietato l'accesso a siti Internet se non, esclusivamente, per consultazioni di natura professionale; di conseguenza, le richieste di connessione in rete potranno riguardare unicamente indirizzi di contenuto adeguato;
- La casella di Posta Elettronica è messa a disposizione dalla Società a favore degli autorizzati per usi prevalentemente professionali. L'invio di E-Mail generalizzato a gruppi di soggetti (interni o esterni alla Società) è consentito solo al personale autorizzato da specifiche disposizioni interne.

1.4) Autorizzazioni agli addetti alla manutenzione del sistema (Società di consulenza informatica esterne)

1.4.1) i soggetti addetti alla manutenzione di elaboratori/software accessibili in rete con i quali vengono svolte operazioni di trattamento dei dati particolari, sono autorizzati ad intervenire su detti elaboratori solo in presenza del Personale Autorizzato cui l'elaboratore è assegnato e devono attenersi alle disposizioni di sicurezza, ivi comprese quelle di cui al presente Regolamento.

1.4.2) Tutti gli interventi di manutenzione sugli elaboratori devono essere eseguiti esclusivamente sul posto di lavoro ed in presenza del collaboratore incaricato, fatta salva l'ipotesi di intervento c.d. "remoto". Nel caso l'intervento di manutenzione dovesse richiedere l'asporto dell'elaboratore fuori dai locali della Società, l'addetto alla manutenzione dovrà curare la temporanea rimozione del disco rigido e consegnarlo in custodia al dipendente incaricato. Nel caso l'intervento di manutenzione dovesse richiedere la sostituzione dell'Hard-Disk, il dipendente incaricato, successivamente al ripristino della regolare operatività, avrà cura di inviare, con comunicazione di accompagnamento, il supporto sostituito all'Amministratore di Sistema per il

successivo smaltimento in conformità alle vigenti disposizioni normative in materia (D. Lgs. n. 22/1997 e successive modifiche ed integrazioni).

1.5) Riutilizzo controllato dei supporti

1.5.1) Il Personale Autorizzato devono custodire e controllare i supporti magnetici (cassette; floppy; CD, "chiavette USB", ecc.) o cartacei (elenchi; registri; tabulati; fascicoli) sui quali sono registrati i dati particolari, in maniera che soggetti non autorizzati non possano venire a conoscenza, neppure occasionalmente o accidentalmente, del contenuto di tali supporti. Al termine di ogni attività lavorativa i supporti in questione dovranno essere custoditi in appositi contenitori e riposti in armadi o cassetti muniti di serratura e chiusi a chiave.

1.5.2) L'uso e la custodia dei supporti di memorizzazione sono disciplinati dai regolamenti interni delle singole aree di lavoro e secondo le procedure indicate dal Titolare. I supporti in argomento non dovranno essere utilizzati da altri soggetti che non possiedono apposito incarico per il trattamento. In caso di malfunzionamento del supporto, che determini l'impossibilità della lettura anche parziale dei dati ivi registrati, lo stesso dovrà essere distrutto o smaltito secondo le previste procedure.

1.6) Autorizzazione all'ingresso nei locali

L'ingresso nei locali degli uffici della Società, è riservato ai dipendenti ed alle persone espressamente autorizzate per lo svolgimento dei propri incarichi.

1.7) Trattamento di dati particolari per fini esclusivamente personali

Non è consentito ad alcuno il trattamento di dati particolari per fini esclusivamente personali, anche se non effettuato con elaboratori stabilmente accessibili da altri elaboratori.

1.8) Ripristino dei dati

In conformità ai principi per la redazione del Documento Programmatico sulla Sicurezza, sono state adottate idonee misure, atte a garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi e compatibili con i diritti degli interessati, comunque non superiori a sette giorni.

1.9) Uso della Posta Elettronica ed Internet

1.9.1) L'utilizzo della Posta Elettronica, così come l'accesso alla Rete Internet, contribuiscono fortemente a rendere la comunicazione tempestiva, efficace ed economica; Internet inoltre consente l'accesso ad una cospicua mole di informazioni, difficilmente reperibili in altre modalità ed in tempi brevi. Per quanto concerne la Posta Elettronica il rispetto delle semplici regole appresso indicate contribuisce significativamente a migliorare l'utilizzo dello strumento:

- La casella di posta personale deve essere mantenuta in ordine, cancellando i messaggi inutili, specialmente se contengono allegati di dimensioni notevoli o se sono stati segnalati problemi dal programma antivirus;
- È fatto divieto di utilizzare la casella E-Mail per inviare messaggi completamente estranei al rapporto di lavoro, limitandone l'uso alle relazioni fra colleghi;
- Per la trasmissione di file all'interno della stessa sede è consigliato l'utilizzo delle unità di rete, piuttosto che allegare il documento ad un messaggio di posta elettronica;
- È fatto divieto di utilizzare la casella E-Mail per altri modi di comunicazione esterna, quali sistemi di messaging (forum; chat), partecipazione a dibattiti, salvo diversa ed esplicita autorizzazione.

1.9.2) Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. Pertanto, fermo restando quanto indicato al punto che precede, si ricorda che in caso di ricezione accidentale di messaggi di valenza ufficiale, gli assegnatari dovranno inoltrarli tempestivamente al destinatario.

1.9.3) Relativamente alla navigazione in Internet è tassativamente proibito:

- Scaricare software, anche gratuiti, se non per esigenze strettamente professionali, fatti salvi i casi di esplicita autorizzazione del responsabile del sistema informatico;
- Effettuare qualunque genere di transazione finanziaria, ivi comprese le operazioni di "remote banking", acquisti "On-Line" e procedure simili, salvi i casi direttamente autorizzati dalla Direzione e nel rispetto delle normali procedure per gli acquisti;
- Effettuare ogni forma di registrazione a siti i cui contenuti non siano direttamente collegati all'attività lavorativa;
- Partecipare a forum non professionali, utilizzare chat-line e bacheche elettroniche (con l'esclusione degli strumenti autorizzati), nonché registrarsi in guest books, anche utilizzando pseudonimi (o nicknames).

L'eventuale consultazione di siti Internet contenenti o divulganti materiale contrario alle norme di buon costume, oltre che costituire in taluni casi specifico reato, è tassativamente vietata a chiunque, anche per la possibilità che lo strumento si trasformi in veicolo di infezioni informatiche.

2. NORME PER I TRATTAMENTI SVOLTI CON STRUMENTI DIVERSI DA QUELLI ELETTRONICI O COMUNQUE AUTOMATIZZATI

La presente Sezione di Regolamento Interno comprende le istruzioni operative generali relative a:

- - Accesso ai dati;
- - Conservazione in archivi ad accesso selezionato;
- - Custodia di atti e documenti;

- - Restituzione di atti e documenti al termine delle operazioni;
- - Conservazione in contenitori muniti di serratura;
- - Custodia e conservazione delle riproduzioni.

2.1) Accesso ai soli dati necessari

Durante le operazioni di trattamento dei dati personali di qualunque natura (dati comuni e particolari), registrati su carta o altri supporti non informatici, il singolo Personale Autorizzato delle diverse operazioni di trattamento devono operare solo su quei dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti previsti per le specifiche attività attribuite alla funzione ricoperta.

2.2) Conservazione in archivi ad accesso selezionato

L'accesso agli archivi contenenti atti e documenti comunque riconducibili al concetto di "dato personale" di qualunque natura (comuni o particolari) è riservato alle sole persone incaricate ed autorizzate a potervi accedere.

2.3) Custodia degli atti e dei documenti

Gli atti ed i documenti contenenti dati personali di qualunque natura (particolari e non) devono essere trattati con la dovuta diligenza, devono essere custoditi e conservati in maniera che le persone non incaricate non possano venire a conoscenza del loro contenuto.

Il Personale Autorizzato abilitati al trattamento dei dati personali, provenienti da archivi ad accesso selezionato o direttamente tratti da tali archivi, devono conservare e custodire i dati trattati con diligenza e riservatezza, evitando che vengano volontariamente o involontariamente conosciuti da soggetti privi della medesima qualificazione di Incaricato.

2.4) Restituzione di atti e documenti al termine delle operazioni

Gli atti ed i documenti oggetto di trattamento devono essere trattenuti solo per il periodo strettamente necessario allo svolgimento delle operazioni inerenti i propri compiti ed al termine di dette operazioni devono essere restituiti o riposti nell'archivio dal quale erano stati prelevati o presso il quale devono essere custoditi.

2.5) Conservazione in contenitori muniti di serratura

Nel caso vengano svolte operazioni di trattamento di dati particolari, il Personale Autorizzato del trattamento cui sono affidati atti e documenti, oltre a rispettare le norme generali previste per la custodia, dovranno conservare tali atti e documenti, fino alla loro restituzione, in contenitori (armadi, cassettiere) muniti di serratura e chiusi a chiave. L'accesso ai contenitori è riservato solo alle persone autorizzate a svolgere le stesse operazioni di trattamento. La gestione delle chiavi dei contenitori avviene secondo i regolamenti delle aree e funzioni specifiche.

2.6) Accesso controllato agli archivi

L'accesso agli archivi contenenti atti e documenti di dati particolari viene controllato dal personale incaricato, appartenente alla funzione di competenza.

2.7) Custodia e conservazione delle riproduzioni (fotocopie, tabulati, ecc.)

I supporti cartacei o comunque non informatici contenenti le riproduzioni di informazioni relative al trattamento di dati personali particolari devono essere custoditi con le medesime modalità previste dal presente Regolamento Interno per i trattamenti degli atti e dei documenti originali. Si ricorda che è fatto comunque divieto di riprodurre copie di documenti per uso non di ufficio.

2.8) Macero e/o distruzione di supporti cartacei contenenti dati personali

Il Personale Autorizzato del trattamento hanno il compito di curare che l'inoltro al macero di supporti cartacei contenenti dati personali (schede di rilevazione, tabulati contenenti dati anagrafici, ecc.) sia preceduto da accorgimenti ed interventi idonei ad evitare che altri soggetti vengano a conoscenza, anche in maniera accidentale, dei dati ivi contenuti.