STUDIO LEGALE CIACCI

Diritto delle nuove tecnologie

Roma, 11 ottobre 2023

Spett.le
Università degli Studi di Roma
Unitelma Sapienza
Piazza Sassari, 4
00161 - RM

OGGETTO: Adempimento relativo al Codice di deontologia e buona condotta per un corretto utilizzo dei sistemi informatici di UNITELMA SAPIENZA, come stabilito nel Provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007.

Gentile Cliente,

nel mese di marzo del 2007 il Garante per la protezione dei dati personali, nell'ambito di un più ampio intervento di disciplina del settore del trattamento delle informazioni personali dei dipendenti nei rapporti di lavoro, adottò un provvedimento generale (1 marzo 2007, in G.U. n. 58 del 10 marzo 2007) volto a fornire indicazioni in ordine all'uso di alcune delle dotazioni informatiche sul luogo di lavoro, in particolare di posta elettronica ed Internet. Ciò avviene attraverso la determinazione a carico del lavoratore di una serie di obblighi ed oneri, strettamente correlati a quelli stabiliti in capo al datore di lavoro. Secondo il Garante, infatti, per un corretto contemperamento degli interessi coinvolti, ed allo scopo di un'efficace tutela dei dati personali oggetto di trattamento, è necessario stabilire una serie di regole che dovranno essere rispettate da entrambi i soggetti.

Regole che andranno inserite nell'ambito di un disciplinare interno per un corretto uso di posta elettronica e Internet (come richiesto dal provvedimento del 1 marzo 2007), e più in generale di tutte delle dotazioni informatiche della struttura del datore anche a prescindere dalla Rete: e quindi, ad esempio, i computer, i programmi su di essi eseguibili, ma anche i possibili ulteriori strumenti ad essi afferenti (si pensi ai pen-drive o agli hard disk esterni che il dipendente potrebbe collegare alla propria postazione operativa per diversi motivi).

Nello svolgimento della sua attività di consulenza ed assistenza per UNITELMA SAPIENZA il nostro Studio ha quindi redatto il documento richiesto dal Provvedimento del 1 marzo 2007 nella sua versione più estesa, intitolandolo "Codice di deontologia e buona condotta per un corretto utilizzo delle dotazioni informatiche", il cui testo è rinvenibile nell'Allegato 1 alla presente lettera di presentazione dell'adempimento. Documento che si rivolge quindi ai vostri dipendenti e collaboratori, e che andrà poi

Via Nomentana, n. 373, 00162 ROMA
Tel. 06/86327973 - Fax 06/83390932 e-mail: *studiociacci@jei.it* - web-site: *http://www.jei.it*

riportato su carta intestata, con le modalità grafiche che riterrete più opportune: e quindi reso conoscibile a tali soggetti tramite una consegna diretta dello stesso (raccogliendo la relativa ricevuta insieme all'impegno a prenderne visione e rispettarlo, dichiarazione di cui riportiamo il testo nell'Appendice 3 del documento), oltre alla sua eventuale pubblicazione nella bacheca aziendale, o comunque nelle modalità comunicative utilizzate nella vostra struttura. La versione che alleghiamo dovrà poi essere completata nella parte evidenziata in azzurro, in particolare con riferimento alla data della sua adozione ufficiale (pag. 5 del Codice).

Rimanendo a disposizione per eventuali richieste di chiarimenti, porgiamo distinti saluti.

Avv. Gianluigi Ciacci

Via Nomentana, n. 373, 00162 ROMA
Tel. 06/86327973 - Fax 06/83390932 e-mail: *studiociacci@jei.it* - web-site: *http://www.jei.it*

ALLEGATO 1

CODICE

DI DEONTOLOGIA E BUONA CONDOTTA PER UN CORRETTO UTILIZZO DELLE DOTAZIONI INFORMATICHE DI UNITELMA SAPIENZA

CODICE

DI DEONTOLOGIA E BUONA CONDOTTA PER UN CORRETTO UTILIZZO DELLE DOTAZIONI INFORMATICHE DI UNITELMA SAPIENZA

Premessa

Nel marzo 2007 il Garante per la protezione dei dati personali, nell'ambito di un più ampio intervento di disciplina del settore del trattamento delle informazioni personali dei dipendenti nei rapporti di lavoro, adottò un provvedimento generale (1 marzo 2007, in G.U. n. 58 del 10 marzo 2007) volto a regolamentare l'uso delle dotazioni informatiche sul luogo di lavoro attraverso la determinazione a carico del lavoratore di una serie di obblighi ed oneri, strettamente correlati a quelli stabiliti in capo al datore di lavoro.

Secondo il Garante, infatti, per un adeguato contemperamento degli interessi, ed allo scopo di un'efficace tutela dei dati personali oggetto di trattamento, a fronte delle regole di condotta poste a carico del dipendente, vi sono altrettante regole dettate per il datore di lavoro circa il corretto trattamento delle informazioni relative agli individui generato dall'uso delle nuove tecnologie. Si veda in particolare quanto disposto all'art. 3.1. del Provvedimento, secondo il quale il titolare del trattamento deve adottare un disciplinare interno che indichi con chiarezza *"quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli".*

Gli stessi principi e le medesime regole sono poi state ribadite dall'Autorità in un vademecum del 15 maggio 2015 (finalizzato a fornire chiarimenti sulle modalità pratiche di adeguamento al Provvedimento del 2007), laddove si evidenziano, a carico del datore di lavoro, numerosi obblighi informativi inerenti alle modalità di utilizzo delle strumentazioni informatiche da parte del lavoratore: obblighi ribaditi anche dalla Giurisprudenza ordinaria. In particolare, il Garante per la protezione dei dati personali sottolinea come, in virtù di un eventuale e possibile uso personale delle stesse, il Titolare debba previamente rendere noto all'utente quali attività gli sono consentite e quali, invece, inibite.

Il presente documento, che è stato ufficialmente adottato il …… (con delibera ……) in adempimento a quanto stabilito nel Provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007 e nel vademecum del 15 maggio 2015, costituisce il "Codice di deontologia e buona condotta per un corretto utilizzo delle dotazioni informatiche di UNITELMA SAPIENZA''.

1. Il contesto di riferimento e l'ambito di applicazione.

Il dipendente, con la sottoscrizione del contratto di lavoro, acquisisce una serie di situazioni giuridiche che consistono essenzialmente in diritti di credito, da un lato, e in obblighi di diverso genere, dall'altro. Principale esempio di questo secondo tipo di situazioni giuridiche è, ovviamente, quello che sta alla base del rapporto lavorativo e che vede il lavoratore assumersi l'obbligo di collaborare con il proprio datore di lavoro in modo subordinato, ma anche fedele: prendendosi cioè cura degli interessi di questo, anche in relazione alla natura della prestazione dovuta, e astenendosi dal porre in essere comportamenti che possano in qualsiasi modo e misura pregiudicarli. Non a caso gli articoli 2104 e 2105 del c.c. fanno riferimento agli obblighi di diligenza e fedeltà del

lavoratore, sottolineando il dovere di quest'ultimo, rispettivamente, di eseguire in maniera esatta e puntuale le prestazioni assegnategli e di evitare di porre in essere attività di concorrenza, divulgazione o abuso di segreti che possano danneggiare il proprio Ente.

Sulla base di questi principi generali si evince come, nello svolgimento delle proprie mansioni, i dipendenti abbiano dunque l'obbligo di salvaguardare il patrimonio aziendale (inteso come quel complesso di beni, mobili, immobili e intangibili, che sono stati predisposti dall'imprenditore per l'esercizio dell'attività d'impresa), nonché di utilizzare gli strumenti messi loro a disposizione conformemente alle prestazioni richieste ed alle istruzioni impartite: istruzioni che saranno determinate dal datore di lavoro affinché tali strumenti possano essere idonei per un corretto svolgimento delle attività dell'Ente.

A fronte di tale situazione generale il progresso della tecnologia ha fatto sì che l'utilizzo di elaboratori elettronici e di servizi telematici (in particolare la rete Internet con le sue applicazioni, fra cui nuovi strumenti di comunicazione di seguito illustrati) diventasse strumento indispensabile per ogni tipo di azienda o Ente per svolgere le mansioni più diverse, a prescindere dalla sua dimensione, dalla sua struttura o dall'oggetto della sua attività.

Così, entra a far parte del più generico dovere di rispetto e di corretto utilizzo del patrimonio aziendale, di cui si è parlato, anche l'attenzione nell'uso delle sue risorse informatiche e telematiche, in relazione alle quali viene imposto al dipendente l'onere di seguire regole di condotta specifiche: questo al fine di evitare non solo il grave pericolo di alterare la stabilità delle applicazioni degli elaboratori elettronici che si hanno a disposizione, ma anche il rischio di essere esposti a conseguenze imprevedibili nel momento dello svolgimento della specifica attività informatica (si pensi all'acquisizione di musica o film da Internet in violazione dei relativi diritti di autore, con tutte le conseguenze, anche di natura penale, che ne potrebbero derivare). Ciò a maggior ragione in relazione a quelle che vedremo essere le nuove applicazioni dell'informatica nell'ambito del rapporto di lavoro, ad esempio con riferimento all'uso dei social network o in generale del c.d. Internet 2.0.

Questo in particolare perché, per quanto riguarda tali peculiari strumenti, rispetto ad altri maggiormente caratterizzati dallo specifico impiego cui sono destinati nell'attività di un'impresa (si pensi ad esempio ad una pressa idraulica), risulta molto semplice, proprio per le loro caratteristiche multifunzionali, la possibilità di un uso diverso da quello "lavorativo", di un uso "personale" degli stessi: con ciò aumentando il pericolo di cui si è detto, spesso nella totale inconsapevolezza del loro utilizzatore, ed ancor più del datore di lavoro.

In tale contesto allora il rispetto delle regole circa l'utilizzo delle dotazioni informatiche e telematiche dell'impresa può essere inteso non solo come l'adempimento di un "dovere aziendale", ma il giusto comportamento per evitare di essere esposti a conseguenze sanzionatorie spesso eccessivamente severe e di frequente ricadenti su un ignaro, e generalmente in buona fede, utente. Infatti, l'obbligo di utilizzare le dotazioni informatiche esclusivamente per ragioni di lavoro (con le sole eccezioni di uso personale previste nel presente disciplinare e nei limiti di cui al par. 2.1), escluderebbe indirettamente il rischio, da una parte, per il lavoratore di realizzare comportamenti illeciti e, dall'altra, per il datore di lavoro di essere ritenuto responsabile, ad esempio, per il materiale visto o scaricato da Internet dai propri dipendenti.

Non solo. Nel maggio del 2016 è entrata in vigore una nuova normativa europea, il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, il cosiddetto GDPR, che ha sostituito la disciplina precedente: normativa che detta disposizioni specifiche dedicate all'utilizzo delle nuove tecnologie quando sono impiegate nella raccolta e nella gestione delle informazioni degli individui. Tra tali disposizioni, in particolare, quelle attinenti alle misure tecniche ed organizzative volte alla protezione dei dati, che devono offrire "*un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere"* (cfr. Cons. 83 del Regolamento).

Nell'ambito dell'attività di adeguamento di UNITELMA SAPIENZA alla normativa in materia di "privacy" è di fondamentale importanza l'adempimento degli obblighi stabiliti in tale specifico settore, le misure di sicurezza nel trattamento dei dati personali (in particolare quelli degli iscritti, dei dipendenti e dei fornitori, se persone fisiche): tra questi si deve far rientrare anche l'obbligo di rendere noto ai lavoratori le regole in materia di uso dei nuovi strumenti tecnologici nella propria attività, ed in particolare la predisposizione (e distribuzione) ai dipendenti di un "Disciplinare interno" che raccolga tali regole, e che nello specifico per la vostra struttura è costituito dal presente "Codice di deontologia e buona condotta per un corretto utilizzo delle dotazioni informatiche di UNITELMA SAPIENZA''. Regole che, si badi bene, sono comunque esplicitate a completamento di quanto stabilito dalla legge, dalle prassi aziendali e dalle comuni norme di buona fede e correttezza, che quindi conservano la loro validità.

Acquisito dunque che l'adozione del presente Codice debba essere considerato una misura di sicurezza, occorre evidenziare che esso, rivolgendosi da una parte al datore di lavoro, quale estrinsecazione dei suoi obblighi, si sostanzia dall'altra anche in una serie di regole ed indicazioni utili ed importanti per il lavoratore: quest'ultimo, infatti, attraverso l'uso della tecnologia, anche per fini ed in ambiti personali, potrebbe, come detto, porre in essere comportamenti ed attività non conformi al contesto lavorativo o addirittura in contrasto con la legge (subendone quindi in prima persona le conseguenze negative).

Infine, si sottolinea che le istruzioni impartite con il presente documento sono applicabili, quando compatibili con la natura del rapporto, anche ai collaboratori, stagisti, tirocinanti, studenti in alternanza studio/lavoro e prestatori di lavoro alle dipendenze di altro datore che svolgano la propria prestazione lavorativa presso UNITELMA SAPIENZA.

2. Istruzioni relative all'uso, lavorativo e/o personale, delle dotazioni informatiche

In generale, l'adempimento da parte del lavoratore degli obblighi di diligenza, fedeltà e obbedienza con riferimento al patrimonio aziendale si concretizza essenzialmente nel dovere di:

- utilizzare i beni aziendali conformemente alle mansioni attribuite;
- salvaguardare il patrimonio aziendale da perdita, abuso, danneggiamento e furto;
- segnalare al datore gli eventi dannosi di cui al precedente punto.

Collegando questi obblighi all'uso delle dotazioni informatiche da parte del dipendente, i doveri che ne derivano possono essere riferiti alle varie applicazioni delle nuove tecnologie in uso da parte di UNITELMA SAPIENZA.

Così, si può distinguere un primo settore di regole collegato al "sistema computer" e altri *device* in genere, poi un altro relativo all'uso delle credenziali di autenticazione, e infine quello che si riferisce ad Internet e ai suoi servizi, in particolare il *world wide web*, la posta elettronica e i social network: distinzione che permette, tra l'altro, di meglio identificare, almeno in via generale, il concetto di "dotazioni informatiche" usato in questo "Codice di deontologia e buona condotta'.'

Rispetto ai settori appena indicati si riportano nel presente documento sia le istruzioni che il dipendente deve rispettare in adempimento dei suoi doveri relativi al corretto svolgimento del rapporto di lavoro, sia quelle per le ipotesi in cui le dotazioni informatiche vengano usate per finalità diverse da quelle tipiche connesse alla prestazione lavorativa: ipotesi di uso "personale" delle dotazioni informatiche aziendali che, reso possibile dalla duttilità che caratterizza tali strumenti, pur potendo essere ritenuto molto comune, deve in realtà considerarsi un'eccezione che necessita di attenzioni maggiori rispetto al loro uso "lavorativo". Questo a causa dei rilevanti rischi connessi all'utilizzo delle nuove tecnologie, che lo portano dunque ad essere oggetto di un'attenta e puntuale disciplina, con conseguente obbligo del lavoratore di rispettarla.

L'utilizzo personale delle dotazioni informatiche per essere lecito, in un contesto come quello lavorativo, deve quindi osservare alcune istruzioni fondamentali. In particolare:

- deve rispettare tutte le leggi e i regolamenti dello Stato, le politiche, gli standard e le direttive aziendali;
- non deve mai essere fatto per uno scopo che possa riflettersi negativamente sulla reputazione del datore di lavoro, o che possa comunque incidere negativamente sulla sua immagine;
- non deve interferire con il lavoro dei dipendenti, riducendone la produttività o la qualità, né con la fornitura di servizi agli iscritti;
- non deve servire di supporto per lo svolgimento di attività diverse da quelle di UNITELMA SAPIENZA;
- non deve ostacolare l'accesso da parte del datore di lavoro alle informazioni e ai dati attinenti alla propria attività (ad esempio, attraverso l'apposizione di password ad archivi informatici ad iniziativa del dipendente).

A parte tali principi generali, si procederà ora a determinare, in maniera esemplificativa e non esaustiva, le modalità di utilizzo delle varie realtà tecniche costituenti le dotazioni informatiche ad uso del dipendente.

2.1. Istruzioni sull'uso del "sistema computer" e altri *device*.

Salvo quanto verrà specificato dettagliatamente nel prosieguo con rifermento a particolari argomenti, nel presente paragrafo si indicano, raggruppati per aree di possibile attività

sulle dotazioni informatiche, le regole che il lavoratore deve rispettare nell'usare il suo "sistema computer'' e ''altri *device*'' eventualmente fornitigli.

Con riferimento alla possibilità di utilizzare o memorizzare, anche in via provvisoria, sul proprio elaboratore elettronico *file* non aventi alcuna attinenza con la propria attività lavorativa, siano essi scaricati da internet, contenuti o prelevati da supporti esterni di tipo ottico, magnetico o magneto/ottico (come ad esempio hard disk portatili, pen drive, …), il lavoratore dovrà rispettare quanto già indicato nel precedente paragrafo, ed in particolare:

- i *file* personali devono avere sempre un contenuto lecito e non contrario alle norme di legge e al buon costume;
- essi non devono rivelare le opinioni politiche, religiose, sindacali del dipendente, o comunque informazioni relative alla propria salute o vita sessuale;
- tali *file* devono quindi essere raggruppati in un'apposita cartella nominata in modo da evidenziare il carattere personale del suo contenuto;
- sui computer i dipendenti devono evitare di visionare film e altro in DVD, connettersi a siti web di canali televisivi che diffondano i loro contenuti in *streaming*, sia in genere il c.d. download di video leciti o illeciti (salvo ciò rientri nelle necessità lavorative),

Spetta al datore di lavoro stabilire le configurazioni impostate sull'elaboratore elettronico e la responsabilità delle stesse, e di conseguenza procedere nelle relative decisioni. A tale proposito il lavoratore dovrà comunque:

- astenersi dal modificare autonomamente le configurazioni impostate sul proprio elaboratore e dal manomettere, più in generale, lo strumento in dotazione;
- evitare di creare password di accesso a programmi o a dati senza l'autorizzazione specifica del responsabile della sicurezza informatica;
- astenersi dall'installare mezzi di comunicazione propri (come ad esempio il proprio cellulare come *hotspot* o, più in generale, qualsiasi altro *device*), e quindi realizzare autonomi collegamenti di accesso ad internet, rispetto a quelli della rete aziendale;
- evitare di utilizzare strumenti software o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e documenti informatici;
- utilizzare i computer portatili aziendali ed eventuali ulteriori *device*, se in dotazione, rispettando le regole di cui sopra, e quindi applicando tutte le misure idonee atte a proteggerne il funzionamento ed i dati personali ivi contenuti.

Con riferimento alla possibilità di utilizzare programmi di vario genere sul computer aziendale, sia per installarli, sia per duplicarli, il lavoratore dovrà:

- astenersi da qualsiasi uso o possibile duplicazione di software non distribuiti ufficialmente, qualora tali comportamenti implichino una violazione della legge 22 aprile 1941 n. 633 sul diritto d'autore e sue integrazioni e modificazioni;
- informarsi su tutte le restrizioni relative all'uso o alla duplicazione dei programmi per elaboratore in dotazione del datore, in quanto è di sua responsabilità il pieno rispetto del contratto di licenza di tali software;
- sottoporre al responsabile della sicurezza informatica designato, la richiesta di poter utilizzare, per lo svolgimento delle proprie mansioni, software di pubblico dominio e i c.d. shareware, e quindi, più in generale, programmi diversi da quelli messi a disposizione dal datore di lavoro;

Data inoltre la facilità con cui i software, gli allegati e-mail e i file in genere possono introdurre nel sistema informatico virus o altri elementi dannosi che potrebbero mettere in pericolo la sicurezza del computer e/o della rete aziendale, il lavoratore è tenuto:

- a segnalare al responsabile per la sicurezza il mancato utilizzo di un software antivirus sull'elaboratore che gli viene affidato prima di farne uso;
- ad evitare di scaricare sul proprio elaboratore elettronico file contenuti in allegati e-mail e/o in pagine web e/o in supporti di memoria di cui non sia certa provenienza e contenuto, e che quindi presentino rischi di pericolosità per il sistema informatico aziendale (nel caso ve ne sia la necessità, il lavoratore dovrà ottenere l'autorizzazione dal datore);
- a segnalare comunque qualsiasi anomalia riscontrata nell'uso dello strumento informatico.

Infine, in relazione ad ulteriori e diversi strumenti forniti dal Titolare ai propri dipendenti (come nel caso dei computer portatili, gli smartphone e i tablet), è opportuno evidenziare che il loro utilizzo da parte dell'utente deve rispettare le medesime regole e gli stessi principi previsti nel presente Codice. In particolare, a livello esemplificativo e non esaustivo, il lavoratore dovrà:

- utilizzare gli strumenti messi a sua disposizione seguendo le regole di buona fede e correttezza, senza arrecare un danno reputazionale a UNITELMA SAPIENZA e per scopi esclusivamente legati all'attività di lavoro;
- custodire tali dotazioni con diligenza e correttezza;
- astenersi dal salvare sui dispositivi forniti informazioni di contenuto illecito o di carattere personale, e comunque astenersi dal porre in essere attività illegali tramite il cellulare o con l'utilizzo della SIM aziendale.

2.2. Istruzioni relative all'uso delle credenziali di autenticazione (c.d. user-id e password)

Le "credenziali di autenticazione" (ovvero quei dati e dispositivi, in possesso di una persona, da questa conosciuti - i primi -, o ad essa univocamente correlati - i secondi -, utilizzati per l'autenticazione informatica, cioè per la verifica anche indiretta dell'identità dell'utente al fine di consentirgli l'accesso al sistema), composte dall'associazione di un identificativo di utente (c.d. "*user-id*", che spesso può essere sostituito da badge o tecniche biometriche) e da una parola chiave segreta (c.d. "*password*"), sono un elemento fondamentale per proteggere gli accessi, da parte di terzi, ai sistemi informativi aziendali: sia considerati nella loro realtà "complessiva" (in quanto rete aziendale), sia con riferimento ai singoli computer e/o agli specifici applicativi usati in concreto. Il loro scopo è anche quello di conoscere, nel caso sorgano problemi, l'attività svolta da un determinato soggetto, identificato in entrata, nell'ambito dei sistemi informatici aziendali: informazione che chiaramente sarà poi gestita nella completa osservanza di quanto stabilito nel Regolamento (UE) 2016/679 e nel presente Codice. Per tale motivo il lavoratore non deve accedere ai sistemi informativi aziendali usando *user-id* e *password*

di qualcun altro: in caso di necessità particolari, dovrà essere chiesta l'autorizzazione al proprio responsabile della sicurezza.

Così, i lavoratori sono tenuti, con riferimento alla componente segreta delle credenziali di autenticazione (la parola chiave), al rispetto delle seguenti regole:

1. la *password* deve essere facile da ricordare e contemporaneamente difficile da indovinare, non deve contenere nomi o frasi comuni, né essere in alcun modo collegata alla vita privata (come ad esempio il nome o il cognome, proprio o di parenti, la targa dell'auto, la data di nascita, la città di residenza, ...);

2. la *password* deve avere almeno 8 caratteri (tra cui numeri, caratteri speciali e maiuscola e minuscola);

3. la *password* non può altresì contenere più di due caratteri consecutivi del nome completo dell'utente o del nome dell'account utente.

4. la password, assegnata dal responsabile della sicurezza informatica contestualmente alla *user-id*, deve essere modificata al primo accesso da parte del dipendente;

5. la *password* deve essere cambiata ogni 90 giorni;

6. ogni nuova *password* deve altresì essere diversa dalle ultime quattro utilizzate;

7. la *password* deve essere mantenuta segreta: pertanto non deve essere rivelata né scritta o lasciata in posti dove potrebbe essere facilmente scoperta.

L'utente, in caso di assenza dalla propria postazione per un periodo considerevole di tempo (es. durante la pausa pranzo, una riunione, ecc.), deve chiudere le applicazioni su cui sta lavorando e, se lascia il computer acceso, deve procedere al blocco dello stesso qualora non sia passano il tempo previsto per quello automatico.

Infine, si evidenzia che, in caso di necessità, il datore di lavoro (attraverso l'intervento del responsabile della sicurezza) può entrare nelle aree ad accesso riservato del computer del dipendente, attraverso le credenziali che lo stesso ha previamente inserito in busta chiusa e che vengono custodite a cura del responsabile stesso. In tale evenienza, l'utente, al primo tentativo di accesso al sistema, avrà conferma di quanto accaduto e dovrà nuovamente cambiare la *password*.

2.3. Istruzioni relative all'uso di Internet: la navigazione web, la posta elettronica e gli altri servizi

L'accesso alla rete Internet e l'utilizzo dei suoi servizi, come quello di ogni altro strumento messo a disposizione dal Titolare, deve rispettare precise modalità di impiego e misure di sicurezza affinché venga evitato, come indicato in precedenza, qualunque tipo di interferenza con i doveri professionali del dipendente e degli altri soggetti (anche solo per evitare perdite di tempo e distrazioni), e al contempo eliminato qualsiasi ulteriore

rischio per UNITELMA SAPIENZA. In particolare, ci si riferisce, per quanto riguarda l'uso di Internet e dei suoi servizi, alla possibilità di utilizzi impropri della "navigazione" web o dell'uso dei social network: di conseguenza dovranno essere quindi evitati gli accessi ai siti contenenti informazioni illecite per i più vari motivi, lo svolgimento di attività quali ad esempio la partecipazione a *newsgroup* o *mailing list* collegati ad argomenti illeciti, l'upload o il download di materiale della stessa natura, l'uso improprio della posta elettronica o di uno specifico social, ecc., come dettagliato nei prossimi paragrafi.

Occorre comunque tenere presente che scopo delle regole di seguito elencate non è solo quello di evitare i rischi indicati per la struttura del datore di lavoro e per un più corretto svolgimento del rapporto lavorativo, ma anche quello di minimizzare l'uso di dati identificativi degli stessi lavoratori, e quindi indirettamente di UNITELMA SAPIENZA, in ambienti e situazioni "virtuali" che potrebbero utilizzare le nuove tecnologie (c.d. *privacy enhacing technologies* – PETs) per acquisire informazioni personali degli utenti senza alcuna preoccupazione di tutela delle stesse.

2.3.1. La navigazione web e gli altri servizi

Per il rispetto dei suddetti obiettivi (evitare rischi per il datore di lavoro, corretto svolgimento dell'attività lavorativa, tutelare i dati personali del lavoratore, tutelare le informazioni relative alla struttura), è dunque necessaria la collaborazione costante tra datore di lavoro e dipendente a cui, in base alle regole individuate nel presente Codice, non è consentito l'utilizzo del Web e dei suoi servizi per attività non connesse alle finalità lavorative. In particolare, il lavoratore non deve:

- navigare nei siti dai quali è possibile risalire alle sue opinioni politiche, religiose, sindacali, ad informazioni relative alla propria vita sessuale o comunque attinenti alla propria salute;
- eseguire transazioni finanziarie di ogni genere (ivi comprese le operazioni di c.d. *remote banking*) o acquisti on line, salvo che siano espressamente autorizzate, per la parte tecnologica, dal responsabile della sicurezza informatica.
- registrarsi, e comunque partecipare, a siti, chat, *newsgroup*, *mailing list*, *forum*, *blog*, ..., ed in genere a social network, ad eccezione di quelli eventualmente creati e dedicati allo svolgimento dell'attività professionale, come meglio specificato nel paragrafo successivo;
- memorizzare sui *device* aziendali documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

- realizzare operazioni in contrasto con l'attività lavorativa, o comunque commettere illeciti penali, come disciplinati dalle relative normative, quali, a titolo esemplificativo:

  - accesso abusivo ad un sistema informatico o telematico;

  - detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;

- falsità in un documento informatico pubblico o privato;
- truffe a danno di certificatori di firma elettronica;
- danneggiamento o interruzione di sistemi informatici o telematici, e di informazioni, dati e programmi ad essi attinenti;
- installazione di dispositivi o programmi informatici diretti a danneggiare o interrompere sistemi informatici o telematici;
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
- installazione di dispositivi o programmi informatici atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
- frode informatica.

2.3.2. La posta elettronica

Pur partendo dall'assunto che il contenuto dei messaggi di posta elettronica (come pure i dati esteriori delle comunicazioni e i file allegati) riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, è importante sottolineare come l'account aziendale, cioè l'indirizzo di posta elettronica proprio della struttura in cui il soggetto lavora, per la funzione che ricopre nel contesto lavorativo deve essere consultabile da UNITELMA SAPIENZA: necessità connessa all'onere in capo al datore di lavoro di tutelare la propria struttura, la regolarità dell'attività lavorativa e, non ultimo, di prevenire inutili intrusioni nella sfera personale dei lavoratori e violazioni della disciplina sulla segretezza della corrispondenza da parte di soggetti terzi. Tale necessità, nella specie, riguarda sia gli account aziendali affidati in via esclusiva al dipendente (come ad esempio *nome.cognome@unitelmasapienza.it*), sia quelli demandati ad un uso condiviso (ad esempio *legale@unitelmasapienza.it*), rispetto al quale le persone che possono consultarli ed utilizzarli sono previamente individuate, ed a ciò autorizzate, dal datore). Alla luce dell'esigenza citata, il datore di lavoro, direttamente o attraverso i soggetti a ciò preposti, potrà accedere a tali mail in determinate situazioni, indicate oltre nel testo, rispettando in ogni caso i principi di liceità, correttezza, trasparenza e minimizzazione previsti dal Regolamento 2016/679, e, in generale, la disciplina in materia di protezione dei dati personali e quella giuslavorista, allo scopo di tutelare al meglio la dignità e riservatezza del lavoratore.

A tale proposito, per contemperare in tale ambito le esigenze di un ordinato svolgimento dell'attività lavorativa di cui si è detto, all'onere del datore di lavoro di prevenire inutili intrusioni nella sfera personale dei lavoratori, e violazioni della disciplina sulla segretezza della corrispondenza, consegue pertanto l'obbligo del lavoratore di mantenere un comportamento di assoluta osservanza delle regole per l'utilizzo della mail: tra l'altro perché il funzionamento tipico dei servizi di posta elettronica implica il trattamento di dati personali (nella specie, come minimo, gli indirizzi dei destinatari della e-mail del dipendente, e dei mittenti delle comunicazioni a lui dirette), e di conseguenza l'applicazione dell'obbligo per il datore di lavoro di rispettare, e far rispettare, le stringenti

previsioni del Regolamento 2016/679. A tal fine si precisa che il lavoratore è dunque obbligato a:

8. utilizzare l'indirizzo di posta elettronica c.d. aziendale solo per corrispondenza attinente alla propria attività lavorativa, e mai personale;
9. inserire, in calce ad ogni e-mail (o comunque verificare che sia già stato inserito in maniera automatica), l'indicazione della natura non personale, privata della stessa, e del fatto che le eventuali risposte del destinatario possano essere lette o comunque conosciute anche da altri all'interno della propria struttura lavorativa;
10. nel caso in cui, per errore, pervenga sulla casella di posta aziendale un'e-mail personale, cancellarla immediatamente sia dal *client* di posta elettronica che dal web (direttamente o attraverso il responsabile della sicurezza informatica);
11. non scaricare o salvare le e-mail di natura lavorativa che pervengano sulla casella di posta aziendale su computer differenti da quello aziendale: nel caso si renda necessario accedervi da un diverso elaboratore, il lavoratore dovrà soltanto visualizzarle via web, salvo diversa ed esplicita autorizzazione del datore;
12. attivare, qualora sappia di dover usufruire delle ferie o debba lavorare fuori sede, apposite funzionalità di sistema che consentano di inviare automaticamente messaggi e-mail di risposta contenenti l'avviso generico dell'assenza del lavoratore, nonché indicare le coordinate di altro soggetto, o della competente struttura, per ricevere informazioni;
13. astenersi dall'inviare con posta elettronica documenti di lavoro "strettamente riservati" se non con le opportune precauzioni (individuate insieme al responsabile per la sicurezza informatica), in quanto tali messaggi potrebbero essere intercettati da estranei;
14. non utilizzare l'indirizzo di posta elettronica aziendale per la partecipazione a *newsgroup*, e/o *forum*, e/o *mailing-list*, o simili, salvo diversa ed esplicita autorizzazione;
15. non utilizzare l'indirizzo di posta elettronica aziendale per inviare in allegato file di contenuto illecito o comunque non attinente alla propria attività lavorativa;
16. non utilizzare l'indirizzo di posta elettronica aziendale per inviare, reperire o archiviare messaggi molesti, minacciosi, offensivi, diffamatori, discriminatori per sesso, razza, lingua, religione, origine etnica e appartenenza sindacale e/o politica, o comunque osceni, e altre informazioni di tal genere;
17. nel caso in cui venga autorizzata la consultazione di posta elettronica personale, quindi non aziendale, consultarla solamente via web, e le relative e-mail e/o allegati non possono essere scaricate e/o salvate sul computer aziendale, e comunque possono essere lette solo al di fuori dell'orario di lavoro.

In caso di assenza prolungata dal lavoro o di cessazione del relativo rapporto, il dipendente è consapevole e accetta che il datore di lavoro possa accedere alla casella di posta elettronica, personalmente o individuando una persona a ciò autorizzata, per garantire la continuità e il normale svolgimento dell'attività aziendale: con riferimento

all'ipotesi di cessazione del rapporto si veda comunque quanto riportato nel paragrafo (3.3).

Qualora il lavoratore decida di interrompere il rapporto di lavoro con UNITELMA SAPIENZA, tramite preavviso di 3 mesi (o altro termine stabilito nel contratto di lavoro), dovrà, entro il medesimo lasso temporale, svolgere le seguenti attività:

- eliminare eventuali informazioni di carattere personale conservate, contrariamente a quanto previsto dal presente Codice, nell'account aziendale;
- informare gli interessati dell'Ateneo (con i quali si hanno contatti in relazione alle proprie mansioni di lavoro) fornendo le coordinate (es. indirizzo e-mail) di un altro soggetto preposto agli stessi compiti;
- inviare tutte le informazioni utili riguardo le pratiche aperte al soggetto designato dall'Ateneo.

Qualora, invece, il rapporto di lavoro si interrompa senza preavviso, il lavoratore dovrà immediatamente:

- eliminare eventuali informazioni di carattere personale conservate, contrariamente a quanto previsto dal presente Codice, nell'account aziendale;
- inviare tutte le informazioni utili riguardo le pratiche aperte ad un soggetto designato dall'Ateneo.

Sia nell'ipotesi di preavviso che nel caso di cessazione immediata del rapporto di collaborazione, il prestatore è consapevole che il Titolare procederà al reindirizzamento automatico delle mail ricevute sull'account dell'ex-dipendente inoltrandole al nuovo soggetto designato, portando a conoscenza del cliente l'avvenuto cambio di referente.

2.3.3. I social network

I social network consentono all'utente che ne utilizza i servizi di condividere informazioni, pubblicare contenuti, quali fotografie o video, intrattenere conversazioni con gli altri utenti, o svolgere ulteriori attività.

L'uso dei social network può essere, in primo luogo, legato ad una scelta personale del dipendente a prescindere dall'ambito lavorativo o, in seconda istanza, collegato a questo: in tale ultimo caso è l'Ente stesso ad incentivare l'uso di questi mezzi, quali strumenti di potenziamento, attraverso la condivisione, delle attività istituzionali ed organizzative.

Di qui una prima, fondamentale, distinzione tra l'uso personale (in relazione al quale si dovranno comunque rispettare i principi e le regole di seguito evidenziate) e quello professionale.

Nel primo caso, il dipendente, pur essendo libero di comunicare e condividere con terzi informazioni e contenuti, è tuttavia tenuto ad un utilizzo che sia conforme e rispettoso del contesto lavorativo in cui svolge la propria attività. In particolare, il lavoratore dovrà astenersi:

- dall'utilizzare il social network durante l'orario di lavoro;

- dal pubblicare commenti o informazioni legate all'attività lavorativa;
- dal diffondere dati, comunicazioni o documenti di cui si è venuti a conoscenza nell'ambito del rapporto di lavoro;
- dal pubblicare, in ogni caso, contenuti che possano arrecare in generale nocumento a UNITELMA SAPIENZA.

Nella seconda delle ipotesi prospettate, ovvero qualora sia il datore di lavoro stesso a creare il profilo di UNITELMA SAPIENZA nei vari social network e ad autorizzare alcuni dipendenti al suo utilizzo, ferme restando le regole di buona fede e correttezza nell'espletamento della prestazione professionale (ed in particolare quanto riportato nel presente Codice con riferimento in generale all'uso delle dotazioni informatiche), questi ultimi dovranno:

- custodire diligentemente le proprie credenziali di autenticazione al social network, che verranno fornite da UNITELMA SAPIENZA e quindi, non diffondere tali credenziali, né cederle a terzi;
- utilizzare il social network per finalità esclusivamente collegate alle attività di lavoro ed alle mansioni affidate dal datore, e dunque evitare di intrattenere comunicazioni che esulino dall'ambito della prestazione svolta;
- non pubblicare o trasmettere documentazione aziendale riservata;
- non pubblicare sul social network informazioni di carattere politico, religioso, sindacale, sessuale, riferite alla propria persona o a terzi;
- non scaricare né condividere file dal contenuto illecito;
- non utilizzare il social network per inviare comunicazioni offensive, diffamatorie o discriminatorie nei confronti di colleghi o terzi;
- in generale, non utilizzare il social network come strumento per la realizzazione di illeciti penalmente sanzionati dalle norme di legge.

3. Modalità di gestione del sistema informatico di UNITELMA SAPIENZA

Nel presente paragrafo si descrivono in maniera sintetica le misure adottate da UNITELMA SAPIENZA per garantire la sicurezza dei dati personali trattati con l'ausilio del patrimonio informatico aziendale. Poiché l'uso di tali dispositivi genera un ammontare di dati riferibili all'utente, si forniscono altresì indicazioni relative alle tipologie di informazioni sottoposte a trattamento ed alle modalità di gestione delle stesse. Vengono inoltre riportate le procedure adottate e le finalità perseguite dal datore di lavoro allorché provveda ad effettuare dei controlli all'interno della propria struttura. Nel corso di tali verifiche, il cui svolgimento è necessario in vista del perseguimento di finalità di tipo organizzativo, produttivo o legate alla sicurezza di cose e persone, soggetti specificamente individuati all'interno della struttura di UNITELMA SAPIENZA tratteranno dati inerenti all'attività lavorativa dei dipendenti ed all'uso delle dotazioni informatiche da parte di questi ultimi.

3.1. Descrizione delle prescrizioni interne sulla sicurezza adottate da UNITELMA SAPIENZA.

La sicurezza del patrimonio informatico di UNITELMA SAPIENZA e, più in generale, dei dati personali trattati con l'ausilio della sua strumentazione elettronica, viene garantita attraverso l'adozione di apposite precauzioni, in ottemperanza al principio stabilito dall'art. 5 comma I lett. f) del Regolamento UE 2016/679 (principio di integrità e riservatezza), secondo il quale l'informazione deve essere assicurata con misure tecniche e organizzative adeguate, tali da evitare il rischio di trattamenti non autorizzati, illeciti o che comportino la perdita, la distruzione del dato o il danno accidentale: precauzioni che vengono descritte nel presente paragrafo.

3.1.1. Sistema di autenticazione

L'accesso del solo personale autorizzato alle singole workstation, alla LAN dell'ufficio ed ai diversi software applicativi utilizzati nello svolgimento dell'ordinaria attività di lavoro viene garantito attraverso l'impiego di un sistema di autenticazione: il quale, identificando tutti coloro che effettuano ogni singolo log-in, non permette a soggetti privi di un proprio account aziendale di fare uso del patrimonio informatico di UNITELMA SAPIENZA. Tale sistema si basa sull'impiego di un codice per l'identificazione personale (c.d. "*userid*") dell'utente associato ad una parola chiave (c.d. "*password*") nota solo a quest'ultimo. L'*userid* è assegnato dal responsabile della sicurezza informatica, mentre la *password* è liberamente personalizzata dal dipendente al momento del primo accesso alle dotazioni informatiche aziendali, modificando quella precedentemente ricevuta dal responsabile. La strumentazione elettronica consente a ciascun lavoratore un limite massimo di cinque errori nell'inserimento delle credenziali di autenticazione. Esaurito il numero di tentativi concessi all'utente, il codice identificativo di quest'ultimo viene automaticamente disabilitato. Per assicurare la sicurezza della *password* è poi previsto il mascheramento dei caratteri inseriti dal lavoratore attraverso i dispositivi di input. Nel pieno rispetto delle norme di legge che prevedono l'aggiornamento periodico delle parole chiave, UNITELMA SAPIENZA ha predisposto le apparecchiature elettroniche impiegate dal personale in modo tale da obbligare ogni singolo utente al cambio della password ogni 90 giorni.

3.1.2. Sistema di autorizzazione

A ciascuna coppia di *userid* e parola chiave viene associato uno specifico profilo autorizzativo che consente all'utente di accedere ai dati necessari allo svolgimento della propria attività lavorativa, nonché di effettuare le operazioni di trattamento rientranti nell'ambito delle sue mansioni. La revisione ed il controllo dei profili autorizzativi vengono comunque effettuati, in conformità con le disposizioni di legge, con cadenza annuale.

3.1.3. Firewall, antivirus e patch.

La sicurezza di dati e sistemi viene assicurata attraverso l'implementazione delle seguenti misure:

- impiego di un firewall, al fine di prevenire gli attacchi esterni provenienti da *malware* e/o da soggetti non autorizzati;
- installazione su ogni macchina di un software antivirus, la cui gestione e aggiornamento avviene a cura del responsabile della sicurezza;
- aggiornamento periodico dei programmi per elaboratore impiegati nello svolgimento dell'attività lavorativa, a cura del responsabile della sicurezza.

L'adozione simultanea delle precauzioni appena indicate consente a UNITELMA SAPIENZA di limitare il rischio di intrusioni esterne provenienti da soggetti o programmi non autorizzati e, al contempo, di ridurre gli eventuali danni arrecati a dati e sistemi dall'azione di virus informatici. In questo quadro, l'aggiornamento costante dei software impiegati nello svolgimento della normale attività lavorativa consente tanto di migliorare l'efficienza del lavoratore, mediante l'introduzione di nuove funzionalità all'interno dei programmi medesimi, quanto di ridurre il rischio di sfruttamento delle debolezze del sistema, grazie all'eliminazione delle falle (c.d. "*bug*") presenti in ciascun software al momento della sua creazione.

3.1.4. Back-up dei dati.

Al fine di ridurre al minimo l'impatto di problemi tecnici, o di altra natura, sull'attività di UNITELMA SAPIENZA, la protezione dei dati personali trattati all'interno della struttura viene rafforzata tramite la presenza di specifiche procedure di back-up dei dati contenuti all'interno dei diversi server impiegati nello svolgimento della quotidiana attività lavorativa.

Per quanto concerne, invece, eventuali strumenti di archiviazione utilizzati da parte dei dipendenti (come, ad esempio, chiavi USB, HD esterni, sistemi cloud …), rientrando questi tra le "dotazioni informatiche" oggetto del presente Codice, il loro utilizzo deve rispettare le indicazioni in esso stabilite, assumendo l'utente la responsabilità delle informazioni in tal modo archiviate: questo, per rendere possibile la realizzazione di tale misura di sicurezza, può rivolgersi al responsabile per la sicurezza informatica, il quale avrà cura di indicargli le modalità più idonee per attuarle.

3.1.5. Misure organizzative

Sul piano organizzativo, l'adozione di precise regole comportamentali consente di rafforzare il livello di protezione di dati e sistemi garantito dall'implementazione di misure tecnologiche, riducendo sia la possibilità di accessi abusivi alla strumentazione informatica di UNITELMA SAPIENZA, che i danni prodotti dall'azione di programmi malevoli: e, conseguentemente, limitando il rischio di distruzione, trattamento non autorizzato o perdita accidentale dei dati personali trattati nello svolgimento della

normale attività lavorativa. In particolare, l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli autorizzati e addetti alla gestione o manutenzione degli strumenti informatici, le procedure per la disattivazione degli account alla rete del Titolare ed infine le stesse istruzioni per la corretta gestione e custodia degli strumenti di lavoro, così come impartite nel presente documento, costituiscono misure di sicurezza volte alla protezione di tutti i dati personali trattati da UNITELMA SAPIENZA.

3.2. Descrizione delle informazioni personali memorizzate da UNITELMA SAPIENZA e delle relative modalità di gestione

All'interno di alcuni computer del Titolare sono memorizzate informazioni di natura personale relative ai dipendenti, incluse quelle generate dalla loro attività lavorativa. In particolare, possono essere conservati dati attinenti all'instaurazione, gestione ed estinzione del rapporto di lavoro, quali, a titolo esemplificativo, dati anagrafici, dati fiscali, nonché dati di natura "particolare" (nella precedente disciplina denominati "sensibili" come, ad esempio, quelli desumibili dai certificati medici) o di natura giudiziaria.

Inoltre, per ragioni tecniche e di sicurezza, il sistema informatico aziendale genera specifici file di *log* in cui vengono memorizzati la data e l'ora di accesso alle risorse informatiche da parte di ciascun operatore, inclusi i tentati *log-in* non andati a buon fine, nonché quelli di *log-out* da tali risorse.

Le informazioni così raccolte vengono conservate per il periodo di tempo ritenuto utile al perseguimento di finalità organizzative, produttive e di sicurezza, nei limiti del rispetto della normativa i materia, generale o specifica per le diverse tipologie di trattamento.

In presenza di particolari esigenze tecniche o di sicurezza, o su richiesta dell'autorità giudiziaria o della polizia giudiziaria, o comunque per finalità di esercizio o difesa di un diritto in sede giudiziaria, la conservazione può protrarsi per tempi superiori a quelli stabiliti dalla legge.

Le informazioni personali indicate possono poi essere visionate, oltre che nelle ipotesi legate allo svolgimento dell'attività lavorativa, anche nelle eventuali attività di controllo poste in essere dal datore di lavoro, secondo le modalità indicate al successivo punto 3.3.

3.3 Descrizione dei controlli posti in essere dalla struttura

In presenza di specifiche esigenze produttive, organizzative, o legate alla sicurezza di cose e persone, nonché con riferimento ad informazioni pertinenti e non eccedenti rispetto all'attività di lavoro, il Titolare si riserva la possibilità di effettuare controlli "*ex post*" (vale a dire dopo aver rilevato l'attività sospetta) sull'utilizzo degli strumenti informatici, così come di seguito illustrati.

Qualora si verifichino comportamenti anomali nell'uso delle dotazioni informatiche, UNITELMA SAPIENZA procederà immediatamente ad un controllo su dati aggregati riferiti al singolo ufficio interessato. In seguito a detto controllo, nell'ipotesi in cui si

riscontri un utilizzo effettivamente anomalo degli strumenti aziendali, sarà inviato un avviso generalizzato a tutti i dipendenti dell'ufficio coinvolto. Nel caso in cui si verifichino ulteriori anomalie, UNITELMA SAPIENZA si riserva la piena facoltà di procedere a controlli su base individuale.

Con riferimento poi ai controlli sulla posta elettronica in uso nella struttura di UNITELMA SAPIENZA, il datore di lavoro può accedere alle e-mail aziendali, ad esempio in caso di prolungata assenza del lavoratore o in situazioni impreviste, attraverso l'intervento del responsabile per la sicurezza informatica. In tale evenienza, al primo accesso successivo da parte del lavoratore, un avviso automatico gli comunicherà tale ingresso ed egli avrà cura di modificare la password. Il responsabile della sicurezza dovrà redigere apposito verbale relativo all'accesso effettuato, al fine di rendere edotto il lavoratore, secondo quanto stabilito nel vademecum del Garante per la protezione dei dati personali del 15 maggio 2015.

Nel caso in cui l'assenza del lavoratore sia dovuta alla cessazione del rapporto di lavoro, il datore potrà svolgere dei controlli sulle caselle di posta solo con determinati presupposti.
Qualora la cessazione sia avvenuta dopo il passare dei 3 mesi di preavviso richiesti dal contratto sorto tra le parti, il datore avrà 30 giorni (che intercorrono tra la disattivazione alla cancellazione dell'account del dipendente) per recuperare le informazioni lì presenti senza le quali si rallenterebbe, o fermerebbe, il ciclo produttivo dell'Ateneo. In questa fattispecie, il controllo del datore di lavoro è solo residuale poiché, nei 3 mesi di preavviso, il lavoratore si impegnerà a inoltrare tutte le informazioni di carattere lavorativo ad un soggetto designato.

Qualora, invece, la cessazione sia avvenuta contestualmente al preavviso, il datore di lavoro si riserva la facoltà di accedere e recuperare le informazioni necessarie allo svolgimento dell'attività lavorativa durante i 60 giorni che intercorrono tra la disattivazione e la cancellazione dell'account del dipendente. In questo caso, il controllo ex-post è più marginale poiché il lavoratore, al momento del perfezionamento dello scioglimento contrattualistico, è obbligato a inviare immediatamente tutte le informazioni relative a pratiche aperte ad un soggetto designato.

L'ultima situazione che si può prospettare è la cessazione del rapporto di lavoro dovuto a morte improvvisa. Tutti gli obblighi, in questo caso, sono in capo al datore di lavoro, il quale dovrà attivare automaticamente un avviso di risposta alle mail indirizzate all'account del defunto per informarli e reindirizzare i contenuti ad un soggetto designato. Il titolare dovrà, poi, individuare le informazioni necessarie ed estrapolarle (facendo molta attenzione a non visionare o trattare informazioni di carattere personale) nei 90 giorni che intercorrono tra la disattivazione, immediata, dell'account all'eliminazione della stessa. La ragione per cui il tempo di conservazione è maggiore è dovuta alla mancanza di intervento del soggetto proprietario della casella di posta elettronica rendendo i compiti del datore molto delicati.

Sempre con riferimento ai controlli posti in essere sulla posta elettronica, per quanto concerne gli account condivisi – come quello attribuito ad un ufficio nel suo complesso e

contraddistinto, ad esempio, dall'estensione info@unitelmasapienza.it o ufficiolegale@unitelmasapienza.it in considerazione del loro utilizzo da parte di più dipendenti, appartenenti alla medesima direzione, il Titolare si riserva la possibilità di svolgere controlli più incisivi, pur nel rispetto della disciplina in materia di protezione dei dati personali: in particolare, esclusivamente nei casi in cui vi sia necessità e nell'ipotesi in cui tutte le persone legittimate all'uso dell'account siano assenti, il datore di lavoro può accedere alle predette caselle di posta elettronica, tramite l'intervento del responsabile IT.

Inoltre, il datore di lavoro si riserva la facoltà di raccogliere e conservare, per la durata di sette giorni, i c.d. "metadati", ovvero le informazioni che riguardano i messaggi di posta elettronica, con particolare riferimento al mittente e al destinatario della comunicazione, al suo oggetto e alle sue dimensioni, nonché alla data e all'orario dell'invio: le predette informazioni vengono raccolte e analizzate esclusivamente al fine di accertare eventuali condotte illecite perpetrate a danno del Titolare. Sono oggetto, in ogni caso, di controllo *ex post*, ovvero solo nell'eventualità che si verifichi un fatto illecito e dopo il realizzarsi di quest'ultimo.

Come detto, a prescindere da quanto appena esposto relativamente ai controlli ordinari posti in essere, il monitoraggio sull'attività personale del singolo lavoratore può essere poi svolto anche in caso di specifiche richieste dell'autorità giudiziaria e forze di polizia, o in eccezionali situazioni di pericolo: in queste ipotesi le modalità di svolgimento della relativa attività saranno stabilite e coordinate con tali autorità.

4. Conseguenze dell'uso indebito delle dotazioni informatiche.

Il dipendente (o comunque il collaboratore) di UNITELMA SAPIENZA, dal momento della conclusione del contratto di lavoro, e per tutta la durata del rapporto contrattuale, è tenuto al rispetto degli obblighi di diligenza e fedeltà al datore di lavoro.

Come già evidenziato nella prima parte del presente Codice, nello svolgimento delle mansioni primario è il dovere (da parte del lavoratore) di salvaguardare il patrimonio del Titolare, di cui le dotazioni informatiche costituiscono elementi integranti.

Questi mezzi devono essere utilizzati conformemente alle prestazioni richieste ed in maniera tale da realizzare un pieno soddisfacimento degli interessi di UNITELMA SAPIENZA.

Ogni uso del bene in contrasto con l'originaria destinazione, ovvero con quanto disposto dal Titolare (tra l'altro nel presente documento), integra una violazione del dovere di diligenza del prestatore di lavoro ai sensi dell'art. 2104 del Codice Civile, secondo il quale "*il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quella superiore della produzione nazionale. Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende*".

Il rispetto delle regole circa l'utilizzo delle dotazioni informatiche di UNITELMA SAPIENZA può essere, tra l'altro, inteso non solo come adempimento di un dovere sancito dalla legge, o comunque di un obbligo che ha origine dal rapporto di lavoro, ma anche come una corretta misura preventiva a tutela del lavoratore, che può così evitare di cadere inconsapevolmente in comportamenti illeciti. Come si è detto, infatti, un uso di tali strumenti per finalità diverse da quelle stabilite dal Titolare può concretizzarsi in un'attività illecita a prescindere dall'ambito lavorativo (ad esempio, scaricare musica o film da Internet non solo rappresenterebbe un uso non consentito del computer aziendale, ma andrebbe a costituire violazione delle norme sul diritto di autore).

In virtù del potere disciplinare che il nostro ordinamento riconosce al datore di lavoro, UNITELMA SAPIENZA può verificare, seguendo le modalità di controllo esplicate nel precedente paragrafo 3.3, eventuali infrazioni commesse in tale ambito, e porre conseguentemente in essere le procedure relative alla comminazione di sanzioni disciplinari, secondo quanto stabilito nel Contratto Collettivo Nazionale applicabile.

Nel successivo paragrafo si richiamano sia le sanzioni disciplinari previste dallo Statuto dei lavoratori applicabili (L. 20 maggio 1970 n. 300), sia gli eventuali provvedimenti di sospensione dell'accesso a Internet, finalizzati alla tutela del patrimonio informatico aziendale.

Infine, si ricordano le diverse forme di responsabilità (civile, penale, amministrativa) per le quali il dipendente potrebbe trovarsi a rispondere, come si è detto anche a prescindere dal rapporto di lavoro, in caso di suoi comportamenti illeciti posti in essere utilizzando le dotazioni informatiche di UNITELMA SAPIENZA.

4.1 Sanzioni.

Il dipendente si impegna ad osservare le prescrizioni contenute nel presente Codice.

In caso di mancato rispetto delle regole e/o delle procedure esposte in tale documento, UNITELMA SAPIENZA si riserva la facoltà di promuovere, nei confronti del lavoratore, azioni disciplinari in conformità a quanto prescritto dagli artt. 2104 e 2106 del Codice Civile e dall'art. 7 dello Statuto dei lavoratori (L. 300/1970), di cui si riportano i testi integrali.

Art. 2104 c.c. - Diligenza del prestatore di lavoro

Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale.
Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende.

Art. 2106 c.c. - Sanzioni disciplinari

L'inosservanza delle disposizioni contenute nei due articoli precedenti può dar luogo all'applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione.

Art. 7 l. 300/70 - Sanzioni disciplinari.

Le norme disciplinari relative alle sanzioni alle infrazioni in relazione alle quali ciascuna di esse può essere applicata ed alle procedure di contestazione delle stesse, devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti. Esse devono applicare quanto in materia é stabilito da accordi e contratti di lavoro ove esistano.
Il datore di lavoro non può adottare alcun provvedimento disciplinare nei confronti del lavoratore senza avergli preventivamente contestato l'addebito e senza averlo sentito a sua difesa.
Il lavoratore potrà farsi assistere da un rappresentante dell'associazione sindacale cui aderisce o conferisce mandato.
Fermo restando quanto disposto dalla legge 15 luglio 1966, n. 604, non possono essere disposte sanzioni disciplinari che comportino mutamenti definitivi del rapporto di lavoro; inoltre la multa non può essere disposta per un importo superiore a quattro ore della retribuzione base e la sospensione dal servizio e dalla retribuzione per più di dieci giorni.
In ogni caso, i provvedimenti disciplinari più gravi del rimprovero verbale non possano essere applicati prima che siano trascorsi cinque giorni dalla contestazione per iscritto del fatto che vi ha dato causa.
Salvo analoghe procedure previste dai contratti collettivi di lavoro e ferma restando la facoltà di adire l'autorità giudiziaria, il lavoratore al quale sia stata applicata una sanzione disciplinare può promuovere, nei venti giorni successivi, anche per mezzo dell'associazione alla quale sia iscritto ovvero conferisca mandato, la costituzione, tramite l'ufficio provinciale del lavoro e della massima occupazione, di un collegio di conciliazione ed arbitrato, composto da un rappresentante di ciascuna delle parti e da un terzo membro scelto di comune accordo o, in difetto di accordo, nominato dal direttore dell'ufficio del lavoro. La sanzione disciplinare resta sospesa fino alla pronuncia da parte del collegio.
Qualora il datore di lavoro non provveda, entro dieci giorni dall'invito rivoltogli dall'ufficio del lavoro, a nominare il proprio rappresentante in seno al collegio di cui al comma precedente, la sanzione disciplinare non ha effetto.
Se il datore di lavoro adisce l'autorità giudiziaria, la sanzione disciplinare resta sospesa fino alla definizione del giudizio.
Non può tenersi conto ad alcun effetto delle sanzioni disciplinari decorsi due anni dalla loro applicazione.

Le sanzioni comminabili sono quelle contemplate dal Contratto Collettivo applicabile e sono determinate secondo i principi di proporzionalità e di gradualità, avendo riguardo anche alla gravità dell'infrazione.

In occasione di eventuali contestazioni di addebito, è sempre previsto l'esercizio del diritto di difesa per il dipendente, secondo le modalità prescritte dal citato art. 7 dello Statuto dei lavoratori.

4.2 Ulteriori sanzioni.

A parte quanto indicato nel precedente paragrafo relativo alle sanzioni, e ferme restando le eventuali conseguenze negative derivanti da ulteriori specifiche sanzioni (come ad esempio quelle per violazioni di leggi poste a disciplina del diritto di proprietà

individuale), UNITELMA SAPIENZA si riserva, con la sola finalità di salvaguardare il patrimonio aziendale, la facoltà di sospendere l'accesso a Internet e/o l'utilizzo della posta elettronica di un utente e/o l'utilizzo di una specifica dotazione informatica, nei seguenti casi:

- diffusione o comunicazione di password, procedure di connessione, indirizzi e altre informazioni tecniche imputabili direttamente all'utente;

- attività dell'utente che comportino un danno a terzi, o comunque la possibilità di arrecarlo;

- attività che violino, o possano violare, norme di legge o che si pongano comunque in contrasto con quanto esplicitato nella prima parte del presente Codice.

Lo stato di sospensione provvisorio rimane attivo per il periodo ritenuto opportuno dal datore di lavoro, previo parere del responsabile della sicurezza informatica.

4.3. Responsabilità civile, penale, amministrativa del dipendente.

Come si è più volte ricordato, l'uso non consentito delle dotazioni informatiche di UNITELMA SAPIENZA da parte del dipendente potrebbe costituire una violazione dei doveri dello stesso nei confronti del suo datore di lavoro, nonché di norme di legge generali, cioè "esterne" al rapporto di lavoro: ad esempio in relazione al dovere del lavoratore di corretta custodia ed esclusivo utilizzo delle proprie credenziali di autenticazione, potrebbe sorgere, in capo ad esso, anche una responsabilità per fatti commessi da chiunque utilizzi le sue credenziali di accesso (cioè la sua *user-id* e la sua *password*), se resi possibili da accertate violazioni dei doveri del dipendente, come sopra richiamati.

In tutte queste situazioni il lavoratore potrebbe essere chiamato a rispondere del suo comportamento dinnanzi all'autorità giudiziaria, e il Titolare dunque potrebbe trovarsi coinvolto nei relativi procedimenti.

UNITELMA SAPIENZA si riserva quindi la facoltà di agire dinnanzi alle Autorità competenti per ottenere il risarcimento dei danni cagionati dal lavoratore al patrimonio e all'immagine aziendali. Nelle ipotesi in cui essa si trovi poi a rispondere nei confronti di terzi per danni cagionati dal dipendente, si riserva, inoltre, la piena facoltà di regresso sul dipendente stesso.

APPENDICE 1

DEFINIZIONI

Ai fini del presente "Codice di deontologia e buona condotta per un corretto utilizzo dei sistemi informatici di UNITELMA SAPIENZA'' si intende per:

a) "*trattamento*", qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
b) "*dato personale*", qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
c) "*dati relativi alla salute*", i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
d) "*titolare del trattamento*", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
e) "*responsabile del trattamento*", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
f) "*destinatario*", la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
g) "*responsabile della sicurezza informatica*", si occupa della sicurezza della rete aziendale e delle dotazioni informatiche;
h) "*interessato*", la persona fisica, identificata o identificabile, cui si riferiscono i dati personali;
i) "*comunicazione*", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dai soggetti autorizzati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
l) "*banca di dati*", qualsiasi complesso organizzato di dati personali, ripartito in una o più

unità dislocate in uno o più siti;
m) "*Autorità di controllo*": l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 (Garante per la protezione dei dati personali);
n) "*strumenti elettronici*", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
o) "*autenticazione informatica*", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
p) "*credenziali di autenticazione*", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
q) "*parola chiave*", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
r) "*profilo di autorizzazione*", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
s) "*sistema di autorizzazione*", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;
t) "*posta elettronica*", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza; i relativi indirizzi possono essere
t1) "*personali*" (quelli cioè propri del soggetto che li utilizza, e non della struttura in cui lavora, ad esempio *tizio@gmail.com*),
t2) "*lavorativi*" (anche detti "aziendali", sono quelli propri della struttura in cui il soggetto lavora, anche se a lui assegnati in via esclusiva: come, ad esempio, per tizio è "e-mail aziendale" quella con indirizzo *tizio@unitelmasapienza.it* o
t3) "*condivisi*" (cioè propri della struttura in cui il soggetto lavora, ma non assegnati in via esclusiva: come ad esempio *info@unitelmasapienza.it)*.

Appendice 2

Schema riassuntivo delle regole di uso delle dotazioni informatiche di UNITELMA SAPIENZA

Via Nomentana, n. 373, 00162 ROMA
Tel. 06/86327973 - Fax 06/83390932 e-mail: *studiociacci@jei.it* - web-site: *http://www.jei.it*

Premessa.

L'adempimento degli obblighi di diligenza, fedeltà e obbedienza con riferimento al patrimonio aziendale si concretizza con quanto segue:

- utilizzare i beni aziendali conformemente alle mansioni attribuite;
- salvaguardare il patrimonio aziendale da perdita, abuso, danneggiamento e furto;
- segnalare al datore gli eventi dannosi di cui al precedente punto.

L'utilizzo personale delle dotazioni informatiche per essere lecito, in un contesto come quello lavorativo, deve quindi osservare alcune istruzioni fondamentali. In particolare:

- deve rispettare tutte le leggi e i regolamenti dello Stato, le politiche, gli standard e le direttive aziendali;
- non deve mai essere fatto per uno scopo che possa riflettersi negativamente sulla reputazione del datore di lavoro, o che possa comunque incidere negativamente sulla sua immagine;
- non deve interferire con il lavoro dei dipendenti, riducendone la produttività o la qualità, né con la fornitura di servizi ai clienti;
- non deve servire di supporto per lo svolgimento di attività diverse da quelle di UNITELMA SAPIENZA;
- non deve ostacolare l'accesso da parte del datore di lavoro alle informazioni e ai dati attinenti alla propria attività (ad esempio, attraverso l'apposizione di password ad archivi informatici ad iniziativa del dipendente).

Uso del ''sistema computer'' e altri *device*.

Con riferimento alla possibilità di utilizzare o memorizzare, anche in via provvisoria, sul proprio elaboratore elettronico file non aventi alcuna attinenza con la propria attività lavorativa, dovrai rispettare quanto già indicato precedentemente, ed in particolare:

- i file personali devono avere sempre un contenuto lecito e non contrario alle norme di legge e al buon costume;
- essi non devono rivelare le opinioni politiche, religiose, sindacali del dipendente, o comunque informazioni relative alla propria salute o vita sessuale;
- tali file devono quindi essere raggruppati in un'apposita cartella nominata in modo da evidenziare il carattere personale del suo contenuto;
- sui computer i dipendenti devono evitare di visionare film e altro in DVD, connettersi a siti web di canali televisivi che diffondano i loro contenuti in streaming, sia in genere il c.d. download di video leciti o illeciti (salvo ciò rientri nelle necessità lavorative).

Inoltre, dovrai sempre:

- astenerti dal modificare autonomamente le configurazioni impostate sul proprio elaboratore e dal manomettere, più in generale, lo strumento in dotazione;

- evitare di creare password di accesso a programmi o a dati senza l'autorizzazione specifica del responsabile della sicurezza informatica;
- astenerti dall'installare mezzi di comunicazione propri (come, ad esempio, il proprio cellulare come hotspot o, più in generale, qualsiasi altro device), e quindi realizzare autonomi collegamenti di accesso ad Internet, rispetto a quelli della rete aziendale;
- evitare di utilizzare strumenti software o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e documenti informatici;
- utilizzare i computer portatili aziendali ed eventuali ulteriori device, se in dotazione, rispettando le regole di cui sopra, e quindi applicando tutte le misure idonee atte a proteggerne il funzionamento ed i dati personali ivi contenuti.;
- astenerti da qualsiasi uso o possibile duplicazione di software non distribuiti ufficialmente, qualora tali comportamenti implichino una violazione della legge 22 aprile 1941 n. 633 sul diritto d'autore e sue integrazioni e modificazioni;
- informarti su tutte le restrizioni relative all'uso o alla duplicazione dei programmi per elaboratore in dotazione del datore, in quanto è di sua responsabilità il pieno rispetto del contratto di licenza di tali software;
- sottoporre al responsabile della sicurezza designato, la richiesta di poter utilizzare, per lo svolgimento delle proprie mansioni, software di pubblico dominio e i c.d. shareware, e quindi, più in generale, programmi diversi da quelli messi a disposizione dal datore di lavoro.

Data la facilità con cui attraverso programmi, allegati mail, file e documenti in generale, possono essere introdotti nel sistema informatico virus, malware o codice malevolo che possono mettere a repentaglio la sicurezza del sistema informatico e della sua rete LAN, sei tenuto a:

- a segnalare al responsabile per la sicurezza informatica il mancato utilizzo di un software antivirus sull'elaboratore che gli viene affidato prima di farne uso;
- ad evitare di scaricare sul proprio elaboratore elettronico file contenuti in allegati e-mail e/o in pagine web e/o in supporti di memoria di cui non sia certa provenienza e contenuto, e che quindi presentino rischi di pericolosità per il sistema informatico aziendale (nel caso ve ne sia la necessità, il lavoratore dovrà ottenere l'autorizzazione dal datore);
- a segnalare comunque qualsiasi anomalia riscontrata nell'uso dello strumento informatico.

In particolare, a livello esemplificativo e non esaustivo, dovrai:

- utilizzare gli strumenti messi a sua disposizione seguendo le regole di buona fede e correttezza, senza arrecare un danno reputazionale a UNITELMA SAPIENZA e per scopi esclusivamente legati all'attività di lavoro;
- custodire tali dotazioni con diligenza e correttezza;

- astenerti dal salvare sui dispositivi forniti informazioni di contenuto illecito o di carattere personale, e comunque astenersi dal porre in essere attività illegali tramite il cellulare o con l'utilizzo della SIM aziendale.

La password.

Le credenziali di autenticazione, composte dall'associazione di un "user-id" e una "password", sono un elemento fondamentale per proteggere gli accessi da parte di terzi ai sistemi informatici aziendali.
Sei tenuto, con riferimento alla componente segreta delle credenziali di autenticazione (la parola chiave), al rispetto delle seguenti regole:

- la *password* deve essere facile da ricordare e contemporaneamente difficile da indovinare, non deve contenere nomi o frasi comuni, né essere in alcun modo collegata alla vita privata (come, ad esempio, il nome o il cognome, proprio o di parenti, la targa dell'auto, la data di nascita, la città di residenza, ...);
- la *password* deve avere almeno 8 caratteri (tra cui numeri, caratteri speciali e maiuscola e minuscola);
- la *password* non può altresì contenere più di due caratteri consecutivi del nome completo dell'utente o del nome dell'account utente.
- la password, assegnata dal responsabile della sicurezza informatica contestualmente alla *user-id*, deve essere modificata al primo accesso da parte del dipendente;
- la *password* deve essere cambiata ogni 90 giorni;
- ogni nuova *password* deve altresì essere diversa delle ultime quattro utilizzate;
- la *password* deve essere mantenuta segreta: pertanto non deve essere rivelata né scritta o lasciata in posti dove potrebbe essere facilmente scoperta.

Navigazione web e gli altri servizi.

Per evitare di esporre a rischi il sistema informatico dell'azienda, per il corretto svolgimento dell'attività lavorativa, per tutelare i tuoi dati personali e per tutelare le informazioni relative all'azienda, è necessaria la collaborazione tra datore di lavoro e dipendente a cui, in base alle regole individuate nel presente Codice, non è consentito l'utilizzo del Web e dei suoi servizi per attività non connesse alle finalità lavorative. In particolare, non dovrai:

- navigare nei siti dai quali è possibile risalire alle sue opinioni politiche, religiose, sindacali, ad informazioni relative alla propria vita sessuale o comunque attinenti alla propria salute;
- eseguire transazioni finanziarie di ogni genere (ivi comprese le operazioni di c.d. *remote banking*) o acquisti on line, salvo che siano espressamente autorizzate, per la parte tecnologica, dal responsabile della sicurezza informatica;

- registrarti, e comunque partecipare, a siti, chat, *newsgroup*, *mailing list*, *forum*, *blog*, ..., ed in genere a social network, ad eccezione di quelli eventualmente creati e dedicati allo svolgimento dell'attività professionale, come meglio specificato nel paragrafo successivo;
- memorizzare sui *device* aziendali documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- realizzare operazioni in contrasto con l'attività lavorativa, o comunque commettere illeciti penali, come disciplinati dalle relative normative, quali, a titolo esemplificativo:
  - accesso abusivo ad un sistema informatico o telematico;
  - detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;
  - falsità in un documento informatico pubblico o privato;
  - truffe a danno di certificatori di firma elettronica;
  - danneggiamento o interruzione di sistemi informatici o telematici, e di informazioni, dati e programmi ad essi attinenti;
  - installazione di dispositivi o programmi informatici diretti a danneggiare o interrompere sistemi informatici o telematici;
  - intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
  - installazione di dispositivi o programmi informatici atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
  - frode informatica.

La posta elettronica.

L'account di posta aziendale, per la funzione che ricopre nel contesto lavorativo, deve essere consultabile dalla Società. L'eventuale accesso allo stesso, in uso al dipendente, effettuato dal datore di lavoro, o dai soggetti a ciò preposti, verrà svolto rispettando i principi di correttezza, pertinenza e non eccedenza, e la disciplina in materia di protezione dei dati personali, al fine di meglio tutelare la tua dignità e riservatezza.
Sei obbligato, durante tutto il rapporto di lavoro, a:

- utilizzare l'indirizzo di posta elettronica c.d. aziendale solo per corrispondenza attinente alla propria attività lavorativa, e mai personale;
- inserire, in calce ad ogni e-mail (o comunque verificare che sia già stato inserito in maniera automatica), l'indicazione della natura non personale, privata della stessa, e del fatto che le eventuali risposte del destinatario possano essere lette o comunque conosciute anche da altri all'interno della propria struttura lavorativa;
- nel caso in cui, per errore, pervenga sulla casella di posta aziendale un'e-mail personale, cancellarla immediatamente sia dal *client* di posta elettronica che dal web (direttamente o attraverso il responsabile della sicurezza informatica);

- non scaricare o salvare le e-mail di natura lavorativa che pervengano sulla casella di posta aziendale su computer differenti da quello aziendale: nel caso si renda necessario accedervi da un diverso elaboratore, dovrai soltanto visualizzarle via web, salvo diversa ed esplicita autorizzazione del datore;
- attivare, qualora sappia di dover usufruire delle ferie o debba lavorare fuori sede, apposite funzionalità di sistema che consentano di inviare automaticamente messaggi e-mail di risposta contenenti l'avviso generico dell'assenza del lavoratore, nonché indicare le coordinate di altro soggetto, o della competente struttura, per ricevere informazioni;
- astenerti dall'inviare con posta elettronica documenti di lavoro "strettamente riservati" se non con le opportune precauzioni (individuate insieme al responsabile della sicurezza informatica), in quanto tali messaggi potrebbero essere intercettati da estranei;
- non utilizzare l'indirizzo di posta elettronica aziendale per la partecipazione a *newsgroup*, e/o *forum*, e/o *mailing-list*, o simili, salvo diversa ed esplicita autorizzazione;
- non utilizzare l'indirizzo di posta elettronica aziendale per inviare in allegato file di contenuto illecito o comunque non attinente alla propria attività lavorativa;
- non utilizzare l'indirizzo di posta elettronica aziendale per inviare, reperire o archiviare messaggi molesti, minacciosi, offensivi, diffamatori, discriminatori per sesso, razza, lingua, religione, origine etnica e appartenenza sindacale e/o politica, o comunque osceni, e altre informazioni di tal genere;
- nel caso in cui venga autorizzata la consultazione di posta elettronica personale, quindi non aziendale, consultarla solamente via web, e le relative e-mail e/o allegati non possono essere scaricate e/o salvate sul computer aziendale, e comunque possono essere lette solo al di fuori dell'orario di lavoro.

Qualora tu decida di interrompere il rapporto di lavoro con UNITELMA SAPIENZA, tramite preavviso di 3 mesi (o altro termine stabilito nel contratto di lavoro), dovrai entro tale termine:

- eliminare eventuali informazioni di carattere personale conservate, contrariamente a quanto previsto dal presente Codice, nell'account aziendale;
- informare i clienti (con i quali si hanno contatti in relazione alle proprie mansioni di lavoro) fornendo le coordinate (es. indirizzo e-mail) di un altro soggetto preposto agli stessi compiti;
- inviare tutte le informazioni utili riguardo le pratiche aperte al soggetto designato da UNITELMA SAPIENZA.

Qualora, invece, il rapporto di lavoro si interrompa senza preavviso, dovrai immediatamente:

- eliminare eventuali informazioni di carattere personale conservate, contrariamente a quanto previsto dal presente Codice, nell'account aziendale;
- inviare tutte le informazioni utili riguardo le pratiche aperte ad un soggetto designato da UNITELMA SAPIENZA.

Sia nell'ipotesi di preavviso che nel caso di cessazione immediata del rapporto di collaborazione, devi essere consapevole che il Titolare procederà al reindirizzamento automatico delle mail ricevute sul tuo account inoltrandole al nuovo soggetto designato, portando a conoscenza del cliente l'avvenuto cambio di referente

I social network.

Nel caso in cui tu possegga dei social network di natura personale, dovrai astenerti:

- dall'utilizzare il social network durante l'orario di lavoro;
- dal pubblicare commenti o informazioni legate all'attività lavorativa;
- dal diffondere dati, comunicazioni o documenti di cui si è venuti a conoscenza nell'ambito del rapporto di lavoro;
- dal pubblicare, in ogni caso, contenuti che possano arrecare in generale nocumento a UNITELMA SAPIENZA.

Nel caso in cui tu sia un soggetto autorizzato all'uso del social network di UNITELMA SAPIENZA dovrai:

- custodire diligentemente le proprie credenziali di autenticazione al social network, che verranno fornite da UNITELMA SAPIENZA e quindi, non diffondere tali credenziali, né cederle a terzi;
- utilizzare il social network per finalità esclusivamente collegate alle attività di lavoro ed alle mansioni affidate dal datore, e dunque evitare di intrattenere comunicazioni che esulino dall'ambito della prestazione svolta;
- non pubblicare o trasmettere documentazione aziendale riservata;
- non pubblicare sul social network informazioni di carattere politico, religioso, sindacale, sessuale, riferite alla propria persona o a terzi;
- non scaricare né condividere file dal contenuto illecito;
- non utilizzare il social network per inviare comunicazioni offensive, diffamatorie o discriminatorie nei confronti di colleghi o terzi;
- in generale, non utilizzare il social network come strumento per la realizzazione di illeciti penalmente sanzionati dalle norme di legge.

Appendice 3

Dichiarazione di ricevuta e di presa visione e conoscenza

Via Nomentana, n. 373, 00162 ROMA
Tel. 06/86327973 - Fax 06/83390932 e-mail: *studiociacci@jei.it* - web-site: *http://www.jei.it*

Il Sottoscritto …… dichiara che in data ……. ha ricevuto da UNITELMA SAPIENZA il "Codice di deontologia e buona condotta per un corretto uso delle dotazioni informatiche".

Con la presente il sottoscritto si impegna a prendere visione del contenuto del suddetto documento ed a rispettare quanto in esso stabilito.

Firma

……