REGOLAMENTO
PRIVACY E SICUREZZA
AD USO DEI RESPONSABILI E DEGLI INCARICATI

APPROVATO CON
DELIBERA DEL CONSIGLIO DI AMMINISTRAZIONE DI DATA 03.05.2018

Livenza Tagliamento Acque S.p.A.

Sede Legale:
Piazza della Repubblica, n. 1
30026 PORTOGRUARO (VE)
web: **www.lta.it**

Sede Amministrativa:
Via Leonardo Zannier, n. 9
30025 FOSSALTA DI PORTOGRUARO (VE)
tel 0421 789055 - fax 0421 780150
info@lta.it
info@pec.lta.it

Sede Operativa:
Viale Trieste, n. 11
30020 ANNONE VENETO (VE)
tel 0422 760020 - fax 0421 769974
info@lta.it
info@pec.lta.it

Sede Operativa:
Via San Giacomo, n. 9
33070 BRUGNERA (PN)
tel 0434 1680050 - fax 0434 624235
info.brugnera@lta.it
info.brugnera@pec.lta.it

C.F. e P.IVA 04268260272 - N. Iscr. Registro Imprese di Venezia Rovigo Delta-Lagunare 04268260272 - R.E.A. VE N. 380371 - Capitale Sociale € 18.000.000,00 i.v.

INDICE

PREMESSA

Allo scopo di definire le norme di comportamento che gli Incaricati e i Responsabili devono rispettare nell'utilizzo degli strumenti messi a loro disposizione dall'Azienda, il Titolare del trattamento ha emanato il seguente *Documento*, affinché gli utenti evitino di porre in essere – anche inconsapevolmente – comportamenti incompatibili con la correttezza professionale richiesta, con il corretto svolgimento della prestazione lavorativa e con le regole sancite dal Regolamento Europeo 679/2016 in materia di protezione dei dati personali e dalla normativa vigente in materia.

Normativa di riferimento (Regolamento Europeo 679/2016)

TERMINI E DEFINIZIONI UTILI

DATO PERSONALE	At. 4, co. 1: "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;".	Quindi anche: · il Codice Fiscale, la Partita Iva; · i suoni, in caso di registrazione di voci di persone; · le immagini, video/fotoriprese; · i numeri delle utenze telefoniche fisse e mobili; · gli indirizzi e-mail. I dati di identificazione generali, anche indirettamente, della persona (es. le generalità… nome e cognome, indirizzo) sono da considerarsi dati personali "comuni".
DATO IDENTIFICATIVO	I dati personali che permettono l'identificazione diretta dell'interessato.	Il regolamento richiede che l'utilizzo di dati identificativi avvenga solo se necessario al perseguimento degli scopi del trattamento.
DATO ANONIMO	Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.	Non è dato anonimo il dato che viene criptato, poiché il sistema adottato ne consente la decriptazione e quindi l'identificazione.
DATO SENSIBILE	Art. 9, co. 1: "i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.".	I dati sensibili possono essere trattati solo previo consenso dell'interessato o negli altri casi tassativi previsti dall'art. 9. Con i dati giudiziari costituiscono il "nocciolo duro" della privacy, pertanto godono di una tutela maggiore e in quanto tali vanno custoditi e controllati con particolare attenzione. Nel Regolamento formalmente non è presente la definizione di dato sensibile, sostituita con quella di

		"categorie particolari di dati personali". Esempio: i documenti e certificati medico-sanitari, i documenti da cui si evince l'origine razziale o etnica, la devoluzione dell'8 per mille, le trattenute sindacali in busta paga, il casellario giudiziale, l'appartenenza a categorie di lavoro protette, il certificato di inidoneità al lavoro, le opinioni politiche o filosofiche, componenti biometriche (impronta digitale) a fini identificativi o di autenticazione, ecc.
DATO GIUDIZIARIO	Art. 10: "Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'art. 6, co. 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.".	La definizione è più generica rispetto al D.Lgs. 196/2003, ma riguarda sempre i dati inerenti il procedimento penale e non civile. Il loro trattamento è consentito su base legislativa nazionale o comunitaria.
VIOLAZIONE DEI DATI PERSONALI	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.	
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. Il titolare del trattamento è Livenza Tagliamento Acque S.p.a..	
RESPONSABILE DEL TRATTAMENTO	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo interno o esterno che tratta dati personali per conto del titolare del trattamento. E' nominato con atto scritto e si attiene alle istruzioni ricevute dal titolare.	
RESPONSABILE DELLA PROTEZIONE DEI DATI	E' il soggetto che coadiuva il titolare del trattamento nella sorveglianza del rispetto delle procedure aziendali in tema di protezione dei dati personali. Egli garantisce al titolare e ai suoi collaboratori la consulenza e la formazione in materia di protezione dei dati. Gli incaricati del trattamento e tutti i soggetti autorizzati a trattare dati possono fare riferimento ad egli per ogni questione inerente la privacy. In LTA il Responsabile della protezione dei dati designato è il Dott. Nicola Cignacco.	
INCARICATO DEL TRATTAMENTO	Anche se la definizione non è più presente nel nuovo testo regolamentare, si intende ancora la persona fisica o l'unità organizzativa autorizzata o istruita dal titolare o dal responsabile a compiere operazioni di trattamento sui dati personali.	
INTERESSATO	È il soggetto, persona fisica, cui si riferiscono i dati personali, cui sono riconosciuti i diritti di cui agli artt. 15 e seguenti del Regolamento. In LTA sono da considerarsi interessati: i clienti/utenti; i dipendenti/collaboratori, i fornitori.	

AMMINISTRATORE DI SISTEMA	O anche “servizio IT”. Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione dati o di sue componenti.
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*”.* Qualunque tipo di operazione sui dati, con e senza l’ausilio di strumenti elettronici, costituisce trattamento*.*
INFORMATIVA	Il titolare, anche attraverso i propri incaricati, deve fornire preventivamente all’interessato le informazioni di cui all’art. 13 del Regolamento circa la natura e le modalità del trattamento posto in essere, utilizzando i modelli predisposti dal titolare.
CONSENSO DELL’ INTERESSATO	Il consenso è la manifestazione di volontà che l’interessato dà circa l’utilizzo dei propri dati, pertanto ne costituisce necessario e preventivo presupposto l’informativa di cui all’art. 13. Se il trattamento riguarda dati sensibili o giudiziari, il consenso va espresso per iscritto. Sono previsti dalla Legge dei casi in cui è possibile effettuare il trattamento senza il consenso dell’interessato (ad es. per eseguire obblighi contrattuali o soddisfare richieste dell’interessato, anche in fase pre-contrattuale, come il caso dei fornitori).
COMUNICAZIONE	“Dare conoscenza dei dati personali a uno o più soggetti <u>determinati</u> (“destinatari”) diversi dall'interessato, dagli incaricati o dal responsabile, in qualunque forma, anche mediante la loro messa a disposizione o consultazione”.
DIFFUSIONE	O divulgazione: “Dare conoscenza dei dati personali a soggetti <u>indeterminati</u>, in qualunque forma, anche mediante la loro messa a disposizione o consultazione” (es. pubblicarli su internet).
NECESSITÁ	Uno dei principi fondamentali da rispettare è quello secondo cui non si devono trattare dati che non sono necessari al perseguimento delle finalità per cui sono utilizzati, perciò sono da evitare tutte le informazioni che non sono indispensabili alle mansioni lavorative. Idem i dati personali devono essere conservati per il tempo necessario, dopo di che, salvo obblighi di legge, essi vanno distrutti.
LICEITÁ E CORRETTEZZA	I dati devono essere trattati in modo lecito e corretto, ovvero secondo la legge ed osservando il principio della buona fede contrattuale e precontrattuale. La violazione di predetti principi può comportare conseguenze giuridiche sul piano civile, penale ed amministrativo.

INTRODUZIONE

Questo documento fornisce agli incaricati del trattamento una panoramica sulle responsabilità loro spettanti rispetto alla gestione ed allo sviluppo della sicurezza dell'informazione.
Nell'ambito informatico, il termine "sicurezza" si riferisce a tre aspetti distinti:

- **riservatezza** → prevenzione contro l'accesso non autorizzato alle informazioni;
- **integrità** → le informazioni non devono essere alterabili da incidenti o abusi;
- **disponibilità** → il sistema deve essere protetto da interruzioni impreviste.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi; misure soltanto tecniche, per quanto possano essere sofisticate, non saranno efficienti se non usate propriamente.
In particolare, le precauzioni di tipo tecnico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

1. Linee guida per la sicurezza

Utilizzate le chiavi
Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. Pertanto, chiudete a chiave l'ufficio alla fine della giornata e chiudete i documenti a chiave nei cassetti o negli armadi ogni volta che potete.

Conservate i supporti informatici in un luogo sicuro
Per i dischetti, o supporti di memorizzazione analoghi (es. le chiavette USB), si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni non sensibili, riponeteli sotto chiave non appena avete finito di usarli. Prima di smaltirli tra i rifiuti, anche se apparentemente non funzionanti, è opportuno distruggerli.

Utilizzate le password
Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso.
La password di accesso al computer impedisce l'utilizzo improprio della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio.
La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio.
La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.
La password del salvaschermo, infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di visualizzare il vostro lavoro.
Imparate a utilizzare questi quattro tipi fondamentali di password, e mantenete distinta almeno quella di tipo *a),* che può dover essere resa nota, almeno temporaneamente, ai tecnici incaricati dell'assistenza. Scegliete le password secondo le indicazioni della sezione successiva.

Attenzione alle stampe di documenti riservati
Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Distruggete personalmente le stampe

quando non servono più, magari utilizzando un distruggi-documenti. Non lasciate incustodito il fax quando è in una zona accessibile a terzi.

Non lasciate traccia dei dati riservati
Quando rimuovete un file, i dati non vengono effettivamente cancellati ma soltanto marcati come non utilizzati, e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati; solo l'utilizzo di un programma apposito garantisce che sul supporto non resti traccia dei dati precedenti. Nel dubbio, è sempre meglio usare un supporto nuovo.

Prestate attenzione all'utilizzo dei PC portatili
I PC portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido, e utilizzate una procedura di backup periodico.

Non fatevi spiare quando state digitando le password
Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura.

Custodite le password in un luogo sicuro
Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Seguite le procedure stabilite dal titolare del trattamento in merito alla politica di conservazione delle password (ad es. in busta chiusa da consegnare al Responsabile del trattamento o agli Amministratori di Sistema).

Non fate usare il vostro computer a personale esterno a meno di non essere sicuri della loro identità
Personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

Non installate programmi non autorizzati
Solo i programmi con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici, prima di installarli è necessario ottenere la necessaria preventiva autorizzazione da parte del Responsabile dell'Ufficio sistemi informatici.

Applicate con cura le linee guida per la prevenzione da infezioni di virus
La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.

Controllate la politica locale relativa ai backup
I vostri dati potrebbero essere gestiti da un *file server*, oppure essere gestiti in locale e trasferiti in un server solo al momento del backup. Verificate con il titolare locale la situazione e fate in modo che sia effettuato un salvataggio dei dati ad intervalli regolari.

Avvisate il titolare se ritenete che i dati siano stati violati
Allertate immediatamente il titolare e il Responsabile della protezione dei dati in caso di perdita o distruzione, anche accidentali, di dati personali, e in generale in tutti i caso in cui l'incaricato ragionevolmente ritenga che vi possa essere stata una violazione degli stessi (accessi indebiti, non autorizzati, ecc.).

2. Linee guida per la prevenzione dei virus

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

Come si trasmette un virus

A. Attraverso programmi provenienti da fonti non ufficiali.
B. Attraverso le macro dei programmi di automazione d'ufficio.
C. Attraverso allegati o link contenuti nelle e-mail.

Quando il rischio da virus si fa serio

A. Quando si installano programmi di provenienza dubbia.
B. Quando si copiano dati da dischetti non autorizzati.
C. Quando si scaricano dati o programmi da siti Internet sconosciuti o non attendibili.

Quali effetti ha un virus

A. Effetti sonori e messaggi sconosciuti appaiono sul video.
B. Nei menù appaiono funzioni extra finora non disponibili.
C. Le prestazioni del computer si rallentano inspiegabilmente.
D. Lo spazio disco residuo si riduce inspiegabilmente.
E. I file hanno un formato e un'estensione diversi dal solito e non si riescono ad aprire.

Come prevenire i virus

A. Usate soltanto programmi provenienti da fonti fidate. Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzate programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.
B. Assicuratevi che il vostro software antivirus sia aggiornato, anche utilizzando la procedura manuale di aggiornamento dal menù dei programmi.
C. Non aprite allegati o cliccare i link presenti all'interno di email sospette e o di dubbia provenienza (vedi avanti per rischio da ransomware).
D. Nel caso di individuazione di file infetti, l'utente è immediatamente avvisato dal software antivirus installato con messaggio a video che illustra le procedure da seguire per scongiurare il pericolo. In ogni caso contattare tempestivamente i responsabili del sistema informatico aziendale.

3. Linee guida per la scelta delle password

Il metodo più semplice per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

Cosa Fare

A. Usate password lunghe almeno otto caratteri con un misto di lettere, numeri o segni di interpunzione. La password non deve contenere riferimenti agevolmente riconducibili all'incaricato (es. nome, cognome e anno di nascita *mariorossi72*), per cui NON usate il Vostro nome utente; è la password più semplice da indovinare.

B. NON usate password che possano in qualche modo essere legate a Voi come, ad esempio, il Vostro nome, quello di Vostra moglie/marito, dei figli, date di nascita, numeri di telefono etc.
C. Cambiate la password a intervalli regolari. Questa va modificata almeno ogni sei mesi nel caso in cui si trattino dati personali, diversamente, se il trattamento investe dati sensibili e/o giudiziari, ogni tre mesi.
D. NON dite a nessuno la Vostra password. Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le Vostre risorse o possa farlo a Vostro nome. Un eventuale illecito commesso da altri con le vostre credenziali potrebbe essere addebitato a voi
E. NON scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
F. Quando immettete la password NON fate sbirciare a nessuno quello che state battendo sulla tastiera.

SEZIONE PRIMA

1. Utilizzo della posta elettronica (e-mail)

Per un corretto utilizzo degli indirizzi e-mail assegnati all'utente è necessario attenersi alle seguenti regole.

A. Le caselle di posta elettronica aziendale date in uso all'utente sono destinate ad un utilizzo tassativamente ed esclusivamente inerente all'attività lavorativa e **non devono essere utilizzate per scopi personali**.
B. Inoltre è fatto divieto di configurare all'interno del programma su pc di gestione della posta elettronica indirizzi personali non relativi ai domini di posta lavorativi quali, ad esempio, quelli forniti gratuitamente dai provider (@libero.it, @yahoo.com, @gmail.com, ecc.). Il divieto vale anche per i dispositivi mobili (smartphone e tablet aziendali).
C. L'utente non deve utilizzare l'indirizzo di posta elettronica per iscriversi a newsletter, mailing list, forum, chat, social network, ecc., salvo che questi servizi siano inerenti all'attività lavorativa; in caso di dubbio, l'utente deve rivolgersi al titolare del trattamento o al responsabile del sistema informatico per verificare la loro liceità.
D. L'utente deve utilizzare la posta elettronica in modo appropriato e consapevole.
    a. Non deve rispondere a messaggi indesiderati (spam) e non deve partecipare alle cosiddette "catene di Sant'Antonio", per non dare conferma (implicita) della validità dell'indirizzo di posta.
    b. Deve prestare attenzione al fenomeno del *phishing*, ossia una tecnica utilizzata per ottenere l'accesso ad informazioni personali e riservate con la finalità del furto di identità mediante l'utilizzo di messaggi di posta elettronica fasulli, opportunamente creati per apparire autentici (ad esempio e-mail artatamente contraffatte per sembrare comunicazioni ufficiali di Istituti Bancari, siti istituzionali, ecc.). Con tali messaggi viene richiesto l'accesso a siti web, all'interno dei quali il mittente (che tenta la truffa) impersona una azienda/ente che chiede al destinatario di inserire i suoi dati di accesso a scopo di verifica, in modo da carpirli ed utilizzarli successivamente in modo fraudolento. La pagina web a cui si è inviati dal link indicato dal mittente della e-mail è identica a quella dell'azienda ma non è realmente quella corretta. In tal modo, se non si presta attenzione all'indirizzo indicato nel browser internet, si è portati a credere, a colpo d'occhio, di essere realmente nella pagina web corretta. In realtà si sta utilizzando una pagina web costruita *ad hoc* per scopi fraudolenti. Grazie a questi messaggi, l'utente è ingannato e portato a rivelare dati importanti, come numero di conto corrente, nome utente e password, numero di carta di credito ecc.. In caso di dubbio sul comportamento da tenere, va contattato il referente informatico aziendale.
    c. Stare molto attenti ad aprire documenti allegati alle e-mail apparentemente provenienti da fonti sicure (ad esempio Agenzia Entrate, Enel, Tribunali, o anche da colleghi di lavoro) oppure a cliccare i link (o collegamenti ipertestuali) contenuti nelle predette mail. C'è il rischio infatti che il computer e la rete informatica possano venire infettati da **virus** molto pericolosi (ad es. il *cryptolocker* della famiglia dei cd. *ransomware*) che criptano tutti i dati con la richiesta di un vero e proprio riscatto per ottenere la disponibilità degli stessi. Per riconoscere se il mittente è veramente quello che sembra è sufficiente leggere bene l'indirizzo di provenienza (verificare quindi eventuali errori di battitura o nomi apparentemente sospetti), oppure passando il cursore del mouse sopra l'indirizzo e-mail (comparirà l'indirizzo esatto). Si ricorda infatti che è molto facile camuffare o celare L'indirizzo del mittente per confondere il destinatario.

d. All'indirizzo web https://www.certnazionale.it/documenti/2016/05/05/ransomware-rischi-e-azioni-di-prevenzione/ è possibile consultare una guida utile per la prevenzione dai rischi ***ransomware***. Se avete dei dubbi consultate il titolare prima di procedere.

Il titolare del trattamento rende comunque noto che, in caso di assenza improvvisa o prolungata dell'utente e per improrogabili necessità legate all'attività lavorativa, qualora si debba conoscere il contenuto dei messaggi di posta elettronica, il datore di lavoro potrà accedere alla posta elettronica del singolo utente avvalendosi dell'ausilio dell'Amministratore di Sistema. Proprio per questo motivo, al fine di non ledere il diritto alla riservatezza e segretezza della corrispondenza elettronica, gli utenti non dovranno utilizzare la caselle di posta elettronica per fini che esulano dal contesto lavorativo. Di dette operazioni ne sarà dato avviso tempestivo all'utente.

I messaggi di posta elettronica sono conservati sui server aziendali per sei mesi, dopo di che vengono cancellati. I file di log degli accessi, invece sono conservati per 30 giorni.

Gli account di posta dei dipendenti cessati dal servizio vengono automaticamente cancellati dopo sette giorni dall'interruzione del rapporto lavorativo, ad eccezione dei messaggi di posta elettronica a contenuto e rilevanza giuridica e commerciale che devono essere conservati per dieci anni. Si tratta infatti di documenti informatici che, in quanto corrispondenza, devono essere conservati secondo le prescrizioni dettate dall'art. 2214 del Codice civile, anche a fini fiscali secondo l'art. 22 del DPR 600/1973.

Prima della cessazione del rapporto con LTA, l'assegnatario della casella di posta elettronica deve trasmettere al proprio superiore gerarchico le e-mail rilevanti per il prosieguo dell'attività di LTA e, per ragioni di operatività, deve attivare sul suo account di posta elettronica un messaggio automatico – attivo fino alla soppressione dell'account – che segnala al mittente il reindirizzamento dell'e-mail ad altro soggetto o ufficio avvisandolo al contempo dell'imminente cancellazione dell'account aziendale.

Qualora l'utente non provveda autonomamente ad effettuare la suddetta operazione di avviso dell'imminente soppressione, vi provvederà il Servizio IT di LTA senza che sia necessario accedere alla casella di posta.

Inoltre, in caso di assenza programmata (ad es. ferie) l'utente deve impostare un messaggio di risposta automatica con cui invita il mittente a contattare un ufficio diverso.

2. Utilizzo dei computer e della rete internet

La strumentazione, intesa come insieme di hardware e software messa a disposizione degli utenti, deve essere utilizzata in modo conforme ed esclusivamente per lo svolgimento delle mansioni cui ogni incaricato è preposto: la strumentazione **non deve essere utilizzata per scopi personali**.

La navigazione in internet è consentita limitatamente all'utilizzo pertinente ed indispensabile allo svolgimento delle mansioni di ciascun lavoratore, essendo espressamente vietato ogni altro utilizzo (quali la visione di siti non pertinenti, l'*upload* o il *download* di *files*, l'uso di servizi di rete con finalità ludiche o estranee all'attività). Eventuali deroghe o eccezioni saranno rese note a tutto il personale.

L'utente non deve utilizzare apparecchiature non consentite o per cui egli non è autorizzato. In particolare, l'utilizzo di modem e di collegamenti wireless non criptati su postazioni di lavoro collegate alla rete di ufficio offre una porta d'accesso dall'esterno non solo al computer dell'utente ma a tutta la rete di cui esso fa parte, con ripercussioni negative sulla sicurezza dell'intera rete aziendale. E' quindi vietato l'uso di modem, chiavette e di collegamenti wireless o bluetooth – anche se criptati – all'interno della rete locale.

Ugualmente è fatto divieto all'utente di installare programmi non autorizzati. Oltre alla possibilità di trasferire involontariamente un virus o di introdurre un cosiddetto "cavallo di troia", va ricordato che la maggior parte dei programmi sono protetti da copyright, per cui la loro installazione può essere illegale. E' vietato scaricare per qualsiasi finalità, anche connesse con l'attività lavorativa, programmi reperiti in rete (internet) o da qualunque altra sorgente esterna salvo espressa

autorizzazione del titolare. Peraltro, si ricorda che ai sensi della legge sul diritto d'autore n. 633/41 e s.m.i. assumono rilevanza penale le condotte consistenti nell'illecita duplicazione, riproduzione, condivisione e divulgazione di software e/o materiale (audio e video) protetto da *copyright*.
E' vietato salvare documenti personali – o che comunque non abbiano attinenza con le mansioni svolte – negli spazi di archiviazione condivisa della rete aziendale.
I file di log vengono conservati sui server aziendali per 30 giorni, dopo di che vengono cancellati, salvo diverso ordine da parte dell'Autorità giudiziaria. A questi dati vi possono accedere, per finalità di operatività, sicurezza, manutenzione del sistema informatico, e nel caso di controlli disposti dall'azienda o dall'Autorità giudiziaria, gli Amministratori di Sistema di LTA.

3. Utilizzo della rete Wi-Fi aziendale

LTA ha predisposto presso ogni sede aziendale (Annone Veneto e le sedi amministrativa e commerciale di Fossalta di Portogruaro e Brugnera) un'apposita rete wireless. Tale tecnologia consente di fruire della connettività internet e di accedere alla rete aziendale senza essere collegati via cavo (wireless significa appunto "senza cavo"). Le credenziali di accesso che sono fornite consentono l'accesso alla rete per un tempo illimitato, ma possono essere utilizzate per un solo dispositivo. Pertanto le regole contenute nel presente Regolamento valgono anche nel caso di utilizzo della rete wireless aziendale. Tuttavia si forniscono le seguenti ulteriori istruzioni cui ciascun incaricato dovrà attenersi.

A. È vietato cedere, anche solo temporaneamente, il proprio codice utente e la propria password. L'utente intestatario verrà considerato responsabile di qualunque atto illecito perpetrato con quell'account.
B. È vietato utilizzare servizi o risorse di Rete, collegare apparecchiature o servizi o software alla Rete, diffondere virus, malware o altri programmi in un modo che danneggi, molesti o perturbi le attività di altre persone, utenti o i servizi disponibili sulla Rete.
C. È vietato creare o trasmettere qualunque immagine, dato o altro materiale offensivo, diffamatorio, osceno, indecente, o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza, le opinioni politiche o il credo.
D. È vietato trasmettere materiale commerciale e/o pubblicitario non richiesto ("spamming"), nonché permettere che le proprie risorse siano utilizzate da terzi per questa attività.
E. È vietato danneggiare, distruggere, cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti, compresa l'intercettazione o la diffusione di password, chiavi crittografiche riservate e ogni altro "dato personale" come definito dalle leggi per la protezione della privacy.
F. Tutti gli utenti che accedono alla Rete sono riconosciuti ed identificati. Inoltre tutte le attività sono registrate su appositi file log che saranno conservati per almeno un anno e potranno essere controllati dal personale autorizzato (Amministratore di Sistema) nel caso di uso illecito della Rete.

4. Utilizzo dei dispositivi mobili (smartphone/tablet)

I dispositivi mobili (smartphone/tablet) sono affidati in dotazione ai dipendenti esclusivamente ad uso lavorativo. In generale, detti dispositivi non possono essere ceduti né fatti utilizzare a terzi.
Il Servizio Informatico dell'azienda è stato preposto da LTA alle attività di configurazione, manutenzione e aggiornamento delle componenti software degli smartphone/tablet aziendali, pertanto, ove al dipendente utilizzatore sia richiesto di consegnare il dispositivo per le suddette finalità, egli è tenuto a fornire detto dispositivo consegnandolo al personale del Servizio Informatico.

In ragione della destinazione esclusivamente lavorativa dei dispositivi affidati ai dipendenti, i soggetti affidatari devono osservare scrupolosamente le seguenti regole di comportamento e di utilizzo dei dispositivi medesimi.

A. Non è consentito rimuovere la scheda SIM aziendale dal relativo dispositivo originariamente abbinato (per farne uso su un altro).
B. Non è consentito modificare le caratteristiche hardware e software impostate sul dispositivo.
C. Non è consentita l'installazione di programmi diversi da quelli configurati dall'azienda.
D. Non è consentita la riproduzione, la duplicazione, il salvataggio o lo scarico (cd. download o file sharing) di programmi o file di ogni tipo (testo, immagini, video, audio, eseguibili) in violazione delle norme sul diritto d'autore, anche ai sensi della Legge n. 633/1941 e della Legge n. 128 del 21 maggio 2004.
E. Non è consentito l'uso di qualsiasi dispositivo esterno collegabile al telefono, se non quelli aziendali o quelli autorizzati.
F. L'utilizzatore che abbia necessità di apportare modifiche software o hardware al telefono in dotazione, installando nuovi programmi o dispositivi, deve farne preventiva richiesta al Servizio Informatico.
G. E' vietato salvare documenti personali – o che comunque non abbiano attinenza con le mansioni svolte – nella memoria fisica del dispositivo e negli spazi di archiviazione condivisa della rete aziendale.

5. Furto, guasto, cessazione dell'attività e della responsabilità dell'utilizzatore

Alcune indicazioni operative.

A. In caso di smarrimento o di furto dello smartphone/tablet l'utilizzatore è tenuto a sporgere immediata denuncia alle autorità competenti (Ufficio di Polizia o della località ove si verifica tale situazione) e a darne tempestiva comunicazione scritta alla Servizio IT. Nella comunicazione dovrà essere indicato in particolare il numero telefonico abbinato al cellulare al fine di consentire l'operazione di blocco immediato della scheda SIM e/o del cellulare.
B. A seguito della segnalazione della denuncia di smarrimento/furto si provvederà all'automatica sostituzione dello smartphone/tablet, nei tempi e con le modalità stabilite.
C. Il Servizio IT si riserva inoltre la facoltà di revocare o sospendere l'assegnazione delle apparecchiature di telefonia mobile per mancato utilizzo, per esigenze aziendali e comunque per qualsiasi altra motivazione, con obbligo per l'utilizzatore di immediata riconsegna del bene al Servizio IT.
D. In caso di ripetuti smarrimenti, furti o quant'altro, l'assegnazione delle apparecchiature di telefonia mobile sarà revocata.
E. In caso di cessazione dell'attività istituzionale, a qualsiasi titolo, il telefono con relativa SIM devono essere riconsegnate al referente della telefonia mobile.
F. In caso di guasti o malfunzionamenti, l'utilizzatore dovrà rivolgersi al Servizio IT a cui è demandata la relativa gestione in queste circostanze.
G. In caso di furto o smarrimento o danneggiamento dei telefoni, l'utilizzatore deve dare tempestiva comunicazione al Servizio IT, rimanendo a disposizione nel caso sia necessario denunciare l'accaduto all'Autorità preposta.

Al di fuori dei casi di fisiologica usura, dopo il primo evento (furto e rottura accidentale dovuti a incuria), all'utilizzatore verranno trattenuti in busta paga € 100,00, a titolo di risarcimento, quale costo simbolico per la riparazione o la sostituzione dello smartphone/tablet. Per i semplici cellulari, l'importo trattenuto in busta paga sarà pari ad € 30,00.

6. Dati di traffico e tabulati telefonici

Si informa che i sistemi delle compagnie telefoniche registrano per obbligo di legge le connessioni, ovvero tengono traccia dell'ora, del telefono richiedente e della risorsa richiesta.
I dati di traffico acquisiti dal sistema di telefonia e comunicati a LTA sono utili per la validazione dei prospetti di consumo che le compagnie telefoniche addebitano, sulla base dei tabulati telefonici da esse riscontrati; pertanto l'operazione di trattamento dei dati di traffico mira principalmente a verificare la sussistenza e la veridicità dei conti telefonici.
Potrebbe emergere dall'analisi primaria un interesse ad approfondire la genesi dei costi ed eventualmente a verificare il corretto utilizzo dei telefoni aziendali. Pertanto, è facoltà del Servizio IT effettuare controlli mirati all'individuazione di condotte illecite o vietate, ricorrendo sia ai tabulati telefonici, sia ai dati di traffico registrati dal sistema di telefonia interno, mediante operazioni di analisi, selezione e raffronto.
Tali informazioni verranno conservate da LTA per un periodo non eccedente rispetto agli scopi per cui sono state fatte oggetto di trattamento.

7. Modalità e procedure relative ai controlli sull'utilizzazione degli strumenti di telefonia mobile aziendale

Poiché in caso di violazioni contrattuali e giuridiche sia l'azienda che il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'azienda verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. Ai sensi dell'art. 13 del Regolamento europeo 679/2016, in conformità a quanto disposto anche dal Provvedimento n. 13 del 1° marzo 2007 dell'Autorità Garante per la privacy, si ritiene necessario informare che il Servizio IT, effettua un monitoraggio periodico dell'hardware e del software installato nei cellulari secondo le modalità indicate nel presente Regolamento.

8. Assenza/impedimento dell'utente e necessità di accedere ai dati

In caso di prolungata assenza o impedimento dell'incaricato (malattia, ferie, allontanamento dal posto di lavoro, ecc.) che renda indispensabile e indifferibile intervenire sul suo strumento elettronico (PC/Notebook) per esclusive necessità di operatività e/o di sicurezza del sistema, il titolare del trattamento, tramite il proprio Amministratore di Sistema interno (o A.d.S.), potrà accedere allo strumento elettronico in dotazione al singolo utente. In tale evenienza l'A.d.s. sostituirà la password impostata dall'utente con un'altra, per consentire l'accesso ai dati o agli strumenti necessari per le finalità sopra indicate. Dell'operazione sarà data tempestiva notizia scritta all'incaricato (anche via e-mail), comunicandogli la nuova password temporanea. L'utente, al primo accesso successivo, dovrà modificare la password temporanea e sostituirla con una propria secondo le regole sopra illustrate.

9. Controlli sull'uso degli strumenti elettronici

Il Titolare, per garantire la funzionalità e la sicurezza del sistema informatico, si riserva di effettuare verifiche periodiche sull'integrità del sistema informatico e, indirettamente, sull'osservanza delle regole contenute nel presente Regolamento.
I controlli verranno effettuati dall'Amministratore di Sistema appositamente preposto, dietro indicazione del titolare. I controlli sono di regola generici e non avvengono su base individuale. Qualora venga rilevata un'anomalia nelle attività di trattamento il titolare agirà di conseguenza

emanando una circolare interna generica con cui richiamerà al rispetto di predette regole tutti gli incaricati.
Se il comportamento anomalo dovesse persistere il titolare prenderà i dovuti provvedimenti, nel rispetto della Disciplina rilevante in tema di protezione dei dati personali nonché di quanto previsto dal CCNL e dalla normativa vigente applicabile, potendosi perciò procedere con controlli più mirati all'individuazione degli elementi o dei comportamenti pericolosi per l'integrità del sistema informatico.
L'Azienda, attraverso il proprio Servizio Informatico, effettua un monitoraggio periodico dell'hardware e del software installato nei computer e nei telefoni aziendali.
Tale operazione viene effettuata in modo completamente automatico per le macchine in rete ed in modo semiautomatico per le macchine stand-alone, mediante l'utilizzo di apposito software installato o da installare in ogni dispositivo aziendale.
Il monitoraggio, necessario per finalità di sicurezza ed organizzative (inventario del parco macchine e contabilità delle licenze d'uso dei software), non coinvolge in alcun modo i dati personali e i documenti presenti sui dispositivi fissi e mobili.
Si ricorda, infatti, che l'inosservanza delle regole qui illustrate può pregiudicare seriamente la sicurezza dei dati e delle informazioni contenute nel sistema informatico aziendale, autentico ed imprescindibile patrimonio dell'Azienda.

10. Utilizzo di PC portatili

L'utente è responsabile del PC portatile assegnatogli dal responsabile dei sistemi informatici e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
I PC portatili utilizzati all'esterno (convegni, trasferte, ispezioni, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.

SEZIONE II

1. Regole ulteriori per il trattamento dei dati con l'ausilio degli strumenti informatici

A. La dotazione hardware e software è quindi quella configurata su ciascun pc a cura del Titolare. Ogni modifica deve essergli preventivamente richiesta e da lui autorizzata.
B. Non lasciare il computer acceso se ci si assenta per un periodo più o meno lungo; potrebbe restare a disposizione di terzi non autorizzati. Se possibile utilizzate il blocco automatico con screensaver e password di ripristino.
C. Assicuratevi di distruggere irreversibilmente i supporti elettronici/informatici che contengono dati personali (e soprattutto sensibili o giudiziari) prima di gettarli nei rifiuti.

2. Regole ulteriori per il trattamento dei dati senza l'ausilio di strumenti informatici

A. Riponete i documenti cartacei al loro posto, o in altro luogo idoneo, al termine dell'orario di lavoro.
B. Chiudete a chiave armadi e cassetti ogni volta che potete, specialmente per le stanze e gli archivi prossimi alle zone di attesa di terzi.
C. *Non lasciare documenti sulla scrivania*. Non lasciare documenti, lettere, appunti sopra la scrivania quando vi allontanate dalla postazione di lavoro. In particolare non lasciate sul tavolo materiali che non siano inerenti il servizio che state svolgendo in quel momento, soprattutto se avete mansioni di *front office* a contatto con terzi.
D. Assicuratevi di distruggere i documenti cartacei che contengono dati personali (e soprattutto sensibili o giudiziari) prima di gettarli nei rifiuti.
E. Non comunicare a nessun soggetto non specificatamente autorizzato, o della cui identità non siete certi, i dati personali comuni, sensibili, giudiziari e/o altri dati, elementi, informazioni dei quali venite a conoscenza nell'esercizio delle vostre funzioni e mansioni. In caso di dubbio accertarsi sempre se il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli.
F. Non portare via dall'ufficio documenti o copie di documenti (cartacei e/o elettronici) se non per il normale svolgimento delle mansioni di lavoro o se richiestovi dal titolare o dal responsabile del trattamento.
G. Non comunicate alla stampa giornalistica e/o televisiva notizie, fatti o informazioni di cui venite a conoscenza nello svolgimento della vostra attività lavorativa presso il titolare, salvo non abbiate specifica autorizzazione o delega a farlo.

3. Diritti degli interessati e diritto di accesso

Gli artt. 15 e seguenti del Regolamento UE 679/2016 prevedono che tutti i soggetti interessati (in particolare i clienti dell'azienda) possano esercitare nei confronti del titolare i diritti che la Legge riserva loro, e segnatamente:
Art. 15. *Diritto di accesso dell'interessato.*
Art. 16. *Diritto di rettifica.*
Art. 17. *Diritto alla cancellazione («diritto all'oblio»).*
Art. 18. *Diritto di limitazione di trattamento.*
Art. 20. *Diritto alla portabilità dei dati.*
Art. 21. *Diritto di opposizione.*

Dal momento che tali diritti possono essere fatti valere nei confronti del titolare del trattamento o del responsabile del trattamento, senza particolari formalità (quindi sia oralmente che per iscritto), anche attraverso i suoi incaricati, si raccomanda, nell'ipotesi appena illustrata, di avvertire immediatamente il titolare o il responsabile del trattamento.
Nel caso di istanza scritta, infatti, i tempi di riscontro sono relativamente brevi. Recita l'art. 12: "*Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi* ***entro un mese dal ricevimento della richiesta*** *stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste*".

4. Attività di marketing o promozione commerciale

Per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è necessario il consenso del soggetto destinatario dei messaggi.
Un imprescindibile obbligo in capo al titolare del trattamento è quello del previo rilascio ai destinatari delle comunicazioni promozionali dell'informativa disciplinata dall'art. 13 del Regolamento, al fine di assicurare un'informazione chiara e completa, dunque adeguata, relativamente al trattamento dei loro dati, nonché un eventuale consenso al medesimo che sia effettivamente consapevole.
Pertanto, l'interessato o la persona presso la quale sono raccolti i dati personali deve essere previamente informato oralmente o per iscritto riguardo a una serie di elementi obbligatori e indefettibili. Fra questi, vanno specificate le modalità che saranno eventualmente utilizzate per il trattamento dati, ad es. telefonate automatizzate e modalità assimilate (quali fax, e-mail, sms, mms), oltre che quelle tradizionali come posta cartacea e telefonate con operatore, nonché le finalità del trattamento stesso (ad esempio, ricerca statistica, marketing o profilazione).
E' considerato legittimo interesse del titolare contattare i propri clienti per fini di marketing relativamente a proprie attività o servizi attinenti, purché tale attività non prevalga i diritti e le libertà dell'interessato e gli sia sempre data la possibilità di rifiutare invii successivi.

Per ogni altra informazione o delucidazione in merito al comportamento da tenersi o alle operazioni da effettuarsi è necessario rivolgersi al Titolare del trattamento oppure ai dirigenti responsabili.

SI RINGRAZIA PER LA COLLABORAZIONE.