REGOLAMENTO
PRIVACY E SICUREZZA
AD USO DEI RESPONSABILI E DEGLI INCARICATI

DATA EMISSIONE:	Approvato con Delibera del Consiglio di Amministrazione di data 03.05.2018.
AGGIORNAMENTO:	10.05.2022
AGGIORNAMENTO	04.04.2023

Livenza Tagliamento Acque S.p.A.
Partita IVA, Codice Fiscale e Numero iscrizione Registro Imprese di Venezia Rovigo: 04268260272
Numero R.E.A. VE: 380371
Capitale sociale i.v. € 18.000.000

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

Uffici Amministrativi:
Via Cornia, n. 1/B
33079 SESTO AL REGHENA (PN)
tel. 0434 1854700
info@lta.it
info@pec.lta.it

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

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 e D.Lgs. 196/2003)

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	Cd. "Data breach". 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. Consultate e osservate la policy aziendale sul data breach (Allegato n. 1 al presente Regolamento).	
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 è tenuto a garantire anche l'adeguata sicurezza dei dati personali con misure tecniche ed organizzative idonee rispetto ai rischi rilevati. Il Titolare deve garantire e tutelare i diritti degli interessati. 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 (esterno) che tratta dati personali per conto del Titolare del trattamento. E' nominato con atto scritto e si attiene alle istruzioni ricevute dal Titolare.	
REFERENTE INTERNO PRIVACY	LTA ha designato un Referente interno quale Responsabile della privacy. Tale figura è identificata nel **Dott. Nicola Cignacco** al quale tutti i dipendenti e collaboratori incaricati devono riferirsi per ogni segnalazione, dubbio o questione riguardante il trattamento dei dati personali.	
RESPONSABILE DELLA PROTEZIONE DEI DATI	E' il soggetto che assieme al Referente interno 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. Il Responsabile della protezione dei dati è contattabile all'indirizzo: dpo@lta.it.	
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	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. Nel presente documento la figura è definita anche "Responsabile dell'ufficio dei Servizi Informatici" e compone l'organismo interno definito anche "Servizio IT". Il Servizio IT è rappresentato dal team informatico aziendale talvolta coadiuvato, se necessario, da consulenti specialisti esterni (ad es. sistemisti). Questo organo è deputato ad effettuare i controlli sull'integrità del sistema informatico aziendale con le modalità illustrate nel presente documento e tutte le altre attività a rilievo informatico elencate di seguito.
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.

LTA LIVENZA TAGLIAMENTO ACQUE

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 casi in cui l'incaricato ragionevolmente ritenga che vi possa essere stata una violazione degli stessi (accessi indebiti, non autorizzati, ecc.).
I comportamenti da porre in essere in caso di violazione di dati (c.d. data breach) sono descritti nella apposita policy aziendale, cui integralmente si rimanda.

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 maiuscole e minuscole, numeri e segni di interpunzione/caratteri speciali (~!@#$%^&*-+='|\() {} []:;"' <>,.?/).
B. 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.
C. 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.
D. 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.

E. 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
F. NON scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
G. 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. È vietato configurare l'email aziendale su dispositivi fissi e mobili privati ed è parimenti vietato memorizzare all'interno dei dispositivi personali le credenziali di accesso agli strumenti di lavoro e risorse aziendali. Se intendete operare in tal senso diventate autonomamente responsabili in caso di perdita, utilizzo scorretto, ecc. pertanto si ricorda che tale impostazione non è condivisa dall'azienda.
E. È vietato copiare o trasferire, in tutto o in parte, la corrispondenza elettronica aziendale su dispositivi o sistemi esterni alla struttura del Titolare. In particolare non è consentito inoltrare i messaggi di posta elettronica aziendale a indirizzi email esterni ai domini di posta elettronica diversi da quelli di LTA.
F. Prestare la massima attenzione in fase di invio di email ad una pluralità di soggetti, avendo cura di evitare che gli indirizzi utilizzati siano visibili a tutti i destinatari. Si ricorda, infatti, che l'invio massivo di un messaggio con gli indirizzi dei destinatari in chiaro, costituisce ai sensi della normativa una divulgazione indebita di dati personali. Un suggerimento: quando si compone una mail l'ultima cosa che va scritta è l'indirizzo del destinatario. In questo modo si mitiga il rischio di inviare ad esempio un messaggio non completo o mancante di un allegato (oppure, nel caso di una mail "inoltrato", di diffondere parti del messaggio non opportune). Per invii di mail a più destinatari (per fare in modo che gli stessi non conoscano gli indirizzi/i nomi degli altri) utilizzare la funzione "copia conoscenza nascosta" (cd. "ccn") indicando come destinatario principale se stessi.
G. La stessa accortezza nella verifica della corretta compilazione dei form di invio va prestata comunque in caso di invio di comunicazioni riservate o dal contenuto personale.
H. 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. Sul sito https://www.csirt.gov.it/ sono contenute diverse informazioni sui rischi ***ransomware***. Se avete dei dubbi consultate il titolare prima di procedere.

1.1 Accesso alla casella di posta elettronica

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 casella di posta elettronica per fini che esulano dal contesto lavorativo. Di dette operazioni sull'account aziendale in uso al dipendente ne sarà dato tempestivo avviso all'utente stesso.

1.2 Conservazione dei messaggi di posta elettronica

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.

1.3 Chiusura della casella e-mail aziendale

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. È 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. È 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*.
Non è consentito utilizzare/installare/depositare (nemmeno temporaneamente o tramite versioni portable) strumenti per comunicazioni/navigazione in modalità onion routing, tipo Tor Browser o estensioni per navigazione onion routing per i vari Browser. (Chrome - Mozilla Firefox - Edge - Safari - Opera - UC ecc..). Il divieto è esteso a tutti i dispositivi aziendali (Computer Desktop e Notebook/Tablet/Smartphone) e ai dispositivi privati/personali ai quali è stato concesso l'accesso alla rete aziendale via cavo Lan o wifi o mediante connessione con client Vpn alle rete aziendale (Smart Working o altre necessità).
È 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, Sesto al Reghena, 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 e 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. È 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 dispositivi mobili aziendali 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 del trattamento dei dati, 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.
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 Referente interno di LTA – dott. Nicola Cignacco – e il Responsabile della protezione dei dati e di osservare la procedura prevista dall'Allegato n. 2 al presente Regolamento.

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.
Ogni Incaricato deve gestire correttamente le preferenze espresse dai soggetti interessati; in particolare, nei casi in cui un soggetto manifesti l'opposizione a ricevere comunicazioni commerciali o pubblicitarie, la sua preferenza deve essere immediatamente annotata e processata a livello interno per evitare nuovi invii al medesimo, annotandolo all'interno del gestionale aziendale e nei propri documenti di lavoro. Le informazioni sui consensi degli interessati devono essere condivise tra gli appartenenti alla stessa unità organizzativa affinché non ci siano discostamenti nella prassi aziendale.

SEZIONE III

1. Formazione

Periodicamente (e comunque non oltre un anno dalla presa in servizio), il referente interno privacy, in collaborazione con il DPO, organizza per i nuovi assunti una formazione sui fondamenti del Regolamento (UE) 2016/679 e sugli aspetti specifici riguardanti le procedure adottate in seno alla Società.
La formazione si conclude con una verifica dell'apprendimento e può essere anche fornita attraverso video corsi.
Il referente interno tiene traccia della partecipazione di ciascun dipendente alle iniziative formative proposte.
Un aggiornamento potrà essere proposto a tutto il personale in caso di significative intervenute novità normative o su sollecitazione dei Responsabili per la trattazione di problematiche specifiche.

Per ogni altra informazione o delucidazione in merito al comportamento da tenersi o alle operazioni da effettuarsi è necessario rivolgersi al Servizio IT e al Referente interno Dott. Nicola Cignacco, anche con il supporto del Responsabile della protezione dei dati.

SI RINGRAZIA PER LA COLLABORAZIONE.

ALLEGATO N. 1
POLICY PER LA GESTIONE DEL DATA BREACH

Livenza Tagliamento Acque S.p.A.
Partita IVA, Codice Fiscale e Numero iscrizione Registro Imprese di Venezia Rovigo: 04268260272
Numero R.E.A. VE: 380371
Capitale sociale i.v. € 18.000.000

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

Uffici Amministrativi:
Via Cornia, n. 1/B
33079 SESTO AL REGHENA (PN)
tel. 0434 1854700
info@lta.it
info@pec.lta.it

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

INDICE

PREMESSA

1. Definizione di Data Breach (violazione di dati personali)

Per data Breach si intende una 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 (art. 4, par.12 GDPR).
Distruzione: situazione nella quale il dato non esiste più o non esiste più in una forma che lo renda utilizzabile dal titolare del trattamento.
Modifica: situazione nella quale il dato personale è stato alterato, corrotto o non è più completo.
Perdita: situazione nella quale il dato personale può esistere ancora, ma il titolare del trattamento ha perso il controllo sullo stesso; l'accesso al dato o il dato non è più in suo possesso.
Divulgazione non autorizzata / illegale: situazione nella quale il dato è stato divulgato a destinatari che non erano autorizzati a riceverlo o ad averne accesso; qualunque altro trattamento in violazione del GDPR.

2. Individuazione di un Data Breach

Di seguito si indicano alcuni esempi, senza pretesa di esaustività, di Data Breach al fine di aiutare i dipendenti a riconoscere le situazioni che necessitano di essere prontamente segnalate:

- accesso da parte di terzi non autorizzati (ad esempio, un attacco ransomware che comporta la crittografia dei dati e non è disponibile un backup degli stessi);
- azione deliberata o accidentale (o inerzia) da parte del Titolare o del Responsabile;
- invio di dati personali a un destinatario errato;
- dispositivi informatici (notebook, chiavette usb, cd/dvd, ecc.) contenenti dati personali (non crittografati) persi o rubati;
- alterazione dei dati personali senza permesso;
- perdita di disponibilità di dati personali (situazione nella quale l'unica copia di una parte di dati personali è stata crittografata da un ramsonware o dal titolare del trattamento utilizzando una chiave che non è più in suo possesso; cancellazione accidentale o non autorizzata di dati personali; quando il titolare non può fare un restore dei dati dal backup, significativa interruzione delle normali attività aziendali, ad esempio, a seguito di blackout elettrico, attacco di denial of service che rendano indisponibili i dati personali, ecc.).

Non è da intendersi violazione di sicurezza un'azione di manutenzione pianificata al sistema informativo in quanto non rientra nella definizione data dall'art. 4, par. 12, GDPR.

3. Individuazione dei soggetti interni preposti alla gestione del Data breach

In caso di perdita o distruzione, anche accidentali, di dati personali (quindi anche dei documenti cartacei o informatici e/o dei supporti che li contengono), e in generale in tutti i casi in cui l'Incaricato ritenga ragionevolmente che vi possa essere stata una violazione degli stessi (distruzione o perdita – anche accidentali, accessi indebiti, non autorizzati, modifica non autorizzata, furto/perdita/sottrazione di password, divulgazione non autorizzata di dati personali, ecc.), il dipendente che ne viene a conoscenza è tenuto a darne comunicazione immediata al proprio diretto superiore gerarchico, il quale la trasmetterà immediatamente al Responsabile della protezione dei dati di LTA S.p.a., Cignacco Nicola, quale preposto alla gestione della violazione.

4. Comunicazione della violazione al soggetto preposto alla gestione del Data Breach

I Responsabili esterni e i dipendenti Incaricati che a vario titolo trattano i dati di cui LTA S.p.a. è Titolare devono comunicare la violazione di sicurezza eventualmente subita all'interno della propria struttura quanto prima e comunque non oltre ventiquattro ore dalla presa di coscienza della stessa. La violazione di dati personali va comunicata ai soggetti preposti tramite e-mail all'indirizzo aziendale privacy@lta.it. Tale indirizzo è nella disponibilità del Responsabile della protezione, Cignacco Nicola, e del Direttore Amministrativo, Zille Nicola, cui compete il controllo in assenza del primo.

5. Comunicazione della violazione al Titolare del trattamento dei dati

Dopo essere venuto a conoscenza della violazione, il Responsabile del trattamento (o il sostituto in sua assenza) informa il Titolare del trattamento senza ingiustificato ritardo (art. 33, par. 2, GDPR). L'avviso viene dato verbalmente e via e-mail al Presidente del CDA e al Direttore Generale.

6. Definizione dei tempi di notifica del Data Breach

In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

PROCEDURA

1. Analisi del Data Breach

La violazione di sicurezza dei dati personali può essere di tre tipi. In particolare, può riguardare:
- la perdita di confidenzialità, che si verifica quando c'è una divulgazione non autorizzata o accidentale di dati personali o un accesso agli stessi;
- La perdita di integrità, che si verifica quando il dato personale viene modificato in modo accidentale o non autorizzato;
- la perdita di disponibilità (definita come "garantire l'accesso e l'uso tempestivo e affidabile delle informazioni"), che si verifica quando c'è una perdita di accesso ai dati accidentale o non autorizzata o la distruzione degli stessi.

È necessario identificare subito a quale di queste tipologie appartiene la violazione subita dall'azienda.

2. Tipo di dati coinvolti

I dati personali che possono essere coinvolti in una violazione sono di tre tipi:
- dati personali, ossia qualsiasi informazione riguardante una persona fisica identificata o identificabile («Interessato»); si considera identificabile la persona fisica che può essere individuata, 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 (art. 4, par.1, GDPR);
- categorie particolari di dati, ossia dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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
- dati relativi a condanne penali e reati.

È necessario identificare quale tra queste tipologie di dati sono coinvolti nella violazione di sicurezza.

3. Verifica della gravità e del possibile impatto sui dati

Nella valutazione, il Titolare del trattamento deve tenere conto della probabilità del rischio e della sua gravità basandosi su:
- caratteristiche peculiari degli Interessati (alcune categorie di soggetti, ad esempio i bambini, rischiano di essere maggiormente esposti in caso di violazione);
- numero di individui Interessati (maggiore è il numero di soggetti, maggiori rischiano di essere le implicazioni di un'eventuale Data Breach); anche in questo caso, però, è necessario valutare le circostanze, in quanto, in alcuni casi, la violazione può comportare gravi rischi anche per il singolo;
- eventuali caratteristiche del Titolare del trattamento (anche questo è un elemento da tenere in considerazione, infatti, a seconda del tipo di attività svolta, la violazione può essere più o meno grave).

Il Titolare viene coadiuvato nella valutazione dai preposti alla gestione del Data Breach (Responsabile della protezione dei dati e suo sostituto) che quindi effettuano una verifica della gravità ponderando le possibili conseguenze che la violazione può avere sui diritti e le libertà fondamentali delle persone fisiche coinvolte. Gli Amministratori di Sistema del Titolare coadiuvano

il Titolare e il Responsabile della protezione dei dati in dette attività di verifica e propongono soluzioni tecniche e informatiche per contrastare e mitigare le conseguenze della violazione.

4. Compilazione del registro delle violazioni

Il Titolare del trattamento deve documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'Autorità di controllo di verificare il rispetto di quanto previsto dalla normativa (art. 33, par 5, GDPR).
I preposti alla gestione del Data Breach devono raccogliere dai loro colleghi tutte le informazioni utili ed annotare di conseguenza, senza ingiustificato ritardo, in un registro *ad hoc*, tutte le violazioni di sicurezza che coinvolgono dati personali.
In detto registro vanno documentate anche le violazioni che implicano una perdita temporanea di disponibilità dei dati (ad esempio per l'improvvisa mancanza temporanea di corrente elettrica).

5. Decidere se fare la notifica all'Autorità Garante e agli interessati

Quando una violazione di sicurezza comporta un rischio elevato per i diritti e le libertà degli interessati è necessario fare la notifica all'Autorità Garante.
Di seguito si indicano alcuni esempi, senza pretesa di esaustività, che richiedono la notifica all'Autorità Garante, in modo da facilitare i preposti alla gestione del Data Breach nelle decisioni da adottare in questa situazione.

- il furto di un database di utenti, i cui dati possono essere utilizzati per commettere frodi attraverso le identità sottratte, deve essere notificato, dato l'impatto che questo potrebbe avere su quegli individui che potrebbero subire perdite finanziarie o altre conseguenze;
- perdita di controllo sui dati personali;
- limitazione o compromissione dei diritti degli interessati, loro discriminazione o possibile danno reputazionale;
- perdita di confidenzialità di dati personali protetti da segreto professionale;
- svantaggio economico sociale per gli interessati;
- mancanza di backup dei dati personali oggetto della violazione di sicurezza, anche se crittografati.

6. Definizione del contenuto della notifica all'Autorità e della comunicazione all'interessato

La notifica di una violazione all'Autorità di controllo deve almeno (art. 33, par. 3, GDPR):

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro soggetto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione (art. 34 GDPR) all'Interessato senza ingiustificato ritardo.

La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di seguito indicate:

- il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro soggetto presso cui ottenere più informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali,
- descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Non è richiesta la comunicazione all'Interessato se è soddisfatta una delle seguenti condizioni:

- il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- detta comunicazione richiederebbe sforzi sproporzionati (in tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia).

Nel caso in cui il Titolare del trattamento non abbia ancora comunicato all'Interessato la violazione dei dati personali, l'Autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o, di contro, può decidere che ciò non sia necessario sussistendo una delle condizioni è soddisfatta.

7. Casi da non notificare all'Autorità Garante

Quando la violazione di sicurezza non comporta un rischio elevato per i diritti e le libertà degli interessati la notifica all'Autorità Garante non è richiesta.
Di seguito si forniscono alcuni esempi, senza pretesa di esaustività, di casi che non necessitano la notifica all'Autorità Garante al fine di aiutare i preposti alla gestione del Data Breach nelle decisioni che si troveranno a prendere nell'affrontare questa situazione:

- la perdita o l'alterazione inappropriata di una rubrica del personale;
- la predita di disponibilità di dati personali che erano crittografati con un algoritmo allo stato dell'arte, dei quali esiste un backup per il ripristino degli stessi in tempi brevi e la cui chiave di decriptazione non è stata compromessa;
- mancanza improvvisa di corrente per un lasso di tempo breve che rende indisponibile i dati personali.

8. Processo di verifica della policy

La presente policy sarà verificata dal Titolare del trattamento con cadenza annuale per verificare la sua rispondenza alle esigenze e alle eventuali nuove situazioni che potrebbero verificarsi in azienda.

ALLEGATO N. 2
PROCEDURA PER LA GESTIONE DEI DIRITTI DEGLI INTERESSATI

Livenza Tagliamento Acque S.p.A.
Partita IVA, Codice Fiscale e Numero iscrizione Registro Imprese di Venezia Rovigo: 04268260272
Numero R.E.A. VE: 380371
Capitale sociale i.v. € 18.000.000

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

Uffici Amministrativi:
Via Cornia, n. 1/B
33079 SESTO AL REGHENA (PN)
tel. 0434 1854700
info@lta.it
info@pec.lta.it

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

INDICE

PREMESSA

Il Regolamento UE 2016/679 (di seguito “GDPR”) agli artt. 15 – 21 disciplina i diritti degli interessati, di seguito riepilogati:

- diritto di accesso dell’interessato - art. 15 GDPR;
- diritto di rettifica - art. 16 GDPR;
- diritto alla cancellazione (diritto all’oblio) - art. 17 GDPR;
- diritto di limitazione al trattamento - art. 18 GDPR;
- diritto a ricevere la notifica in caso di rettifica, cancellazione dei dati personali o limitazione del trattamento – art.19 GDPR;
- diritto alla portabilità dei dati - art. 20 GDPR;
- diritto di opposizione al trattamento – art.21 GDPR;

L’interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona – art. 22 GDPR

Rispetto alla precedente normativa (Codice Privacy), il GDPR ha introdotto tre novità in termini di diritti degli interessati e sono: il diritto all’oblio, il diritto alla portabilità, il diritto di limitazione del trattamento.

Le modalità per l’esercizio di tutti i diritti da parte di tutti gli interessati sono stabilite, in via generale, negli artt. 11 e 12 del Regolamento.

Al fine di agevolare l’esercizio dei diritti dell’interessato, il titolare deve fornire idonea informativa ai sensi degli artt. 13 e 14 del Regolamento, avendo cura di richiamare i contenuti degli artt. 15 – 21.

I diritti dell’interessato sono sempre esercitabili, salvo il Titolare non dimostri che non è in grado di identificare l’interessato (esempio dati anonimi).

Il Titolare deve dare seguito alle eventuali richieste di esercizio degli interessati entro un mese (30 giorni) dal ricevimento di tale richiesta. Il termine può essere prorogato a due mesi (60 giorni), tenuto conto della complessità e del numero di richieste, informando l’interessato dei motivi del ritardo.

Se le richieste pervengono a mezzo elettronico si richiede, ove possibile, di dar seguito alle risposte con mezzi elettronici. Il Regolamento, tuttavia, prevede anche la risposta orale solo se così richiede l’interessato.

Nel caso in cui il titolare non possa o non voglia dare seguito alla richiesta nei termini previsti deve comunque informare l’interessato e fornire le motivazioni dell’inottemperanza e della possibilità di proporre reclamo verso il Garante o verso l’Autorità Giudiziaria.

In via generale le richieste per l’esercizio dei diritti degli interessati sono gratuite; tuttavia, se le richieste sono manifestamente infondate o eccessive, il Titolare può prevedere un addebito o un contributo spese tenuto conto dei costi amministrativi sostenuti per fornire le informazioni oppure rifiutare di soddisfare la richiesta. L’onere di dimostrare l’infondatezza o il carattere eccessivo della richiesta è in capo al Titolare del trattamento.

In ogni caso se il Titolare nutre dei dubbi circa l’identità del richiedente può richiedere a sua volta ulteriori informazioni necessarie a confermare l’identità prima di dar corso alla richiesta.

Benché sia il Titolare a dover dare riscontro in caso di diritti dell’interessato, gli eventuali responsabili del trattamento sono tenuti a collaborare, così come sancito dal Regolamento all’art. 28 par.3, lett. e).

Deroghe all’esercizio dei diritti degli interessati sono concesse solo sul fondamento di disposizioni normative nazionali riprese negli art. 17 par.3 per quanto attiene al diritto all’oblio/cancellazione (libertà di espressione e di informazione, interesse pubblico, difesa di un diritto in sede giudiziaria, etc.), art. 23 (sicurezza nazionale e pubblica, difesa), art. 83 (trattamenti di natura giornalistica) e art. 89 (trattamenti per finalità di ricerca scientifica storica o statistica).

1. Definizioni

Di seguito si forniscono alcune definizioni e specifiche:

Diritto di accesso: diritto di ricevere una copia dei dati personali oggetto di trattamento, consultabile anche da remoto e in modo sicuro (considerando 68).
Diritto di cancellazione o "oblio": diritto alla cancellazione dei propri dati personali in forma rafforzata. Nello specifico comporta l'obbligo per i titolari che hanno reso pubblici i dati degli interessati pubblicandoli ad esempio su un sito web di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi copie, link o riproduzioni.
Diritto di limitazione: tale diritto costituisce un'alternativa alla cancellazione dei dati; il diritto alla limitazione è più esteso rispetto al "blocco" ed è esercitabile anche in assenza di violazioni da parte del titolare, ovvero se l'interessato chiede rettifica dei propri dati o si oppone al trattamento. Il diritto alla limitazione presuppone che il titolare sia in grado di "contrassegnare" i dati oggetto di limitazione prevedendo misure idonee nei propri sistemi informativi.
Diritto alla portabilità: si applica esclusivamente ai trattamenti automatizzati di dati; in particolare, sono "portabili" i dati forniti dall'interessato previo consenso o sulla base di un contratto stipulato con l'interessato (esempio dati forniti all'atto di una registrazione o creazione di un account). La trasmissione dei dati da un titolare all'altro richiede l'utilizzo di formati interoperabili (formato di uso comune e leggibile da dispositivo automatico).
Il WP 29 (ora EDPB - European Data Protection Board) ha pubblicato la linea guida n. 242 del 05 aprile 2017, dove ne sono definiti i requisiti e le caratteristiche del Diritto alla Portabilità; in linea generale, tale diritto è stato concepito per i settori della "telefonia", "internet", "sanità", "utenze domestiche".

2. Finalità e campo di applicazione

Questa procedura si applica a tutto il personale della società e a tutti gli interessati.
Gli interessati che potrebbero dare seguito a richieste di esercizio dei loro diritti sono:
- Dipendenti
- Clienti/Utenti del servizio
- Utenti del sito web
- Fornitori

L'obiettivo di questa procedura è quello di esplicitare e fornire indicazioni circa le modalità organizzative adottate dalla Società per dar corso alle richieste di esercizio degli interessati.

3. Misure organizzative per l'esercizio dei diritti degli interessati

Le modalità organizzative poste in essere dalla società sono:
- Richiamare in ogni informativa redatta ai sensi degli artt. 13 e 14 del Regolamento l'elenco dei diritti esercitabili;
- Aver adottato misure organizzative e tecniche idonee per consentire l'accesso al dato, la rettifica, la limitazione, la cancellazione e, ove possibile, la portabilità (cfr. Regolamento Privacy e Sicurezza);
- Aver sensibilizzato i propri responsabili esterni con nomina ai sensi dell'art. 28 del Regolamento;
- Aver formato internamente il proprio personale;
- Aver adottato la presente procedura.

LTA si conforma inoltre alle tempistiche previste dal Regolamento per l'inoltro delle risposte che fissa in 30 giorni solari (un mese) dalla ricezione, salvo proroga ai sensi di quanto previsto dal Regolamento.

4. Riferimenti normativi

A) Art. 15 - Diritto di accesso dell'interessato

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

- le finalità del trattamento;
- le categorie di dati personali in questione;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- il diritto di proporre reclamo a un'autorità di controllo;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.
Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

B) Art. 16 - Diritto di rettifica

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

C) Art. 17 - Diritto alla cancellazione (Diritto all'oblio)

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti altrimenti trattati;
- l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
- l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
- i dati personali sono stati trattati illecitamente;

- i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:

- per l'esercizio del diritto alla libertà di espressione e di informazione;
- per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
- a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

D) Art. 18 Diritto di limitazione del trattamento

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

- l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

E) Art. 19 Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

F) Art. 20 Diritto alla portabilità dei dati

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

- il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'art. 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b);
- il trattamento sia effettuato con mezzi automatizzati.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.
L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'art. 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

G) Art. 21 Diritto di opposizione

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'art. 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni.
Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.
Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.
Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la Direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.
Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

5. Cosa fare in caso di esercizio dei diritti da parte di un interessato

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 a ciascun dipendente e collaboratore di Livenza Tagliamento Acque SpA, nell'ipotesi appena illustrata, di avvertire immediatamente il Referente interno (privacy@lta.it) o il Responsabile della protezione dei dati (dpo@lta.it) fornendo ogni informazione circa la richiesta manifestata dall'interessato e prestandogli tutta l'assistenza necessaria.

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, previo avviso all'interessato*".
Nel caso di istanza presentata personalmente dall'interessato, così come in caso di ricezione tramite altri canali (avvocati o procuratori degli aventi diritto), è obbligatorio sincerarsi preventivamente dell'identità del richiedente con ogni modalità idonea.
Avvisate immediatamente il Referente interno e il Responsabile della protezione dei dati (DPO) per garantire la tempestiva e adeguata gestione di tutte le istanze.
Per ogni altra informazione o delucidazione in merito al comportamento da tenersi o alle operazioni da effettuarsi è necessario rivolgersi al Referente Interno.

ALLEGATO N. 3
SOCIAL MEDIA POLICY

Livenza Tagliamento Acque S.p.A.
Partita IVA, Codice Fiscale e Numero iscrizione Registro Imprese di Venezia Rovigo: 04268260272
Numero R.E.A. VE: 380371
Capitale sociale i.v. € 18.000.000

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

Uffici Amministrativi:
Via Cornia, n. 1/B
33079 SESTO AL REGHENA (PN)
tel. 0434 1854700
info@lta.it
info@pec.lta.it

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

INDICE

PREMESSA

Per coinvolgere sempre più persone nell'attività di comunicazione istituzionale Livenza Tagliamento Acque S.p.A. è presente anche sui social network (LinkedIn™) con l'intento di informare gli utenti riguardo le iniziative e i servizi dalla stessa offerti.
La presente Social Media Policy costituisce un codice di condotta che permette di regolare la relazione su internet, e in particolare sui social media, sia tra l'Azienda e i suoi dipendenti/collaboratori, sia nei confronti degli utenti esterni.
La presente Social Media Policy si rivolge al dipendente specificatamente addetto alla comunicazione aziendale, che con la firma in calce alla presente, si impegna a rispettare le prescrizioni in essa contenute.

SOCIAL MEDIA POLICY INTERNA

La Social Media Policy interna individua le principali norme di comportamento che il personale è tenuto ad osservare quando utilizza i social media e pubblica contenuti e commenti. È infatti sempre opportuno tenere presente che un utilizzo scorretto dei social network può comportare rischi elevati per chi ne usufruisce, con conseguenze anche gravi circa la propria immagine e reputazione.
Il presente documento intende individuare le modalità d'uso interno dei Social Media dallo stesso utilizzati, in particolare nei seguenti aspetti:

- Gestione degli account;
- Criteri per la produzione e pubblicazione dei contenuti;
- Linguaggio e stile;
- Norme di comportamento.

1. Gestione degli account

L'amministrazione e l'aggiornamento del profilo LinkedIn™ è affidata al dipendente specificatamente addetto alla comunicazione aziendale, il quale si impegna a gestirlo in maniera coerente con l'obiettivo per il quale è stato creato, nel rispetto delle regole della presente Policy.
In ogni caso, si ricorda che sono soggetti a tali regole tutti i dipendenti e i collaboratori che abbiano la gestione, anche solo temporanea, dei profili social dell'Azienda.

2. Produzione e pubblicazione di contenuti

LTA promuove con cadenza regolare sui propri canali di comunicazione contenuti testuali, fotografici e video, idonei a diffondere notizie relative ai progetti, agli eventi o ai servizi dalla stessa organizzati.
I post pubblicati si riferiscono a eventi attuali, o che si realizzeranno nel breve periodo. Gli utenti sono autorizzati a lasciare dei commenti sotto ogni post e possono altresì manifestare apprezzamenti in relazione al loro contenuto tramite le apposite funzioni del social network

3. Linguaggio e stile

Il linguaggio deve adeguarsi allo stile del social utilizzato.

In ogni caso valgono le stesse regole utilizzate per la redazione di qualunque altro documento testuale: controllare l'ortografia, scrivere usando un italiano corretto, assicurarsi circa la veridicità di quanto ci si appresta a pubblicare, non mancare di rispetto agli utenti che interagiscono con il profilo e considerare sempre le regole della buona educazione.

4. Norme di comportamento

Al fine di un corretto e decoroso utilizzo dei profili social, il personale è tenuto all'osservanza di una serie di norme di comportamento; in particolare:

- i dipendenti/collaboratori non sono autorizzati a divulgare informazioni riservate di cui sono a conoscenza (ad esempio: corrispondenza interna, informazioni di terze parti, dati personali comuni o sensibili di altri dipendenti e/o collaboratori o di clienti o fornitori, o altresì informazioni relative all'attività lavorativa, ai servizi offerti, ai progetti e ai documenti che non sono ancora stati resi pubblici), né a diffondere foto, video o altro materiale di tipo multimediale che riprenda locali o personale senza l'espressa autorizzazione dei soggetti coinvolti o dell'Azienda stessa.
- I dipendenti/collaboratori non sono altresì autorizzati a divulgare contenuti che si pongono in contrasto con i valori di LTA.
- Fermo restando l'esercizio delle libertà sindacali e del diritto di critica, ai dipendenti/collaboratori è fatto divieto di diffondere messaggi o commenti a carattere offensivo, minatorio, ingiurioso o diffamatorio, sia nei confronti delle attività promosse che nei confronti dell'utenza che interagisce con la pagina.
- I dipendenti/collaboratori sono sempre tenuti a ricordare che quanto viene pubblicato online può avere delle ripercussioni a livello globale.
- Il personale non può aprire altre pagine social, blog o altri canali telematici in nome o per conto di LTA senza la preventiva approvazione dello stesso.
- Nel caso di condivisione di contenuti (nello specifico, foto o video) aventi ad oggetto minori, per i quali non sia possibile ottenere il consenso alla divulgazione del genitore o di chi esercita la responsabilità genitoriale, i dipendenti/collaboratori sono tenuti a rendere il minore irriconoscibile (ad esempio, pubblicando esclusivamente foto dove il minore è ritratto in gruppo, o di spalle).
- I dipendenti/collaboratori che hanno in gestione le pagine social e che posseggono altresì un account personale sono tenuti a prestare la massima attenzione nell'utilizzo dei profili, adottando le accortezze necessarie al fine di evitare l'interscambio degli account durante l'uso.
- I dipendenti/collaboratori che condividono contenuti sulle pagine social di LTA devono tassativamente assicurarsi che quanto si apprestano a pubblicare risulti libero da copyright, nonché dai vincoli imposti dal diritto d'autore.

La violazione delle regole qui menzionate può comportare, in capo al singolo dipendente/collaboratore, una responsabilità di tipo disciplinare, da accertarsi tramite un apposito procedimento interno.

SOCIAL MEDIA POLICY ESTERNA

La Social Media Policy esterna disciplina i rapporti tra LTA e gli utenti (c.d. *followers*) e più in generale con chi interagisce con la pagina social; in particolare, la presente Policy intende regolamentare i seguenti aspetti:

- Finalità;
- Moderazione e regole di conversazione (*netiquette*);

– Risposte a quesiti o messaggi.

1. Finalità del Social Media

I contenuti che vengono pubblicati sulla piattaforma social sono ideati per informare gli utenti circa le attività, i servizi e le iniziative promosse da LTA, nonché per favorire lo scambio e il dialogo tra gli stessi utenti.

2. Moderazione e regole di conversazione (*netiquette*)

Gli utenti hanno il diritto di interagire liberamente all'interno della pagina social, esprimendo preferenze ed opinioni tramite la pubblicazione di commenti che siano inerenti al contenuto pubblicato; è pertanto vietato utilizzare la pagina social per esigenze personali.
L'utente è sempre tenuto all'osservanza delle seguenti regole di comportamento:

- l'interazione deve essere educata e rispettosa degli altri utenti e di LTA; non saranno pertanto tollerati insulti, offese, minacce o volgarità di qualsiasi genere;
- è assolutamente vietato, nei commenti, utilizzare espressioni violente, offensive e discriminatorie per quanto concerne genere, età, origini etniche, opinioni personali, orientamento sessuale e religioso, disabilità;
- è altresì vietata la pubblicazione di messaggi privi di rilevanza pubblica, nonché fuori contesto (c.d. *off topic*), *spam* o promotori di attività illegali;
- non è ammessa la pubblicazione di messaggi contenenti dati personali di terze persone (ad esempio indirizzo e-mail, numero di telefono, dati identificativi, ecc.);
- non è altresì ammessa la pubblicazione di commenti che violino il diritto d'autore, né l'utilizzo non autorizzato di marchi registrati.

I messaggi pubblicati in violazione di tali regole saranno rimossi dall'Amministratore del profilo, il quale si riserva inoltre la facoltà di bloccare l'utente che, dopo un primo richiamo, continui a non rispettare le suddette norme provvedendo, se del caso, anche a trasmettere una segnalazione alle Autorità competenti.
L'attività di moderazione della pagina social da parte dell'Amministratore viene effettuata a posteriori, ed è unicamente finalizzata alla verifica e alla limitazione, in tempi ragionevoli, di comportamenti contrari alle sopra menzionate regole di comportamento.

3. Risposte a quesiti o messaggi

Eventuali domande, quesiti o richieste di informazioni pubblicate dagli utenti, sia in forma pubblica che privata, verranno prese in carico dall'Amministratore e inoltrate all'Ufficio competente, che provvederà a fornire una pronta risposta.
I tempi di risposta variano in base alla tipologia della richiesta. Nel caso in cui la pagina social non sia lo strumento adeguato al soddisfacimento della richiesta, l'Amministratore provvederà a indicare il corretto canale di comunicazione a cui rivolgersi.

Per il Titolare del trattamento
Il Referente interno
Dott. Nicola Cignacco

L’Incaricato

data _____

firma _____