REGOLAMENTO IN TEMA DI UTILIZZO E CONTROLLO DEGLI STRUMENTI ELETTRONICI, INFORMATICI E TECNOLOGICI

Aggiornamento giugno 2024

Approvato con deliberazione del Consiglio di Amministrazione n. 58 del 20 giugno 2024

Premessa

Il presente Regolamento intende fornire ai dipendenti, collaboratori, nonché a chiunque abbia accesso autorizzato agli strumenti informatici del Consorzio (di seguito anche denominati "incaricati"), le indicazioni per una corretta e adeguata gestione delle informazioni, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici messi a disposizione dal Consorzio.

Ogni utente è tenuto a rispettare il Regolamento, che è reso disponibile tramite le modalità specificate al successivo art. 9.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni fornite a tutti gli Autorizzati al trattamento dei dati personali in attuazione della normativa vigente in materia di privacy e di trattamento dei dati personali (Regolamento UE 2016/679), nonché implementano le informazioni fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse o di danni provocati da un eventuale Data Breach verificatosi a causa di un comportamento addebitabile al dipendente stesso.

Il presente regolamento si applica a tutti i dipendenti, nonché a tutti i collaboratori del Consorzio e consulenti che, a prescindere dal rapporto contrattuale con lo stesso intrattenuto (lavoratori somministrati, collaboratori coordinati e continuativi, stagisti, agenti di commercio, prestatori d'opera intellettuale, ecc.) abbiano accesso alle risorse informatiche e tecnologiche sopra citate, alla posta elettronica aziendale o ai servizi di rete.

Art. 1) - Soggetti che possono utilizzare strumenti elettronici, informatici e tecnologici

1.1 L'utilizzo degli strumenti tecnologici assegnati in dotazione (computer, telefoni, modem, tablet o altro tipo di dispositivo elettronico, comprese chiavette usb, hard disk, smart card o altri sistemi di memorizzazione o di gestione dei dati ecc.) e l'accesso ad internet è accordato al dipendente con la lettera di designazione ad "incaricato" e con le relative istruzioni riguardanti anche la sicurezza dei dati.

1.2 L'utilizzo è altresì accordato al collaboratore che abbia accesso alle dotazioni informatiche del Consorzio per necessità strettamente legate all'espletamento del proprio incarico, nonché a chiunque abbia accesso autorizzato agli strumenti informatici del Consorzio.

1.3 Il datore di lavoro potrà designare uno o più "responsabili", fornendo loro precise istruzioni sui tipi di controllo ammessi e sulle relative modalità.

1.4 Agli incaricati alla manutenzione è vietato l'accesso a dati personali presenti in cartelle o spazi di memoria eventualmente assegnati ai dipendenti ed è posto l'obbligo di svolgere solo le operazioni strettamente necessarie per adempiere al loro incarico, con divieto di realizzare attività di controllo a distanza, soprattutto di propria iniziativa; ai dipendenti sono resi noti i nominativi ed i compiti dei manutentori.

1.5 L'amministratore di sistema può compiere le operazioni strettamente necessarie per adempiere al suo incarico.

Art. 2) Divieti

Al fine di garantire la funzionalità, la sicurezza ed il corretto impiego degli strumenti elettronici e, al tempo stesso, la protezione della riservatezza dei dipendenti, messa a rischio dalla possibilità di costante monitoraggio offerte dalla tecnologia (es.: profilazioni, comunicazione/diffusione di dati personali, anche particolari ex art. 9-10 del Regolamento 679/2016), con particolare riferimento a device e PC, è vietato:

2.1 l'utilizzo del sistema informatico del Consorzio per motivi non lavorativi o non di servizio;

2.2 l'installazione di programmi ulteriori rispetto a quelli forniti dal Consorzio;

2.3 la modificazione delle configurazioni impostate;

2.4 aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani;
2.5 ostacolare l'azione dell'antivirus;
2.6 cancellare o formattare o alterare o manomettere o distruggere i device assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo, compresa la cifratura dei dati;
2.7 memorizzare (anche temporaneamente) il trattamento di file, documenti e/o informazioni personali dell'incaricato o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere;
2.8 modificare le configurazioni già impostate sul personal computer;
2.9 utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta dal Consorzio;
2.10 installare software di cui il Consorzio non possieda la licenza;
2.11 aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa dell'Azienda;
2.12 creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'Azienda, quali per esempio virus, trojan horses ecc;
2.13 accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte;
2.14 effettuare in proprio attività manutentive;
2.15 permettere attività manutentive da parte dei soggetti non espressamente autorizzati dal Consorzio.

A seguito di una cessazione del rapporto lavorativo o di consulenza dell'Incaricato con il Consorzio o, comunque, al venir meno, della permanenza dei presupposti per l'utilizzo di dati cartacei aziendali, gli incaricati hanno i seguenti obblighi:
2.16 procedere immediatamente alla restituzione dei dati cartacei in loro possesso;
2.17 divieto assoluto di cancellare o alterare o manomettere o distruggere i dati cartacei assegnati o renderli inintelligibili tramite qualsiasi processo.

Rispetto all'utilizzo di internet, in particolare, i divieti riguardano:
2.18 la navigazione su siti non correlati con la prestazione lavorativa;
2.19 il download di programmi o di file, non correlati con la prestazione lavorativa salvo espressa autorizzazione da parte del Consorzio;
2.20 la partecipazione a forum, non preventivamente autorizzata e l'utilizzo di chat line, partecipazione ad aste on-line (es.: e-bay); l'attività di trading online;
2.21 la conservazione di file a contenuto offensivo, discriminatorio, illecito penalmente e civilmente;
2.22 l'uso per finalità ludiche;
2.23 l'uso di strumenti di comunicazione non attinenti all'attività lavorativa;
2.24 utilizzare l'accesso ad Internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248 e s.m.i.). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, ...).

Rispetto all'utilizzo della posta elettronica, i divieti riguardano:
2.25 l'uso della posta elettronica per ragioni non attinenti ai compiti affidati;
2.26 l'invio o la memorizzazione di messaggi offensivi o discriminatori;
2.27 l'uso della posta elettronica per documenti classificati come riservati o confidenziali;
2.28 l'uso per partecipare a dibattiti, forum o mail list di contenuto offensivo o discriminatorio;
2.29 la costituzione di cartelle segrete, nascoste o criptate;

2.30 l'uso della posta elettronica per la registrazione a servizi non aziendali o per la registrazione ad account non aziendali (gmail, google drive, dropbox, ecc.), salvo che si tratti di uso necessario per la fruizione del servizio nell'interesse aziendale.

Rispetto all'utilizzo dei telefoni, smartphone, tablet, fax, fotocopiatrici aziendali, si stabilisce quanto segue:

2.31 è consentito l'uso esclusivamente per lo svolgimento dell'attività lavorativa, fatto salvo quanto previsto in materia dal Codice di Comportamento;

2.32 l'assegnatario è custode e responsabile del bene aziendale;

2.33 è vietata l'installazione di app non autorizzate e l'utilizzo della fotocamera per motivi personali e la configurazione di account personali, ad eccezione dei casi in cui ciò sia necessario per la fruizione del servizio nell'interesse aziendale;

2.34 l'eventuale uso promiscuo del telefono aziendale è possibile in presenza di preventiva autorizzazione scritta e in conformità ai principi generali sull'uso diligente di strumenti aziendali.

Art. 3) Prevenzione all'utilizzo improprio

Al fine di prevenire l'utilizzo improprio degli strumenti informatici non è tollerato l'uso privato di internet e della posta elettronica.

Ogni incaricato del trattamento è tenuto a garantire e conservare la riservatezza e la segretezza dei dati personali di cui ha conoscenza e ad usarli esclusivamente per finalità congruenti con la base giuridica che ne autorizza il trattamento.

In caso di intervento tecnico da parte degli AdS (Amministratori di Sistema), per il ripristino di dati accidentalmente cancellati e per il ripristino della funzionalità e delle impostazioni della posta elettronica questi, limitatamente alle necessità proprie dell'intervento, possono visualizzare l'indirizzo e l'oggetto delle mail.

È consentito ai dipendenti avvalersi di funzionalità automatiche del sistema in caso di assenze programmate (ferie, lavoro fuori sede, etc.), al fine di consentire o l'invio automatico di messaggi di risposta contenenti le "coordinate" (elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto del Consorzio. In caso di assenza improvvisa o prolungata del dipendente, se improrogabili necessità di lavoro richiedano la conoscenza dei messaggi di posta elettronica, l'interessato può delegare un altro lavoratore (fiduciario); il delegato riferirà al datore di lavoro i "dati rilevanti" per lo svolgimento dell'attività lavorativa; il datore di lavoro ne darà comunicazione all'interessato. Nel caso si verificasse la necessità di visualizzare per motivi di servizio il pc del lavoratore assente in concomitante assenza del lavoratore indicato come fiduciario il datore di lavoro potrà accedere al pc direttamente o tramite un proprio incaricato utilizzando le credenziali depositate presso il custode delle credenziali. L'evento dovrà essere reso noto al lavoratore che alla ripresa del lavoro dovrà provvedere alla sostituzione delle password.

L'e-mail contenente i nomi degli ex dipendenti (licenziati, dimessisi) andrà "chiusa"; nel caso in cui però il titolare, per non perdere comunicazioni aziendali, intenda comunicare a terzi tale chiusura dovrà segnalare un account aziendale alternativo rispetto al contatto precedentemente utilizzato.

Alla dismissione di un dipendente dall'attività CON.AMI si dovrà procedere a:

- inserimento di un messaggio di risposta automatico per la comunicazione agli utenti che scrivono al dipendente per il quale è cessato il rapporto di lavoro, a far data dal momento di cessazione del contratto stesso;
- creazione di un archivio pst della relativa posta elettronica e dei file dal dipendente/ coloro che abbiano avuto accesso autorizzato agli strumenti informatici del Consorzio) elaborati/modificati su rete, entro 60 giorni naturali consecutivi dal momento di cessazione del contratto stesso;
- inserimento in rete di una cartella inerente il dipendente/incaricato del trattamento per il quale è cessato il contratto di lavoro/rapporto, alla quale un dipendente all'uopo nominato potrà accedere per proprie esigenze di servizio o anche su richiesta di terzi, per la ricerca/controllo

dell'avanzamento di talune attività che interessavano il dipendente/incaricato del trattamento in questione;
- cancellazione dell'utente dal Dominio Utenti CON.AMI entro 60 giorni naturali consecutivi dal momento di cessazione del contratto stesso.

L'uso della posta elettronica deve rispettare i seguenti principi:
- tutela dell'immagine del Consorzio;
- rispetto dell'etica aziendale espressa nell'ambito del MOG 231;
- osservanza della riservatezza da parte dei lavoratori;
- correttezza nei rapporti tra colleghi;
- impiego di un linguaggio appropriato;
- uso succinto dello strumento (scrivere e allegare lo stretto necessario);
- rispetto delle normative vigenti.
- La veicolazione per posta elettronica di informazioni che possano "impegnare" il Consorzio deve essere autorizzata preventivamente.
- non si possono inviare informazioni confidenziali, critiche, riservate senza autorizzazione, più in generale, non è consentito inoltrare a utenti esterni mail di corrispondenza interna aziendali.
- nel caso in cui ci si accorga di aver sbagliato il destinatario del messaggio contenente dati del consorzio, si dovrà procedere con l'immediata richiesta al destinatario di cancellare l'e-mail ricevuta per errore e con la comunicazione dell'avvenuto al titolare del trattamento.

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, via mail etc. pertanto, il Consorzio impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente.
L'incaricato, da parte sua, deve impegnarsi a controllare il funzionamento e l'aggiornamento del sistema antivirus installato sul proprio computer, e, in particolare, deve rispettare le regole seguenti:
- comunicare al Consorzio ogni anomalia o malfunzionamento del sistema antivirus;
- comunicare al Consorzio eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, all'incaricato:
- è vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione;
- è vietato ostacolare l'azione dell'antivirus aziendale;
- è vietato disattivare l'antivirus senza l'autorizzazione espressa dell'Azienda e anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer;
- è vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani;
- è vietato contattare i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

Art. 4) Gestione password

Ogni lavoratore è munito di un nome Utente e Password che lo abilitano ad utilizzare il PC presente nella postazione aziendale e a collegarsi al wi-fi aziendale.
La Password è strettamente personale, deve essere costituita da un minimo di 8 caratteri alfanumerici che non contengano riferimenti personali all'incaricato.
Ogni lavoratore dovrà modificare la Password almeno ogni sei mesi. Una volta modificata la password, il titolare della stessa dovrà compilare il "modulo password incaricato" in suo possesso, chiudere il modulo in una busta che dovrà essere consegnata al custode delle credenziali indicato come depositario delle stesse presso l'ufficio Segreteria.

Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare).
Le password devono essere sostituite almeno nei tempi indicati dalla normativa, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password.
Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera.

Art. 5) Possibilità di controlli e loro gradualità

Potranno essere effettuati controlli sul server volti ad individuare in forma cumulativa l'accesso alla rete e ai siti visitati nelle circostanze in cui si verificassero flussi anomali di dati o nelle altre condizioni in appresso specificate. Nel caso in cui da queste verifiche emergesse un uso in contrasto con la linea del presente regolamento la direzione aziendale valuterà modalità diverse delle attività di controllo.
In linea generale, fermi i divieti di cui alla legge n. 300/1970 (art. 4)[1], il diritto del datore di lavoro di effettuare controlli identificativi del lavoratore, sussiste quando ciò sia dettato da:

- esigenze per l'esercizio o la difesa in sede giudiziaria;
- riscontri di gravi inadempienze della prestazione lavorativa o comunque di attività idonee a compromettere il vincolo fiduciario con il datore di lavoro;
- oggettivi indizi di commissione del reato;
- esigenze di salvaguardia della vita o dell'incolumità di terzi;
- norme specifiche di legge o dall'autorità giudiziaria.

Le esigenze organizzative, produttive, di sicurezza, il mancato rispetto del presente regolamento, nonché l'attuazione delle norme e le procedure che disciplinano l'istituto del Whistleblowing, in quanto possano evidenziare comportamenti anomali (evento dannoso, situazione di pericolo, rischi di responsabilità per il Consorzio, interferenze, rischio o danno per altri dipendenti), legittimano il datore di lavoro al controllo sull'utilizzo del web e dell'e-mail.

Potrebbero intervenire da parte del Datore di Lavoro controlli delle comunicazioni private in circostanze legate alle

- esigenze di sicurezza del sistema;
- per esigenze difensive nel caso in cui il datore di lavoro sia responsabile per le azioni del lavoratore o vittima delle sue condotte;
- per il rilevamento della presenza di virus informatici ed altri situazioni similari.

In dette circostanze (esigenze di sicurezza del sistema, esigenze difensive nel caso in cui il datore di lavoro sia responsabile per le azioni del lavoratore o vittima delle sue condotte, rilevamento della presenza di virus informatici ed altri situazioni similari, segnalazioni rivenienti dal Whistleblowing che abbiano superato il vaglio di fondatezza da parte del gestore delle segnalazioni) potrebbero intervenire da parte del Datore di

1 Articolo 4, L. n. 300/1970, Impianti audiovisivi e altri strumenti di controllo:
"1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi. (2)
2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.
3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro ***a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli****".*

Lavoro controlli *ex post* (eseguiti a posteriori) legati alla posta elettronica ed alla navigazione su Internet del lavoratore, per finalità di carattere difensivo (volti ad accertare le condotte illecite dei lavoratori) cioè, per soddisfare esigenze legate all'accertamento di un illecito penale e/o disciplinare. In detti casi, qualora l'interessato non si dimostri collaborativo, il datore di lavoro potrà forzare l'accesso. Inoltre, per l'ipotesi di Whistleblowing, il gestore della segnalazione potrà verbalizzare la mancata collaborazione del dipendente e, se determinante, il datore di lavoro potrà anche valutare se esporre tale circostanza alle autorità competenti (Anac o PM) come elemento impeditivo all'ultimazione dell'istruttoria e all'adozione di misure di prevenzione utili a gestire il rischio segnalato.

Relativamente ai dati rinvenibili mediante impiego del sistema di videosorveglianza, adottato dalla società per finalità unicamente di prevenzione e salvaguardia dell'immobile aziendale, gli stessi saranno trattati nell'ambito della finalità sopra indicata.

Tali eventuali controlli saranno eseguiti avvalendosi di un Amministratore di Sistema secondo modalità tecniche ed organizzative dal medesmo individuate nel pieno rispetto dei principi di cui all'art. 5 del GDPR n. 679/2026.
In caso di anomalie che compromettano il corretto funzionamento dei dispositivi o della rete aziendale, il Consorzio, sempre mediante l'Amministratore di sistema, effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali saranno evidenziati l'utilizzo irregolare degli strumenti aziendali, con invito agli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni loro impartite. Controlli su base individuale potranno essere compiuti soli in caso di particolari anomalie e sempre su disposizione scritta del Titolare del trattamento. In nessun caso verranno posti in essere controlli con finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa.
Si avvisa che per motivi di sicurezza del sistema informatico, per motivi tecnici oppure per motivi manutentivi, o ancora per finalità di controllo nei limiti sopra specificati, il personale incaricato (AdS) ha la facoltà di accedere direttamente a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, sempre comunque nel rispetto della normativa in materia di privacy e di protezione dati personali.

Art. 6) Conservazione sui dati
Sono memorizzate temporaneamente le informazioni relative all'uso degli strumenti informatici ed elettronici indispensabili per le seguenti finalità:

- protezione dell'intera rete da e verso l'esterno (firewall);
- più efficiente utilizzo del collegamento Internet (proxy server);
- difesa della corrispondenza e navigazione informatica (antispamming/antivirus);
- controllo automatico del contenuto dei siti (web filtering).

I sistemi software sono programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati relativi agli accessi ad Internet e al traffico telematico. Eccezionalmente la conservazione può essere protratta, per il tempo indispensabile e per le sole informazioni necessarie, in relazione:

- all'indispensabilità dei dati rispetto all'esercizio o difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Ogni strumento informatico o tecnologico affidato agli incaricati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti al Consorzio che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento. In particolare il Consorzio provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati in quanto non più necessari.

Art. 7) Sanzioni

La mancata osservanza delle disposizioni comporterà l'applicazione delle sanzioni previste dal vigente contratto collettivo di lavoro applicato dal Consorzio e/o dal codice sanzionatorio adottato nell'ambito del Modello 231.

È richiamata l'attenzione dei lavoratori sul fatto che l'uso improprio degli strumenti aziendali può anche integrare le seguenti ipotesi di reato:

- furto;
- turbato funzionamento di sistemi informatici;
- accesso abusivo a sistemi informatici/telematici;
- diffusione di programmi diretti a danneggiare o interrompere un sistema informatico;
- violazione, sottrazione e soppressione di corrispondenza;
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche/telematiche;
- danneggiamento di sistemi informatici/telematici;
- frode informatica.

Art. 8) Esercizio dei diritti del dipendente/incaricati

I diritti di cui all'art. 15 del GDPR n. 679/2016 vanno esercitati rivolgendosi al soggetto indicato nell'informativa resa dal Titolare del Trattamento Dati. Il Titolare si riserva la facoltà di proporre altro soggetto o unità operativa, previa informativa ai dipendenti/incaricati.

Art. 9) Pubblicazione del Regolamento

Il presente Regolamento:

- è pubblicato sul sito del Consorzio – www.conami.it- nella sezione "Amministrazione Trasparente";
- è divulgato a tutti i dipendenti.

Art. 10) Informativa

Ai sensi degli artt. 13 e ss. GDPR n. 679/2016, fermo e richiamato quanto riportato sul sito internet del consorzio, si comunica che:

- l'Amministratore di sistema può effettuare il trattamento dei dati relativi al traffico sulla rete;
- il titolare dei dati di traffico è il Direttore Generale;
- la presa visione e l'accettazione delle condizioni contenute nel presente regolamento costituiscono l'informativa e l'esplicito consenso da parte dell'utente alla raccolta ed all'eventuale trattamento dei dati relativi al traffico.

Art. 11) Entrata in vigore del regolamento

Il nuovo regolamento entra in vigore a partire dalla data di approvazione dello stesso da parte del Consiglio di Amministrazione.

Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.