Regolamento
Interno

Regolamento per l'utilizzo degli strumenti informatici, posta elettronica e Internet di AZIENDA MUNICIPALE GAS BARI S.p.A.

Redatto	da	**RETEGAS BARI**
Approvato	da	C d A / A U
Data creazione		09/01/2024
Distribuzione		Solo uso interno
Destinatari		**Tutto il personale dipendente (compreso stagisti e tirocinanti)**
Aggiornato il		10/06/2025

INTRODUZIONE

In un mercato sempre più competitivo, dove i margini temporali d'azione si riducono in modo esponenziale, una delle chiavi dell'efficacia dei processi aziendali è rappresentata sicuramente dalle informazioni che tali processi ricevono, producono, processano e trasmettono.

I moderni sistemi informatici, con il loro prezioso carico informativo, si sono trasformati negli anni in uno dei principali asset sul quale costruire il successo del business e dal quale la sua durata nel tempo può dipendere.
La pronta **disponibilità** delle informazioni, la loro **accuratezza** e **integrità**, la loro **riservatezza** rivestono oggi un ruolo centrale nella tutela del patrimonio informativo.
Difendere questi aspetti significa porre delle solide basi per la continuità del business e per preservare l'immagine aziendale.

Con il presente documento, pertanto, s'intende uniformare la gestione e l'utilizzo degli strumenti informatici personali/collettivi in relazione alle attività svolte all'interno di Azienda Municipale Gas S.p.A., (d'ora in avanti "RETEGAS BARI"). Attraverso l'utilizzo delle risorse informatiche e telematiche della società, infatti, si deve evitare che comportamenti inconsapevoli possano generare problemi o minacce alla protezione dei dati personali, agli strumenti e a tutti i documenti aziendali rilevanti.
Tutte le tecnologie informatiche ed elettroniche a disposizione, che vengono fornite configurate in modo sicuro, devono essere utilizzate ispirandosi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro.
Le prescrizioni e le indicazioni che seguono si aggiungono ed integrano le altre policy aziendali e le specifiche istruzioni già fornite a tutti gli "incaricati al trattamento".
Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione della presente Policy, è possibile rivolgersi al Responsabile della Protezione dei Dati o alla funzione IT aziendale.

SCOPO E CAMPO DI APPLICAZIONE

Il presente documento ha l'obiettivo di fornire indicazioni relative alla produzione, gestione e trasmissione delle informazioni aziendali con particolare attenzione a quelle di tipo elettronico che, per loro natura, risultano particolarmente critiche.
L'ampia diffusione delle tecnologie dell'informazione avvenuta nel corso degli ultimi anni, infatti, ha rappresentato sicuramente un traguardo importante per il mondo del lavoro. Tuttavia, accanto ai benefici generati da tali tecnologie, si insinuano potenziali lesioni della riservatezza dei dati personali dei lavoratori e di terzi soggetti (Interessati al trattamento). In considerazione di ciò, e sollecitato da diverse segnalazioni, il Garante per la protezione dei dati personali ha avvertito la necessità di predisporre delle linee guida per i datori di lavoro pubblici e privati, affinché prevedano un'apposita disciplina interna per l'utilizzo dei dispositivi tecnologici da parte dei lavoratori (Deliberazione del Garante, 1° marzo 2007, n. 13, punto 1.1).
Gli obiettivi che il Garante si prefigge attraverso l'elaborazione di tali linee guida sono molteplici. Da un lato si auspica la predisposizione, da parte dei datori di lavoro, di regole interne volte alla definizione delle modalità di utilizzo delle tecnologie informatiche da parte dei lavoratori (Deliberazione del Garante, 1° marzo 2007, n.13, punto 1.1, lett. a); dall'altro lato, le linee guida si propongono di soddisfare le esigenze di tutela dello stesso lavoratore o dei terzi, contro le condotte dei datori di lavoro che si traducano in una violazione della riservatezza.
Per tali ragioni, in considerazione dei peculiari riconoscimenti che il nostro ordinamento assegna al luogo di lavoro - come cornice nella quale sia assicurata la tutela dei diritti del lavoratore e sia garantita una ragionevole protezione della sfera di riservatezza nelle relazioni personali e professionali - il Garante ha ritenuto imprescindibile stabilire specifiche regole a presidio dell'integrità della privacy del lavoratore (Deliberazione del Garante, 1 marzo 2007, n. 13, punto 1.2).

All'interno del documento non sempre vengono fornite indicazioni puntuali in quanto, dato l'ambito in continuo sviluppo, risulterebbe difficile se non impossibile contemplare ogni tipologia di dispositivo informatico e di informazione di interesse aziendale.
Risulta per tale ragione un fattore chiave comprendere le idee alla base e le finalità del presente documento per poter seguire in modo efficace le indicazioni fornite.

Il presente documento è destinato ai dipendenti di RETEGAS BARI compreso eventuali suoi collaboratori, consulenti, stagisti o altre forme similari di collaborazione che prevedano all'utilizzo di strumenti informatici aziendali o
che sono interessati al trattamento. Più in generale, i contenuti devono essere noti a tutti coloro che gestiscono informazioni appartenenti a RETEGAS BARI.
È necessario, pertanto, che ciascun dipendente di RETEGAS BARI (di seguito denominata anche "Titolare") che tratta dati personali - sia che operi a titolo di lavoratore subordinato sia come collaboratore esterno a contratto, somministrato o stagista ("personale dipendente") - si uniformi al rispetto delle seguenti regole predisposte nell'osservanza della soprarichiamata Deliberazione del Garante e al fine di adempiere correttamente alle disposizioni legislative.

Allo scopo di chiarire definitivamente le norme di comportamento, pertanto, viene emanato il presente "**Regolamento Interno":**
- affinché i dipendenti o collaboratori evitino di porre in essere inconsapevoli comportamenti incompatibili con la correttezza professionale richiesta e/o con il diligente svolgimento della prestazione lavorativa da parte degli stessi;
- affinché ciascun dipendente o collaboratore sia reso edotto delle misure organizzative e di sicurezza implementate dal Titolare per prevenire tali condotte e per garantire la sicurezza all'interno dell'intera struttura organizzativa del Titolare.

Quanto segue è redatto nel pieno rispetto delle leggi regolatrici dei rapporti di lavoro e del Provvedimento a carattere generale emesso Garante per la protezione dei dati personali il 1° marzo 2007 (relativo all'utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro) ed è pertanto indispensabile la sua conoscenza da parte di tutti i dipendenti e collaboratori della Società.

RIFERIMENTI NORMATIVI E DOCUMENTALI

NORMATIVA EUROPEA

Regolamento UE 2016/679 ("Regolamento Generale sulla Protezione dei Dati personali" "Art. 5"). Decreto Legislativo N° 65 del 18 maggio 2018 e successive integrazioni e modificazioni ("codice recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'unione Europea") NIS

NORMATIVA ITALIANA

Decreto Legislativo 30 giugno 2003, n. 196 e successive integrazioni e modificazioni ("Codice in materia di protezione dei dati personali").

Norme sulle misure minime di sicurezza emanata dall'Agenzia per l'Italia Digitale ("AGID") come da linee guida indicate dalla Direttiva del Presidente del Consiglio dei Ministri il 1° Agosto 2015, Circolare 18 aprile 2017 n 2/2017 dell'AGID

Legge 20 maggio 1970, n. 300, norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e nell'attività sindacale nei luoghi di lavoro e norme sul collocamento (detta anche "statuto dei lavoratori").

Decreto Legislativo 8 giugno 2001, n.231, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300", pubblicato in Gazzetta Ufficiale n. 140 del 19 giugno 2001, e successive modificazioni e integrazioni.

Codice Civile
- Art. 2049 Responsabilità indiretta dell'imprenditore;
- Art. 2086 Direzione e gerarchia nell'impresa;

- Art. 2087 Tutela dell'integrità fisica e della personalità morale dei dipendenti, da parte dell'imprenditore;
- Art. 2104 Diligenza del dipendente nel rispetto delle disposizioni impartite dall'imprenditore.

PROVVEDIMENTI AUTORITA' GARANTE PRIVACY

Linee Guida del Garante Privacy su Posta Elettronica e Internet (Deliberazione n. 13 del 1 marzo 2007 – G.U. n. 58 del 10 marzo 2007);

Provvedimento del Garante Privacy del 27 novembre 2008 e successive modificazioni relativo a "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di sistema

DOCUMENTI INTERNI

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
Ultimo aggiornamento del Modello di Organizzazione, Gestione e Controllo ex D.lgs. 231/01 adottato dalla Società

CODICE ETICO

ELENCO AMMINISTRATORI DI SISTEMA

LETTERE AFFIDAMENTO INCARICO AI RESPONSABILI DELLA SICUREZZA INFORMATICA

PREMESSE

1) Ai sensi del Regolamento UE 679/2016, i dati possono essere classificati come segue:

- Personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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. Sono dati personali: nome e cognome, indirizzo, codice fiscale, foto, l'indirizzo IP o qualsiasi altra ripresa audiovisiva. La persona difatti può essere identificata anche attraverso altre notizie che non siano direttamente identificative (ad esempio, associando la registrazione della voce di una persona alla sua immagine, oppure alle circostanze in cui la registrazione è stata effettuata: luogo, ora, situazione).

- Categorie particolari di dati: dati personali che, per la propria delicatezza, richiedono particolari cautele; essi sono quei dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, nonché i dati relativi alla salute o all'orientamento sessuale della persona.

- Dati relativi a condanne penali e reati: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (quali dati personali idonei a rilevare provvedimenti emessi dalle Autorità Giudiziarie e contenuti nel casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reati e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 c.p.p.)

2) Per **trattamento dei dati** si intende "qualunque operazione o complesso di operazioni concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati". In tale ottica è indifferente che le operazioni vengano svolte con o senza l'ausilio di mezzi

elettronici, o comunque automatizzati, per cui anche i trattamenti effettuati su supporto cartaceo sono assoggettati alla normativa privacy.

Pertanto, le operazioni di trattamento si possono idealmente suddividere in tre macro-tipologie, in funzione del fatto che il loro fine sia:

A) IL REPERIMENTO DELLE INFORMAZIONI.
Tale fase è tecnicamente definita raccolta di dati, ovvero l'acquisizione delle informazioni, in qualunque modo essa avvenga: ad esempio, direttamente dalla persona interessata, presso terzi, o mediante consultazione di elenchi o un sito web.

B) IL TRATTAMENTO "INTERNO" DELLE INFORMAZIONI.
Si raggruppano in tale macro-tipologia le varie operazioni, poste in essere da chi raccoglie informazioni per organizzarle e renderle agevolmente usufruibili.

Esse sono:

- la registrazione dei dati, cioè il loro inserimento in supporti, automatizzati o manuali, al fine di rendere i dati disponibili per i successivi trattamenti;
- l'organizzazione dei dati in senso stretto, cioè il processo di lavorazione che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione, eccetera;
- l'elaborazione, ovvero le operazioni che attribuiscono significatività ai dati in relazione allo scopo per il quale essi sono stati raccolti;
- la selezione, l'estrazione ed il raffronto, specifiche che rientrano nella ipotesi più generale della elaborazione;
- la modificazione dei dati registrati, in relazione a variazioni o a nuove acquisizioni;
- l'interconnessione, ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;
- il blocco, ovvero la conservazione dei dati con sospensione temporanea dei trattamenti;
- la conservazione dei dati, alla quale la legge dedica particolari attenzioni sotto il profilo della sicurezza;
- la cancellazione o la distruzione dei dati, anch'esse operazioni il cui compimento fa sorgere l'obbligo di effettuare taluni adempimenti.

***C*) L'USO DELLE INFORMAZIONI NEI RAPPORTI CON L'ESTERNO.**
Sono i trattamenti più delicati, in quanto è con essi che si può concretamente ledere la sfera della riservatezza altrui: essi vengono genericamente definiti come utilizzo, ovvero la realizzazione dello scopo per cui si è provveduto alla raccolta ed ai trattamenti interni.
L'utilizzo può essere:

- diretto, instaurando cioè un rapporto con la persona sul conto della quale si sono raccolte informazioni;
- indiretto, ovvero consistere nel mettere a disposizione di terzi le informazioni raccolte.

Le operazioni di utilizzo cui la legge dedica le maggiori attenzioni, in quanto si tratta di quelle potenzialmente più lesive della privacy, sono quelle con cui si mettono a disposizione di terzi i dati personali. Esse sono:

- la **comunicazione**, cioè il dare conoscenza dei dati personali a uno o più soggetti determinati

- diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

la **diffusione**, cioè il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

3) Per lo svolgimento delle quotidiane attività lavorative, il Titolare necessita dell'utilizzo di apparecchiature informatiche per l'espletamento di molteplici compiti, nell'ambito di diversi ruoli e posizioni organizzative.
L'uso di tali apparecchiature deve essere disciplinato da norme certe in quanto da comportamenti - anche inconsapevolmente non leciti - possono derivare conseguenze gravi, sia sul piano tecnico (come un blocco della funzionalità o una perdita di dati) sia sul piano giuridico (che possono determinare l'insorgere di responsabilità sia penali sia civili a carico, contestualmente, del Titolare e del lavoratore coinvolto).

4) L'allegato A) costituisce parte integrante del presente Regolamento.

NORME COMPORTAMENTALI

NORME TECNICHE

Tutti i dipendenti e collaboratori che utilizzano strumenti elettronici sono tenuti a prendere visione e attenersi a quanto previsto nel presente Regolamento Interno. Tali documenti sono reperibili presso la Intranet aziendale di RETEGAS BARI.

Gli operatori tecnici addetti alla sala CED e i soggetti detentori delle chiavi di accesso sono tenuti ad operare con la massima oculatezza, accertandosi che la sala stessa sia sempre chiusa e che le chiavi della stessa siano correttamente custodite.

Il personale che tratta dati personali (incaricati al trattamento) è tenuto al rispetto di tutte le apparecchiature messe a disposizione dalla Società, provvedendo alla buona conservazione delle stesse, avendo cura al termine dell'orario di lavoro di lasciare la propria postazione di lavoro ordinata, efficiente e **con le apparecchiature spente** (se non diversamente previsto da elaborazioni che proseguono oltre l'orario di lavoro). Al momento di lasciare i locali e gli uffici, il personale dovrà altresì accertarsi della chiusura di finestre dei locali da loro occupati.

Gli operatori non devono modificare la configurazione del proprio PC; in caso di mal funzionamento dovranno richiedere l'intervento dei tecnici preposti. Si fa inoltre assoluto divieto di installare sulle apparecchiature software non autorizzati. Si ricorda che il mancato rispetto delle norme relative alle licenze d'uso è perseguibile penalmente.

Tutta la documentazione prodotta dal personale incaricato al trattamento dovrà essere elaborata solo ed esclusivamente con gli strumenti messi a disposizione dalla Società e dovranno essere inseriti nelle cartelle di rete autorizzate; periodicamente potranno eseguirsi controlli dei dischi fissi al fine di verificarne l'efficienza, provvedendo all'eliminazione dei file non pertinenti l'attività lavorativa dell'utilizzatore. È fatto divieto di salvare file e/o cartelle in posizioni non autorizzate.

Poiché i malware, ovvero un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al sistema su cui viene eseguito (rientrano in questa categoria virus, worm, spyware e altri programmi dannosi), costituiscono una delle minacce più frequenti alla sicurezza, è necessario che il personale incaricato al trattamento si attenga alle seguenti norme:

- il sistema informatico presenta software di protezione che vengono aggiornati automaticamente. Si raccomanda, pertanto, di verificare periodicamente l'effettivo funzionamento del sistema e di non disattivarli in nessuna occasione;
- è necessario evitare il materiale che potrebbe contenere virus o altri software dannosi;
- non scaricare mai file da mittenti sconosciuti o sospetti e, quando necessario, effettuare sempre un controllo prima di acquisire o aprire qualunque programma o documento acquisito via posta elettronica (in caso di dubbio contattare la sezione IT).

SISTEMI INFORMATIVI

SALVA SCHERMO PROTETTO CON PASSWORD

All'interno della rete i dispositivi sono protetti da una impostazione del sistema operativo che dopo un breve periodo di inattività dell'elaboratore lo blocca attivando uno screen saver protetto con password.
Ciononostante, il personale dipendente è tenuto a bloccare il proprio computer (fisso o laptop) nelle pause previste o nel momento in cui debba allontanarsi da esso per più di qualche minuto.

UNITÀ DISCO DI RETE

La Società dispone dei così detti "Dischi di Rete". Si tratta di spazi di memorizzazione dedicati ai file degli utenti e che vengono protetti con sistemi avanzati di back up online per 14 giorni solari. Questa protezione garantisce la disponibilità del dato in caso di perdita dei dispositivi di memorizzazione. I file che vengono prodotti in locale devono essere salvati anche nel disco di rete e una volta che non sussistano più ragioni di convenienza i file locali devono essere eliminati a favore della sola conservazione sul disco di rete. Le cartelle nei dischi di rete possono essere create per area e per un singolo dipendente. Vedere anche il punto successivo per la cartella personale nei dischi di rete.

CARTELLA PERSONALE

Nei dischi di rete è presente una cartella nominativa per il salvataggio dei propri dati. In tale cartella devono essere salvati tutti i file del personale dipendente, anche se memorizzati inizialmente in locale su personal computer e laptop.

CARTELLE LOCALI

Le cartelle create localmente nei personal computer e laptop sono da intendersi come temporanee e l'eventuale contenuto deve esistere in copia di sicurezza anche nei dischi di rete.

ACCESSO ED USO DEI SISTEMI E PASSWORD

Le unità disco (locali o di rete) sono aree di condivisione di informazioni strettamente lavorative e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia connesso all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. È vietata, anche, la conservazione e l'archiviazione dei dati in locale sui singoli PC, salvo alcune specifiche eccezioni legate a esigenze produttive.

Il personale dipendente si connette alla rete della Società tramite autenticazione univoca personale.
Il titolare della password è tenuto a non rivelarla ad alcuno, colleghi, superiori amministratori di sistema inclusi, dovendo avere la massima diligenza nella custodia della stessa e preservandone la segretezza anche durante il momento della digitazione. Qualora il dipendente prenda coscienza che taluno possa aver visionato la digitazione o essere comunque a conoscenza della password, deve immediatamente cambiarla. Qualora sia richiesto di riferire in qualunque forma la password (telefonicamente, via e-mail, etc.) il personale dipendente è obbligato a rifiutarsi; contemporaneamente deve dare immediata comunicazione dell'accaduto al tecnico informatico preposto.

È vietato comunicare, scambiare o condividere password tra più utenti (neanche se appartenenti al medesimo team di lavoro) o divulgare password personali a terzi (anche se colleghi o amministratori di sistema); la condotta non conforme a questa prescrizione può comportare sanzioni disciplinari, salvo casi autorizzati *(es. applicazioni web di terze parti, o che non contemplano autenticazione a doppio fattore).*

La password scelta non deve avere relazione con la propria vita privata e aziendale e deve rispettare requisiti di complessità (essere di almeno otto caratteri, contenere lettere maiuscole, minuscole, numeri e caratteri speciali)

È vietato riutilizzare le proprie password lavorative di accesso ai sistemi, (es. di accesso al pc, alla posta o ai vari applicativi) per la registrazione in altri siti web.

Come previsto dalla procedura di gestione delle password, il dipendente ha l'obbligo di cambiare la password di accesso agli strumenti informatici almeno ogni 42 giorni. Solo in casi eccezionali la password potrà essere resettata a cura del tecnico informatico preposto.

Occorre conservare le password con diligenza per impedire che soggetti terzi ne vengano a conoscenza, segnalandone sollecitamente agli amministratori di sistema designati l'eventuale smarrimento, sottrazione o diffusione.

In nessun caso devono essere annotate password in chiaro sia su supporto cartaceo sia informatico. I requisiti minimi di complessità delle password sono:
- redazione con caratteri maiuscoli e/o minuscoli;
- utilizzo di simboli, numeri, punteggiatura e lettere;
- numericamente devono essere password di almeno 8 caratteri;
- non deve trattarsi di password basate su informazioni personali, riferimenti familiari o comunque dati inerenti direttamente al soggetto titolare della password stessa.

I su elencati requisiti di complessità devono essere applicabili su tutti i sistemi informativi e su tutte le applicazioni gestionali con cui vengono utilizzati dati personali, compreso la posta elettronica.
La parola chiave deve essere mantenuta segreta, adottando gli opportuni accorgimenti per la sua custodia.

Come previsto dal presente regolamento, il personale dipendente ha l'obbligo di cambiare la password di accesso del sistema operativo almeno ogni 42 giorni. La modifica delle password, infatti, è gestita in maniera automatica dai sistemi di autenticazione utilizzati, i quale al 43° giorno obbligano al cambio della stessa; solo in casi eccezionali la password potrà essere resettata a cura del personale IT. Il sistema in ogni caso avvisa il personale dipendente qualche giorno prima della scadenza.

MANUTENZIONE DELL'ELABORATORE A DISPOSIZIONE

Dotare il Personal Computer in dotazione di una password di accesso per avere maggiori garanzie circa riservatezza e disponibilità dei dati presenti sulla propria stazione di lavoro. Contattare il responsabile della sezione IT aprendo un ticket all'indirizzo http://sondo/ticket per stabilire se il proprio personal computer può essere configurato con una password del Sistema Operativo e per ottenere assistenza nella predisposizione di questa operazione.

Su ogni personal computer dell'azienda è stato installato un software antivirus per prevenire eventuali danneggiamenti al sistema operativo e ai software causati dalla presenza o dall'azione di programmi contenenti virus informatici. Questi software antivirus hanno il compito di controllare gran parte dei file utilizzati dall'utente. I software antivirus devono essere aggiornati periodicamente per permettere l'individuazione di tutti i nuovi virus che vengono via via scoperti. RETE GAS è dotata di un sistema centralizzato automatico di aggiornamento dei client, per cui è importante che se ne controlli il corretto funzionamento prestando attenzione ad eventuali messaggi di errore sull'obsolescenza delle definizioni dei virus. Si ricorda che, nonostante la presenza del software antivirus, è possibile che riescano ugualmente ad installarsi nei computer virus informatici non identificati o riconoscibili. Pertanto, nel caso si evidenzino anomalie di funzionamento del computer, è importante darne segnalazione a responsabile del settore IT.
Non installare software, anche di prova, o software portabile, senza l'autorizzazione o senza informarne i responsabili IT interni. L'unico software utilizzabile è quello fornito da RETE GAS in dotazione alle postazioni. Si ricorda che la copia non autorizzata (o l'installazione senza licenza) di software è punita ai sensi dell'art. 13 della legge n° 248/2000 e s.m.i.

Spegnere correttamente la macchina alla fine della giornata lavorativa.

Riporre i supporti in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi dove sono custoditi.

n caso di furto o forzatura di una stazione di lavoro, avvisare al più presto i Responsabili IT interni.

UTILIZZO DELLA POSTA ELETTRONICA

Al personale dipendente, qualora sia attribuito un indirizzo di posta elettronica aziendale, non è consentito l'utilizzo per motivi diversi da quelli inerenti all'espletamento degli adempimenti lavorativi.
Si rende noto che per motivi organizzativi e funzionali, potrebbero essere archiviati tutti i messaggi di posta elettronica (anche nelle copie di back up), in uscita ed in entrata dalle caselle di posta elettronica della Società. Conseguentemente, stante la natura di strumento di comunicazione aziendale del sistema di posta elettronica, il personale dipendente è consapevole che sullo stesso non potrà essere garantita la riservatezza dei del messaggio e dei documenti inviati e ricevuti; pertanto, sarà impegno del personale dipendente evitare l'utilizzo delle caselle di posta elettronica per comunicazioni di carattere personale o che esulino dal contesto aziendale a cui sono preposte.

Si fa presente che alcuni indirizzi di posta sono ad uso promiscuo (es. Jamio, etc.) e il loro utilizzo permette l'accesso ai messaggi da parte di tutti gli iscritti alla lista di distribuzione collegata a quell'indirizzo. Per tale motivo, sugli account sopra indicati non può essere garantita la riservatezza delle comunicazioni.
Le informazioni aziendali riservate, inoltre, sono segrete e oggetto di specifica tutela e, come tali, sono sottoposte a misure di sicurezza adeguate a mantenerle segrete.
A tal fine, pertanto, si ricorda che:

- non è consentito l'utilizzo degli indirizzi di posta elettronica della Società per la partecipazione a dibattiti, Forum, newsletter o mailing list, non attinenti all'attività lavorativa;
- non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, handicap o stato di salute o che costituiscano comunque condotta illecita;
- è vietato l'inoltro dei messaggi ricevuti sull'account di posta aziendale ad altro indirizzo e-mail personale del personale dipendente;
- è severamente vietato inviare messaggi, con allegati file con contenuti inerenti alle attività della Società a destinatari che non sono in relazione con la stessa e/o non sono autorizzati a riceverli, salvo espressa autorizzazione scritta del Titolare.
  Nel caso gli allegati da trasferire via mail superino le dimensioni massime consentite, l'Azienda metterà a disposizione degli utenti che n'è facciano richiesta il cloud aziendale autorizzato https://eu-cloud.acronis.com/services, previa richiesta formale alla sezione IT che genererà un account personalizzato con approvazione del Dirigente. Anche gli allegati trasferiti con tali strumenti devono essere protetti da password, che devono essere comunicate ai fruitori in una successiva e-mail.
- è severamente vietato inviare messaggi con allegati file (o nel corpo del testo) contenenti categorie particolari di dati (c.d. dati "sensibili") o dati relati a condanne penali o reati (c.d. dati "giudiziari"), a meno di utilizzare le trasmissioni di tali documenti via PEC.

In conformità delle disposizioni di legge e nel pieno rispetto del principio di non eccedenza, la Società si riserva la facoltà di effettuare controlli circa le modalità e le finalità di utilizzo della posta elettronica, soprattutto al fine di verificare la funzionalità e la sicurezza del sistema informatico. Ciò avverrà avvalendosi della facoltà di effettuare i c.d. "controlli difensivi" (attraverso soggetti all'uopo preposti e designati di norma membri della direzione aziendale), che saranno effettuati saltuariamente e/o a campione e solo in caso di stretta necessità, sull'intera area del traffico dati della posta elettronica della Società ed esclusivamente per finalità di difesa e tutela del patrimonio e della sicurezza della struttura titolare del trattamento. A tal fine e per esigenze tecniche o di manutenzione, gli amministratori di sistema possono trovarsi ad avere accesso ai contenuti delle email aziendali (in ogni caso non saranno effettuate verifiche massive, prolungate e/o indiscriminate).

N.B.: La Società fa presente al personale dipendente che il servizio di posta elettronica fornito mediante l'attribuzione di un account aziendale è uno "strumento di lavoro", al pari degli altri servizi della rete aziendale, fra cui anche il collegamento a determinati siti internet. Costituiscono parte integrante di questi strumenti, anche i sistemi e le misure – in uso presso la Società - che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore (ad esempio:; sistemi di filtraggio anti-virus che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui server per l'erogazione dei servizi di rete; sistemi di inibizione automatica della consultazione di contenuti in rete inconferenti rispetto alle competenze istituzionali).

Salvo quanto sotto indicato, in nessun caso verrà effettuato l'accesso diretto alle caselle di posta elettronica in uso al personale dipendente, se non in seguito a gravi e comprovati motivi che possano rilevare il compimento di reati o condotte illecite oppure su segnalazione dell'Autorità Giudiziaria nell'ambito di indagini svolte per la repressione, accertamento e prevenzione di reati.
In caso di un eventuale accesso all'account di posta elettronica concesso in uso al personale dipendente, i dati dei terzi saranno tutelati e l'identità degli interlocutori del lavoratore non sarà rivelata (nemmeno in eventuali sedi giurisdizionali).
Il personale dipendente, eventualmente, potrà richiedere la possibilità di utilizzare un account di posta elettronica privata, per le comunicazioni di carattere personale; in ogni caso, la Società si riserva il diritto di concedere o meno tale privilegio a seconda della effettiva necessità.
Nel caso di assenza programmata e al fine di non interrompere, né rallentare i processi produttivi e/o lavorativi, il personale dipendente ha la facoltà di predisporre la funzionalità che permette l'invio di un messaggio automatico di risposta che segnali altro nominativo e relativo indirizzo di posta elettronica di un collega da contattare nel caso di urgenze; il delegato potrà in questo modo ricevere i messaggi di posta elettronica del dipendente assente e a lui indirizzati.

Si dispone, inoltre, che nel messaggio automatico di risposta siano evidenziati l'inizio e la fine del periodo di assenza del dipendente, secondo il seguente modello:
"Sarò assente dal ___Per urgenze, contattare il ____al ____o all'indirizzo e-mail _____ "
al sig. n.

In caso di assenza improvvisa o prolungata del dipendente, se è necessario conoscere il contenuto di messaggi di posta elettronica inviati all'indirizzo aziendale o nel caso di motivi di manutenzione o urgenza, un soggetto delegato dalla Società sarà legittimato a visionare i messaggi di posta elettronica del lavoratore assente.

Il personale dipendente è tenuto a scaricare la casella e-mail assegnata con frequenza almeno giornaliera e a usare tale strumento per qualsiasi comunicazione interpersonale nell'ambito delle finalità lavorative.

È fatto divieto in ogni caso di divulgare a soggetti non autorizzati le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal dovere di segretezza a cui sono tenuti i dipendenti in ottemperanza agli obblighi di fedeltà e correttezza.

Tutti i messaggi di posta elettronica (inviati e ricevuti), i cui contenuti possono avere una rilevanza giuridica e istituzionale per la Società, costituiscono corrispondenza (disciplinata dalle norme del Codice Civile e, in particolare, in base al combinato disposto degli articoli 2214 e 2220) e pertanto potrebbero essere conservati per un periodo di dieci anni. In ogni caso, il tempo di conservazione dei messaggi di posta elettronica, anche per le altre tipologie documentali, non sarà superiore a quello necessario agli scopi che si intendono perseguire (e, per tale motivo, può variare anche in base al ruolo a cui l'account era stato assegnato), nel rispetto dei principi di finalità, pertinenza e non eccedenza previsti dalla normativa in materia di protezione dei dati.

Al termine della collaborazione lavorativa con la Società, l'eventuale account nominativo di posta elettronica aziendale del dipendente (di proprietà della Società) sarà disattivato e la stessa Società potrà disporre del suo utilizzo futuro, limitatamente alla corrispondenza intercorsa che ha un valore aziendale perché attinente all'attività lavorativa del dipendente cessato (che verrà conservata per un periodo di tempo congruo rispetto agli scopi che si intendono perseguire, che può variare anche in base al ruolo e alla figura a cui l'account era stato assegnato e fino a un massimo di 6 mesi); un messaggio automatico sull'account del dipendente cessato segnalerà al mittente il reindirizzamento dell'e-mail ad altro dipendente (su di un account alternativo). Inoltre, una volta consegnata la lettera di dimissioni o in caso di licenziamento o pensionamento non sarà possibile inviare mail verso l'esterno a meno di una deroga concessa dalla Società.

NAVIGAZIONE IN INTERNET

La finalità dell'accesso e della navigazione su Internet è il reperimento di informazioni e di documentazione utili all'azienda; l'utilizzo dei servizi di rete per scopi non inerenti ai fini aziendali è consentito limitatamente alla pausa lavorativa e nel rispetto delle leggi e dei regolamenti vigenti. Non saranno normalmente esercitati controlli in relazione alla navigazione effettuata in tale lasso temporale, salvo in caso di segnalazione o richieste da parte di Autorità competenti preposte alla prevenzione di illeciti informatici.

Durante il resto della giornata lavorativa è fatto divieto ai dipendenti di navigare in siti non attinenti con l'attività lavorativa (così come meglio descritti nell'Allegato A al presente Regolamento), in quanto l'utilizzo al collegamento ad Internet deve essere funzionale all'attività espletata in favore della Società; una violazione di tale prescrizione - e qualora vengano perpetrati eventuali illeciti nella navigazione in Internet - potrebbe comportare sanzioni disciplinari a carico del contravventore attraverso le modalità e le procedure in seguito indicate al paragrafo "Controlli indiretti".

Al fine di garantire la sicurezza dei propri dati, nonché di favorire un utilizzo corretto dello strumento Internet, il Titolare potrebbe adottare alcuni accorgimenti tecnici per prevenire illeciti da parte del personale dipendente (è facoltà dell'azienda, infatti, implementare delle "black list" di siti Internet aventi l'obiettivo di impedirne la visione in quanto non ritenuti d'interesse aziendale). Nel caso in cui un evento dannoso o una situazione di pericolo non siano stati impediti con preventivi accorgimenti

tecnici, la Società adotterà eventuali misure che consentano la verifica di comportamenti anomali, attraverso le modalità e le procedure indicate al paragrafo "Controlli indiretti".

La Società, al fine di prevenire determinate operazioni non consentite, ha implementato dei sistemi di filtro della navigazione che puntano a mitigare i rischi sopra esposti; ciononostante la prima e più efficace misura di sicurezza è rappresentata dalla consapevolezza dell'utente. Nel caso in cui un evento dannoso o una situazione di pericolo non siano stati impediti con preventivi accorgimenti tecnici, la Società adotterà eventuali misure che consentano la verifica di comportamenti anomali, attraverso le modalità e le procedure di seguito specificate:
la Società ha attivato sistemi di monitoraggio della navigazione aziendale secondo le previsioni di cui al Provvedimento del Garante in materia di trattamento dati personali, (Provvedimento del 1° marzo 2007), effettuando monitoraggio generalizzato ed anonimo dei log di connessione. Pertanto, in seguito al rilevamento di anomalie nel sistema dei dati, per motivi di manutenzione o in caso di comportamenti anomali individuati in una determinata area o a seguito di controlli a campione saltuari, la Società potrà attivare meccanismi di monitoraggio delle attività di rete (file di log) e di controllo del traffico internet o del traffico della posta elettronica o dei file di back up per fini organizzativi o di manutenzione, per verifiche sulla funzionalità del sistema o di controllo della sicurezza dell'impianto. Gli archivi di log risultanti da questo monitoraggio, effettuati in determinate aree della società e allo stesso tempo sufficientemente grandi da garantire la riservatezza dei lavoratori, contengono traccia di ogni operazione di collegamento effettuata dall'interno della Società verso Internet.
In caso di accertata violazione, l'area IT provvederà prontamente a segnalare l'accaduto all'ufficio aziendale competente.

In rispetto al principio di finalità, pertinenza e non eccedenza, tali log vengono tenuti negli archivi della Società per [centottanta giorni] e può accedere a tali informazioni solo il personale dell'area IT specificatamente autorizzato.

Al fine di evitare il grave rischio di importazione di virus informatici e di pregiudizio alla stabilità delle applicazioni dell'elaboratore, non è consentita l'autonoma installazione di programmi provenienti dall'esterno. Analogamente, non è possibile effettuare il download di file o di software aventi particolari caratteristiche dimensionali, tali da ridurre l'efficienza del sistema. Qualora, a seguito di controlli effettuati saltuariamente e a campione sul pc in uso all'utilizzatore, risultino presenti file o software non espressamente autorizzati, saranno posti in essere richiami disciplinari, motivati dal fatto che qualsiasi file o programma estraneo a quelli contenuti e autorizzati può cagionare incompatibilità con i programmi forniti e già in uso per lo svolgimento dell'attività lavorativa e/o costituire una minaccia per la sicurezza informatica. Il Titolare, peraltro, ricorda all'utilizzatore che costituiscono illecito penale le condotte consistenti nella illecita duplicazione o riproduzione di software ai sensi della legge sul diritto d'autore n. 633/41 come novellata, art. 171 bis.

Non è permessa la partecipazione, per motivi non lavorativi, a Forum, l'utilizzo di chat line, di bacheche elettroniche, mail list o altri mezzi di comunicazione telematica non attinenti con l'attività lavorativa, attuate mediante il pc affidato in uso.

UTILIZZO DEL FAX, TELEFONO, CELLULARE E FOTOCOPIATRICI

Il fax, il telefono fisso, gli eventuali cellulari aziendali e le fotocopiatrici devono essere utilizzati per scopi puramente lavorativi, in modo appropriato, efficiente, corretto e razionale

Non è consentito rivelare numeri telefonici interni o informazioni sulla Società non già pubblici a persone non preventivamente identificate, nonché autorizzate a conoscerle, ed è fatto divieto di lasciare documenti incustoditi presso le postazioni di fax o presso i locali delle fotocopiatrici. Ogni comportamento scorretto potrà anche essere oggetto di specifiche sanzioni disciplinari che potranno variare a seconda della gravità.

La Società fa presente che i telefoni aziendali, al pari della posta elettronica, dei software o degli applicativi, sono strumenti di lavoro e non possono essere utilizzati per fini privati (eventuali eccezioni devono essere autorizzate e limitate a situazioni di emergenza); pertanto, il loro utilizzo deve essere in funzione esclusiva per lo svolgimento degli incarichi affidati in base a principi di massima correttezza e professionalità, nel rispetto della normativa vigente, in quanto ogni uso anomalo può comportare dei rischi per la Società e per il lavoratore.
Gli usi consentiti sono i seguenti:
- comunicazioni di lavoro (es. per effettuare e ricevere chiamate, inviare messaggi o email relativi alla propria attività lavorativa);
- accessi a strumenti aziendali (es. utilizzare applicazioni e piattaforme approvate per la gestione delle attività lavorative);
- organizzazione del lavoro (pianificare appuntamenti, gestire contatti lavorativi e consultare o inviare documentazione aziendale).
Di norma sono comportamenti vietati:
- l'uso del telefono per attività non lavorative durante l'orario di lavoro, inclusi social media e giochi;
- utilizzare il telefono durante riunioni, salvo necessità operative;
- registrare conversazioni o informazioni riservate senza autorizzazione;
- archiviare documenti, foto o video personali, non attinenti con l'attività lavorativa;
- invio massivo di SMS se non strettamente necessario per esigenze di servizio e, comunque, preventivamente autorizzato;

Un non corretto utilizzo può essere causa di un aggravio economico per la Società in termini di costi di manutenzione, disservizi, vulnerabilità nella gestione della sicurezza dei dati e delle informazioni

acquisite (disponibilità, integrità, confidenzialità), con conseguenti gravi ripercussioni sulla dimensione reputazionale aziendale.

È vietata l'installazione di applicazioni non autorizzate o non necessarie per l'attività lavorativa. La Società autorizza l'installazione sul telefono aziendale e l'utilizzo delle applicazioni di cui all'**allegato B**

Si precisa che l'utilizzo di WhatsApp e WhatsApp web sul pc devono essere limitati all'invio di informazioni strettamente necessarie allo svolgimento dell'attività lavorativa e i messaggi devono essere cancellati dalla chat con una frequenza almeno settimanale e da non sottoporre a backup.

Il detentore di telefono cellulare aziendale, affinché possa essere immediatamente rintracciabile nei casi di necessità, ha l'obbligo di mantenere in funzione il telefono cellulare durante le ore di servizio e in tutti i casi in cui le circostanze concrete lo rendano opportuno o indispensabile.
La durata delle chiamate deve essere la più breve possibile in relazione alle esigenze di servizio.
Il dipendente dotato di cellulare aziendale che deve chiamare un terzo dotato di cellulare deve utilizzare di norma il cellulare in dotazione. Per le chiamate su rete fissa è fatto obbligo di utilizzare gli apparecchi della rete fissa.
Ogni assegnatario di telefono cellulare aziendale è tenuto all'uso appropriato e alla diligente conservazione sia dell'apparecchio sia della SIM card, nonché ad adottare tutti gli accorgimenti per la sicurezza in termini informatici e di protezione dei dati.
Al fine di garantire adeguata sicurezza e protezione dei Dati, il dipendente deve:
- utilizzare password sicure e, se disponibile, l'autenticazione a due fattori;
- mantenere il dispositivo aggiornato con le ultime patch di sicurezza;
- consentire, se previsto, il backup dei dati aziendali e la cancellazione remota in caso di smarrimento o furto.

In caso di furto o smarrimento dell'apparecchio o della SIM card, il dipendente assegnatario deve darne immediata comunicazione al Responsabile dei servizi di telefonia mobile) ai fini dell'immediato blocco dell'utenza.

La Società, al fine di prevenire le situazioni di rischio sopra indicate e nel rispetto delle disposizioni previste dalla vigente normativa in materia di tutela dei dati personali - Regolamento (UE) 2016/679 – c.d. GDPR, può effettuare controlli su tutti gli strumenti di telefonia mobile messi a disposizione dei dipendenti, al fine di verificarne i consumi e il corretto utilizzo (in linea con le policy aziendali), monitorare le spesa di telefonia mobile e intervenire prontamente in caso di comportamenti impropri. I controlli potranno essere eseguiti ed effettuati sulle base delle informazioni trasmesse dagli operatori telefonici alla struttura competente ovvero flussi anomali di traffico telefonico, utilizzo di applicazioni non autorizzate, episodi di infedeltà aziendale o su segnalazione dell'Autorità Giudiziaria o nell'ambito di indagini da parte delle Forze di Polizia.

I controlli sono effettuati nel rispetto dei principi di necessità, proporzionalità, imparzialità, trasparenza e protezione dei dati personali e sono volti anche a tutelare l'immagine della Società e di coloro che vi prestano la propria attività.
I controlli effettuati dalla Società, pertanto, rispettano i seguenti principi:
a) necessità: i dati trattati durante l'attività di controllo devono essere sempre e soltanto quelli strettamente necessari a perseguire le finalità di sicurezza e tutela del patrimonio aziendale, sia rilevando eventuali danni patrimoniali già posti in essere, sia agendo quale deterrente rispetto a comportamenti impropri e potenzialmente dannosi per la Società;
b) proporzionalità: i controlli saranno sempre eseguiti con modalità tali da garantire, nei singoli casi concreti, la pertinenza e non eccedenza delle informazioni rilevate rispetto alle finalità perseguite e specificate;
c) imparzialità: i controlli saranno eseguiti su tutte le strumentazioni telefoniche messe a disposizione dalla Società. I controlli puntuali possono essere effettuati soltanto sulla base di specifiche, oggettive e circostanziate segnalazioni o su indicazione dell'Autorità Giudiziaria;
d) trasparenza e correttezza: in base a tale principio la Società notizierà tutti i soggetti potenzialmente sottoposti ai controlli ai sensi del presente disciplinare;

e) protezione dei dati personali: i controlli saranno in ogni caso eseguiti rispettando la dignità e la libertà personale dei soggetti sottoposti a controllo, garantendo altresì la riservatezza dei dati personali raccolti durante la procedura di controllo. I dati devono essere gestiti soltanto dai soggetti preventivamente designati quali autorizzati al trattamento. I controlli saranno eseguiti rispettando la normativa vigente in materia di protezione dei dati personali ed in particolare le prescrizioni di cui all'art. 5 del Regolamento UE 2016/679

La Società potrà effettuare controlli sull'utilizzazione degli strumenti di telefonia messi a disposizione dei dipendenti per lo svolgimento dell'attività lavorativa ad esclusione dei telefoni assegnati in uso promiscuo. A seguito dei controlli eventualmente effettuati (in forma anonima), ove emergano comportamenti in violazione del presente regolamento, o comunque "anomali", il personale incaricato invierà al Responsabile della Struttura e personale assegnatario delle utenze telefoniche in cui è stata rilevata l'anomalia, avvisi generalizzati, in cui si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite nel presente regolamento. In tale circostanza saranno nuovamente effettuati controlli su quelle utenze per assicurarsi dell'assenza di ulteriori anomalie. Qualora le violazioni persistessero la Società si riserverà di procedere a controlli nei confronti dei singoli consegnatari. In questa ipotesi il responsabile del servizio provvederà ad inviare al Responsabile della Struttura assegnataria dell'utenza e all'assegnatario dell'utenza stessa l'estratto delle telefonate oggetto di controllo. Il Responsabile della Struttura procederà, quindi, in contradditorio con l'assegnatario dello strumento di telefonia per la verifica della correttezza nell'utilizzo e a trasmettere l'esito di suddetta verifica alla Struttura Economato per le successive attività di competenza.
Un controllo mirato, infine, può essere effettuato quando dall'esame del traffico si rileva uno scostamento significativo dalla media dei consumi o e in caso di traffico zero da parte del telefono cellulare aziendale per un periodo di almeno due bimestri consecutivi. In tal caso ne viene data immediata comunicazione al Responsabile della Struttura da cui l'assegnatario dipende e viene segnalato all'assegnatario medesimo, con richiesta di motivazione e di giustificazione che le telefonate risultanti dal tabulato analitico siano state effettuate per motivi di servizi o con richiesta di motivazione del mantenimento dell'utenza.
Infine, la Società, tramite il Responsabile dei servizi di telefonia mobile può procedere in caso di anomalie di fatturazione a verifiche sul traffico telefonico effettuato dal titolare della SIM card
L'inosservanza delle presenti disposizioni può comportare sanzioni disciplinari, fino alla risoluzione del rapporto di lavoro, in conformità con la normativa vigente e il contratto collettivo applicabile

MEMORIZZAZIONE DELLE INFORMAZIONI

Con riferimento all'utilizzo della posta elettronica e alla navigazione in Internet, si segnala che le informazioni relative al traffico telematico, sono memorizzate temporaneamente, secondo quanto previsto dalla vigente normativa in materia.

Alle informazioni relative alle componenti di file di log memorizzate temporaneamente vi può accedere solo personale tecnico appositamente delegato dal Titolare (Amministratori di Sistema interni o esterni).

Un eventuale prolungamento dei tempi di conservazione di tali log, rispetto a quelli stabiliti, va valutato come eccezionale e può aver luogo solo in relazione:
- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria.

UTILIZZO DI PERIFERICHE USB

È fatto obbligo di utilizzare solo chiavette USB avute in dotazione dall'azienda, che sono protette automaticamente da password d'accesso, su tali dispositivi non è possibili memorizzare dati personali, altri dispositivi non registrati, non potranno essere utilizzati sui computer aziendali. Dispositivi diversi da quelli registrati, possono essere utilizzati solo dai personal presenti in sala CDA, saletta tecnica, e sala cral

CONTROLLO DI PERIFERICHE USB

L'azienda potrà predisporre, in piena autonomia, strumenti di Data Loss Prevention (DLP) ovvero software utilizzati per l'individuazione degli archivi che vengono trasferiti su unità esterne (es. USB) non autorizzate e utilizzate dal personale dipendete dell'Azienda. Nell'utilizzo di tali strumenti, i dati personali sono trattati allo scopo di individuare e prevenire l'uso non autorizzato, la perdita o il furto di dati aziendali. Tali controlli possono essere eseguiti con l'ausilio dell'antivirus e del software in dotazione al firewall aziendale.

CONTROLLI SUI PERSONAL E PORTATILI AZIENDALI

L'azienda in piena autonomia dovendo far fronte al Decreto Legislativo N° 65 del 18 maggio 2018 e in vigore dal 24 giugno 2019 sulla sicurezza delle reti e dei sistemi informativi), **(NIS2)** potrà predisporre strumenti di Telemetria atti a individuare preventivamente minacce che potrebbero causare fermi accidentali dei sistemi informativi utilizzati e conseguentemente stallo del Servizo Pubblico che Retegas eroga, a tal proposito nell'ambito dei controlli che si implementeranno si potranno evidenziare anche azioni volontarie o non di uso improprio e/o fraudolenti che possono avvenire sui sistemi informativi da parte di chi utilizza e gestisce le informazioni utilizzate dagli utenti.

DATI PERSONALI RACCOLTI TRAMITE APPARECCHIATURE E SOFTWARE ATTI A IDENTIFICARE DATA LOSS PREVENTION

I dati raccolti sono generalmente dati generati direttamente dal sistema operativo, dati che vengono generati dall'antivirus. Nel caso di DLP Data Loss Prevention sono dati generati dall'antivirus e dai firewall in automatico, sistema operativo, che tracciano il comportamento dell'utente autenticato, monitorando i dispositivi collegati sulle porte USB e che cosa viene trasferito sia in output che in input.

REGISTRAZIONE, CONSERVAZIONE E ANALISI DEGLI ACCESS LOG (AUTENTICAZIONI INFORMATICHE) DEGLI AMMINISTRATORI DI SISTEMA

Si rende noto che la Società - in qualità di titolare del trattamento e in ottemperanza alle disposizioni contenute nel Provvedimento del Garante della Privacy del 27 Novembre 2008 recante "Misure e accorgimenti, prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e successive modificazioni – ha attivato meccanismi di controllo delle attività dei propri Amministratori di Sistema, in modo da controllare la rispondenza delle loro attività alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti. In particolare, viene verificato e documentato (con cadenza almeno annuale) mediante un internal audit e apposita relazione scritta, che le attività svolte dagli amministratori di sistema siano conformi alle mansioni attribuite mediante lettera di nomina e alle misure organizzative e di sicurezza adottate dalla società.

A tal fine, la Società si è dotata di un sistema idoneo alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione (client, server, apparati di sicurezza, apparati di rete etc.) e agli archivi elettronici (file, database, posta elettronica, gestionali, ERP, log etc.) effettuati da parte degli

amministratori di sistema, e dagli utenti di dominio nonché software-house esterne. Tali registrazioni (*access log*) hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste, ovvero per verificare eventuali abusi e/o violazioni della riservatezza dei dati da parte di amministratori di sistema o utenti di dominio. È, pertanto, esclusa la finalità, anche indiretta, del controllo dei lavoratori.

Gli archivi di log (ovvero degli *access log*) risultanti da questo monitoraggio e attività di verifica (accessi, tentativi di accesso, disconnessioni ai sistemi di elaborazione, intesi sia come server che client, a software e database), contengono traccia di alcune operazioni effettuate dagli amministratori di sistema e dagli utenti di dominio nonché software-house esterne. Le informazioni relative alle componenti di file di log eventualmente registrati sono memorizzate e conservate temporaneamente (per una durata minima di almeno 6 mesi). Sono altresì generati automaticamente dai firewall anche per connessioni VPN (connessione e disconnessione)

La Società, inoltre, poiché è tenuta a rendere nota o conoscibile a tutti i dipendenti l'identità di tali soggetti nell'ambito della propria organizzazione, comunica periodicamente, mediante una circolare interna, ad integrazione dell'informativa privacy resa al personale dipendente, il nominativo delle persone fisiche preposte quali amministratori di sistema. La comunicazione a terzi (clienti), solo su loro richiesta, dell'elenco delle persone fisiche preposte quali amministratori di sistema all'interno della società deve essere sempre oggetto di una specifica approvazione da parte del Titolare.

Gli Amministratori di Sistema sono nominalmente e formalmente individuati dalla società con comunicazione diretta.

SEGRETO PROFESSIONALE E INFORMAZIONI RISERVATE

Nella valutazione delle informazioni, il personale dipendente si impegna a osservare ogni cautela perché le stesse rimangano riservate, essendo inteso che, in caso di divulgazione non autorizzata, sarà a suo carico l'onere di provare di avere adottato tali misure.

Il personale dipendente non può divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in tutto o in parte, le informazioni apprese in occasione dello svolgimento delle mansioni, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi. Tali comportamenti includono l'inoltro di mail verso l'esterno, se non per attività lavorative e vietano altresì il re-inoltro ad altri account che non siano quelli aziendali.

Gli obblighi del dipendente in tema di riservatezza dei dati non termineranno all'atto di cessazione del rapporto di lavoro, come previsto dalla legge.

MISURE ORGANIZZATIVE E DI SICUREZZA IN AMBITO PRIVACY

Tutto il personale dipendente che tratta dati ed è stato nominato incaricato al trattamento è tenuto al rispetto dei principi e delle misure organizzative e di sicurezza di cui alla normativa in materia di protezione dei dati personali e, in particolare, devono:

- trattare i dati personali secondo i principi indicati dalla legge, in modo lecito, corretto e trasparente; ciò vuol dire che deve verificare
  i. se il trattamento sia consentito da una norma di legge o di regolamento (es. in materia di sicurezza sul lavoro o normative fiscali) o,
  ii. se il soggetto i cui dati afferiscono abbia ricevuto idonea informativa e/o abbia eventualmente rilasciato il consenso (ove necessario)

- controllare la pertinenza e non eccedenza dei dati raccolti e trattati rispetto alle finalità perseguita, evitando di accogliere dati inutili rispetto al raggiungimento della stessa attuando il "principio di minimizzazione" nel trattamento);

- controllare l'esattezza dei dati ed eventualmente, qualora si renda necessario, provvedere al loro aggiornamento;

- conservare i dati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario agli scopi della raccolta e mettere in atto procedure tali da realizzare la cancellazione degli stessi (ovvero la loro trasformazione in forma anonima) al termine del trattamento;

- rispettare le procedure di autenticazione informatica e di gestione delle credenziali di autenticazione predisposte dall'ufficio IT;

- rispettare le procedure adottate per garantire l'attività di back up e la custodia di copie di sicurezza, salvando i documenti nelle specifiche cartelle di rete a ciò riservate;

- custodire in modo riservato (e per i dati sensibili o giudiziari in maniera separata e in archivi chiusi a chiave) banche dati e comunque ogni documentazione raccolta nello svolgimento dell'attività lavorativa;

- adottare cautele organizzative per garantire che tutte le persone con cui si collabora siano informate sulle regole di riservatezza adottate per proteggere i dati e seguire le istruzioni fornite per evitare abusi per negligenza, imprudenza o imperizia;

- verificare sempre l'origine dei dati utilizzati;

- segnalare al proprio referente IT qualsiasi anomalia riscontrata sui sistemi informatici;

- segnalare qualsiasi anomalia riscontrata nella qualità dei dati presenti nei data base all'amministratore di sistema opportunamente designato;

- attenersi alle istruzioni che sono state e che verranno impartite (mediante apposite lettere di incarico) dal Titolare (o dal Responsabile della Protezione dei Dati nominato) per garantire la corretta gestione dei dati stessi.

GESTIONE DELLE COMUNICAZIONI VERBALI

Durante l'attività lavorativa è consuetudine scambiare comunicazioni e informazioni in forma verbale, pertanto si rivela necessario tenere in considerazione i seguenti principi:
- nel corso di conversazioni di lavoro occorre tutelare le informazioni coerentemente con il loro livello di classificazione e criticità;

- lo scambio di informazioni concernente l'attività lavorativa deve avvenire all'interno di aree che consentano il mantenimento di adeguati livelli di riservatezza (uffici, sale riunioni);
- gli uffici e le sale riunioni devono rimanere chiusi durante lo svolgimento di riunioni, conversazioni telefoniche, ecc., rilevanti per l'attività della Società;
- nel corso di conversazioni telefoniche, qualora non risulti strettamente necessario, è preferibile non fare ricorso al sistema viva voce. Nel caso debba essere utilizzato tale sistema, l'interlocutore deve essere avvisato prima della sua attivazione;
- prima di condividere verbalmente dati ed informazioni di lavoro occorre accertarsi che la propria controparte, date le mansioni e le responsabilità assegnate, sia autorizzata a venirne a conoscenza;
- coloro che sono stati provvisti di un telefono cellulare devono cercare di garantire il massimo riserbo sulle proprie comunicazioni; ciò con particolare attenzione al caso in cui vengano ricevute telefonate in aree affollate, in special modo all'esterno della sede della Società.

DOCUMENTAZIONE CARTACEA

La documentazione cartacea viene spesso sottovalutata rispetto ai file presenti sul proprio pc. La riduzione del numero di fogli stampati rappresenta un grande obiettivo dal punto di vista della salvaguardia delle risorse naturali, ma anche un ottimo sistema per proteggere l'accidentale diffusione di informazioni.
Si ricordano a titolo esemplificativo alcune misure utili a proteggere la riservatezza e la disponibilità delle informazioni in formato cartaceo:

- fare ricorso alla stampa solo in caso di reale necessità e comunque il meno possibile;
- in caso di stampa ritirare immediatamente i documenti stampati;
- non lasciare mai incustoditi sul proprio tavolo documenti riservati, anche in caso di assenza breve. In generale riporli in contenitori sotto chiave o distruggerli in modo sicuro quando non più utili;
- la distruzione dei documenti in modo sicuro avviene con i "raccoglitori di carta" o strappandoli in piccoli pezzi. Evitare in ogni caso di gettare i documenti interi nel cestino dei rifiuti o del riciclo;
- i documenti devono essere controllati e custoditi dagli utilizzatori fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate negli appositi archivi;
- al termine della giornata lavorativa la propria postazione di lavoro deve essere sgombra da tutti i documenti di tipo riservato e da quelli ad uso interno nel caso il posto di lavoro non si trovi in un'area riservata al proprio dipartimento.

CONTROLLI INDIRETTI

La Società si riserva la facoltà, nel rispetto della tutela del diritto alla riservatezza e del principio di proporzionalità e non eccedenza, di svolgere dei controlli difensivi e/o indiretti - mirati e non massivi - che consentano di verificare l'effettiva conformità dell'uso degli strumenti informatici alle presenti prescrizioni, mediante l'ausilio di personale tecnico interno o esterno appositamente autorizzato.
La verifica circa il rispetto del presente Regolamento sarà effettuata anche attraverso gli "strumenti" affidati al personale dipendente per rendere la prestazione lavorativa e per esclusive finalità organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio della Società. Le informazioni raccolte potranno essere utilizzate per tutte le finalità connesse al rapporto di lavoro e – nel caso di comportamenti contrari a quanto indicato nel presente Regolamento - essere utilizzate anche per l'applicazione di eventuali provvedimenti disciplinari. Per strumenti di lavoro si intende – a titolo esemplificativo - l'utilizzo di personal computer, browser utilizzati per internet, utilizzo della mail via web o con strumenti dedicati outlook, del cellulare/tablet istituzionale, (per verifica degli accessi internet, della posta elettronica, etc.).
Un responsabile dei sistemi informativi, nel caso sia necessario procedere a un controllo su incarico del Titolare e per garantire la piena sicurezza della Rete o per motivi di manutenzione, si riserva di superare ogni accesso e limitazione predisposta (ad esempio password) su computer, account e- mail, dischi di rete, server, etc.

Le eventuali attività di controllo e monitoraggio, al fine di prevenire utilizzi indebiti della rete o degli strumenti informatici (su pc, posta elettronica o navigazione Internet, la cui raccolta dati può avvenire anche mediante la consultazione dei file di back up), per le attività del personale dipendente che possono causare danni o essere fonte di responsabilità per la Società, saranno svolte mediante indagine a campione e solo da soggetti a ciò preposti (Titolare o responsabili IT, amministratori e manutentori dei servizi informatici, società esterne nominate responsabili del trattamento) e saranno comunque mirate all'area di rischio individuata. A tal proposito si fa presente che in caso di accesso al pc, file o cartelle contenenti documentazione aziendale non sarà effettuato alcun accesso ad eventuali altri documenti non attinenti allo svolgimento della prestazione lavorativa archiviati sul computer del personale dipendente.

Pertanto, i controlli - proporzionati e non eccedenti anche rispetto allo scopo di verifica dell'adempimento contrattuale - non potranno mai svolgersi direttamente e in modo puntuale, ma saranno preliminarmente compiuti su dati aggregati, riferiti all'intera struttura organizzativa o a suoi Uffici. A seguito di detto controllo anonimo, potrà essere emesso un avviso generalizzato di rilevazione

di eventuali anomalie nell'utilizzo dei presidi tecnologici e con l'invito ad attenersi scrupolosamente a compiti assegnati e alle istruzioni impartite. Se a detta comunicazione non dovessero seguire ulteriori anomalie, la Società non procederà a ulteriori controlli su base individuale e non saranno comunque ammessi controlli prolungati, costanti o indiscriminati. In caso contrario, verranno inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni e a, seconda della gravità della violazione perpetrata, la sanzione prevista potrà prevedere o un semplice richiamo verbale o il divieto temporaneo o permanente dell'utilizzo di strumenti informatici, sino ad arrivare alla risoluzione del rapporto di lavoro, limitatamente alle ipotesi di gravi violazioni e condotte illecite indicate nell'allegato A al presente Regolamento.

Nei casi di accertata violazione dei principi fissati nelle presenti norme generali, è prevista anche l'applicazione dei provvedimenti disciplinari come in seguito specificato, con le modalità ivi previste per il personale dipendente o equiparato e l'applicazione delle sanzioni previste nelle clausole contrattuali per i soggetti non dipendenti.

CONTROLLI SULL'USO DEI SERVIZI DI NAVIGAZIONE INTERNET

Il controllo sull'uso dei servizi di navigazione Internet avviene mediante registrazione automatica delle operazioni effettuate (file di "log").

L'elaborazione dei log e la consultazione dei dati aggregati e anonimi avvengono solo ed esclusivamente nei casi di:
- statistiche sull'uso dei servizi;
- presenza di virus nella navigazione o nei messaggi di posta elettronica, allo scopo di inserire gli eventuali siti compromessi nelle black-list;
- risoluzione di problemi tecnici.

L'associazione dell'operazione alla postazione di lavoro del dipendente può essere effettuata solo tramite specifici ed eccezionali controlli. Questo avviene solo ed esclusivamente nei casi di:
- connessioni massive a siti potenzialmente pericolosi per la sicurezza della rete aziendale, allo scopo di intervenire su client eventualmente infetti da virus;
- risoluzione di problemi tecnici;
- specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria;
- ulteriori usi consentiti dalla Legge.

La registrazione dei log è configurata, ove possibile, in maniera tale da essere automaticamente e periodicamente conservata per le 25 settimane successive sui relativi sistemi. Un eventuale prolungamento può avvenire per motivi legali e in caso di specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

FORMAZIONE E AWARENESS

La prima misura di sicurezza per la protezione delle informazioni aziendali è indubbiamente la preparazione e consapevolezza del personale dipendente nello svolgere il proprio lavoro in modo sicuro.

Consapevolezza e preparazione sono aspetti che fanno parte del background del personale dipendente ma che possono essere sviluppati anche attraverso la formazione nelle varie fasi della vita lavorativa (corsi di inserimento e richiami periodici).

Sono state previste aree dedicate alla formazione. In tali aree si potranno reperire varie risorse per accrescere le proprie competenze e di riflesso migliorare la gestione delle informazioni aziendali.

Periodicamente si procede a interventi formativi specifici per tutti coloro che trattano dati personali e che sono stati istruiti mediante lettera di incarico al trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure organizzative e di sicurezza adeguate adottate dalla Società. La formazione viene

programmata al momento dell'ingresso in servizio, in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

Il Responsabile della Protezione dei Dati personali (privacy@retegasbari.it), ove nominato o il Referente per la privacy aziendale, punto di contatto per tutto il personale dipendente per le attività che riguardano e impattano sul trattamento dei dati personali, è a disposizione del personale dipendente per qualsiasi dubbio o segnalazione.

Si ricorda che i corsi di formazione previsti non sono facoltativi e che la mancata ed ingiustificata assenza può portare a provvedimenti di tipo tecnico-disciplinare.

SANZIONI E PROVVEDIMENTI DISCIPLINARI

Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento, ivi incluso quelle indicate a titolo esemplificativo e non esaustivo nell'allegato A, sono perseguibili con provvedimenti disciplinari individuati nel CCNL vigente (allegato al presente Regolamento) nonché, nei casi più gravi, con azioni civili e penali. È comunque immediatamente applicato, a scopo cautelativo, il temporaneo divieto di utilizzo di strumenti informatici.

A seconda della gravità della violazione perpetrata la sanzione disciplinare prevista può prevedere:

- un semplice richiamo verbale;
- un rimprovero scritto;
- l'applicazione della multa (nella misura determinata nel CCNL);
- la risoluzione immediata del rapporto di lavoro (giusta causa).

Prima di assumere qualsiasi decisione disciplinare per un uso non corretto degli strumenti informatici, della mail aziendale o di internet per fini personali, tuttavia, il dipendente sarà invitato a motivare la ragione di tale utilizzo.

La non osservanza del presente regolamento e disposizioni ivi presenti può comportare, oltre alle sanzioni disciplinari, anche sanzioni civili e penali.

Si precisa inoltre che, ai fini disciplinari, le presenti disposizioni e procedure operative interne, oltre a essere state pubblicate sulla Intranet aziendale, sono affisse in luoghi accessibili a tutti (es. bacheca aziendale), ai sensi dell'art. 7 della Legge 20 maggio 1970 n. 300.

DEROGHE E MODIFICHE DEL PRESENTE REGOLAMENTO

Le modifiche al presente regolamento saranno approvate dall'AU/CdA e comunicate ai dipendenti.

ALLEGATO A

1) Elenco delle condotte vietate:

a) Navigazione intenzionale all'interno di siti web pornografici o pedo-pornografici, detenzione di files di tale natura e/o loro scambio con soggetti terzi;

b) Utilizzo intenzionale della rete aziendale ai fini di:

- 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 o il credo;
- danneggiare, distruggere, cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti, compresa l'intercettazione o la diffusione di parole di accesso (password) e ogni altro "dato personale" come definito dalle leggi sulla protezione della privacy;
- effettuare di qualsiasi tipo di attività volta a raggirare o compromettere i meccanismi di protezione dei sistemi informativi
- sfruttare qualsiasi vulnerabilità derivante da difetti di configurazione o difetti intrinseci ai programmi e/o ai sistemi al fine di commettere azioni illecite o non autorizzate;
- falsificare la propria identità
- svolgere sulla Rete ogni altra attività vietata dalla Legge dello Stato e dalla normativa Internazionale

c) Download intenzionale da internet di files non correlati all'attività lavorativa e per i quali derivi un danno in capo alla Società, di natura civile e/o penale, quale conseguenza della violazione degli obblighi imposti dal d.lgs. 29 dicembre 1992, n. 518, sulla tutela giuridica del *software* e/o dalla l. 18 agosto 2000, n. 248, contenente nuove norme di tutela del diritto d'autore (a titolo esemplificativo: file musicali, film o altro materiale coperto da diritti d'autore);

d) Accesso reiterato e per periodi di tempo complessivamente rilevanti a siti internet di contenuto non attinente all'attività lavorativa, anche dopo avere aziendalmente ricevuto specifici richiami in materia;

e) Comunicazione della password aziendale a terzi, senza a ciò essere stati preventivamente autorizzati, nell'ipotesi che da tale comunicazione deriva un danno alla Società;

f) Utilizzo del telefono o del palmare, con costi a carico della Società, per scopi palesemente non aziendali e non attinenti alla propria attività lavorativa;

g) Comunicazione/distribuzione/diffusione a terzi documenti classificati come "RISERVATI", ricevuti via mail o con altro mezzo, senza un'autorizzazione scritta del proprietario\creatore del documento\file o del Titolare del trattamento;

h) copiare qualsiasi dato o file aziendale ovvero comunicare o diffondere all'esterno dati o file aziendali, soprattutto se "Ad uso interno" o "Riservati", in assenza di una preventiva autorizzazione.

2) Elenco delle tipologie di siti web correlati all'attività lavorativa e liberamente navigabili:

- Siti di Enti Pubblici in genere;

- Siti di Clienti e Fornitori
- Siti di Informazione
- Motori di ricerca

La Società, nella persona del proprio legale rappresentante, ha facoltà di promuovere azione di rivalsa per danni provocati dall'inosservanza del Regolamento aziendale interno o per danneggiamento delle apparecchiature informatiche.

L'utente/dipendente e ogni destinatario del Regolamento è sempre direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet. La responsabilità si estende anche alla violazione degli accessi protetti, del copyright e delle licenze d'uso.

La violazione del Regolamento aziendale interno comporta l'applicazione dei provvedimenti sanzionatori nello stesso descritti o la sospensione d'ufficio dell'utilizzo delle risorse informatiche a disposizione, fatte salve le più gravi sanzioni previste dalle norme di legge e inoltre per il personale dipendente risultano applicabili gli articoli del CCNL di riferimento e l'articolo 7 dello Statuto dei Lavoratori.

3) Estratto dal CCNL GAS-ACQUA

Si rimanda alle disposizioni contenute nel Contratto Nazionale GAS-ACQUA

INFORMATIVA INTEGRATIVA RILASCIATA AI SENSI DELL'ART.13 REG. UE 2016/679

Al fine di assicurare la disponibilità e l'integrità dei sistemi informativi e dei dati e per prevenire utilizzi indebiti che possono essere fonte di responsabilità, vengono introdotti dei sistemi di sicurezza attraverso i quali si configura un trattamento di dati personali riferibili agli utilizzatori dei sistemi informatici.
In particolare per l'utilizzo della risorsa Internet vengono adottati dei meccanismi di cd. "sicurezza perimetrale" (Firewall) atti a limitare e regolamentare l'utilizzo della risorsa per quanto possibile,

La informiamo inoltre che:

1) Per le finalità di

a. controllo della funzionalità dei servizi Internet presenti in azienda, per elaborare statistiche di utilizzo delle risorse Internet, limitarne l'utilizzo alle finalità aziendali e per garantire la sicurezza dell'infrastruttura informatica, oltre che per prevenire (o reprimere) eventuali comportamenti illeciti che possano recare danno all'azienda o a terzi (utilizzo di Peer to Peer, download di materiale coperto da diritti d'autore, etc), i suoi dati personali potranno essere oggetto di controllo attraverso l'analisi dei log generati degli stessi servizi Internet utilizzati o da software di protezione, filtraggio di contenuti dannosi o di regolamentazione dell'utilizzo del traffico web, da parte degli incaricarti dell'ufficio Sistemi informativi nei limiti della finalità indicata e nel rispetto della sua privacy;

b. controllo della funzionalità dei servizi informatici interni all'azienda (diversi dai servizi Internet, a titolo esemplificativo e non esaustivo i log dei server interni, etc), della loro sicurezza e di quella dell'intera infrastruttura, i suoi dati personali potranno essere oggetto di controllo attraverso l'analisi dei log generati degli stessi software (di sistema o applicativi) nei limiti delle finalità indicate e nel rispetto della sua privacy.

2) Il conferimento dei dati è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali e, pertanto, l'eventuale rifiuto a fornirli in tutto o in parte può dar luogo all'impossibilità per l'azienda di dare esecuzione al contratto di lavoro o di svolgere correttamente tutti gli adempimenti, quali quelli di natura retributiva, contributiva, fiscale e assicurativa, connessi al rapporto di lavoro; per tale motivo

a. il conferimento dei dati personali per le finalità di cui al punto 1.a e 1.b è facoltativo ma il relativo trattamento è automaticamente effettuato dal primo utilizzo dei servizi Internet fruibili dall'interno dell'azienda, pertanto l'eventuale rifiuto comporta l'impossibilità di utilizzare tali servizi;
b. il conferimento dei dati personali per le finalità di cui al punto 1.b è obbligatorio in quanto necessario all'assolvimento di un obbligo normativo collegato alla sicurezza degli strumenti elettronici;

Dati trattati: dati riferiti a log presenti sui sistemi di sicurezza o in alert inviati generalmente via posta elettronica, il cui dettaglio lo si può reperire nella scheda del singolo strumento (Firewall, etc). Le registrazioni riguardano esclusivamente azioni, connessioni, eventi vietati in base alla configurazione dello stesso strumento; per quelle derivanti dalle attività consentiteci si limita ad informazioni tecniche (tipi di protocolli, etc) escludendo ogni forma di controllo sui contenuti e altre informazioni aggregate anonime.

Il trattamento dei dati è obbligatorio in quanto imprescindibile da obblighi normativi in carico al titolare del trattamento per la protezione dei sistemi e dei dati.

Le informazioni vengono trattate da personale specificamente autorizzato al trattamento dell'Ufficio sistemi Informativi e la comunicazione di informazioni rivenienti dai log o dagli alert possono essere comunicate agli organi direzionali nei casi di ripetute o gravi comportamenti non conformi alle regole aziendali o che possono rappresentare un pericolo, anche solo in linea teorica, ai sistemi o ai dati, al fine di reprimere eventuali comportamenti non leciti. Altresì le informazioni possono essere comunicate alle autorità giudiziarie in caso di reati.

I dati vengono cancellati periodicamente quando non sussiste più la necessità di trattarli e il periodo varia a seconda dello strumento utilizzato. Tale periodo temporale è desumibile dalla scheda del singolo strumento di controllo.

Relativamente ai dati medesimi potrete esercitare i diritti previsti dagli artt. 15-22 del Reg. UE 2016/679 nei limiti ed alle condizioni previste dalla normativa in materia di protezione dei dati personali.

Il designato interno al trattamento, responsabile dei trattamenti che si configurano attraverso gli strumenti di protezione, è il Sig. Eugenio Pirozzi, Responsabile Sezione IT, raggiungibile alla email eugenio.pirozzi@retegasbari.it

SCHEDA STRUMENTI ELETTRONICI PER TRATTAMENTO DI DATI PERSONALI

Antivirus e Firewall: Un firewall è principalmente una soluzione di sicurezza di rete progettata per filtrare il traffico in entrata o in uscita da una rete o da un endpoint protetto, mentre un antivirus è principalmente una soluzione Endpoint Security progettata per ispezionare i file e il software in esecuzione su un host (client) o un server

1. Firewall / Proxy/ Antivirus.

Informazione trattata: nei log del firewall sono registrate le connessioni effettuate per tipologia e indirizzo, oltre ad info statistiche su tipologia e quantità di traffico, protocolli e sistemi operativi, APP utilizzate e tipi di oggetti.

Descrizione: è possibile risalire a informazioni sulla navigazione utente per utente, cosa viene generato sulle cartelle condivise, cosa viene modificato e/o eliminato, nonché le tipologie di accesso alle banche dati (se in VPN o System, ora di connessione e di chiusura connessione, quanto tempo si rimane connessi)
Frequenza di controllo dello strumento: settimanale antivirus firewall
Tempo di conservazione dei log: 3 mesi
Identificativo Strumento: Firewall / Proxy/ Antivirus (total security whatchgarde e vision – one trend micro)
Finalità specifica: sicurezza degli strumenti elettronici e dei dati trattati (obbligo normativo)
Tipologia di dato trattato: Dati riferibili alla postazione di lavoro o all'utente autenticato, classificabili come dati personali.
Natura del dato trattato: personale e anonimo
Modalità di trattamento: aggregato e non
Soggetti abilitati ad accedere alle informazioni: Eugenio Pirozzi e società esterne che svolgono il servizio di Amministrazione di sistema.

2. Antivirus firewall

Identificativo Strumento: Antivirus firewall (total security whatchgarde e vision – one trend micro)
Tipologia di dato trattato: nome del virus rilevato, nome del client (postazione di lavoro), locazione dell'infezione
Natura del dato trattato: personale e sensibile
Modalità di trattamento: aggregato e non
Informazione trattata: nome del virus rilevato, nome del client (postazione di lavoro) sulla quale è stata rilevata una infezione da virus informatico, dal quale si può desumere l'utilizzatore nel caso in cui il nome del client contenga il nome dell'utilizzatore (o sia presente nella descrizione), o se il virus è presente sulle cartelle utente ed eventualmente informazioni che potrebbero assumere il carattere di dato sensibile nei casi in cui la segnalazione riguardi un documento che riveli ad esempio l'accesso ad un sito per adulti.
Controllo dei log: ogni 30 giorni sul server
Ricezione notifiche email: giornaliera
Tempo di conservazione dei log: 3 mese
Soggetti abilitati ad accedere alle informazioni: Eugenio Pirozzi e società esterne che svolgono il servizio di Amministrazione di sistema.