PROVVEDIMENTO N. 51 DEL 05/10/2023 DELL'AMMINISTRATORE UNICO
OGGETTO: ADOZIONE REGOLAMENTO TELEMATICO E DISCIPLINARE SULL' USO CORRETTO STRUMENTI TELEMATICI DELLA SOCIETA' ARPAC MULTISERVIZI S.R.L.

PREMESSO CHE

- la società ARPAC Multiservizi S.r.l., avente come oggetto l'espletamento di servizi strumentali necessari per lo svolgimento delle attività dell'ARPAC, veniva costituita in data 20/02/2004.
- la società svolge attività esclusivamente per il socio unico ARPA CAMPANIA, così come disciplinato dagli art. 13 e seguenti del D.L. 233/2006 (chiarito e ribadito dal D.lgs 175/16).
- in data 28/12/2016, a seguito dell'entrata in vigore del d.lgs. n. 175/2016, la società ha adeguato lo statuto alle nuove disposizioni che regolano le società partecipate dalla Pubblica Amministrazione, riscrivendo l'oggetto sociale.
- pertanto la società realizza, per conto del socio, tra le altre, le seguenti attività:
  - **a)** servizi di supporto operativo agli Uffici Amministrativi e Tecnici dell'ARPA CAMPANIA (segreterie di direzione, digitazione e scritturazione di documenti e quant'altro necessario per il buon funzionamento degli Uffici;
  - **b)** manutenzione ordinaria e straordinaria, pulizia, disinfezione e disinfestazione, lavaggio e custodia dei beni immobili e mobili, impianti, complessi e laboratori;
  - **c)** Servizi di supporto operativo per l'attività di consulenza tecnico-scientifica nel campo della prevenzione e della tutela ambientale;
  - **d)** monitoraggio ambientale;
  - **e)** verifica, censimento, bonifica di siti inquinati;
  - **f)** gestione di sistemi informativi per l'ambiente;
  - **g)** qualsiasi altra attività collegata alle funzioni esercitate dal Socio ARPA CAMPANIA

TENUTO CONTO CHE

- il progresso e la costante diffusione delle nuove tecnologie informatiche in uno al libero accesso alla rete internet, ha rappresentato fonte di criticità nell'approccio, mancando lo sviluppo in parallelo della cultura del settore ed una vera e propria rete di cyber security.
- E' necessario redigere e mantenere aggiornata una regolamentazione netta e precisa internamente all' amministrazione.
- La volontà di implementare e specificare le regole già contenute nel Codice di Comportamento adottato riguardante i corretti modi d'uso della rete e delle risorse informatiche aziendali.

VISTO

- **Legge 20.05.1970, n. 300** (Statuto dei lavoratori).
- **Il Regolamento (UE) n. 2016/679** (GDPR - Decreto Legislativo 30.06.2003, n. 196 (Codice in materia di protezione dei dati personali).
- **Art. 64-bis[co1] D. Lgs. n. 82 del 73/2005** e s.m.i., CAD"i soggetti di cui all'articolo 2, comma 2, rendono fruibili i propri servizi in rete, in conformità alle Linee guida, tramite il punto di accesso telematico attivato presso la Presidenza del Consiglio dei ministri [...]".
- **Art. 64-bis [co1-bis]**, "[...] i soggetti di cui all'art. 2 [co 2.] i fornitori di identità digitali e i prestatori di servizi fiduciari qualificati, in sede di evoluzione, progettano e sviluppano i propri sistemi e servizi in modo da garantire l'integrazione e l'interoperabilità tra i diversi sistemi e servizi e con i servizi di cui ai commi 1 e 1 ter, espongono per ogni servizio le interfacce applicative [...]".
- **Circ. AGID 18 aprile 2017, n. 2/2017**- complesso misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto e indicazioni operative per la verifica delle condizioni minime di sicurezza e del trattamento dei dati.
- **"Linee guida del Garante per posta elettronica e internet"** in Gazzetta Ufficiale n. 58/2007;
- **Art. 23 del D.lgs. n. 151/2015 (c.d. Jobs Act)** mod e rimodulaz. fattispecie del divieto dei controlli a distanza, tenuto conto dell'attuale contesto e degli impianti e strumenti dell'attività dei lavorator e di quelli utilizzati dal lavoratore per rendere la prestazione lavorativa.
- **Tutte le disposizioni Anac Trasparenza e Anticorruzione**
- **Piano triennale integrato prevenzione della corruzione e trasparenza**
- **Codice Etico e di Comportamento AMS adottato e pubblicato sul sito**
- **Contratto Collettivo Nazionale di Lavoro di riferimento Igiene Ambientale – Aziende Municipalizzate.**
- **Modello di Organizzazione, Gestione e Controllo ex D. Lgs 231/01**
- **Regolamento Arpac per il controllo analogo degli organismi partecipanti** (Deliberazi. n.304/2019).

CONSIDERATO CHE

- La società AMS dispone di una rete informatica e telematica, costituita da un insieme di strumenti e mezzi informatici quali le componenti hardware e software (personal computer, server, strumenti per la stampa e la riproduzione, programmi ecc.) e dei necessari collegamenti telematici che veicolano le informazioni da e verso le banche dati .
- L'azienda è tenuta a garantire a tutti i soggetti autorizzati ed alla platea dei dipendenti e collaboratori un'adeguata e continuativa informazione in merito ai rischi e alle problematiche relative alla sicurezza in materia di trattamento dei dati tramite l'utilizzo degli strumenti informatici.

DATO ATTO CHE

- L'utilizzo della rete informatica e telematica, di internet e della posta elettronica, sono strumenti ormai indispensabili per perseguire con efficienza, efficacia ed economicità le funzioni istituzionali e gestionali delle amministrazioni come imposto dalle normative vigenti, che sempre più tendono alla globalità delle informazioni telematiche.
- E' compito del'azienda assicurare la piena funzionalità del sistema informatico e promuovere ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati.
- Resta ferma la responsabilità civile e penale di ogni utente del corretto utilizzo delle risorse informatiche a cui ha accesso e dei dati trattati a fini istituzionali

PRESO ATTO CHE

- Risulta fondamentale individuare il complesso delle misure che configurano il livello minimo di protezione del sistema informatico e del patrimonio informativo digitale della Società.
- E' obiettivo fondamentale omologarsi e conformarsi alle regole interne e alla specifica normativa di settore fornendo a tutti i dipendenti, per lo svolgimento delle proprie mansioni istituzionali, uno schema preciso di comportamento che eviti violazioni in ed output, nonché regole chiare per la tutela dei beni di proprietà della Società consegnati in uso ai propri dipendenti, al fine di evitare condotte inconsapevoli e/o scorretti che possono esporre a rischi connessi con la sicurezza, oltre ad eventuali danni patrimoniali a terzi.
- Risulta necessario disciplinare le misure con le quali si può eventualmente accertare e inibire le eventuali condotte illecite sull'utilizzo delle predette risorse, ponendo in essere adeguati e commisurati sistemi di controllo, senza che ciò possa violare la sfera personale del lavoratore e il suo diritto alla riservatezza ed alla dignità (L. 20/05/1970 n. 300).

L'Amministratore Unico p.t. dott. Antimo Piccirillo

DELIBERA

le premesse e le considerazioni che precedono fanno parte integrante della presente delibera con la quale si approva e si adotta il **REGOLAMENTO TELEMATICO E DISCIPLINARE SULL' USO CORRETTO STRUMENTI TELEMATICI DELLA SOCIETA' ARPAC MULTISERVIZI S.R.L.**

Il presente atto è immediatamente esecutivo ed avrà efficacia come per legge dalla pubblicazione .

Si trasmette il presente provvedimento al Responsabile per la Trasparenza e la Pubblicità degli atti per la pubblicazione sul sito istituzionale nella sezione "Società Trasparente" nei tempi e nei modi previsti dalla legge di riferimento in modo che siano osservati tutti gli adempimenti del caso.

Verrà affisso nella bacheca aziendale, nonché nelle sedi ARPAC dove prestano servizio i dipendenti dell'Arpac Multiservizi.

Sarà comunicato a cura della Segreteria Generale ai seguenti destinatari:

- Ai Coordinatori di Area affinché ne diano la necessaria diffusione e a tutti i dipendenti dell'azienda a mezzo delle mail aziendali di ciascuno;
- Ai Rappresentanti Sindacali;
- Al Collegio Sindacale;
- Ai membri dell'ODV;
- Al Responsabile del controllo Analogo dell'Arpa Campania.

L'Amministratore Unico
Dott. Antimo Piccirillo

REGOLAMENTO ACCESSO TELEMATICO
E
DISCIPLINARE SUL CORRETTO UTILIZZO DEGLI STRUMENTI INFORMATICI

ARPAC MULTISERVIZI SRL

A CURA DEL
COORDINATORE UFFICIO AFFARI LEGALI
IN COLLABORAZIONE CON SUPPORTO INFORMATICO
Giuseppe Morvillo

RPCT AVV. ANGELA PESCE

ADOTTATO DA

AMMINISTRATORE UNICO
DOTT. ANTIMO BICCIRILLO

INDICE

❖ SIGNIFICATO DI TERMINI INFORMATICI

1. Backup: duplicazione di un file o di un insieme di file su un supporto esterno al computer, per avere una copia di riserva.
2. Cloud: sistema configurato su server remoto che consente di disporre di risorse software e hardware (memorie di massa per archiviazione dati, o applicazioni).
3. Dato: (datum -letteralmente fatto) una descrizione codificata di una transazione o avvenimento o altro che può portare alla conoscenza di un'informazione.
4. Dato pubblico: dato che può esso reso disponibile per chiunque.
5. Dato a conoscibilità limitata: dato la cui conoscibilità è riservata per legge o Regolamento a specifici soggetti o categorie di soggetti.
6. Dato personale: informazioni relative alla persona fisica identificabile, anche indirettamente, mediante riferimento a qualsiasi altro dato, ivi compreso un numero di riconoscimento personale (sono sottoposti alla normativa Privacy).
7. Dati di tipo aperto: alcune tipologie di dati liberamente accessibili a tutti, privi di brevetti o altre forme di controllo che ne limitino la riproduzione e le cui restrizioni di copyright eventualmente si limitano ad obbligare di citare la fonte o al rilascio delle modifiche allo stesso modo.
8. Documento: il termine indica qualsiasi cosa sia portatrice di significato, a prescindere dal supporto sul quale è registrato.
9. Download: scaricamento tramite rete telematica di uno o più file, trasferendolo sul disco rigido del computer o su altra periferica.
10. File sarin : sistema per lo scambio di file tra utenti di Internet tramite un server comune.
11. Hard disk: principale unità di memorizzazione dei dati sul computer, in cui vengono memorizzati il sistema operativo, i programmi applicativi, i dati di configurazione del computer, ed eventualmente i documenti creati dall'utente.
12. Login: procedura di accesso a un sistema informatico, che prevede l'inserimento di un codice identificativo (UserID o nome utente) e di una parola d'ordine (Password) da parte dell'utente.
13. Logout: procedura di scollegamento da un sistema informatico a cui si era avuto accesso tramite un'operazione di login
14. Titolare del dato: Società Arpac Multiservizi srl che ha originariamente raccolto, elaborato, archiviato o commissionato ad altro soggetto pubblico o privato il documento o una informazione;
15. Pubblicazione: disponibilità di dati e documenti nel sito istituzionale di AMS, con accesso diretto senza necessità di richiesta formale diretta o indiretta;
16. Riutilizzo: uso del dato, di cui è titolare AMS, da parte di persone fisiche o giuridiche, per qualsiasi utilità consentita dalla legge;
17. Licenza per il riutilizzo: un contratto, Regolamento o altro strumento negoziale, nel quale sono definite le modalità di riutilizzo dei dati.
18. Banca dati: archivio dati in cui le informazioni in esso contenute sono strutturate e collegate tra loro secondo un particolare modello logico.
19. Data set: è un insieme di dati strutturati in forma tabellare, dati statistici, in cui ogni colonna rappresenta una particolare variabile, e ogni riga corrisponde ad un determinato membro del dataset in questione.
20. Metadato: "dato su un (altro) dato è un'informazione che descrive un insieme di dati.
21. Interoperabilità informatica: la capacità di un sistema di cooperare e di scambiare informazioni con altri sistemi in maniera più o meno completa e priva di errori, con affidabilità e con ottimizzazione delle risorse.
22. PDL: Postazione di Lavoro al PC, notebook o altro dispositivo assegnato ad un utente per lo svolgimento delle proprie attività lavorative.
23. Trattamento : qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati. Il Trattamento diventa informatico se è effettuato con l'ausilio di strumenti elettronici.
24. Data breach: violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati personali trasmessi, conservati o comunque trattati.
25. Dato personale: qualunque informazione riguardante persona fisica, persona giuridica, ente od associazione, identificata o identificabile, anche indirettamente.
26. Password: parola d'ordine dell'utente.
27. Phishing: Truffa informatica effettuata inviando un'e-mail con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati (numero di carta di credito, password di accesso al servizio di home banking, ecc.), motivando tale richiesta con ragioni di ordine tecnico.
28. PIN: codice alfanumerico breve (di solito non più di 8 caratteri) abbinato a nome utente e password, che integra la sicurezza negli accessi ai sistemi informatici.
29. Risorse informatiche: tutte le risorse informatiche di AMS: i server; le workstation, i personal computer, i notebook e qualsiasi altra tipologia di elaboratore elettronico, compresi i dispositivi mobili;le apparecchiature telefoniche VoIP; le stampanti, i plotter, i fotocopiatori e i fax; gli apparati di rete; il software ed i dati acquisiti o prodotti da parte degli utenti o di terzi autorizzati; file di qualsiasi natura, archivi di dati anche non strutturati.
30. Server: computer di elevate prestazioni, che in una rete distribuisce un servizio o l'accesso a cartelle e file di dati agli elaboratori degli utenti collegati, detti client.
31. Software: è l'insieme delle componenti immateriali di un sistema informatico, costituito principalmente dai programmi che vengono elaborati dal computer; è contrapposto all'hardware, cioè la parte materiale, tangibile, dello stesso sistema.
32. SPAM: messaggio pubblicitario non richiesto
33. Smartworking: (lavoro agile): SW modalità di svolgimento della prestazione lavorativa al di fuori dei locali dell'Azienda, senza una locazione fissa, decidendo in piena autonomia i tempi ed il luogo di lavoro: il dipendente è quindi libero di scegliere e cambiare l'ambiente dove lavorare (da casa, da una camera d'albergo o in treno): gli obiettivi/risultati da raggiungere vengono definiti in un accordo scritto che deve inoltre individuare i tempi di riposo del lavoratore e le misure idonee per assicurarne la disconnessione.
34. Software: insieme procedure in un sistema elaborazione dati usati da AMS (Iperius Remote – Zucchetti- Coopera- Profis).
35. Spyware: software scaricato, per lo più in maniera inconsapevole, durante la navigazione in Internet o l'installazione di un software gratuito, programmato per registrare e trasmettere a terzi dati personali e informazioni sull'attività online di un utente, generalmente a scopo pubblicitario.
36. Worm: sottoclasse di virus, software che crea diverse copie di se stesso in uno stesso computer

❖ LINEE GUIDA GENERALI

La presente regolamentazione ai sensi della normativa vigente disciplina:

- ✓ la modalità di pubblicazione dei dati, metadati e delle relative banche dati in possesso dell'azienda AMS, compreso l'esercizio della facoltà di accesso telematico e riutilizzo degli stessi;
- ✓ le condizioni di utilizzo delle risorse informatiche e dei dispositivi fissi e mobili (personal computer, smartphone, tablet, modem/router, etc.), qualora utilizzate come strumenti informatici, informativi e digitalizzazione messi a disposizione del personale dipendente e non dipendente ("Utenti") per l'esecuzione delle funzioni istituzionali di competenza, non solo all'interno dei locali dell'Azienda AMS, ma anche in modalità remota o agile (smart working).

I dati pubblici detenuti dall'Arpac Multiservizi srl, prodotti o acquisiti nell'ambito dell'esercizio delle funzioni istituzionali sono accessibili e riutilizzabili liberamente ovvero resi disponibili, sul portale web https://www.arpacmultiservizi.it che favorisce la partecipazione consapevole degli stakeholder nei limiti consentiti dalla legge.

L'applicazione ed il rispetto puntuale delle disposizioni contenute nel presente Regolamento è responsabilità di tutti i soggetti che utilizzano gli strumenti informatici messi a disposizione dall'Ente.

Ferme restando le disposizioni normative in materia e tutte le prescrizioni previste per il trattamento dei dati sensibili o giudiziari, il contenuto del presente Regolamento costituisce disposizione di servizio.

❖ RIFERIMENTI NORMATIVI

Art. 64-bis[co1] D. Lgs. n. 82 del 73/2005 e s.m.i.., il Codice dell'amministrazione digitale (CAD), prevede che "i soggetti di cui all'articolo 2, comma 2, rendono fruibili i propri servizi in rete, in conformità alle Linee guida, tramite il punto di accesso telematico attivato presso la Presidenza del Consiglio dei ministri [...]".

Art. 64-bis [co1-bis], "[...] i soggetti di cui all'art. 2, co 2, i fornitori di identità digitali e i prestatori di servizi fiduciari qualificati, in sede di evoluzione, progettano e sviluppano i propri sistemi e servizi in modo da garantire l'integrazione e l'interoperabilità tra i diversi sistemi e servizi e con i servizi di cui ai commi 1 e 1 ter, espongono per ogni servizio le interfacce applicative [...]".

Circ. AGID 18 aprile 2017, n. 2/2017

Le misure minime di sicurezza ovvero il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto sono individuate dall'AgID come riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti. Esse consistono in controlli di natura tecnologica, organizzativa e procedurale e utili alle Amministrazioni per valutare il proprio livello di sicurezza informatica.

Tutte le disposizioni Anac Trasparenza e Anticorruzione

RIFERIMENTI INTERNI

- Piano triennale integrato prevenzione della corruzione e trasparenza
- Codice Etico e di Comportamento AMS adottato e pubblicato sul sito
- Contratto Collettivo Nazionale di Lavoro di riferimento Igiene Ambientale – Aziende Municipalizzate.
- Modello di Organizzazione, Gestione e Controllo ex D. Lgs 231/01

❖ SCOPO OBIETTIVI

Il progresso e la costante diffusione delle nuove tecnologie informatiche in uno al libero accesso alla rete internet, ha rappresentato fonte di criticità nell'approccio, mancando lo sviluppo in parallelo della cultura del settore ed una vera e propria rete di cyber security.

A questo scopo risponde la necessità di redigere e mantenere aggiornata una regolamentazione netta e precisa internamente all' amministrazione.

Il presente Regolamento, che integra e completa le regole già contenute nel Codice di Comportamento adottato cui fa riferimento, contiene le disposizioni riguardanti i corretti modi d'uso della rete informatica e di tutte le risorse informatiche aziendali, proponendosi come obiettivo l'omologazione e la conformità delle regole interne a quanto previsto dalla specifica normativa di settore allo scopo di fornire agli utenti :

- uno schema preciso di comportamento evitando le violazioni in generale (in ed output).
- regole per la tutela dei beni di proprietà della Società consegnati in uso ai propri dipendenti, al fine di evitare condotte inconsapevoli e/o scorrette, che possono esporre a rischi connessi con la sicurezza, oltre ad eventuali danni patrimoniali a terzi, o di immagine.

❖ AMBITO DI APPLICAZIONE

Il presente Regolamento si applica a tutto il personale dipendente dell'ARPAC Multiservizi srl , senza distinzione di ruolo o livello ed a tutti i collaboratori a prescindere dal rapporto contrattuale intrattenuto con la stessae a tutti i soggetti che a qualsiasi titolo vengano in contatto con la società .

Condotte non conformi al presente regolamento saranno valutate anche ai fini disciplinari.

❖ CRITERI ISPIRATORI

I principi ispiratori sono:

a) rispetto delle leggi e norme vigenti, in particolare le leggi in materia di sicurezza dei dati, tutela della privacy, tutela del copyright e modalità di accesso e uso dei sistemi informatici e telematici;
b) rispetto delle norme e procedure lavorative generali;
c) rispetto delle norme e procedure specifiche definite dall'Azienda.

❖ STRUMENTI INFORMATICI

Tra le risorse informatiche sono annoverate :

- i server
- le workstation
- i personal computer
- i notebook
- qualsiasi altra tipologia di elaboratore elettronico, compresi i dispositivi mobili;
- le apparecchiature telefoniche Voip
- le stampanti, i plotter, i fotocopiatori e i fax
- gli apparati di rete e tutti gli strumenti informatici interconnessi connessi in rete
- il software ed i dati acquisiti o prodotti da parte degli utenti o di terzi autorizzati
- file di qualsiasi natura, archivi di dati anche non strutturati ed applicazioni informatiche.

❖ TITOLARITÀ DEI BENI E DELLE RISORSE INFORMATICHE

I beni e le risorse informatiche, i servizi IT (Information Technology) e le reti informative **costituiscono beni aziendali rientranti nel patrimonio sociale di esclusiva proprietà di ARPAC MULTISERVIZI SRL.**

Il loro utilizzo è consentito solo per finalità di adempimento delle mansioni lavorative affidate ad ogni utente in base al rapporto in essere (ovvero per scopi professionali afferenti all'attività svolta e comunque per l'esclusivo perseguimento di obiettivi aziendali).

❖ RAPPORTO CON LA NORMATIVA PRIVACY

La pubblicazione di dati personali deve avvenire nel rispetto di quanto indicato dalle norme vigenti in materia di protezione dei dati personali e, in particolare, selezionando accuratamente i dati personali che possono essere resi conoscibili on-line, fermo restando che la pubblicazione degli stessi è ammessa unicamente quando la legge lo consente.

In ogni caso occorre rispettare il principio di proporzionalità e pertinenza dei dati pubblicati e procedere all'anonimizzazione o alla pubblicazione di dati aggregati che non consentano l'identificazione degli interessati.

I dati e le banche dati oggetto di riutilizzo seguono la disciplina individuata nel Regolamento Privacy AMS adottato e pubblicato sul sito istituzionale. Essi devono comunque salvaguardare:

- la sicurezza pubblica, la difesa nazionale, lo svolgimento di indagini penali o disciplinari;
- il diritto di terzi al segreto industriale;
- la disciplina sulla protezione del diritto d'autore, anche compatibilmente con le disposizioni di accordi internazionali sulla protezione dei diritti di proprietà intellettuale;
- la disciplina in materia di accesso ai documenti amministrativi, di cui al Capo V della legge 7 agosto 1990, n. 241;
- la disciplina sulla protezione dei dati personali di cui al D. Lgs. 30 giugno 2003, n. 196 e s.m.i.

In base all' art. 9 del GDPR a all' art.10 del Regolamento (UE) 2016/679 sono da puntualizzare alcune nozioni.

✓Dati identificativi sono i dati personali che permettono l'identificazione diretta del soggetto ovvero i dati anagrafici (es: CF indirizzo IP- Tg

✓Dati personali particolari sono quelli che per loro natura, sono maggiormente sensibili e rivelano:

- l'origine razziale o etnica;
- le opinioni politiche;
- le convinzioni religiose o filosofiche;
- l'appartenenza sindacale;
- dati genetici;
- dati biometrici intesi a identificare in modo univoco una persona fisica;
- dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

✓Dati giudiziari i dati relativi a condanne penali e reati, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (es: i provvedimenti penali di condanna definitivi, liberazione condizionale, divieto od obbligo di soggiorno, misure alternative alla detenzione) o la qualità di imputato o di indagato.

✓Il titolare" è la persona fisica o giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

✓Il responsabile" - la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali; in riferimento al trattamento dei dati con strumenti elettronici particolare rilevanza assume il "Responsabile del Trattamento Dati Informatici e Telematici", di cui al punto successivo.

✓Responsabile del Trattamento Dati Informatici e Telematici"

✓Interessato è la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

✓Utente è il soggetto che accede ed utilizza i servizi e gli strumenti del sistema informatico dell'Azienda.

✓Accessibilità è la capacità dei sistemi informatici, ivi inclusi i siti web e le applicazioni mobili nelle forme e nei limiti consentiti dalle conoscenze tecnologiche, di erogare servizi e fornire informazioni fruibili, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari.

✓Cloud è un sistema di elaborazione e di archiviazione dei dati della rete aziendale che consente l'accesso ad applicazioni e dati memorizzati su un hardware remoto invece che su workstation locale.

L'art. 30 del Regolamento (RGPD -EU) n. 679/2016 prevede tra gli adempimenti principali del titolare e del responsabile del trattamento la tenuta del registro delle attività di trattamento.
E' un documento contenente le principali informazioni relative alle operazioni di trattamento svolte dal titolare e dal responsabile del trattamento e costituisce uno dei principali elementi di accountability del titolare.
E'uno strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.
Il registro deve avere forma scritta, anche elettronica e deve essere esibito su richiesta al Garante.
Tutti i titolari e i responsabili del trattamento sono tenuti a redigere il Registro delle attività di trattamento (v. art. 30, par. 1 e 2 del RGPD).
In particolare, in ambito privato, i soggetti obbligati sono stati individuati e tassativamente elencati e tra questi :

- ✓ imprese o organizzazioni con almeno 250 dipendenti;
- ✓ qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che possano presentare un rischio – anche non elevato – per i diritti e le libertà dell'interessato;
- ✓ qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti non occasionali;
- ✓ qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle categorie particolari di dati di cui all'articolo 9, paragrafo 1 RGPD, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10 RGPD.

Si precisa che le imprese e organizzazioni con meno di 250 dipendenti obbligate alla tenuta del registro potranno comunque beneficiare di alcune misure di semplificazione, potendo circoscrivere l'obbligo di redazione del registro alle sole specifiche attività di trattamento sopra individuate.
Pertanto alla luce di quanto alla normativa generale e per ottemperare alle raccomandazione del Garante Arpac Multiservizi si adeguerà a tale principio di accountability per agevolare in maniera collaborativa l'attività di controllo del Garante stesso.

❖ PUBBLICITÀ

Il presente Regolamento entra in vigore alla data della sua approvazione, che avviene mediante Deliberazione sottoscritta dall'A.U. aziendale e sarà pubblicato nell'apposita sezione del sito web istituzionale denominata "Amministrazione Trasparente" garantendone la massima diffusione a tutto il personale con invio, a mezzo della segreteria generale, sulle rispettive mail aziendali a tutto il personale, all'OdV e al Socio. Per completezza il documento sarà esposto nella bacheca aziendale.
Il Regolamento potrà essere soggetto a revisioni periodiche sulla base dell'evoluzione normativa, tecnologica e delle nuove esigenze di sicurezza.

❖ ACCESSO E PUBBLICAZIONE

Come già dedotto in precedenza, ARPAC Multiservizi srl è dotata di un portale istituzionale https://www.arpacmultiservizi.it/ su cui si mettono a disposizione diretta degli utenti tutte le informazioni pertinenti alle attività istituzionali dell'Azienda.
Esso è realizzato secondo le norme e con le caratteristiche delle Pubbliche Amministrazioni, ove rende disponibili i dati, avendo presente che la messa a disposizione di dati in formato aperto non preclude anche l'impiego di altri formati (non aperti), laddove ciò possa facilitarne il riutilizzo
L'aggiornamento dei dati pubblicati con modalità automatica è effettuato, per quanto possibile, in tempo reale tenendo conto dei tempi di validazione/valutazione e comunque nei tempi e nelle modalità stabilite dalle disposizioni "Linee Guida" Anac.
Ogni oggetto scaricabile presente sul sito, quali documentazione tecnica, normativa, modulistica e software, salvo diversa indicazione, è liberamente e gratuitamente disponibile, citando la fonte, sotto licenze che ne consentono il riutilizzo gratuito fatta salva l'attribuzione dei dati stessi.
Chiunque può chiedere informazioni .

❖ TUTELA DEL LAVORATORE

Alla luce dell'art. 4 [co1] L. n. 300/1970, la regolamentazione della materia indicata nell'art. 1 del presente Regolamento, non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.
È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. 679/16 .

❖ OBBLIGHI DEL DIPENDENTE

Tra le conseguenze derivanti dall'esistenza del contratto di lavoro subordinato è previsto il diritto del datore di lavoro di esercitare un potere disciplinare di natura sanzionatoria, a fronte di comportamenti del lavoratore in violazione degli obblighi contrattuali, della normativa interna in ogni ambito ordinato.
I dipendenti dell'Arpac Multiservizi srl conformano la propria condotta alle disposizioni sul comportamento ed i doveri del dipendente come stabilito dalla normativa generale del Codice Civile del Codice Etico e di Comportamento adottato,pubblicato e diffuso tra dipendenti e collaboratori, ferma la disciplina vigente in materia di responsabilità civile, amministrativa, penale e contabile.
Gli strumenti informatici e telematici, sono messi a disposizione dell'Utente esclusivamente per finalità di tipo lavorativo, per cui non è permesso utilizzare questi strumenti per altre finalità non connesse all'attività lavorativa o in violazione delle leggi italiane ed europee vigenti
I principi a fondamento del presente Regolamento sono gli stessi espressi nel GDPR in particolare e sono legati alla riservatezza nelle comunicazioni ovvero:

1. **il principio di necessità**, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e 6 del Reg. 679/16);
1. **il principio di pertinenza e non eccedenza** i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art.5 commi 1 e 2).

Tutta la normativa è stata già delineata nel Codice di Comportamento adottato e presente sul sito istituzionale e comunque non è consentito.

Il datore di lavoro

- ✓ deve trattare i dati nella misura meno invasiva possibile
- ✓ ha il potere di svolgere l'attività di monitoraggio, che nella fattispecie saranno svolte da un Amministratore di Sistema ovvero un soggetto preposto a gestire e mantenere il sistema informatico aziendale, amministrando banche dati e RSM informatiche, apparati di sicurezza o software complessi.

Al dipendente non è consentito:

1. **accedere a siti ed acquisire o diffondere prodotti informativi lesivi del comune senso del pudore;**
2. **diffondere prodotti informativi lesivi dell'onorabilità, individuale e collettiva oppure di natura politica;**
3. **diffondere in rete, o con qualsiasi altro mezzo di comunicazione, informazioni riservate di qualunque natura;**
4. **svolgere ogni tipo di attività commerciale;**
5. **compiere attività che possano rappresentare una violazione della legge in materia di Copyright, fra le quali la copia non autorizzata di software, supporti audio e video, clonazione o programmazione di smartcard;**
6. **compiere attività che compromettano in qualsiasi modo la sicurezza delle risorse informatiche e della rete aziendale.**
7. **comunicare a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, elementi e informazioni dei quali il dipendente / collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile di area/funzione.**
8. **È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro.**

❖ ESCLUSIONI

La pubblicazione di dati personali deve avvenire nel rispetto delle indicazioni generale selezionando accuratamente i dati personali che possono essere resi conoscibili on-line, fermo restando che la pubblicazione degli stessi è ammessa unicamente quando è prevista da una norma di legge e che, comunque, occorre rispettare il principio di proporzionalità e pertinenza dei dati pubblicati.

Eventualmente si può procedere all'anonimizzazione o alla pubblicazione di dati aggregati che non consentano l'identificazione degli interessati cui i dati si riferiscono.

I dati e le banche dati oggetto di riutilizzo, saranno pubblicati in modo tale da salvaguardare:

- la sicurezza pubblica, la difesa nazionale, lo svolgimento di indagini penali o disciplinari;
- il diritto di terzi al segreto industriale;
- la disciplina sulla protezione del diritto d'autore, anche compatibilmente con le disposizioni di accordi internazionali sulla protezione dei diritti di proprietà intellettuale;
- la disciplina in materia di accesso ai documenti amministrativi, di cui al Capo V della legge 7 agosto 1990, n. 241;
- la disciplina sulla protezione dei dati personali di cui al D. Lgs. 30 giugno 2003, n. 196 e s.m.i.

❖ LOCALI E POSTAZIONE DI LAVORO

Il lavoratore deve:

1) Tenere la propria area di lavoro in ordine e pulita, evitando di lasciare residui di cibo e bevande durante l'orario di lavoro.
2) Utilizzare il telefono aziendale, di rete fissa o mobile, nonché il fax, internet e la posta elettronica esclusivamente per scopi inerenti all'attività lavorativa.
3) Evitare di utilizzare il telefono cellulare personale durante l'orario di lavoro, salvo per casi di comprovata necessità e urgenza e per motivi di lavoro per chi non ha telefoni aziendali.
4) Evitare di accedere in uffici diversi da quelli a cui è adibito in assenza dei dipendenti addetti a quell'ufficio;
5) È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni quando il dipendente/collaboratore si allontana dalla postazione di lavoro.
6) È vietato lasciare sulla postazione di lavoro materiali contenente dati sensibili in evidenza .

❖ MEZZI DI TRASPORTO OPERATIVI E ATTREZZATURE

Non è consentito l'uso dei mezzi operativi per usi personali o estranei all'attività aziendale.
Il lavoratore deve aver cura dei mezzi assegnati per il servizio nonché delle attrezzature e strumenti di lavoro e al termine del turno di servizio aziendale dovrà compilare i moduli previsti dalle procedure aziendali. In fase di lavoro e di guida il lavoratore deve

1. Aver cura del veicolo assegnato nonché riconsegnarlo in perfetto stato.
2. Parcheggiare la propria autovettura nei luoghi consentiti
3. Segnalare tempestivamente qualsiasi guasto o malfunzionamento al responsabile.
4. Osservare le disposizioni del Codice della Strada, nonché tutte le possibili misure precauzionali di sicurezza volte a prevenire possibili rischi per la salute e l'incolumità di se stessi e dei terzi.
5. Compilare in caso di incidente stradale la documentazione necessaria, nonché informare tempestivamente il responsabile dell'azienda o, se necessario, la polizia stradale.
6. Il rifornimento a mezzo di carte carburante da utilizzarsi presso i punti di distribuzione convenzionati di carburante può essere effettuato secondo le modalità previste per prassi aziendale consolidata.
7. Il lavoratore deve utilizzare i veicoli aziendali non operativi (automobili) esclusivamente per ragioni inerenti l'attività lavorativa, previa autorizzazione del responsabile: **non è permesso** l'utilizzo del mezzo in giornate non lavorative, né ritirare il mezzo la sera prima o rientrare a casa con il mezzo aziendale, salvo casi di comprovata necessità autorizzati dall'azienda.
8. Prendersi cura della propria sicurezza e della propria salute e di quella delle altre persone presenti sul luogo di lavoro, su cui possono ricadere gli effetti delle proprie azioni o omissioni, conformemente alla formazione e alle istruzioni ricevute e ai mezzi forniti dal datore di lavoro.
9. Osservare le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti, per la protezione della salute e della sicurezza collettiva e individuale.
10. Utilizzare correttamente i dispositivi di sicurezza.
11. Utilizzare in modo appropriato i dispositivi di protezione messi a disposizione
12. Segnalare immediatamente le carenze circa i dispositivi di sicurezza, nonché le altre eventuali condizioni di pericolo, adoperandosi per eliminare o ridurre pericoli.
13. Non compiere di propria iniziativa operazioni o manovre che non sono di propria competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori.
14. Rispettare l'obbligo di formazione di riferimento e tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza dei lavoratori durante il lavoro.
15. segnalare con tempestività al proprio superiore eventuali irregolarità nell'andamento del lavoro di cui venga a conoscenza.

❖ **IN TEMA DI LAVORO AGILE (SMART WORKING)**

Il lavoro agile consiste in una prestazione di lavoro subordinato che prevede lo svolgimento di parte dell'attività lavorativa in parte al di fuori dei locali aziendali con l'obiettivo di incrementare la produttività aziendale, favorire la conciliazione dei tempi di vita e di lavoro e facilitare una maggiore sostenibilità ambientale.

Il lavoro agile non comporta modifica degli obblighi e dei doveri del lavoratore, che assolverà alle proprie mansioni con diligenza attenendosi all'osservanza delle norme legali e contrattuali e alle istruzioni ricevute dall'azienda per l'esecuzione del lavoro, adottando ogni cautela, al fine di assicurare l'assoluta segretezza delle informazioni aziendali e nel rispetto tassativo della idoneità del luogo individuato nel contratto individuale.

Con lo Smart working il lavoro viene svolto a distanza, fuori dagli ambienti aziendali, utilizzando tecnologie informatiche private secondo un'intesa scritta per il corretto svolgimento del rapporto di lavoro.

La prestazione dell'attività lavorativa in "lavoro agile" non incide sull'assoggettamento al potere direttivo, di controllo e disciplinare dell'azienda né sulla connotazione giuridica del rapporto di lavoro subordinato, né incide sull'inquadramento, sul livello retributivo e sulle possibilità di crescita professionale del lavoratore (CCNL riferimento).

Per quanto non regolato dal presente articolo si fa riferimento al Regolamento Smart Working (Delibera n.23 del 20/03/2023) adottato e pubblicato sul sito ed alle norme legali vigenti in materia.

Il datore di lavoro deve garantire la salute e la sicurezza del lavoratore e il dipendente deve seguire le regole; le stesse dettate per lo svolgimento del lavoro in sede.

UTILIZZO CORRETTO DEGLI STRUMENTI ELETTRONICI

INDICAZIONI GENERALI

Si ribadisce che tutti gli "Strumenti Informatici"indicati, i dispositivi e le relative reti di accesso sono domicilio informatico dell'Azienda e sono messi a disposizione dall'Arpac Multiservizi srl e utilizzati dal lavoratore per rendere la prestazione lavorativa.

Per tutela del patrimonio si intende altresì la tutela del sistema e la sicurezza informatica, ovvero le precauzioni di tipo tecnico predisposte dall'azienda che possono proteggere le informazioni durante il loro transito fra i sistemi della rete locale, anche quando queste rimangono inutilizzate su un disco di un computer, ma unicamente se presenti su sistemi server.

Nel momento in cui esse raggiungono fisicamente la postazione dell'utente finale, la loro protezione dipende esclusivamente da quest'ultimo.

L'Azienda garantisce a tutti gli incaricati un adeguato aggiornamento in merito ai rischi, alle procedure operative, alla prevenzione dei danni e, più in generale, alle problematiche relative alla sicurezza in materia di trattamento dei dati tramite l'utilizzo di elaboratori elettronici e dell'infrastruttura informatica aziendale.

I dati personali e le altre informazioni dell'Utente registrati negli Strumenti o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio.

L'azienda, per adeguarsi ai processi normativamente previsti finalizzati all'aggiornamento e allo sviluppo di digitalizzazione volti ad ottimizzare le tempistiche di lavoro e implementare strategie organizzative, ha scelto di servirsi di piattaforme telematiche (es. MEPA) soprattutto nel settore degli acquisti.

❖ UTILIZZO DEL PERSONAL COMPUTER

A. Gestione, assegnazione e revoca delle credenziali di accesso

La legge prevede che l'accesso alle procedure informatiche che trattano dati personali sia consentito agli incaricati in possesso di "credenziali di autenticazione" che permettano il superamento di una procedura di autenticazione.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato (user-id) associato ad una parola chiave riservata (password) che vengono assegnate a ciascun soggetto incaricato che deve utilizzare e gestire le proprie credenziali di autenticazione attenendosi a dettate istruzioni perché esse devono essere mantenute riservate.

Nel caso di cessazione del rapporto di lavoro con il dipendente dovrà comunicarsi formalmente e preventivamente la data effettiva a partire dalla quale le credenziali saranno disabilitate.

Le user-id individuali per l'accesso alle applicazioni non devono mai essere condivise tra più utenti e nel caso altri utenti debbano poter accedere ai dati è necessario richiedere l'autorizzazione al Responsabile del trattamento.

LE PASSWORD : CARATTERISTICHE

- devono essere sostituite, a cura del singolo Incaricato, al primo utilizzo e successivamente almeno ogni sei mesi
- devono essere composte da almeno **otto caratteri** o comunque da un numero di caratteri pari al massimo consentito,
- non posono contenere riferimenti agevolmente riconducibili all'Incaricato (es. nomi di familiari)
- devono essere scelte nel rispetto della normativa sulla costruzione ed utilizzo delle password.

B. Protezione del PC e dei dati

Tutti i PC devono essere dotati di

1. password rispondenti alle normative e, ove possibile, va impostata anche la password di BIOS.
2. account "Supporto" che è anche account administrator e gli altri account saranno guest.
3. software antivirus aggiornato costantemente.

Sui PC devono essere installati esclusivamente software necessari all'attività lavorativa, dotati di licenza e forniti dalle strutture di appartenenza. Sono vietati i software scaricati da Internet o acquisiti autonomamente.

Per evitare accessi illeciti, deve essere sempre attivato il salva schermo con password.

Sui PC devono essere installati, appena vengono resi disponibili (e comunque almeno annualmente), tutti gli aggiornamenti software necessari a prevenirne vulnerabilità e correggerne i difetti.

Deve essere effettuato, con cadenza almeno settimanale un salvataggio di back-up di eventuali dati personali presenti unicamente sul PC personale.

C. Cancellazione dei dati dai PC

I dati personali conservati sui PC devono essere cancellati in modo sicuro (es. formattando i dischi) prima di destinare i PC ad usi diversi.

D. DIVIETI

- ✓ Non aprire messaggi con allegati di cui non si conoscono l'origine, possono contenere virus in grado di cancellare i dati sul PC.
- ✓ Evitare di aprire filmati e presentazioni non attinenti l'attività lavorativa per evitare situazioni di pericolo per i dati contenuti sul vostro PC.
- ✓ Non è consentito diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.
- ✓ Evitare di scaricare dalla rete file e software di uso non direttamente riferibile all'attività di lavoro, in quanto questo può essere pericoloso per i dati e la rete.
- ✓ Usare Internet solo per lavoro, i siti web spesso nascondono insidie per i visitatori meno esperti.
- ✓ Non leggere le caselle personali esterne via webmail in quanto alcuni provider esterni non proteggono dai virus.
- ✓ Non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, è raccomandabile utilizzare un messaggio "Out of Office" facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo preferibilmente di tipo collettivo, tipo ufficio...@ Dominio Azienda. rivolgersi all'Amministratore di Sistema per tale eventualità
- ✓ È vietato inviare messaggi di posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione.

Ciascun dipendente si deve quindi attenere alle seguenti regole di utilizzo degli Strumenti.

1. Il dipendente consapevole che gli Strumenti forniti sono di proprietà della Società, deve utilizzarli esclusivamente per rendere la prestazione lavorativa e ogni lavoratore è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione, per cui è vietato ogni utilizzo non inerente l'attività lavorativa in quanto può contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza.
2. L'accesso agli Strumenti è protetto edevono essere utilizzati **Username e password** assegnate perchè non è consentita l'attivazione della password di accensione (BIOS), senza preventiva autorizzazione.
   Username e password sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza.
3. Gli strumenti informatici devono essere custoditi con cura da ciascun assegnatario evitando ogni possibile forma di danneggiamento, anzi segnalando tempestivamente all'A.diS. malfunzionamento e/o danneggiamento. Non è consentito all'utente modificare le caratteristiche hardware e software impostate sugli Strumenti assegnati, salvo preventiva autorizzazione da parte dell'A.di S..
4. L'utente è tenuto a scollegarsi dal sistema, o bloccare l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro (PC) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un PC incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.
5. Non è consentita l'installazione di programmi diversi da quelli autorizzati dall'A di S.. È obbligatorio consentire l'installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC sempre protetto.
6. È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.
7. È vietato l'utilizzo di supporti di memoria (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli Strumenti, salvo che il supporto utilizzato sia stato fornito dall'Amministratore di Sistema. In tale caso, il supporto fornito può essere utilizzato esclusivamente finalità lavorative.
8. È vietato connettere al PC qualsiasi periferica non autorizzata preventivamente dall'Amministratore di Sistema (ad esempio, ma non limitatamente a, smartphone, fotocamere, webcam, stampanti).
9. È vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, stampanti, etc.) non autorizzato preventivamente dall'Amministratore di Sistema.

❖ UTILIZZO DELLE PASSWORD

- ✓ Usare almeno 8 caratteri o nel caso in cui lo strumento elettronico non lo permetta, usare un numero
- ✓ di caratteri pari al massimo consentito.
- ✓ Usare lettere, numeri e almeno un carattere tra . ; $! @ - > <
- ✓ Non utilizzare date di nascita, nomi o cognomi propri o di parenti
- ✓ Non sceglierla uguale alla matricola o alla user-id ARPAC Multiservizi srl Via Nuova Poggioreale 61 edificio 80143 Napoli P. IVA 04709971214 usato dal supporto informatico
- ✓ Custodirla sempre in un luogo sicuro e non accessibile a terzi
- ✓ Non divulgarla a terzi
- ✓ Non condividerla con altri utenti
- ✓ Come comportarsi in presenza di ospiti o di personale di servizio
- ✓ Fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali.
- ✓ Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e attivare il salvaschermo del PC .
- ✓ Non rivelare o fare digitare le password dal personale di assistenza tecnica.
- ✓ Non rivelare le password al telefono né inviarla via fax - nessuno è autorizzato a chiederle.
- ✓ Segnalare qualsiasi anomalia o stranezza al Responsabile.

❖ UTILIZZO POSTA ELETTRONICA

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.

Ad ogni utente viene fornito un account e-mail nominativo, generalmente coerente con il modello ***nome.cognome@dominio dell'azienda*** *il cui* utilizzo deve essere limitato esclusivamente a scopi lavorativi, ed è assolutamente vietato ogni utilizzo di tipo privato.

L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa

AMS fornisce caselle di posta elettronica associate a **ciascuna Unità organizzativa/Ufficio** il cui utilizzo è da preferire rispetto alle e-mail nominative qualora le comunicazioni siano di interesse collettivo.

L'iscrizione a mailing-list o newsletter esterne con l'indirizzo ricevuto è concessa esclusivamente per motivi professionali.

Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.

Allo scopo di garantire sicurezza alla rete bisogna evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito, oppure contengano allegati di tipo ***.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif**.

È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi informatiche.

In qualunque situazione di incertezza contattare l'AdS per una valutazione dei singoli casi.

Nel caso fosse necessario inviare allegati "pesanti" (fino a 50MB) è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti.

Tuttavia la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell'allegato sulle condivisioni.

Tutte le informazioni personali o sensibili posso esser inviati solo a destinatari persone o enti qualificati.

La casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria.

I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l'eliminazione dello spam e quelli contenenti virus vengono eliminati dal sistema.

❖ UTILIZZO DEI TELEFONI, FAX, FOTOCOPIATRICI, SCANNER E STAMPANTI

Il dipendente è consapevole che gli Strumenti di stampa, così come anche il telefono, sono di proprietà dell'Azienda e sono resi disponibili all'utente per rendere la prestazione lavorativa pertanto ne viene concesso l'uso esclusivamente per tale fine.

Il telefono affidato è uno strumento di lavoro ed ne è concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza.

Ai cellulari e smartphone si applicano le medesime regole sopra previste per gli altri dispositivi informatici per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica per cui è vietata l'installazione e l'utilizzo di applicazioni (app) diverse da quelle autorizzate dall'Amministratore di Sistema.

È vietato l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, fatta salva esplicita autorizzazione da parte del Responsabile di Ufficio.

È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Ufficio.

Stampanti

È consentito stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative prediligendo stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili);

Nel caso in cui si rendesse necessaria la stampa di informazioni riservate l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni a persone terze non autorizzate.

❖ UTILIZZO DELLA RETE INTERNET

La navigazione su Internet, attraverso cavo di rete o Wi-Fi, qualora disponibile, è un servizio che viene messo a disposizione degli Utenti a supporto delle loro attività istituzionali.

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.

Ciascun dipendente si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi

1. È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa (ad es. i siti istituzionali, i siti degli Enti locali, di fornitori e partner e l'accesso è regolato dal proxy con le sue policy di sicurezza debitamente implementate e aggiornate.
2. È vietato compiere azioni che siano potenzialmente in grado di arrecare danno all'Azienda.
3. È vietato a chiunque il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dagli Amministratori di Sistema. L'Azienda si riserva di bloccare l'accesso a siti "a rischio" attraverso l'utilizzo di blacklist pubbliche in continuo aggiornamento e di predisporre filtri, basati su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri. In caso di blocco accidentale di siti di interesse, potrà contattare l'AdiS per uno sblocco selettivo. Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri, è necessario richiedere lo sblocco mediante una mail indirizzata all'Amministratore di Sistema, ed in copia alla Direzione Generale, nella quale siano indicati chiaramente: motivo della richiesta, utente e postazione da cui effettuare la navigazione libera, intervallo di tempo richiesto per completare l'attività.

4. È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dalla Direzione Generale e dall'Amministratore di Sistema, con il rispetto delle normali procedure di acquisto.
5. È assolutamente vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet tranne in casi del tutto eccezionali e previa autorizzazione dell'Amministratore di Sistema e della Direzione Generale.
6. È assolutamente vietata la partecipazione a Forum non professionali, ai Social Network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).
7. È consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati dall'Amministratore di Sistema. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche ed e-mail. È consentito un utilizzo legato esclusivamente a scopi professionali. Anche su tali strumenti di messaggistica istantanea è attivo il monitoraggio e la registrazione dell'attività degli utenti.
8. Per motivi tecnici e di buon funzionamento del sistema informatico è buona norma, salvo comprovata necessità, non accedere a risorse web che impegnino in modo rilevante banda, come a titolo esemplificativo: filmati (tratti da youtube, siti di informazione, siti di streaming ecc.) o web radio, in quanto possono limitare e/o compromettere l'uso della rete agli altri utenti.

❖ UTILIZZO INFRASTRUTTURA DI RETE E FILESYSTEM

Per l'accesso alle risorse informatiche della Società attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione laddove è assolutamente proibito accedere alla rete ed ai sistemi informativi utilizzando credenziali di altre persone.

L'accesso alla rete garantisce all'utente la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno inseriti e salvati i files di lavoro, organizzati per area/ufficio o per diversi criteri o per obiettivi specifici di lavoro.

Il disco C : è disco rigido principale, la directory principale dell'unità , che contiene il sistema operativo e i relativi file di sistema utilizzata per archiviare e organizzare i file di sistema, altre applicazioni e relativi dati

Senza il consenso del Titolare, è vietato trasferire documenti elettronici dai sistemi informativi e Strumenti dell'azienda a device esterni (hard disk, chiavette, CD, DVD e altri supporti).

Gli Strumenti Informatici e tutte le cartelle di rete possono ospitare esclusivamente contenuti professionali; perciò è vietato il salvataggio sui server aziendali di documenti non inerenti l'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, mail personali, film. etc.

Ogni materiale personale rilevato a seguito di interventi di sicurezza informatica di manutenzione e/o aggiornamento su server viene rimosso ferma ogni ulteriore responsabilità civile, penale e disciplinare.

Tutte le risorse di memorizzazione, diverse da quelle citate non sono sottoposte al controllo regolare e non sono oggetto di backup periodici.

Con regolare periodicità ciascun utente provvede alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili con attenzione alla duplicazione dei dati, essendo necessario evitare un'archiviazione ridondante.

ASSISTENZA AGLI UTENTI E MANUTENZIONI

L'Amministratore di Sistema può accedere ai dispositivi informatici sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

- ✓ verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale.
- ✓ verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete.
- ✓ richieste di aggiornamento software e manutenzione preventiva hardware e software.

Gli interventi tecnici possono avvenire previo consenso dell'utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso.

Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, l'AdiS è autorizzato ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

L'accesso in teleassistenza sui PC della rete richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Amministratore di Sistema, per le verifiche delle modalità di intervento per il primo accesso.

Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale. Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o l'Amministratore di Sistema devono presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente regolamento.

CONTROLLI

Il log di accesso al sistema o alla intranet sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio.

I controlli possono avvenire secondo le disposizioni previste.

Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection Regulation".

✓ Controlli sugli Strumenti (art. 6.1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/16)

Poiché in caso di violazioni contrattuali e giuridiche, sia il datore di lavoro, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, sono previsti controlli nei limiti consentiti dalle norme legali e contrattuali per il rispetto delle regole e l'integrità del proprio sistema informatico.

Il datore di lavoro, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, co 2), di sistemi che consentono indirettamente un accertamento, determinando un trattamento di dati personali riferiti o riferibili ai lavoratori.

Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

I controlli devono essere effettuati nel rispetto della normativa generale seguendo i di principi:

- ✓ **Proporzionalità:** il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi.
- ✓ **Trasparenza:** l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.
- ✓ **Pertinenza e non eccedenza:** ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.

L'uso degli Strumenti Informatici può lasciare traccia delle informazioni che possono contenere dati personali eventualmente anche sensibili che possono essere oggetto di controlli al fine di garantire sicurezza del lavoro e tutela del patrimonio aziendale.

- ✓ **Controlli per la tutela del patrimonio le, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.).**

Tali controlli si verificano nel caso in cui risulti necessario l'accesso agli Strumenti e alle risorse informatiche. In tali casi il Responsabile del trattamento dei dati personali e l'Amministratore di Sistema, potrà attivare una serie di verifiche secondo il seguente iter :

1. Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento.
2. Dopo almeno 7 giorni, se il comportamento anomalo persiste, si autorizza il controllo, potendo così accedere alle informazioni e di rilevare files trattati, siti web visitati, software installati, documenti scaricati nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP, dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.
3. Qualora il rischio di compromissione del sistema informativo sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti il RdP unitamente all'AdS. potrà intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia prendendo tutte le misure tecnicamente necessarie alla soluzione del problema.

✓ Controllo Degli Accessi

L'accesso alla rete aziendale ed ai sistemi aziendali è protetto da password individuale, che ha il compito di prevenire accessi da parte di soggetti non autorizzati ai sistemi.
In relazione a ciò, allo scopo di cautelare l'Azienda e la platea aziendale da ogni tipo di manomissione, furto o distruzione di dati e delle relative conseguenze, sia sul piano operativo che legislativo (penale e civile), vigono le seguenti disposizioni:

1. è vietato connettere in rete stazioni di lavoro diverse da quelle di proprietà dell'Azienda, comprese quelle personali dei dipendenti, se non dietro esplicita e formale autorizzazione dell'Ufficio Sistemi Informativi;
2. è vietato condividere cartelle in rete con servizi non messi a disposizione dall'Ente;

✓ Controlli per esigenze produttive e di organizzazione

Qualora risulti necessario l'accesso alle risorse informatiche non reperibili per esigenze produttive e di organizzazione si dovrà attuare la seguente procedura :

1. Pubblicare una disposizione di servizi sottoscritta dall'A.U. che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
2. Accede alla risorsa con credenziali di AdS.
3. Redazione di un verbale che riassuma e descriva i passaggi effettuati.
4. In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.

✓ Conservazione dei dati

In riferimento agli articoli 5 e 6 del GDPR - Regolamento n. 679/16 e in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza,accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet e dal traffico telematico (log di sistema e del server proxy), la cui conservazione non sia necessaria, saranno **cancellati entro al massimo 365 giorni dalla loro produzione**.
E' consentito il prolungamento dei tempi di conservazione limitatamente al soddisfacimento delle esigenze sopra esplicitate solo in casi eccezionali:

1. per esigenze tecniche o di sicurezza;
2. per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria
3. per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria

Partecipazioni a Social Media

L'utilizzo a fini promozionali e commerciali di Facebook, Twitter, Linkedin, dei blog e dei forum, anche professionali, (ed altri siti o social media) è gestito ed organizzato esclusivamente dall'Azienda attraverso specifiche direttive ed istruzioni operative al personale.
Fermo restando il diritto della persona alla libertà di espressione, AMS detta alcune regole comportamentali al fine di tutelare la propria immagine ed il patrimonio, anche immateriale, ma anche la platea dei dipendenti e i collaboratori, e fornitori, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che **è vietata la partecipazione agli stessi social media durante l'orario di lavoro.**

La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni considerate riservate ed in genere sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in svolgimento presso gli uffici.

Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore.

Nelle comunicazioni private i dipendenti

1) non potranno inserire il nominativo e il logo dell'Ente, né pubblicare disegni, modelli od altro connesso ai citati diritti a meno che non ci sia preventiva e specifica autorizzazione della Direzione.
2) comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori, se non con il preventivo personale consenso di questi,
3) postare nei social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro, se non con il preventivo consenso del Responsabile d'ufficio.
4) qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ente.

NORME FINALI

Come stabilito la pubblicazione del presente Regolamento adottato con provvedimento sottoscritto dall'A.U p.t. di AMS, a cura della segreteria Generale, avverrà per pubblicazione sul sito, rete informatica interna(mail dei dipendenti) e mediante affissione nei luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 Statuto lavoratori e tutti gli utenti possono chiedere chiarimenti e proporre integrazioni che saranno, se del caso, inseriti negli aggiornamenti previsti.

Tutti i comportamenti difformi alla normativa vigente saranno sottoposti all'AU che valuterà le misure da assumere in ottemperanza alle prescrizioni di legge ed alla normativa interna.

I log relativi all'utilizzo di Strumenti, reperibili nella memoria degli Strumenti stessi, ovvero sui Server o sui router, nonché i file con essi trattati possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio

Le informazioni eventualmente raccolte da soggetti preposti sono utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e i controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection Regulation".

Viene precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori

SANZIONI PER INOSSERVANZA DELLE NORME

Gli strumenti, le reti e le banche dati possono essere utilizzati esclusivamente per ragioni di servizio perciò tutti i comportamenti difformi alle regole individuate che possono causare gravi rischi alla sicurezza ed alla integrità dei sistemi informativi aziendali saranno suscettibili di valutazione ai sensi del:

- **Codice Civile (art. 2214)**
- **Codice Comportamento**
- **Codice Disciplinare**
- **CCNL (articoli 59 e seguenti)**
- **Dpr n 600/73 (art.22), GDPR - Regolamento 2016/679 in materia di privacy.**

Le presenti istruzioni sono impartite ai sensi delle normative vigenti e l'inosservanza delle stesse comporterà sanzioni anche di natura penale come da normativa generale (es. per gli hosting provider nelle ipotesi di diffusione online di contenuti terroristici, al cui contrasto sono dedicati il Regolamento UE n. 7842021).

In caco di richiesta documentazione da parte di Organi di controllo competenti, la mancata ottemperanza alla richiesta ovvero la trasmissione di informazioni o dati parziali o non veritieri è punita con applicazione di sanzione amministrativa pecuniaria nel minimo di euro 10.000 e nel massimo di euro 100.000.

Ove si accerti la sussistenza di violazioni contestate, si assegna al trasgressore un congruo termine perentorio, proporzionato rispetto al tipo e alla gravità della violazione, per conformare la condotta agli obblighi previsti dalla normativa vigente, segnalando le violazioni all'ufficio competente per i procedimenti disciplinari, nonché ai competenti del'OdV.

Per quanto non espressamente previsto si applica la disciplina della legge n. 689 del 24 novembre 1981 (Legge Bosetti & Gatti).

ATTESTAZIONE DI PUBBLICAZIONE

Si pubblichi con ogni effetto di legge sul sito ufficiale dell'Arpac Multiservizi il Provvedimento dell'A.U. **n. 51 del 05.10.2023** avente ad oggetto: **ADOZIONE REGOLAMENTO TELEMATICO E DISCIPLINARE SULL' USO CORRETTO STRUMENTI TELEMATICI DELLA SOCIETA' ARPAC MULTISERVIZI S.R.L.**

Napoli, 05/10/2023

Responsabile Pubblicazione Atti

Avv. Angela Pesce

ARPAC Multiservizi Srl
Via Nuova Poggioreale 61 – Centro Polifunzionale INAIL Ed. 5 – 80143 NAPOLI
Tel. +39 081 0901461 Fax. +39 081 0901456
PEC segr.generale@pec.arpacmultiservizi.it Mail segr.generale@arpacmultiservizi.it
P.IVA 04709971214