MODALITA' OPERATIVE

DI UTILIZZO

DEGLI STRUMENTI INFORMATICI

AI SENSI DELL'ART. 4 DELLO STATUTO DEI LAVORATORI

Approvato con delibera di G.C. n. 136 del 23.10.2019

INDICE

1 PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete internet dai personal computer, espone il Comune di Montanaro e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto di autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'azienda stessa.

Premesso, quindi, che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, il Comune di Montanaro ha adottato il seguente documento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Detto documento sarà oggetto di successive revisioni ed estensioni ad altre tematiche relative alla privacy ed alla sicurezza dei dati, che sono attualmente oggetto di specifico esame.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite in sede di lettera di designazione a persona autorizzata al trattamento dei dati personali.

Considerato inoltre che il Comune di Montanaro, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer portatili, telefonici cellulari, palmari, ecc.) sono state inserite nelle Modalità operative di utilizzo degli strumenti informatici alcune clausole relative alle modalità ed ai doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

2 ENTRATA IN VIGORE DEL REGOLAMENTO E PUBBLICITÀ

Il Documento è in vigore dalla data della sua approvazione.

Copia delle Modalità operative di utilizzo degli strumenti informatici, oltre ad essere affisse nella bacheca comunale, verranno inviate/consegnate a ciascun dipendente.

3 OBIETTIVI

Il presente Documento ha l'obiettivo di:

- definire i criteri per l'assegnazione a personale dipendente e non, di risorse ICT ad uso individuale e i relativi flussi autorizzativi;
- disciplinare le modalità di corretto utilizzo e conservazione delle risorse ICT sopra indicate;
- definire le modalità per la conservazione e l'utilizzo dei dati relativi all'uso delle risorse e servizi informatici aziendali;
- stabilire ruoli e responsabilità dei soggetti coinvolti.

4 AMBITO DI APPLICAZIONE

Il presente Documento si applica a tutti i dipendenti, senza distinzione di ruolo e di livello, nonché a tutti i collaboratori del comune a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori a progetto, in stage, ecc.).

5 RIFERIMENTI A LEGGI E REGOLAMENTI

- D.Lgs 196/03 (per quanto non in contrasto con la normativa europea);
- Deliberazione 1° marzo 2007, n. 13- Lavoro: le linee guida del Garante per la posta elettronica e Internet" (Gazzetta Ufficiale n. 58 del 10 marzo 2007) e s.m.i.;
- Regolamento Europeo 2016/679;

- Raccomandazione 5/15 del Comitato dei Ministri avente ad oggetto il trattamento dei dati personali in ambito occupazionale;
- Parere n. 2/2017 de Garanti europei Wp 29 sul trattamento dei dati dei lavoratori nei luoghi di lavoro.

6 DEFINIZIONI

Ai fini delle presenti Modalità operative di utilizzo degli strumenti informatici si intende per :

Utente	ogni dipendente e collaboratore (lavoratore somministrato, in stage, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "persona autorizzata al trattamento dei dati personali".
Mezzi di telecomunicazione	sistemi mobili con tecnologia che consentono lo svolgimento di funzioni di telefonia e/o trasmissione dati e/o funzioni video
Risorse ICT ad uso individuale (o risorse ICT)	le risorse e servizi informatici e i mezzi di telecomunicazione forniti dall'azienda per uso individuale
Tablet	sistema mobile con tecnologia che garantisce la trasmissione dati e funzioni video
Risorse e servizi informatici	qualsiasi tipo di hardware, mezzi di comunicazione elettronica, rete di trasmissione dati, software, informazioni in formato elettronico e, in generale, applicativi
Fax	servizio telefonico consistente nella trasmissione (invio e ricezione) di immagini fisse (tipicamente copie di documenti).

7 ART. 4 STATUTO LAVORATORI

Premessa

Il Comune di Montanaro:

- Ha il diritto/ dovere di precisare ai sensi dell'art 4 comma 2 dello statuto dei lavoratori gli strumenti che l'azienda ritiene necessari per svolgere la prestazione lavorativa;
- ha il diritto/dovere di indicare in modo chiaro e dettagliato le indicazioni sul corretto utilizzo degli strumenti messi a disposizione e se, in quale misura e con quali modalità possano essere effettuati eventuali controlli;
- non effettua controlli a distanza dell'attività dei dipendenti, ai sensi art. 4 dello Statuto dei lavoratori (L. n. 300/1970), mediante sistemi hardware e software finalizzati, ad esempio:
    - alla lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
    - potranno essere istallati software anche in automatico tramite Agente che avranno il compito di adeguare l'infrastruttura dell'Ente alla normativa AGID "Misure Minime di Sicurezza ICT nella P.A." del 18/04/2017 e s.m.i. si cita a titolo non esaustivo la funzione software inventory;
    - potranno essere rilevate ed archiviate le informazioni relative agli eventi di connessione e disconnessione dal sistema degli utenti;
    - relativamente ai dispositivi mobili in uso ai dipendenti, potranno essere adottate tecnologie di gestione remota di tipologia MDM (Mobile Device Manager).
- privilegia, rispetto alle misure repressive, quelle organizzative e tecnologiche volte a prevenire utilizzi impropri degli strumenti, minimizzando in ogni evenienza l'uso dei dati riferibili ai dipendenti e comunque nel rispetto dei principi di necessità, pertinenza e non eccedenza, tenendo conto altresì della disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali;

- si impegna a rispettare la protezione dei dati personali attraverso il pieno rispetto del Regolamento Europeo 2016/679 nonchè delle linee Guida del Garante Italiano e del Gruppo dei Garanti europei 29.

7.1 SUGLI STRUMENTI NECESSARI A RENDERE L'ATTIVITÀ LAVORATIVA EX ART 4 COMMA 2 STATUTO LAVORATORI

A seguito dell'entrata in vigore dell'art. 23, D. Lgs. 14 settembre 2015 n. 151, che ha modificato l'art. 4, L. 20 maggio 1970 n. 300, è stata riformata la disciplina relativa agli impianti audiovisivi e agli altri strumenti da cui derivi anche la possibilità di controllo a distanza dei lavoratori.

Ai sensi del comma 2 del citato art. 4 gli strumenti utilizzati dai lavoratori, per rendere la prestazione lavorativa nonché quelli finalizzati ad attestare gli accessi e presenze, **dai quali può derivare anche la possibilità di un controllo a distanza** non richiedono, per la loro applicazione, la sussistenza di esigenze organizzative, produttive, di sicurezza o di tutela del patrimonio Ente e non necessitano del preventivo accordo sindacale né dell'autorizzazione degli Uffici ministeriali (DTL o MINISTERO).

Gli strumenti che il Comune di Montanaro considera necessari a svolgere la prestazione lavorativa, come già indicato nell'informativa consegnata in fase di assunzione, sono:

a) Il personal computer (fisso e/o portatile) con i relativi software operativi e/o applicazioni istallate;

b) La rete informatica Ente;

c) La posta elettronica Ente;

d) I dispositivi di archiviazione hardware;

e) Le periferiche aziendali annesse (stampanti, fax, masterizzatori, supporti, magnetici, ecc.);

f) Gli apparati di comunicazione fissi (telefoni, ecc.).

L'utilizzo degli strumenti sopra indicati può comportare l'acquisizione, da parte del Comune, dei dati relativi alla prestazione lavorativa svolta, nonché alle modalità e procedure di esecuzione della stessa.

Tali strumenti di lavoro sono affidati esclusivamente per l'esercizio delle funzioni assegnate, pertanto, non debbono essere utilizzati per uso personale o comunque estraneo all'attività Ente, né modificati.

Per maggiori dettagli sulle modalità di utilizzo degli strumenti sopra elencati si vedano i paragrafi successivi.

8 MODALITA' OPERATIVE DEGLI STRUMENTI ELETTRONICI

8.1 SOGGETTI CHE POSSONO UTILIZZARE GLI STRUMENTI ELETTRONICI

L'utilizzo delle risorse informatiche in generale, della posta elettronica e di Internet in particolare, come già anticipato, sono accordati al dipendente, all'apprendista, al collaboratore, allo stagista. L'utilizzo delle risorse (sistemi hardware, programmi e applicazioni software, apparati di rete, risorse di stampa, telefoni fissi, cellulari e tablet) è concesso solo in quanto strumenti di esecuzione delle normali prestazioni di lavoro o strumenti atti all'apprendimento del lavoro.

A tal fine, il lavoratore deve sempre mantenere comportamenti in linea con il Codice di comportamento dei dipendenti pubblici secondo il DPR 16 aprile 2013, n 62.

Non devono essere in nessun caso modificate le configurazioni di sicurezza, predisposte dagli ADS.

L'accesso e l'utilizzo delle risorse ICT dovrà essere limitato allo stretto indispensabile e comunque senza pregiudicare l'attività lavorativa.

Non è consentito trattare documenti non pertinenti l'attività lavorativa.

Le persone autorizzate alla manutenzione dei sistemi informatici hanno l'obbligo di svolgere solo le operazioni strettamente necessarie per adempiere al loro incarico, con divieto di svolgere attività di controllo a distanza, anche di propria iniziativa.

8.2 RISERVATEZZA DELLE INFORMAZIONI

La responsabilità di proteggere il patrimonio informativo dell'Ente in coerenza con le norme di legge in vigore e con le procedure dell'Ente coinvolge tutto il personale relativamente alle attività di competenza.

Tutti i supporti (chiavi USB, CD/DVD, elaboratori, ecc.) devono essere forniti dall'Amministrazione Comunale.

Non è ammesso l'utilizzo di supporti personali.

Le periferiche di massa contenenti informazioni riservate devono essere protette in modo adeguato, conservandole ad esempio, quando non utilizzate, in vani chiusi a chiave, preservando la sicurezza della chiave stessa. In assenza di specifiche autorizzazioni, non devono, inoltre, venire duplicate e consegnate a terzi.

Lo smaltimento dei supporti di memorizzazione anche contenuti all'interno delle postazioni di lavoro (hard disk, ecc.) può avvenire a condizione che il contenuto non sia recuperabile. Eventuali supporti non cancellabili devono essere resi inutilizzabili prima dello smaltimento.

8.3 REGOLE DI UTILIZZO

Al fine di garantire la sicurezza ed il corretto impiego del sistema informatico si ritengono necessari i seguenti accorgimenti:

8.4 GESTIONE DELLA PASSWORD

1. PROCEDURE CORRETTE

- modificare al primo accesso la password così che da quel momento, sia conosciuta solo dall'utente stesso;
- mantenere la password segreta nei confronti di chiunque compresi i colleghi di lavoro;
- sostituire la password anche in caso di semplice sospetto circa la venuta meno della sua segretezza. In caso di dubbio sull'utilizzo anomale della propria credenziale di accesso si deve avvisare il Titolare del trattamento;
- comporre le passwords con almeno 8 caratteri di cui almeno 3 delle seguenti tipologie :

  a) un carattere maiuscolo (da A a Z)

  b) un carattere minuscolo (da a a z)

  c) una cifra numerica (da 0 a 9)

L'utilizzo combinato del nome utente e della password attribuisce in modo univoco al singolo dipendente la responsabilità delle operazioni compiute.

2 PROCEDURE VIETATE:

- utilizzare le ultime 5 password;
- assicurare l'univocità delle password distinguendo i vari ambiti in cui sono utilizzate;
- ogni condotta che possa comprometterne la segretezza.

8.5 UTILIZZO POSTAZIONI DI LAVORO

1 . PROCEDURE CORRETTE

- Utilizzare gli Strumenti ICT per il perseguimento di fini strettamente connessi agli incarichi lavorativi, e comunque coerentemente al tipo di attività svolta ed in linea con le disposizioni normative vigenti;
- Spegnere l'elaboratore ed eventuali periferiche (stampanti, scanner …) prima di lasciare l'ufficio al termine dell'attività lavorativa e, in generale, rispettare le istruzioni impartite.
- Effettuare prima di assentarsi dal proprio posto di lavoro, la disconnessione dell'utente;
- Accertarsi che le operazioni di manutenzione/riparazione degli Strumenti ICT avvengano da parte del personale autorizzato dalla Direzione ICT;

- I dati particolari non devono essere archiviati sulle postazioni di lavoro ma esclusivamente su aree di rete protette, con particolare attenzione alle aree di interscambio eventualmente non protette.

2. PROCEDURE VIETATE

- usare le risorse o i servizi in violazione di normative comunitarie, leggi, regolamenti, provvedimenti, prescrizioni, o per commettere attività illecite o discriminanti;
- modificare le configurazioni impostate;
- installare ed utilizzare prodotti software che non siano stati autorizzati dalla Direzione;
- installare, utilizzare software che consentano l'intercettazione automatica del traffico o la violazione delle password;
- usare le risorse o i servizi per scopi personali;
- utilizzare tecnologie di anonimizzazione;
- utilizzare le credenziali di autenticazione di altri utenti;
- tentare di violare password o altri sistemi di protezione o tentare di superare le restrizioni imposte dal sistema;
- riprodurre o distribuire materiale Ente senza autorizzazione;
- copiare o modificare files, protetti da copyright, senza autorizzazione;
- interferire con il corretto funzionamento o danneggiare le attrezzature di rete;
- intercettare o alterare qualunque tipo di dato o di comunicazione digitale.
- partecipare a forum/ social network per finalità non pertinenti l'attività lavorativa (es.: facebook, etc).
- attivare strumenti di chat in videochiamata (es.: skype/msn messenger) se non pertinenti l'attività lavorativa.

8.6 UTILIZZO PC PORTATILI E DISPOSITIVI PORTATILI (SMARTPHONE, TABLET)

1. PROCEDURE CORRETTE

- conservare in un luogo sicuro a fine giornata lavorativa;
- avvertire tempestivamente, in caso di furto, l'Ente;
- almeno ogni 30 giorni, in caso di prolungato distacco dalla rete dell'Ente, connettere il disositivo alla rete dell'Ente per consentire gli aggiornamenti automatici;
- segnalare immediatamente all'Ente il malfunzionamento dei beni comunali;
- utilizzare un "codice di blocco" per prevenire l'uso improprio dei telefoni cellulari aziendali assegnati, con un PIN il più lungo possibile, in uso e l'accesso ai dati in esso contenuti;

2.PROCEDURE VIETATE

- concedere il proprio elaboratore portatile, tablet, smartphone in uso a terzi
- configurare mail aziendali su dispositivi personali

3. DISATTIVAZIONE O CESSAZIONE DEL RAPPORTO DI LAVORO

Il Comune si riserva la facoltà di disabilitare l'utilizzo dei mezzi sopra elencati. Tali mezzi, infatti, sono strumenti aziendali al fine di consentire lo svolgimento delle proprie mansione ma, la proprietà dei beni rimane nella completa e totale disponibilità dell'Ente.

In caso di disattivazione o di cessazione del rapporto di lavoro gli strumenti vanno riconsegnati al Titolare del trattamento.

Al momento della restituzione dei beni, il Comune provvederà al totale rispristino del dispositivo.

9 PROTEZIONE FIREWALL, ANTIVIRUS, ANTIMALWARE, ANTIRANSOMEWARE

1. PROCEDURE CORRETTE

- tenere sempre attivati ed aggiornati i software firewall, antivirus, antimalware, antiransomeware installati sul pc ;
- seguire le istruzioni specificatamente indicate in caso di avviso da parte del software antimalware, in particolare, in caso di minaccia rilevata come non risolvibile procedere a:

    - disconnettere il cavo di rete e di alimentazione e nel caso di PC portatile o palmare spegnerlo;
    - contattare il referente interno.

Si fa presente che i softaware di protezione locali alla postazione sono oggetto di gestione centralizzata.

10 POSTA ELETTRONICA

1. PROCEDURE CORRETTE

- modificare la password almeno ogni 90 giorni ed immediatamente qualora si sospetti che essa sia venuta a conoscenza di terzi;
- gestire la casella di posta elettronica, la cui dimensione è stabilita in funzione delle necessità operative, in modo opportuno, eliminando i messaggi personali non necessari all'attività lavorativa, contenendo la dimensione degli stessi e dei relativi allegati, al fine di garantire il funzionalità del sistema di messaggistica;
- cancellare immediatamente, anche dal cestino, la mail in caso di messaggi sconosciuti o insoliti;
- memorizzare solo le email necessarie alla propria attività;
- utilizzare sempre i formati compressi (zip, rar etc) per inviare allegati pesanti;
- trasferire i files contenenti dati sensibili in modalità FTP "sicuro" se diretti verso destinatari privati;
- trasferire i files contenenti dati sensibili in modalità FTP "sicuro" o tramite PEC se diretti verso Pubblica Amministrazione.

2 PROCEDURE VIETATE

- non inviare informazioni contenenti dati particolari all'interno di messaggi e-mail non PEC;
- inviare o memorizzare messaggi il cui contenuto sia illegale, oltraggioso o osceno ovvero possa costituire o incitare alla discriminazione per ragioni di sesso, razza, lingua, religione, origine etnica, opinioni ed appartenenza sindacale e/o politica;
- inviare documenti aziendali se non nei limiti delle proprie mansioni, responsabilità ed esigenze di progetto;
- usare false identità durante lo scambio di messaggi;
- qualora la ricezione di un messaggio sia fonte di dubbio da parte dell'utente se ne sconsiglia l'apertura. Si consiglia eventualmente di contattare direttamente il mittente per maggiori infomazioni.

3.PROCEDURE IN CASO DI ASSENZA

In caso di assenza programmata (ad esempio per ferie o attività di lavoro fuori sede che pregiudichino la visibilità della posta elettronica) qualora le esigenze di servizio lo impongano è opportuno impostare messaggi di risposta automatici per permettere ai mittenti delle mail di essere consapevoli dell'assenza dall'Ente nonché di ricevere indicazioni in merito a possibili referenti alternativi.

In ogni caso qualora il comune al fine di perseguire finalità strettamente aziendali dovesse avere necessità di accedere alla posta Ente del soggetto assente si segue la procedura per le assenze improvvise.

Qualora, in caso di assenza improvvisa e/o prolungata, ricorrano improrogabili necessità legate all'attività lavorativa per cui si debba conoscere il contenuto dei messaggi di posta elettronica, il Responsabile di Funzione/Direzione di appartenenza dell'utente può richiedere all'Amministratore di sistema che venga effettuato il reset della password dell'utente stesso. Di tale attività deve essere informato non appena possibile l'utente interessato.

11 CESSAZIONE DEL RAPPORTO DI LAVORO

In caso di cessazione del rapporto di lavoro il Comune provvede alla disattivazione (chiusura) dell'account Ente riferita all'ex dipendete.

12 TELEFONI FISSI, FAX, STAMPANTI E FOTOCOPIATRICI

1. PROCEDURE CONSENTITE

- l'uso privato, purché occasionale, non prolungato e limitato alle situazioni di effettiva necessità, degli apparati di telefonia fissa e cellulare assegnati in uso;
- cancellare, nel caso in cui gli apparati debbano essere restituiti o inviati in manutenzione, dalle memorie degli apparati stessi qualsiasi dato personale proprio o di soggetti terzi.
- ritirare prontamente la stampa dai vassoi delle stampanti / fotocopiatori comuni.

2. PROCEDURE VIETATE

- effettuare o ricevere telefonate personali e comunque non attinenti ai compiti affidati;
- comunicare i numeri telefonici aziendali a call center, società di servizi di informazione o di intrattenimento in abbonamento via SMS, comunità virtuali, ecc;
- l'uso di fax, stampanti e fotocopiatori per fini personali;
- utilizzare, in ogni caso, gli apparati per attività non pertinenti con lo svolgimento delle mansioni affidate.

13 ACCESSO AI DATI TRATTATI – AMMINISTATORE DI SISTEMA O SUO DELEGATO

Il personale incaricato alla gestione tecnica degli strumenti informatici può:

a) accedere ai dati trattati dall'utente tramite posta elettronica, navigazione in rete per motivi di sicurezza, protezione del sistema informatico e tutela del patrimonio Ente (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, ecc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa e/o su segnalazione di presunti comportamenti illeciti. Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e sicurezza, il personale incaricato accederà ai dati su richiesta dell'utente e/o previo avviso al medesimo. Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la continuità della normale attività operativa, il personale incaricato avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni;

b) nei casi indicati alla lett. a) che precede, effettuare tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico dell'Ente (ad es. rimozione di file o applicazioni pericolose);

c) procedere a controlli finalizzati a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti o mediante "file di log" della navigazione svolta. L'eventuale controllo sui file di log da parte del personale incaricato alla gestione tecnica degli strumenti informatici non è comunque continuativo ed è limitato:

   - per la posta elettronica all'indirizzo del mittente e del destinatario, alla data e all'ora dell'invio e della ricezione e all'oggetto;

d) può accedere ai dati contenuti negli strumenti informatici restituiti dall'utente all'azienda per cessazione del rapporto, sostituzione delle apparecchiature, ecc. Sarà cura dell'utente la cancellazione preventiva di tutti i dati personali eventualmente ivi contenuti.

14 POSSIBILITA' DI CONTROLLI E LORO GRADUALITA'

Al fine di prevenire le succitate criticità e rischi, il Comune si riserva la facoltà di effettuare rilevazioni, in forma aggregata e anonima, in merito alla corretta applicazione dei principi e delle regole comunali.

Le modalità di svolgimento delle sopraindicate rilevazioni garantiranno il rispetto dei principi di pertinenza e non eccedenza, evitando qualunque immotivato accesso a dati personali contenuti nelle risorse informatiche dell'Ente.

In caso di anomalie riscontrate nell'utilizzo delle risorse informatiche, l'ADS effettua le operazioni necessarie ad identificare la causa del problema.

Le rilevazioni verranno effettuate in maniera tale da salvaguardare l'anonimato, saranno oggetto di un reporting al Titolare del trattamento circa le anomalie rilevate relativamente al corretto utilizzo delle risorse informatiche aziendali.

Qualora le predette rilevazioni mostrino anomalie nell'utilizzo delle risorse informatiche, il Titolare richiama tutti i collaboratori ad attenersi alle regole di comportamento per l'utilizzo delle risorse informatiche aziendali, fermo restando l'eventuale successivo approfondimento delle verifiche e, ove necessario, l'accertamento di **responsabilità individuali.**

In ogni caso, non saranno effettuati controlli prolungati, costanti od indiscriminati.

I dati sull'utilizzo della posta elettronica dell'Ente sono registrati e archiviati in banche dati informatiche a cura del gestore del servizio di posta elettronica. La gestione e la sicurezza delle banche dati è realizzata in conformità alle disposizioni vigenti in materia di tutela dei dati personali. I relativi trattamenti, sono eseguiti da personale incaricato. Il Titolare del trattamento è il Comune di Montanaro.

I dati registrati sono conservati per il tempo strettamente necessario al perseguimento delle finalità per le quali sono stati registrati e conservati secondo i termini legge.

I dati personali di un singolo dipendente, eventualmente anche particolari, ricavabili dai dati registrati sono trattati, per un periodo di tempo anche superiore, comunque non eccedente alle finalità, in caso di:

- richiesta scritta, ordinanza, decreto o altro provvedimento da parte degli organi competenti, nell'ambito dell'esercizio delle loro funzioni istituzionali.

15 CASI DI INOTTEMPERANZA

Il rispetto delle prescrizioni contenute nella presente normativa costituisce parte essenziale delle obbligazioni contrattuali alle quali gli utenti devono attenersi secondo la diligenza richiesta nello svolgimento dell'attività lavorativa.

L'eventuale utilizzo improprio delle risorse informatiche aziendali rappresenta violazione degli obblighi derivanti dal rapporto di lavoro e, conseguentemente, illecito disciplinare perseguibile secondo quanto previsto dal CCNL applicabile.

Per l'utilizzo dei dati tracciati con gli strumenti di cui al presente documento a tutti i fini connessi al rapporto di lavoro si rinvia altresì alla specifica informativa effettuata ai sensi dell'art. 4, comma 3, della legge n. 300 del 1970 che si considera parte integrante del presente Regolamento.

Data *Firma*

_____ _____