AUTORITÀ DI SISTEMA PORTUALE
DEL MARE ADRIATICO SETTENTRIONALE
PORTI DI VENEZIA E CHIOGGIA

DECRETO N. 346 DEL 12 DIC. 2019

Adozione del Regolamento per l'utilizzo dei sistemi informatici e di telecomunicazione dell'Ente.

IL PRESIDENTE

VISTO il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 *«relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»* (di seguito *RGPD*), in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018, che introduce la figura del Responsabile dei dati personali (RDP) e il Decreto di adeguamento n. 101 del 4 settembre 2018;

CONSIDERATO quanto previsto dal provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008" (G.U. n. 300 del 24 dicembre 2008) del Garante per la Protezione dei Dati personali;

VISTI gli artt. 31, 34 e 35 del D.lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";

VISTI inoltre i provvedimenti dell'Autorità Garante per la protezione dei dati personali del Provvedimento del 12 febbraio 2009 [1598443]e del 25 giugno 2009 "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento", relativi alle misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di "amministratore di sistema", ai requisiti tecnici, professionali e di condotta dei soggetti incaricati all'assolvimento di tale ruolo e agli obblighi e alle modalità di nomina di uno o più incaricati;

VISTO il Decreto n. 1985 del 27 dicembre 2016 "Adozione del Regolamento per l'utilizzo dei sistemi informatici e di telecomunicazione dell'Ente"

DECRETA

ARTICOLO 1

Con effetto immediato entra in vigore l'allegato Regolamento per l'utilizzo dei sistemi informatici e di telecomunicazione dell'Ente, che sostituisce quello precedente di cui al Decreto n. 1985 del 27 dicembre 2016.

ARTICOLO 2

L'area Gestione Operativa Servizi IT è incaricata di vigilare sulla corretta applicazione del presente Regolamento.

IL PRESIDENTE
Dott. Pino Musolino

REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATICI E DI TELECOMUNICAZIONE

Sommario

Premessa

Si specifica che tutti gli strumenti utilizzati dal lavoratore, intendendo con ciò PC, notebook, tablet, smartphone, kit di firma digitale, e-mail ed altri strumenti ICT con relativi software e applicativi (di seguito più semplicemente "Strumenti Informatici o strumenti"), sono messi a disposizione da AdSPMAS per rendere efficace la prestazione lavorativa. Gli Strumenti Informatici, nonché le relative reti alle quali è possibile accedere tramite gli stessi, sono domicilio informatico di AdSPMAS. Nell'utilizzo delle risorse informatiche, telematiche e del patrimonio informativo dell'Ente l'utente è tenuto ad usare la massima diligenza, nel rispetto degli obblighi di cui agli **articoli 2104 e 2105 del codice civile**. Gli strumenti, le reti e le banche dati possono essere utilizzati esclusivamente per ragioni di servizio. Comportamenti difformi possono causare gravi rischi alla sicurezza ed alla integrità dei sistemi informativi dell'Ente, sono suscettibili di valutazione ai sensi della normativa di cui al CCNL, e possono assumere rilevanza anche sotto il profilo penale.

Le precauzioni di tipo tecnico predisposte dall'Ente 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'Ente si impegna per garantire 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 dell'Ente.

Ogni utente è tenuto a rispettare il presente Regolamento, che è reso disponibile tramite le modalità specificate al punto 16.

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. Per tutela del patrimonio si intende altresì la sicurezza informatica e la tutela del sistema informatico. Tali informazioni sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, visto che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "General Data Protection Regulation".

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati al trattamento (già "persone autorizzate al trattamento", ex art. 4, comma 10, Regolamento (UE) 2016/679) in attuazione del seguente quadro normativo:

- "Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE", in vigore in tutti gli Stati dell'Unione europea a partire dal 25 maggio 2018;
- Decreto legislativo 10 agosto 2018, n. 101 che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679;
- D. Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", che contiene la disciplina rilevante in materia di privacy;
- Provvedimenti del Garante per la protezione dei dati personali in materia di "misure di sicurezza", in particolare con riguardo agli Amministratori di Sistema (Provvedimento generale del 27 novembre 2008);

nonché le informazioni già fornite in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

1. Oggetto e finalità

Il presente Regolamento è redatto:

- alla luce della Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
- in attuazione del Regolamento Europeo 679/16 "General Data Protection Regulation" (d'ora in avanti Reg. 679/16 o GDPR);
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;

alla luce dell'articolo 23 del D.lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti ***«dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori»*** e di quelli *«utilizzati dal lavoratore per rendere la prestazione lavorativa»*. La finalità è quella di promuovere in tutto il personale una corretta "cultura informatica" affinché l'utilizzo degli Strumenti informatici e telematici forniti dall'Ente sia conforme alle finalità per le quali sono state messe a disposizione del personale e nel pieno rispetto della legge. Si vuole fornire a tutto il personale le indicazioni necessarie con l'obiettivo principale di evitare il verificarsi di qualsiasi abuso o uso non conforme, muovendo dalla convinzione che la prevenzione dei problemi sia preferibile rispetto alla loro successiva correzione.

Il presente Regolamento intende fornire le indicazioni per una corretta e adeguata gestione delle informazioni, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente e si applica a tutti gli utenti intesi come: i dipendenti (senza distinzione di ruolo e/o livello), i collaboratori e consulenti dell'Ente a prescindere dal rapporto contrattuale con lo stesso intrattenuto (lavoratori somministrati, collaboratori coordinati e continuativi, in stage, prestatori d'opera intellettuale, ecc.), che venissero autorizzati a far uso di strumenti tecnologici dell'Ente o di accedere alla rete informatica dell'Ente e ad eventuali dati ed informazioni ivi conservati e trattati. Pertanto, le regole di seguito previste devono intendersi a carico tanto dei primi quanto dei secondi, ferma restando la necessità che si dia opportuno conto del presente Regolamento nel contratto concluso con quest'ultimi.

Tutti gli interventi sono finalizzati a garantire la confidenzialità, l'integrità e la disponibilità delle informazioni dell'Amministrazione. In particolare: la confidenzialità o riservatezza riguarda la conoscibilità e fruibilità delle informazioni ai soli soggetti autorizzati; l'integrità è relativa alla completezza ed inalterabilità delle informazioni; la disponibilità concerne l'accessibilità ed usabilità delle informazioni nel tempo da parte dei soggetti autorizzati. La finalità è, altresì, quella di garantire l'integrità e la disponibilità anche dei beni materiali dell'Amministrazione.

Viene, infine, 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.

2. Principi generali e di riservatezza nelle comunicazioni

I principi che sono a fondamento del presente Regolamento sono gli stessi espressi nel GDPR, e, precisamente: a) 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); b) i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 5 commi 1 e 2), osservando il principio di pertinenza e non eccedenza.

Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza".

È riconosciuto al datore di lavoro di potere svolgere attività di monitoraggio, che nella fattispecie saranno svolte solo dal Responsabile Area GOIT (cfr Decreto Amministratori di Sistema) o dal personale da lui delegato, sempre nel rispetto della succitata normativa.

L'utente si attiene alle seguenti regole di trattamento:

- È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, elementi e informazioni dei quali l'utente 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.
- 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.
- È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni quando l'utente si allontana dalla postazione di lavoro. È vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti alla pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di front office e di ricezione di Clienti / Fornitori o colleghi di lavoro.
- Per le riunioni e gli incontri con Clienti, Fornitori, Consulenti e Collaboratori dell'Ente è necessario utilizzare le eventuali / zone sale dedicate.

3. Tutela del lavoratore

Alla luce dell'art. 4, comma 1, 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.

4. Campo di applicazione

Il presente regolamento si applica a tutti gli utenti così come descritti al punto 1 ed in particolare a coloro in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata come "incaricato del trattamento".

5. Gestione, assegnazione e revoca delle credenziali di accesso

Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate o gestite per iscritto dal Responsabile Area GOIT, previa formale richiesta scritta del Responsabile dell'Area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori esterni la richiesta dovrà essere inoltrata direttamente dalla Direzione o dal Responsabile dell'Area con il quale il collaboratore si coordina nell'espletamento del proprio incarico. La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell'utente ed elenco dei sistemi informativi per i quali deve essere abilitato l'accesso. Ogni successiva variazione delle abilitazioni di accesso ai sistemi informativi dovrà essere richiesta formalmente e per iscritto al Responsabile Area GOIT o al Responsabile di riferimento.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (altresì nominati username, nome utente o *user-id*), assegnato dal Responsabile Area GOIT, ed una relativa password. La password è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza senza divulgarla.

In particolare, per quanto riguarda l'accesso al personal computer assegnato, questo avverrà con privilegi "*User*" e credenziali di accesso di Dominio che vengono assegnate/rimosse/sospese dal Responsabile Area GOIT unicamente su indicazione scritta: del Segretario Generale, dell'Area Amministrazione del Personale, dell'Area Risorse Umane, del Titolare/Responsabile del trattamento.

La password deve essere di adeguata robustezza: deve essere composta da almeno 8 caratteri, formata da un insieme di lettere maiuscole, minuscole, numeri e caratteri speciali. Non deve contenere riferimenti agevolmente riconducibili all'utente (username, nomi o date relative alla persona o ad un familiare).

È necessario procedere alla modifica della password a cura dell'utente al primo accesso e, successivamente, almeno ogni sei mesi; in particolare, nel caso di trattamento di categorie particolari di dati personali (art. 9, Regolamento (UE) 2016/679,) nonché dei dati personali relativi a condanne penali e reati (art. 10, Regolamento (UE) 2016/679) la periodicità della variazione dovrà essere ridotta a tre mesi.

La password deve essere immediatamente sostituita nel caso si sospetti che abbia perso segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Responsabile Area GOIT, che provvederà a ricrearne una nuova.
Nel caso venga dimenticata la password, ne dovrà essere richiesta una nuova, per iscritto, al Responsabile Area GOIT.

Nel caso di cessazione del rapporto di lavoro con l'utente, questi verrà disabilitato nel Dominio e in tutti gli applicativi per i quali era stato autorizzato all'accesso/uso.

6. Utilizzo infrastruttura di rete e Filesystem

Per l'accesso alle risorse informatiche dell'Ente attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo l'art. 5.

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 file di lavoro, organizzati per area/ufficio o per diversi criteri o per obiettivi specifici di lavoro. Gli Strumenti Informatici e tutte le cartelle di rete possono ospitare esclusivamente contenuti professionali. Pertanto è vietato il salvataggio sui server dell'Ente, ovvero sugli Strumenti, di documenti non inerenti all'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, e-mail personali, film e quant'altro. 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, l'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico, con le modalità e secondo i principi meglio descritti al successivo punto 13. Ogni materiale personale rilevato dal Responsabile Area GOIT a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche sugli Strumenti, viene rimosso secondo le regole previste nel successivo punto 13 del presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare. Tutte le risorse di memorizzazione, diverse da quelle citate al punto precedente, non sono sottoposte al controllo regolare del Responsabile Area GOIT e non sono oggetto di backup periodici. A titolo di esempio e non esaustivo si citano: il disco C: o altri dischi locali dei singoli PC, la cartella "Documenti" o "Desktop" dell'utente, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come Hard disk portatili o NAS ad uso esclusivo. Tutte queste aree di memorizzazione non devono ospitare dati di interesse, poiché non sono garantite la sicurezza e la protezione contro l'eventuale perdita di dati. Pertanto la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.

Senza il consenso scritto del Titolare del trattamento o suo apposito delegato, è vietato trasferire documenti elettronici dai sistemi informativi e Strumenti dell'Ente a *device* esterni (hard disk, chiavette, CD, DVD e altri supporti).

Senza il consenso scritto del Responsabile Area GOIT è vietato salvare documenti elettronici dell'Ente (ad esempio pervenuti via e-mail o salvati sul Server o sullo Strumento in dotazione) su *repository* esterne (quali ad esempio *Dropbox, Google Drive, OneDrive, WeTransfer*, ecc.). In caso di necessità l'Ente metterà a disposizione modalità in linea con le presenti direttive.

Con regolare periodicità (almeno una volta al mese), ciascun utente provvede alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

La risorsa di rete denominata "COMUNE" è messa a disposizione degli utenti principalmente per lo scambio temporaneo di file tra utenti, così da evitarne la trasmissione via e-mail; i file ivi depositati dovranno essere rimossi non appena si completa lo scambio; il Responsabile Area GOIT provvederà d'ufficio ad una pulizia periodica della risorsa "COMUNE" cancellando file e cartelle più vecchi di 2 mesi e che non appartengano a richieste specifiche regolarmente autorizzate per iscritto dal Responsabile Area GOIT.

L'Ente mette a disposizione dei propri utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno. Tale accesso potrà avvenire mediante rete VPN (Virtual Private Network). Qualora presente un apposito accordo di riservatezza, l'accesso mediante VPN, o altra modalità, viene anche concesso a

consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche.

Le richieste di abilitazione all'accesso mediante VPN, o altra modalità congrua, dovranno seguire le prescrizioni del punto 5.

All'interno della sede lavorativa è resa disponibile anche una rete senza fili, c.d. "WiFi". Tale connessione consente l'accesso ad alcune risorse informatiche e ad internet per i dispositivi non collegati alla rete LAN mediante cavo. L'accesso mediante rete WiFi viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a utenti nell'Ente che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse. L'impostazione della connessione WiFi sarà effettuata dal Responsabile Area GOIT.

Il Responsabile Area GOIT si riserva la facoltà di negare o interrompere l'accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica.

I log di accesso al sistema o alla intranet sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso il Responsabile Area GOIT, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio. I controlli possono avvenire secondo le disposizioni previste al successivo punto 13 del presente Regolamento.
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*".

7. Utilizzo degli Strumenti

L'utente è consapevole che gli Strumenti forniti sono di proprietà dell'Ente e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Ciascun utente si deve quindi attenere alle seguenti regole di utilizzo degli Strumenti.

L'accesso agli Strumenti è protetto da password; per l'accesso devono essere utilizzati username e password assegnate dal Responsabile Area GOIT (cfr. 5). A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza.

Gli strumenti devono essere custoditi con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente e per iscritto al Responsabile Area GOIT ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione della password di accensione (BIOS), senza preventiva autorizzazione scritta da parte del Responsabile Area GOIT.

Non è consentito all'utente modificare le caratteristiche hardware e software impostate sugli Strumenti assegnati, salvo preventiva autorizzazione scritta da parte del Responsabile Area GOIT.

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.

Non è consentita l'installazione di programmi diversi da quelli autorizzati dal Responsabile Area GOIT.

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.

È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.

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 dal Responsabile Area GOIT. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative.

È vietato connettere al PC qualsiasi periferica non autorizzata preventivamente per iscritto dal Responsabile Area GOIT (ad esempio, ma non limitatamente a: smartphone, fotocamere, webcam, stampanti, etc.).

È vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, stampanti, etc.) non autorizzato preventivamente per iscritto dal Responsabile Area GOIT.

Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, l'utente è tenuto a comunicarlo tempestivamente al Responsabile Area GOIT.

Dal momento della cessazione del rapporto di lavoro gli strumenti elettronici messi a disposizione dell'utente verranno resettati alle condizioni iniziali.

Nei casi di smarrimento, furto accertato o grave manomissione dei dispositivi assegnati o del contenuto degli stessi, gli utenti devono segnalare immediatamente e per iscritto il fatto ai soggetti di seguito indicati:

- Responsabile Area GOIT
- Autorità Giudiziaria (sporgere denuncia)

- Direttore della propria Struttura di appartenenza.

L'Ente si riserva di poter autorizzare i dipendenti all'utilizzo dei propri dispositivi mobili al fine di accedere, conservare e trattare informazioni e applicazioni aziendali. Si parla in tal caso di modalità BYOD (acronimo di *Bring Your Own Device*).

I dispositivi BYOD dovranno rispondere a un livello di sicurezza almeno pari a quello dei dispositivi dell'Ente, in particolare per quanto riguarda l'accesso tramite username e password, la frequenza di backup e l'adozione di un programma antivirus regolarmente aggiornato. A tal fine i dispositivi BYOD dovranno venire preventivamente sottoposti a verifica da parte del Responsabile Area GOIT, il quale potrà proporre eventuali modifiche della configurazione del dispositivo, e/o l'installazione di software per adeguarne i livelli di sicurezza.

I dispositivi BYOD, nonché di quelli di proprietà dell'Ente per i quali e stato esplicitamente autorizzato l'uso promiscuo, dovranno essere gestiti in modo da evitare commistioni fra i dati di proprietà dell'utilizzatore e quelli (personali o comunque riservati) di proprietà dell'Ente; per questi ultimi valgono tutte le limitazioni precedentemente indicate.

Sui dispositivi BYOD potranno essere installati solo software precedentemente concordati con il Responsabile Area GOIT, e comunque coperti da una licenza regolare e documentabile.

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, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso il Responsabile Area GOIT, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio. I controlli possono avvenire secondo le disposizioni previste al successivo punto 13 del presente Regolamento. 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*".

8. Utilizzo di internet

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 utente si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi.

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. L'accesso è regolato dal proxy con le sue policy di sicurezza debitamente implementate e aggiornate.

È vietato compiere azioni che siano potenzialmente in grado di arrecare danno all'Ente, ad esempio, il download o l'upload di file audio e/o video, l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa.

È vietato a chiunque il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dal Responsabile Area GOIT.

L'Ente 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 si dovrà contattare per iscritto il Responsabile Area GOIT 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 e-mail indirizzata al Responsabile Area GOIT, ed in copia al Segretario 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. L'utente, nello svolgimento delle proprie attività, deve comunque tenere presente in modo particolare i punti 13 e 14 del presente regolamento. Al termine dell'attività il Responsabile Area GOIT ripristinerà i filtri alla situazione iniziale.

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 per iscritto dal Segretario Generale e dal Responsabile Area GOIT, con il rispetto delle normali procedure di acquisto.

È assolutamente vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet tranne in casi del tutto eccezionali e previa autorizzazione scritta del Responsabile Area GOIT e del Segretario Generale.

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*)

È consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati dal Responsabile Area GOIT. 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, secondo le disposizioni dei punti 13 e 14 del presente regolamento.

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.

Si informa che l'Ente, per il tramite del Responsabile Area GOIT, non effettua il controllo sistematico delle pagine web visualizzate dal singolo utente, né controlla con sistemi automatici i dati di navigazione dello stesso. Si informa tuttavia che al fine di garantire il Servizio Internet e la sicurezza dei sistemi informativi, nonché per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, l'Ente registra per un massimo di 365 giorni i dati di navigazione (file di log riferiti al traffico web). Eventuali controlli avverranno nelle forme indicate al successivo punto 13 del presente Regolamento. 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*".

9. Utilizzo della 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. Ciascun utente si deve attenere alle seguenti regole di utilizzo dell'indirizzo di posta elettronica.

Ad ogni utente viene fornito un account e-mail nominativo, generalmente coerente con il modello nome.cognome@port.venice.it dell'Ente e ne viene inibito l'accesso alla cessazione del rapporto di lavoro; la casella di posta rimarrà comunque attiva con apposito messaggio di risposta automatica per n. 30 giorni e, al termine di tale data, verrà disattivata. L'utilizzo dell'e-mail 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.

L'Ente fornisce, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro il cui utilizzo è da preferire rispetto alle e-mail nominative qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività su dati.

L'iscrizione a *e-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, evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito, oppure che 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 il Responsabile Area GOIT per una valutazione dei singoli casi.

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.

Nel caso fosse necessario inviare allegati "pesanti" (consentito sino a 10 Mb) è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti. Nel caso di allegati ancora più voluminosi è necessario rivolgersi per iscritto al Responsabile Area GOIT. Per opportuna informazione inoltre, è consentita la ricezione di allegati sino a 30 Mb.

Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password). La password di cifratura deve essere comunicata al destinatario attraverso un canale diverso dalla e-mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati. Tutte le informazioni, i dati personali e/o sensibili di competenza possono essere inviati soltanto a destinatari - persone o Enti – qualificati e competenti.

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 e-mail alternativo preferibilmente di tipo collettivo, tipo ufficio...@port.venice.it. Rivolgersi al Responsabile Area GOIT per tale eventualità.

In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione *auto-replay* o l'inoltro automatico su altre caselle e si debba

conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta ha la facoltà di delegare per iscritto un altro utente (fiduciario) per verificare il contenuto di messaggi e per inoltrare al Titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del Dirigente responsabile assicurarsi che sia redatto un verbale attestante quanto avvenuto e che si sia informato il lavoratore interessato alla prima occasione utile;

La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio, possibilmente su autorizzazione scritta del Dirigente responsabile competente. Per evitare che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo ed indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn) se la tipologia del messaggio lo consente.

È vietato inviare messaggi di posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione;

La casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell'allegato sulle condivisioni.

I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e *malware* e per l'eliminazione dello *spam*. I messaggi che dovessero contenere virus vengono eliminati dal sistema e il mittente/destinatario viene avvisato mediante messaggio specifico.

Si informa che, ai sensi dell'articolo 2214 del Codice civile e dell'articolo 22 del D.P.R. 600/73, l'Ente deve conservare per dieci anni sui propri Server tutti e soli i messaggi di posta elettronica a contenuto di rilevanza giuridica e commerciale provenienti da e diretti a domini della stessa; sarà cura del dipendente, ove cessato, segnalarne la rilevanza ed inoltrare tali messaggi al destinatario delle proprie consegne, così come individuato dall'Ente. Si informa altresì che l'Ente, per il tramite del Responsabile Area GOIT, non controlla sistematicamente il flusso di comunicazioni e-mail né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail. Tuttavia, in caso di assenza improvvisa o prolungata dell'utente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, ovvero per motivi di sicurezza del sistema informatico, l'Ente per il tramite del Responsabile Area GOIT può, secondo le procedure indicate al successivo punto 13 del presente Regolamento, accedere all'account di posta elettronica, prendendo visione dei messaggi, salvando o cancellando file. Si informa inoltre che, in caso di cessazione del rapporto lavorativo, verrà immediatamente inibito l'accesso alla casella e-mail affidata all'incaricato, che rimarrà comunque attiva con apposito messaggio di risposta automatica per n. 30 giorni, al termine dei quali verrà completamente disattivata e i contenuti cancellati, salvo quanto sopra previsto. Le informazioni eventualmente 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*".

10. Utilizzo dei telefoni, fax, fotocopiatrici, scanner, stampanti e plotter

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

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

Qualora venisse assegnato uno smartphone e relativa SIM card all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Agli smartphone si applicano le medesime regole sopra previste per gli altri dispositivi informatici (cfr. 7), per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare si raccomanda il rispetto delle regole per una corretta navigazione in Internet (cfr. 8), se consentita.

Per gli smartphone di proprietà dell'Ente è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "*app*" nel contesto degli smartphone) diverse da quelle autorizzate dal Responsabile Area GOIT.

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.

Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:

- Stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative;
- Prediligere le 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 od utilizzare la stampa protetta da PIN, per evitare la possibile perdita o divulgazione di tali informazioni a persone terze non autorizzate.

11. Assistenza agli utenti e manutenzioni

Il Responsabile Area GOIT o i suoi delegati possono 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, il Responsabile Area GOIT o i suoi delegati sono autorizzati 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 per iscritto dal Responsabile Area GOIT, 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 il Responsabile Area GOIT devono presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente regolamento.

E' possibile rivolgersi al Responsabile Area GOIT utilizzando l'apposito applicativo per l'Help Desk (http://apvticketing.intranet.apv) oppure, in alternativa se l'applicativo non è raggiungibile, via telefono interno al 4285 o 4261.

12. Sicurezza delle applicazioni. Data breach.

È obbligatorio attenersi alle disposizioni in materia di protezione dei dati personali ed in particolare alle misure tecniche ed organizzative messe in atto dal Titolare del trattamento per garantire un livello di sicurezza adeguato, come previsto dall'art. 32 del Regolamento (UE) 2016/679 rubricato "Sicurezza del trattamento".
I dati personali, oggetto di trattamento, devono essere custoditi e controllati anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
All'atto della dismissione di supporti che contengano dati personali è necessario distruggere o rendere inutilizzabile (cancellare il contenuto) i supporti medesimi, secondo quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008 sui "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali" (doc. web n. 1571514).
Tutti gli utenti devono porre attenzione nei trattamenti di categorie particolari di dati personali (art. 9, Regolamento (UE) 2016/679) nonché dei dati personali relativi a condanne penali e reati (art. 10, Regolamento (UE) 2016/679).

Sicurezza delle applicazioni.

Le strutture che sviluppano applicazioni informatiche devono rispettare l'approccio della "privacy by design", incorporando i principi e le misure a tutela della privacy nell'intero ciclo di vita delle applicazioni (1). Il nuovo Regolamento (UE) 2016/679, al 78° "considerando" iniziale stabilisce infatti che: "in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici."

Le strutture dell'Ente che affidino ad un fornitore esterno l'incarico di sviluppare applicazioni devono, pertanto, prevedere nei relativi contratti di appalto, che siano rispettate le prescrizioni del sopra citato GDPR, attraverso la previsione di apposite clausole, la sottoscrizione di opportune informative, l'individuazione e la nomina, ove necessaria, del Responsabile esterno del Trattamento, ai sensi dell'art 28 del GDPR, e la sottoscrizione di uno specifico Accordo di riservatezza.

Le stesse considerazioni valgano, inoltre, anche nel caso di applicazioni acquistate sul mercato.

Gestione degli incidenti e data breach.

Ogni incidente (ad es. malfunzionamento PC, indisponibilità dei servizi applicativi e di rete) deve essere segnalato in modo tempestivo al Responsabile Area GOIT, con le modalità previste al precedente punto 11, che raccoglierà le segnalazioni e avvierà il relativo processo di classificazione e risoluzione dell'incidente medesimo al fine di minimizzare gli eventuali impatti negativi sul normale svolgimento delle attività lavorative.

Nel caso l'incidente di una particolare gravità riguardi il patrimonio informativo e di conoscenza detenuto dall'Amministrazione oppure le applicazioni informatiche, l'utente dovrà avvisare anche il Direttore della struttura di riferimento/appartenenza.

Ogni incidente che coinvolge dati personali (cd. "data breach") deve essere segnalato in modo tempestivo al Responsabile Area GOIT, con le modalità previste al precedente punto 11, che raccoglierà le segnalazioni e avvierà il relativo processo di classificazione e risoluzione dell'incidente medesimo al fine di minimizzare gli eventuali impatti negativi sul normale svolgimento delle attività lavorative.

Per ottemperare agli obblighi imposti dalla normativa europea ogni utente, nel caso di incidente di una certa gravità sotto il profilo del rischio per i diritti e le libertà delle persone fisiche (considerando 85, Regolamento (UE) 2016/679); chiunque evidenzi un data breach deve comunicare il fatto al Responsabile del trattamento (DPO), il quale è tenuto ad avvisare il Titolare del trattamento. La notifica alle autorità è obbligatoria nel caso in cui il data breach rischi di ledere i diritti e le libertà degli interessati.

13. 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, l'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, 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, comma 2), di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinano 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

[1] Ad es. gli applicativi, di default, non devono consentire la conoscibilità delle informazioni a chiunque, ma devono consentire agli utenti ambiti di operatività non eccedenti rispetto al profilo di appartenenza.

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 dell'art. 2 del presente Regolamento e dei seguenti 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 dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nei riquadri di cui ai punti 6 – 7 – 8 – 9 del presente Regolamento. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'Utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite del Responsabile Area GOIT, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi (di seguito descritti ai due punti seguenti) e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli Strumenti.

Controlli per la tutela del patrimonio nonché per la sicurezza e la salvaguardia del sistema informatico o per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.). Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche e relative informazioni descritte ai punti 6 – 7 – 8 – 9 il Titolare/Responsabile del trattamento dei dati personali per il tramite del Responsabile Area GOIT, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo):

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. Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni descritte ai punti 6 – 7 – 8 – 9 con possibilità di rilevare file trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. 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 ai punti 1 e 2, il Titolare/Responsabile del Trattamento, unitamente al Responsabile Area GOIT, potrà intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia prendendo tutte le misure tecnicamente necessarie alla soluzione del problema.

Controlli per esigenze produttive e di organizzazione. Per esigenze produttive e di organizzazione si intendono – fra le altre – l'urgente ed improrogabile necessità di accedere a file o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un utente (quali file salvati,

posta elettronica, chat, SMS, etc) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato. Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni descritte ai punti 6 – 7 – 8 – 9 il Titolare/Responsabile del Trattamento, per il tramite del Responsabile Area GOIT, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo):

- Redazione di un atto da parte del Direttore e/o Responsabile Area che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
- Incarico al Responsabile Area GOIT di accedere alla risorsa con credenziali di Amministratore oppure tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.
- Redazione di un verbale che riassuma i passaggi precedenti.

In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.

Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "*General Data Protection Regulation*".

Tutti i controlli sopra descritti avvengono nel rispetto del principio di necessità e non eccedenza rispetto alle finalità descritte nel presente Regolamento. Dell'attività sopra descritta viene redatto verbale, sottoscritto dal Titolare/Responsabile del Trattamento e dal Responsabile Area GOIT che ha svolto l'attività. In caso di nuovo accesso da parte dell'utente allo Strumento informatico oggetto di controllo, lo stesso dovrà avvenire previo rilascio di nuove credenziali (salvo diverse esigenze tecniche). Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "*General Data Protection Regulation*".

14. Conservazione dei dati

In riferimento agli articoli 5 e 6 del Reg. 679/16 e in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed 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.

In casi eccezionali, ad esempio per esigenze tecniche o di sicurezza o per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria è consentito il prolungamento dei tempi di conservazione limitatamente al soddisfacimento delle esigenze sopra esplicitate.

L'Ente si impegna ad applicare le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

15. 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'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

Fermo restando il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, 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.

Il presente articolo deve essere osservato dall'utente sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come utente dell'Ente.

La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni considerate dall'Ente riservate ed in genere, a titolo esemplificativo e non esaustivo, 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, sia di terzi che dell'Ente. L'utente, nelle proprie comunicazioni, non potrà quindi inserire il nominativo e il logo dell'Ente, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione.

L'utente deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà 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, e comunque non potrà 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.

Qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali (es. post su prodotti, servizi, fornitori, partner, ecc.) egli esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Ente, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ente.

16. Sanzioni e norme finali

E' fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL e, nei confronti degli altri utenti, verificata la gravità della violazione contestata, con la risoluzione od il recesso dal contratto ad essi relativo nonché con tutte le azioni civili e penali consentite.

Il presente Regolamento è soggetto a revisione periodica.
Copia del presente Regolamento verrà affissa nella bacheca aziendale, anche per quanto prevede l'art.7 della Legge n. 300/1970, nonché ai fini dell'art.4, comma 3, dello Statuto dei lavoratori.
Verrà inoltre reso disponibile per la visualizzazione e il download sul portale web dell'Ente e all'interno del portale web HR Infinity Zucchetti, nella sezione MyWork di ciascun dipendente. Si invita a renderlo noto e richiederne l'applicazione, eventualmente richiamandolo, dove possibile, nella relativa documentazione contrattuale, anche a collaboratori, consulenti, agenti od altri incaricati esterni (es. incaricati software house, incaricati dei professionisti di cui si avvale l'Ente, ecc.) che venissero autorizzati a far uso di strumenti tecnologici dell'Ente o ad accedere alla rete informatica aziendale e ad eventuali dati ed informazioni ivi conservati e trattati. Pertanto, il presente regolamento entra a far parte, per quanto occorra, del Codice disciplinare aziendale.

Il Segretario Generale