ENTE DI GOVERNO DELL'AMBITO DELLA SARDEGNA

Regolamento per l'utilizzo della posta elettronica e di internet da parte dei dipendenti EGAS

Art. 1
Oggetto e finalità

1. Il presente Regolamento è redatto:
   - alla luce della Legge 20 maggio 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*";
   - ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
   - alla luce dell'art. 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 di tutti gli 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";
   - in attuazione del Regolamento Europeo n. 679/16 "General Data Protection" (Reg. UE n. 679/16 o GDPR);
   - al DPR 13 giugno 2023, n. 81, "*Regolamento concernente modifiche al decreto del Presidente della Repubblica 16 aprile 2013, n. 62, recante: «Codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165*»".
2. 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, quali la posta elettronica, internet e i personal computer con i relativi software, sia conforme alle finalità istituzionali ed alla legge, evitando il verificarsi di qualsiasi abuso o uso non conforme.

Art. 2
Principi generali e di riservatezza nelle comunicazioni

1. I principi a fondamento del presente Regolamento, richiamati dal GDPR, sono:
   - **il principio di necessità**, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzo di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e 6 del Reg. n. 679/16);
   - **il principio di correttezza**, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori. L'Ente favorisce la formazione continua di tutto il personale al fine di acquisire la necessaria consapevolezza nell'uso delle tecnologie informatiche e più in generale del corretto utilizzo dei

dati personali che per motivi di lavoro si trova a trattare;

- **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.

2. Il dipendente si attiene alle seguenti regole di trattamento:

   a) è vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, elementi e informazioni istituzionali dei quali il dipendente 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;

   b) è vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni istituzionali quando il dipendente si allontana dalla postazione di lavoro;

   c) per le riunioni e gli incontri di particolare riservatezza si avrà cura di utilizzare sale dedicate.

Art. 3
Tutela del lavoratore

1. Alla luce dell'art. 4, comma 1, L. 300/1970, la disciplina fissata con il presente Regolamento non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a consentire a quest'ultimo di utilizzare sistemi informativi per far fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.
2. È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-78 del Reg. UE n. 679/2016.

Art. 4
Campo di applicazione

1. Il presente regolamento si applica a tutti i dipendenti dell'Ente, senza distinzioni di ruolo e/o di livello, nonché agli amministratori e ai collaboratori dell'Ente dotati di indirizzo mail EGAS, a prescindere, per questi ultimi, dal rapporto contrattuale in corso.
2. Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata come "incaricato del trattamento" o "autorizzato" o "dipendente/collaboratore".

Art. 5
Gestione, assegnazione e revoca delle credenziali di accesso

1. Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dall'Amministratore di sistema, previa formale richiesta del Responsabile dell'ufficio/servizio/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 dal Responsabile dell'Ufficio/servizio/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 all'Amministratore di sistema dal Responsabile di riferimento.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (altresì nominati username, nome utente o user id), assegnato dal Servizio Sistemi Informativi, ed una relativa password. La password è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza e non divulgata.
3. La password deve essere di adeguata robustezza: deve essere composta da almeno 8 caratteri, formata da lettere maiuscole e minuscole e/o numeri. Non deve contenere riferimenti agevolmente riconducibili all'utente.
4. È necessario procedere alla modifica della password a cura dell'utente al primo accesso e, successivamente, almeno ogni sei mesi. Nel caso in cui l'utente svolga mansioni che, in astratto, possano comportare il trattamento di dati personali sensibili, è obbligatorio il cambio password almeno ogni tre mesi. Tali utenti saranno individuati mediante l'indicazione riportata sul Registro dei trattamenti (art. 30 del Reg. n. 679/16).
5. Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore, il Responsabile dell'ufficio/servizio/area di riferimento dovrà comunicare formalmente e preventivamente all'Amministratore di sistema la data effettiva a partire dalla quale le credenziali saranno disabilitate.

Art. 6
Utilizzo della rete dell'EGAS

1. Per l'accesso alle risorse informatiche dell'EGAS attraverso la rete locale, ciascun dipendente/collaboratore deve essere in possesso di credenziali di autenticazione secondo l'art. 5 del presente Regolamento.
2. È assolutamente proibito accedere alla rete e nei sistemi informativi utilizzando credenziali di altre persone.
3. L'accesso alla rete garantisce a ciascun dipendente/collaboratore la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno inseriti e salvati i files di lavoro. Ciascun dipendente/collaboratore dispone di un'area riservata e personale nel cloud dell'Ente. Tutte le cartelle di rete, siano esse condivise o personali, possono ospitare esclusivamente contenuti professionali: è vietato il salvataggio di documenti non inerenti all'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, mail personali, film e quant'altro. Ogni materiale personale rilevato dal Servizio Sistemi Informativi a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche su strumenti viene rimosso secondo le regole previste nel successivo art. 12 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 degli amministratori di sistema 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 istituzionale, poiché non sono garantite la sicurezza e la protezione contro la eventuale perdita di dati; pertanto, la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.
4. Senza il consenso del Titolare, è vietato trasferire documenti elettronici dai sistemi informativi e strumenti dell'Ente a device esterni (hard disk, chiavette, CD, DVD e altri supporti).
5. Con regolare periodicità (almeno una volta al mese), ciascun dipendente/collaboratore 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.
6. I log relativi all'utilizzo di Strumenti, reperibili nella memoria degli Strumenti stessi ovvero sui Server nonché i file con essi trattati sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso il Servizio Sistemi Informativi, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente. I controlli possono avvenire secondo le disposizioni previste al

successivo punto 12 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 n. 679/16 "General Data Protection".

Art. 7
Utilizzo degli strumenti elettronici (PC, notebook e altri strumenti con relativi software e applicativi)

1. Il dipendente/collaboratore 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.
2. L'accesso agli strumenti messi a disposizione dall'Ente è protetto da password; per l'accesso devono essere utilizzati Username e password assegnate dall'Amministratore di Sistema così come disciplinato dall'art. 5 del presente regolamento. A tal proposito si rammenta che essi sono strettamente personali e ciascun dipendente/ collaboratore è tenuto a conservarli nella massima segretezza.
3. Il Personal Computer, notebook, tablet ed ogni altro hardware deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente all'Amministratore di Sistema ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione della password d'accensione (BIOS) senza preventiva autorizzazione da parte dell'Amministratore di Sistema.
4. Non è consentito ai dipendenti/collaboratori modificare le caratteristiche hardware e software impostate sugli strumenti assegnati, salvo preventiva autorizzazione da parte dell'Amministratore di Sistema.
5. Ciascun dipendente/collaboratore 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.
6. Le informazioni archiviate sul PC locale devono essere esclusivamente quelle necessarie all'attività lavorativa assegnata.
7. Costituisce buona regola la pulizia periodica degli archivi memorizzati sul proprio PC, con cancellazione dei file obsoleti o non più utili.
8. La gestione dei dati su PC è demandata ciascun dipendente/collaboratore che dovrà provvedere a memorizzare sul cloud dell'Ente dati che possono essere utilizzati anche da altri utenti, evitando di mantenere l'esclusività su di essi. Non è consentita l'installazione di programmi diversi da quelli autorizzati dall'Amministratore di Sistema.
9. L'Amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza dei PC, della rete locale e dei server, nonché tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici dell'Ente.
10. 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.
11. È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.

12. È vietato l'utilizzo di supporti di memoria (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli strumenti dell'Ente, salvo che il supporto utilizzato sia stato fornito dall'Amministratore di Sistema. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative.
13. È assolutamente vietato connettere al PC qualsiasi periferica non autorizzata preventivamente dall'Amministratore di Sistema.
14. È assolutamente vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) non autorizzato preventivamente dall'Amministratore di Sistema.
15. Nel caso in cui l'utente dovesse notare comportamenti anomali del pc, ciascun dipendente/collaboratore è tenuto a comunicarlo tempestivamente al Servizio Sistemi Informativi.
16. I log relativi all'utilizzo di Strumenti, reperibili nella memoria degli Strumenti stessi ovvero sui Server o sui router dell'Ente, nonché i file con essi trattati 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 dell'Ente. I controlli possono avvenire secondo le disposizioni previste al successivo art. 12 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 n. 679/16 "General Data Protection".

Art. 8
Utilizzo di internet

1. Il collegamento ad Internet è finalizzato all'utilizzo per lo svolgimento dell'attività lavorativa. L'amministrazione, tuttavia, ammette in via eccezionale che tale connessione venga utilizzata anche per scopi non immediatamente correlati alla prestazione lavorativa, purché ciò avvenga nel rispetto di principi di ragionevolezza e di buona fede e, comunque, non metta a repentaglio l'integrità e la riservatezza dei dati, delle informazioni e dell'intero sistema informatico dell'Amministrazione ovvero provochi per la stessa un danno economico.
2. Il dipendente/collaboratore, fermo restando le diposizioni di legge in materia di privacy, del Contratto di lavoro, degli obblighi di riservatezza e degli standars applicati, non può utilizzare l'accesso ad Internet, per motivi personali, se non per un tempo breve ed occasionale e, comunque, con modalità che non arrechino intralcio/rallentamento alla normale attività lavorativa propria e di terzi.
3. Ciascun dipendente /collaboratore 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. L'accesso è consentito dal proxy dell'Ente con le sue policy di sicurezza debitamente implementate e aggiornate, ad es. i siti istituzionali, i siti degli Enti locali, di fornitori e partner istituzionali;
    - è vietato compiere azioni 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 dall'Amministratore di Sistema;
    - 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 dell'Ente, è necessario contattare l'Amministratore di Sistema per uno sblocco selettivo;

- nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri del suddetto proxy, è necessario richiedere lo sblocco mediante una mail indirizzata all'Amministratore di Sistema, ed in copia al Titolare del Trattamento, 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'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili di ciascun dipendente/collaboratore, possono essere oggetto di controlli da parte dell'Ente, per il tramite dell'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, 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, descritti all'art. 12, e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta. Al termine dell'attività l'Amministratore di Sistema ripristinerà i filtri nella situazione iniziale;
- è 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 dal Datore di Lavoro e dal Servizio Sistemi Informativi, 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 dell'Amministratore di Sistema;
- è 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);
- 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 o web radio, in quanto possono limitare e/o compromettere l'uso della rete agli altri dipendenti/collaboratori.

4. Al fine delle verifiche di cui al presente regolamento, l'Ente, per il tramite dell'Amministratore di Sistema, non effettua la memorizzazione sistematica delle pagine web visualizzate dal singolo utente, né controlla con sistemi automatici i dati di navigazione dello stesso.

   Solo in casi eccezionali e di comprovata urgenza rispetto alle finalità sopra descritte, l'Ente può trattare i dati di navigazione riferendoli specificatamente ad un singolo nome utente. In tali casi i controlli avverranno nelle forme indicate al successivo punto 12 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 n. 679/16 "General Data Protection".

Art. 9
Utilizzo della posta elettronica

1. Ad ogni utente viene fornito dall'Ente un account e-mail nominativo; l'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi istituzionali, 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. E' vietato l'invio di

messaggi di posta elettronica, all'interno o all'esterno dell'amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione.

2. L'iscrizione a mailing-list o newsletter esterne con il proprio indirizzo personale dell'Ente è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.
3. Allo scopo di garantire sicurezza alla rete, il personale deve 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 è necessario contattare l'Amministratore di Sistema per una valutazione dei singoli casi.
4. Nel caso fosse necessario inviare allegati "pesanti" (oltre i 20 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 occorre depositare la documentazione dul cloud dell'Ente e creare un link di condivisione della stessa, secondo le indicazioni dell'Amministratore di Sistema.
5. Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali sensibili, è obbligatorio che questi ultimi vengano omessi o resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password). La password di crittazione deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati.
6. 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 eventualmente, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo, individuato in quello dell'Ufficio protocollo. Sarà cura del dipendente interessato rivolgersi all'Amministratore di Sistema per tale eventualità.
7. In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione autoreply o l'inoltro automatico su altre caselle di posta e si debba conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta ha la facoltà di delegare un altro dipendente al fine di verificare il contenuto di messaggi e di inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del Responsabile di Area assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore interessato alla prima occasione utile.
8. La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti al servizio. 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.
9. È vietato inviare posta elettronica in nome e per conto di un altro utente, salvo sua espressa indicazione e/o autorizzazione.
10. La casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non sia più necessaria. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell'allegato sul cloud dell'Ente.
11. 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.

12. L'Ente, tramite l'Amministratore di Sistema, non controlla sistematicamente il flusso di comunicazioni mail né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori. Tuttavia, in caso di assenza improvvisa o prolungata del dipendente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro ovvero per motivi di sicurezza del sistema informatico, l'Ente può, tramite l'Amministratore di Sistema, accedere all'account di posta elettronica istituzionale, prendendo visione dei messaggi, salvando o cancellando files, secondo le procedure indicate al successivo art.12 del presente Regolamento
13. In caso di cessazione del rapporto lavorativo, la mail affidata all'incaricato verrà sospesa per un periodo di 6 mesi e successivamente disattivata. Nel periodo di sospensione l'account rimarrà attivo e visibile ad un soggetto incaricato dall'Ente solo in ricezione, che tratterà i dati e le informazioni pervenute per esigenze organizzative e produttive, e per la sicurezza del lavoro, trasmettendone il contenuto ad altri dipendenti (se il messaggio ha contenuto lavorativo) ovvero cancellandolo (se il messaggio non ha contenuto lavorativo). Il sistema in ogni caso genererà una risposta automatica al mittente, invitandolo a rispedire il messaggio ad altro indirizzo mail dell'Ente. 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 n. 679/16 "General Data Protection".

Art. 10
Utilizzo dei telefoni, fax, fotocopiatrici, scanner e stampanti dell'Ente

1. Il dipendente è consapevole che i telefoni presenti nella sede dell'Ente sono di proprietà dell'EGAS e sono resi disponibili al dipendente/collaboratore esclusivamente al fine di rendere la prestazione lavorativa. Non sono 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.
2. Qualora venisse assegnato un cellulare istituzionale al dipendente/collaboratore, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone dell'Ente si applicano le medesime regole sopra previste per gli altri dispositivi informatici, 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, se consentita; è inoltre vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate dal Servizio Sistemi informativi.
3. Relativamente agli strumenti di stampa, è vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione, parte del Responsabile di Area. Nel caso in cui si rendesse necessaria la stampa di informazioni riservate il dipendente/collaboratore/amministratore dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni e persone terze non autorizzate.
4. Il dipendente/collaboratore è inoltre tenuto 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);
   - prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, se possibile.

Art. 11
Assistenza agli utenti e manutenzioni

1. L'Amministratore di Sistema, in base alla tipologia dell'intervento richiesto, può accedere ai dispositivi informatici dell'Ente 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.
2. Gli interventi tecnici posso avvenire previo consenso del dipendente/collaboratore, quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora per l'intervento tecnico in loco o in remoto non sia necessarioi accedere mediante credenziali utente, l'Amministratore di sistema è autorizzato ad effettuare gli interventi senza il consenso del dipendente/collaboratore cui la risorsa è assegnata.
3. L'accesso in teleassistenza sui PC della rete dell'Ente 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.
4. Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o l'Amministratore di Sistema devono presenziare alla sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente regolamento.

Art. 12
Controlli sugli Strumenti

1. Poiché in caso di violazioni contrattuali e giuridiche, sia l'Ente sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'EGAS 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 consentano indirettamente il controllo a distanza e determinino 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'utilizzo dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. Le attività di monitoraggio saranno svolte solo dall'Amministratore di Sistema, sempre nel rispetto della succitata normativa e 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 e solo in caso segnalazione che necessita un accertamento, quindi non come controllo a distanza e disancorato da situazioni che richiedono l'accesso;

   Trasparenza: l'adozione del presente Regolamento ha l'obiettivo di informare i dipendenti/collaboratori sui diritti ed i doveri di entrambe le parti.

   Pertinenza e non eccedenza: occorre evitare un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.
2. L'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nel presente Regolamento. Tali informazioni, che possono contenere dati personali

eventualmente anche sensibili del dipendente/collaboratore, possono essere oggetto di controlli da parte dell'Ente, tramite l'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro 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:

- controlli 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, ecc.). A tal fine occorre seguire il processo descritto nel seguito:
    - 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;
    - 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 negli articoli 6 – 7 – 8 – 9 con possibilità di rilevare files 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;
    - qualora il rischio di compromissione del sistema informativo dell'Ente sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali sopra descritti, il delegato al Trattamento, unitamente all'amministratore di sistema, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.
- controlli per esigenze di organizzazione, come l'urgente ed improrogabile necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un dipendente/collaboratore (quali file salvati, posta elettronica, chat, SMS, ecc) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato. A tal fine occorre seguire il processo descritto nel seguito:
    - redazione di un atto da parte del Titolare del Trattamento che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento;
    - incarico all'Amministratore di sistema di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione del dipendente/collaboratore interessato, con avviso che, al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali;
    - redazione di un verbale che riassuma i passaggi precedenti;
    - 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 n. 679/16 "General Data Protection".

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

3. In caso di nuovo accesso da parte del dipendente/collaboratore 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 n. 679/16 "General Data Protection".

4. Per lo svolgimento degli accertamenti e per l'adozione delle misure atte a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati, si rinvia altresì alle regole stabilite mediante linee guida adottate dall'Agenzia per l'Italia Digitale, sentito il Garante per la protezione dei dati personali

Art. 13
Conservazione dei dati

1. In riferimento agli articoli 5 e 6 del Reg. n. 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 ed al traffico telematico (log di sistema e del server proxy), la cui conservazione non sia necessaria, saranno cancellati entro dodici mesi dalla loro produzione.
2. 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.
3. L'Ente si impegna ad assumere le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

Art. 14
Partecipazioni a Social Media

1. 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 dipendenti/collaboratori. A tal fine si rinvia al "Regolamento per l'utilizzo dei social network", allegato integrativo al Regolamento sulla protezione dei dati personali, approvato con deliberazione del CIA n. 18 del 16 giugno 2022, ed al Codice di comportamento dei dipendenti EGAS.

   Ad ogni modo, nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente alla pubblica amministrazione di appartenenza. In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'amministrazione di appartenenza o della pubblica amministrazione in generale.
2. Il dipendente/collaboratore deve garantire la tutela della riservatezza e dignità delle persone; non potrà dunque comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e 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 di Area.

Art. 15
Sanzioni disciplinari

1. È fatto obbligo a tutti i dipendenti/collaboratori di osservare le disposizioni portate a conoscenza con il presente Regolamento. Eventuali violazioni del presente Regolamento da parte dei dipendenti/collaboratori, a seconda della gravità della infrazione, possono dare luogo a sanzioni disciplinari.

Art. 16
Utilizzo degli strumenti informatici degli amministratori

1. Qualora i servizi di accesso ad internet e/o di utilizzo della posta elettronica siano messi a disposizione degli amministratori per l'espletamento dei compiti connessi alla loro funzione, questi sono tenuti al rispetto delle regole contenute nel presente regolamento.

Art. 17
Disposizioni finali

1. La diffusione del presente Regolamento avviene nelle seguenti forme:
   - trasmissione per posta elettronica interna a tutti i dipendenti/collaboratori provvisti di e-mail istituzionale;
   - pubblicazione sulla sezione Amministrazione trasparente- sotto sezione "atti generali".
2. Tutti i dipendenti/collaboratori possono proporre, qualora ritenuto necessario, integrazioni e modifiche al presente Regolamento tramite comunicazione scritta al Direttore Generale e all'Amministratore di Sistema.