Deliberazione della Giunta Regionale 3 agosto 2022, n. 2-5456
Nuovo disciplinare per l'uso degli strumenti informatici. Revoca della D.G.R. n. 2-12269 del 05.10.2009.

A relazione del Presidente Cirio:

Premesso che:

il 27 aprile 2016 è stato approvato il Regolamento (UE) 2016/679 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), entrato in vigore il 24 maggio 2016;
Il Regolamento (RGPD) nasce per proteggere i diritti e le libertà fondamentali delle persone fisiche, in particolare per assicurare un'applicazione coerente e omogenea delle norme a protezione dei dati personali con regole equivalenti a livello europeo (considerando 10) ed offre un quadro di riferimento aggiornato e fondato sul principio di responsabilizzazione (accountability);
Il 18 maggio 2018 è stata approvata la D.G.R. n. 1-6847 avente ad oggetto "Adempimenti in attuazione del Regolamento (UE) 2016/679 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). Revoca D.G.R. n. 1-11491 del 3.06.2009".

Considerato che, per adempiere al Regolamento UE, sono necessari provvedimenti specifici richiamati solo in via essenziale nella D.G.R. di cui sopra.

Visto che l'art. 5 del Regolamento, introducendo il principio di responsabilizzazione (accountability), attribuisce direttamente al Titolare del trattamento il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali, verificando che i dati vengano trattati secondo "liceità, correttezza e trasparenza"; raccolti per "finalità determinate, esplicite e legittime"; adeguati, pertinenti e limitati rispetto alle finalità; esatti; limitati nella conservazione, garantendo sicurezza e integrità.

Visto che la Giunta regionale ha deciso di adottare un disciplinare per l'uso degli strumenti informatici a disposizione dei soggetti che svolgono attività lavorative a beneficio della Giunta regionale.

Dato atto che il disciplinare è uno strumento di garanzia per i lavoratori, collaboratori e consulenti mediante il quale viene introdotta una disciplina che dà indicazione agli stessi di come devono essere trattati i dati personali e, allo stesso tempo, li tutela informandoli di come vengono trattati i propri dati personali e delle indicazioni che la Giunta regionale e l'Amministratore di sistema mettono in atto per evitare un utilizzo scorretto o illecito degli strumenti informatici dell'Ente.

Il disciplinare è stato oggetto di informativa alle Organizzazioni Sindacali e alla RSU Categorie in data 05.04.2022 e successivamente, in data 04/05/2022 al Comitato di coordinamento dei Direttori della Giunta regionale.

Il disciplinare sarà applicabile a ogni utente, intendendosi con ciò ogni dipendente, senza distinzione di ruolo e/o di livello e ogni collaboratore ed organo politico in possesso di specifiche credenziali di autenticazione per l'accesso alle risorse informatiche dell'Ente.

Il testo del disciplinare redatto sulla base del principio di accountability, verrà reso noto a tutti i dipendenti con le forme più efficaci ed immediate: trasmissione alle Direzioni e diffusione sul sito ufficiale della Regione Piemonte e sulla Intranet aziendale.

Considerato, inoltre, che a seguito dell'adozione della presente deliberazione si intende revocare la D.G.R. 12269 del 5 ottobre 2009 "Approvazione del disciplinare in materia di utilizzo della posta elettronica e della Rete internet nel rapporto di lavoro, alle dipendenze della Giunta regionale del Piemonte".

Visto il Regolamento generale sulla protezione dei dati 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

Vista la Legge n. 300 del 5 maggio 1970, 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".

Visto il D.lgs. n. 196 del 30 giugno 2003 come modificato dal D.lgs. n. 101 del 10 agosto 2018;

visto il D.lgs. 82/2005 "Codice dell'amministrazione digitale;

vista la legge regionale n. 23 del 28 luglio 2008;
viste le "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007.

Vista la deliberazione di Giunta regionale n. 1- 6847 del 18.05.2018 recante "Adempimenti in attuazione del Regolamento (UE) 2016/679 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). Revoca D.G.R. n. 1-11491 del 3.06.2009";

Attestata l'assenza degli effetti diretti ed indiretti, del presente provvedimento, sulla situazione economico-finanzaria e sul patrimonio regionale, ai sensi della D.G.R. 1-4046 del 17 ottobre 2016, come modificata dalla D.G.R. 1-3361 del 14 giugno 2021".

Attestata la regolarità amministrativa del presente provvedimento ai sensi della D.G.R. n. 1-4046 del 17.10.2016 "Approvazione della "Disciplina del sistema dei controlli interni" parziale revoca della D.G.R. 8-29910 del 13.4.2000, come modificata dalla D.G.R. 1-3361del 14 giugno 2021.

Tutto quanto premesso e considerato, la Giunta regionale, a voti unanimi resi nelle forme di legge;

delibera

- di approvare il nuovo disciplinare per l'uso degli strumenti informatici allegato alla presente deliberazione per farne parte integrante e sostanziale, revocando la D.G.R. n. 2-12269 del 5 ottobre 2009 "Approvazione del disciplinare in materia di utilizzo della posta elettronica e della Rete internet nel rapporto di lavoro, alle dipendenze della Giunta regionale del Piemonte";

- di dare comunicazione della presente deliberazione a tutti i dipendenti della Giunta regionale attraverso la diffusione sulla intranet aziendale e con ogni altro mezzo idoneo;

- di dare atto che il presente provvedimento non comporta oneri per il bilancio regionale.

La presente deliberazione sarà pubblicata sul B.U. della Regione Piemonte ai sensi dell'art. 61 dello Statuto e dell'art. 5 della L.R. 22/2010 e in Amministrazione Trasparente ai sensi dell'art. 12 del D.lgs. 33/2013.

(omissis)

Allegato

REGIONE PIEMONTE

DISCIPLINARE PER L'UTILIZZO DEI SISTEMI INFORMATICI

Sommario

Premessa 3

1 Oggetto e finalità 3

2 Principi generali e principi di riservatezza nelle comunicazioni 4

3 Tutela del lavoratore 5

4 Descrizione dell'architettura dei servizi informatici 5

5 Il referente SIRe 5

6 Gestione, assegnazione e revoca delle credenziali di accesso al dominio, alla posta elettronica, alle procedure con autenticazione AprIride e alle procedure con autenticazione propria. 6

7 Strumenti informatici (PC - fisico o desktop remoto, notebook e altri strumenti con relativi software e applicativi) di proprietà dell'Ente. 7

8 Infrastruttura di rete e File System 9

9 Help Desk 11

10 Regole applicabili all'utilizzo di internet mediante gli strumenti informatici dell'Ente 11

11 Utilizzo della posta elettronica istituzionale 11

12 Processo di abilitazione/disabilitazione alle procedure 14

13 Utilizzo dei telefoni, fotocopiatrici, scanner e stampanti messi a disposizione dall'Ente. 14

14 Assistenza agli utenti e manutenzioni 15

15 LOG di sistema 16

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

17 Controlli per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, ecc.). 17

18 Conservazione dei dati 18

19 Utilizzo dei Social Network 19

20 Pubblicazione e messa a disposizione 19

21 Sanzioni disciplinari 20

Premessa

Il presente disciplinare 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.

Ogni utente, intendendosi con ciò ogni dipendente, senza distinzione di ruolo e/o di livello e ogni collaboratore ed organo politico in possesso di specifiche credenziali di autenticazione per l'accesso alle risorse informatiche dell'Ente, è tenuto a rispettare il presente disciplinare, che è reso disponibile tramite le modalità specificate al punto 20.

Si specifica che tutti gli strumenti utilizzati dagli utenti per prestare la propria attività lavorativa, intendendo con ciò, ad esempio, PC, notebook, strumenti informatici, e-mail ed altri strumenti con relativi software e applicativi (di seguito più semplicemente "strumenti"), sono messi a disposizione dall'Ente, come dispositivi o come servizio (DaaS – Desktop as a service); ma è anche consentito l'utilizzo di dispositivi propri (BYOD[1]) per rendere la prestazione lavorativa al di fuori della rete regionale.

In ogni caso, sui dispositivi di proprietà degli utenti, sia utilizzati come terminali del desktop remoto, sia per accedere a risorse disponibili sul web, non sono previste né l'installazione di programmi e/o procedure regionali né l'impiego di alcun sistema di monitoraggio delle attività e/o delle connessioni.

Le disposizioni contenute nel presente disciplinare si applicano, a compendio delle regole definite dall'Ufficio competente, anche ai dispositivi mobili (smartphone e tablet) in grado di interconnettersi all'infrastruttura di rete ed ai relativi servizi.

I dati personali e le altre informazioni degli utenti, registrati automaticamente negli strumenti durante il loro uso (log di sistema), sono memorizzati sugli strumenti stessi e possono essere utilizzati 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 raggiungibili solo dall'amministratore di sistema, nei casi previsti dalla Legge, con gli strumenti nativi dei sistemi operativi.

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.

1 Oggetto e finalità

1.1 Il presente Disciplinare 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";
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;

1 Bring Your Own Device

- in attuazione del Regolamento Europeo 679/16 “General Data Protection Regulation” (d’ora in avanti Reg. 679/16 o GDPR);

1.2 La finalità del presente disciplinare è quella di promuovere in tutti gli utenti una corretta "cultura informatica", definire le norme di comportamento per l'uso degli strumenti messi a disposizione dall'amministrazione, fornire le indicazioni necessarie per evitare il verificarsi di qualsiasi uso non conforme o abuso dei succitati strumenti ed informare gli utenti rispetto alle attività memorizzate nei log di sistema.

2 Principi generali e principi di riservatezza nelle comunicazioni

2.1 I principi che sono a fondamento del presente Disciplinare sono gli stessi espressi nel GDPR, e, precisamente:

a il principio di liceità, secondo il quale ogni trattamento deve trovare fondamento in un’idonea base giuridica. I fondamenti di liceità del trattamento di dati personali sono indicati all’articolo 6 del GDPR: consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

b 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. 679/16);

c il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori;

d 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".

2.2 L’utente si attiene alle seguenti regole di trattamento dati:

a è vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, particolari e giudiziari, 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 Responsabile della struttura in cui opera;

b è vietata l’estrazione per uso personale di originali e/o copie cartacee ed informatiche di documenti, fascicoli, lettere, data base e quant’altro.

2.3 Le misure per il trattamento dei dati personali e le procedure da adottarsi in caso di *data breach* sono contenuti in appositi provvedimenti adottati dalla Giunta Regionale[2].

2 Il link contenuto nel testo è operativo solo se la consultazione avviene all’interno della rete regionale

2.4 L'Amministrazione regionale effettuerà, inoltre, attività di monitoraggio e verifica dell'efficacia delle misure di protezione predisposte sul sistema informativo rispetto ad aggressioni esterne senza che siano necessarie preventive ulteriori informative. Le risultanze di tali attività di monitoraggio e verifica potranno essere utilizzate soltanto in modo proporzionato e pertinente alle finalità e alla natura delle stesse e non, ad esempio, al fine di attuare indirettamente un controllo a distanza dell'attività lavorativa svolta dall'utente.

3 Tutela del lavoratore

3.1 Alla luce dell'art. 4, comma 1, L. n. 300/1970, le disposizioni di cui al presente disciplinare non sono finalizzate 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 di servizio e di sicurezza nel trattamento dei dati personali.

3.2 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 Descrizione dell'architettura dei servizi informatici

4.1 Ogni postazione di lavoro all'interno degli uffici regionali è dotata di una connessione di rete aziendale sulla quale transitano sia i servizi informatici che quelli di telefonia fissa (VoIP).

4.2 In aggiunta alla connessione di rete tramite cavo, può essere disponibile il servizio di rete Wi-Fi; attraverso la tecnologia Wi-Fi è possibile connettersi sia alla rete aziendale identificata dal SSID "GR-WiFi", che prevede l'autenticazione automatica dei dispositivi dell'Ente iscritti al dominio mediante protocollo 802.1x, sia alla rete pubblica denominata "Wi-Pie la rete per tutti", la cui fruizione è disciplinata da apposito Regolamento regionale.

4.3 Attraverso qualsiasi dispositivo idoneo collegato alla rete (sia aziendale che internet) ogni utente può connettersi al proprio desktop remoto personale (RDS). Negli uffici regionali è previsto anche l'utilizzo di dispositivi con sistema operativo locale per la fruizione di programmi non disponibili in ambiente RDS.

4.4 Ai sensi dell'art. 6, comma 2, della L.R. 26 marzo 2009, n. 9, la Giunta regionale nella scelta dei programmi per elaboratore elettronico, privilegia quelli appartenenti alla categoria del software libero e i programmi il cui codice è ispezionabile dal titolare della licenza. Qualora si renda necessaria l'acquisizione di programmi software, si adottano le prescrizioni di cui al Codice dell'Amministrazione Digitale (CAD) e alle relative Linee guida definite dall'Agenzia per l'Italia Digitale (AgID).

5 Il referente SIRe

5.1 Ogni Assessorato ed ogni Direzione regionale nomina:

- almeno un dipendente, tra il personale assegnato, nel ruolo di referente SiRE Asset, con funzioni di supporto a tutti i processi relativi alle postazioni di lavoro dell'Ente e ai servizi informatici;

- almeno un dipendente, tra il personale assegnato, nel ruolo di referente SiRE ICT, con funzioni di supporto allo sviluppo del Sistema Informativo nell'ambito della propria Direzione;

I ruoli di referente SIRe Asset ed ICT possono essere svolti, nell'ambito della Direzione/Assessorato, dalle medesime persone.

6 Gestione, assegnazione e revoca delle credenziali di accesso al dominio, alla posta elettronica, alle procedure con autenticazione AprIride e alle procedure con autenticazione propria.

6.1 Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate secondo le indicazioni fornite dal tavolo di coordinamento tra i Settori regionali competenti a definire il processo di de/provisioning e moving del personale.

6.2 Le credenziali di autenticazione relative ai diversi ambiti, consistono in:

- una username per l'accesso al dominio *regpient01* e relativa password;
  - per i dipendenti dell'Ente la username coincide con la matricola;
  - per le altre persone abilitate ad accedere al dominio (collaboratori/organi politici) la username è personalizzata in funzione della tipologia contrattuale in essere con l'Amministrazione (UNR, RAS, ……)
- una login per l'accesso al sistema di posta elettronica e servizi di rete (psnet) associati, del tipo nome.cognome@regione.piemonte.it ovvero per i collaboratori del tipo nome.cognome@mail.regione.piemonte.it e relativa password; è garantita la gestione di credenziali univoche in caso di omonimia;
- un certificato digitale per l'accesso alle procedure che ne richiedono l'uso con relativo codice di installazione, richiesto ad ogni accesso al dominio, fornito dal CSI Piemonte;
- altre credenziali, per servizi esterni ad AprIride, con autenticazione propria.

6.3 Per ogni evento riguardante ciascun utente (assunzione, cessazione, mobilità) la procedura di Alerting provvede alla tempestiva informazione della variazione agli uffici deputati alla gestione delle credenziali medesime.

6.4 Abilitazioni, disabilitazioni e profilazione nell'accesso alle procedure e/o alle cartelle di rete avvengono, su istanza del Dirigente/Direttore e ad opera del referente SIRe Asset, in coerenza alle modalità di svolgimento delle funzioni e delle singole attività all'interno dell'Ente e nel rispetto della normativa in materia di privacy. È cioè necessario che ogni Dirigente e Direttore consideri come le singole attività sono attribuite e svolte dai dipendenti loro assegnati con particolare attenzione alla configurazione del trattamento dei dati personali che ne deriva e alle relative autorizzazioni e profilazioni specifiche per utente e per applicativo utilizzato. Analoga procedura si applica per gli Assessorati in funzione dell'organizzazione dei relativi uffici di comunicazione.

6.5 Le credenziali di accesso alle risorse informatiche devono essere periodicamente modificate e rispettare regole di sicurezza nella loro composizione. Il periodo di validità e le regole applicate possono variare a seconda degli applicativi interessati (di norma la password deve rispettare 3 dei seguenti requisiti minimi di complessità: almeno 8 caratteri, uso di lettere maiuscole e minuscole, numeri e caratteri speciali oltre, preferibilmente a non contenere parole di senso compiuto).

6.6 In caso l'utente dimentichi (o faccia scadere) la password di accesso ad un servizio, se non è disponibile una procedura autonoma, presenterà richiesta di reset della stessa all'ufficio competente che verificherà l'identità del richiedente prima del rilascio della nuova password.

7 Strumenti informatici (PC - fisico o desktop remoto, notebook e altri strumenti con relativi software e applicativi) di proprietà dell'Ente.

7.1 L'utente è consapevole che gli strumenti di proprietà dell'Ente sono forniti per rendere la prestazione lavorativa e per scopi professionali, estendendo a tale ambito anche quelli connessi alla ricerca, alla didattica e alla crescita delle competenze nell'uso delle tecnologie dell'informazione e della comunicazione. Ognuno è responsabile dell'utilizzo degli strumenti assegnati dall'Amministrazione ed ha il compito di farne un uso conforme ai principi di diligenza sanciti dal codice civile; ciascun utente si deve quindi attenere alle regole di utilizzo degli strumenti di cui al presente disciplinare.

7.2 L'accesso agli strumenti è protetto da password; per il primo accesso devono essere utilizzate le credenziali fornite dall'Amministratore di sistema (cfr. punto 6.2), la password deve essere quindi modificata dall'utente con una personale. A tal proposito si rammenta che le credenziali sono strettamente private e l'utente è tenuto a conservarle nella massima segretezza.

7.3 Ogni dispositivo hardware assegnato, identificato univocamente da un numero di censimento informatico, deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione delle password d'accensione (BIOS) e protezione disco, senza preventiva autorizzazione da parte dell'Amministratore di sistema.

Ogni dispositivo hardware, indipendentemente dall'assegnazione, può essere utilizzato da tutti gli utenti in possesso delle credenziali di accesso al dominio; nel caso di dispositivi con sistema operativo Windows viene creata un'area riservata sul disco locale per ogni utente che ha avuto accesso allo stesso, nel caso di dispositivi configurati per l'accesso diretto ad RDS non viene memorizzato alcun dato in locale.

Al fine di garantire la riservatezza e sicurezza dei propri dati è necessario memorizzarli sulle share di rete (cfr. punto 8 – infrastruttura di rete).

7.4 Le impostazioni dei personal computer e dei relativi programmi per elaboratore installati sono predisposte dagli addetti informatici incaricati secondo standard decisi dall'Amministrazione regionale e volti a garantire la fruizione di tutti i servizi necessari allo svolgimento delle mansioni degli utenti.

L'utente non può modificarle autonomamente; può ottenere cambiamenti nelle impostazioni solo previa autorizzazione da parte del Settore competente, su richiesta del referente SIRe Asset

attraverso la procedura definita, in funzione di particolari attività che necessitano di software o impostazioni *ad hoc*.

7.5 L'installazione sui personal computer di sistemi operativi e programmi applicativi e, in generale, di software, avviene generalmente ad opera dei tecnici informatici incaricati, che operano seguendo i necessari criteri di sicurezza. L'uso di tali programmi deve avvenire nel rispetto dei contratti di licenza che li disciplinano e delle specifiche prescrizioni di volta in volta indicate.

7.6 L'installazione di programmi da parte dell'utente, ove sia consentito dal personal computer e dalle relative impostazioni, deve avvenire senza aggirare divieti o restrizioni eventualmente previsti, nel pieno rispetto delle condizioni che disciplinano l'utilizzo di tali programmi e, in generale, della normativa vigente, con particolare riferimento alle disposizioni in materia di protezione di diritti di proprietà intellettuale: abusi o utilizzi illeciti saranno puniti conformemente alle disposizioni che disciplinano il rapporto di lavoro. In ogni caso, l'utente sarà responsabile e sarà chiamato a manlevare e tenere indenne l'Amministrazione regionale da qualsiasi danno o richiesta di risarcimento che venga avanzata da soggetti terzi.

7.7 Tutti i software presenti sui Personal Computer al momento della consegna ed in particolare i software necessari per la protezione dello stesso o della rete internet (quali antivirus o firewall) non possono essere disinstallati o in nessun modo manomessi dagli utenti.

7.8 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 postazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare uno strumento incustodito con una sessione di lavoro attiva può essere causa del suo utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

7.9 È obbligatorio consentire l'installazione degli aggiornamenti di sistema operativo che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC sempre protetto.

Per gli aggiornamenti degli applicativi proposti durante il loro uso è necessario l'intervento dell'Amministratore di Sistema che provvederà a rilasciarli dopo averne verificato la compatibilità con le policy di sicurezza e con i sistemi informativi coinvolti.

7.10 È vietato utilizzare i dispositivi informatici per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.

7.11 È vietato connettere alla rete locale cablata o alla rete Wi-Fi dipendenti (GR-WiFi) qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) non autorizzato preventivamente dall'Amministratore di sistema.

7.12 Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, è tenuto a comunicarlo tempestivamente all'Help Desk (cfr. punto 9).

7.13 In regime di telelavoro e lavoro agile si applicano anche le ulteriori disposizioni previste dai relativi disciplinari e dai contratti individuali.

7.14 In caso di furto e/o smarrimento è compito dell'utente assegnatario dell'attrezzatura presentare denuncia all'autorità giudiziaria ed informare, inoltrando copia della denuncia presentata, il proprio referente SIRe Asset e i Settori coinvolti nella gestione delle attrezzature.

8 Infrastruttura di rete e File System

8.1 Il dominio dell'Ente, *regpient01*, comprende tutti i servizi di identificazione utente e accesso personalizzato alla rete aziendale, al suo file system e alle altre risorse di rete e di stampa condivise.

8.2 Per l'accesso al dominio dell'Ente, ciascun utente deve essere in possesso di credenziali di autenticazione secondo quanto previsto al punto 6.2

8.3 È vietato accedere alla rete ed ai sistemi informativi utilizzando credenziali di altri utenti.

8.4 L'accesso al dominio garantisce all'utente la disponibilità dei dispositivi multifunzione di stampa e delle seguenti share di rete (cartelle condivise su server):

- home directory, identificata con la lettera H:/, denominata come la username ed accedibile esclusivamente dall'utente[3];
- cartella condivisa della struttura di assegnazione;
- cartella comune denominata *common*, utilizzabile da tutti gli utenti del dominio, destinata allo scambio di documenti e file, nel rispetto della normativa privacy[4], tra utenti di strutture diverse; i contenuti di questa cartella vengono automaticamente cancellati tutte le notti;
- eventuali altre cartelle condivise, rese disponibili secondo specifica abilitazione (cfr. 6.4).

Tutte le cartelle di rete, siano esse condivise o personali, ospitano esclusivamente contenuti professionali e sono quotidianamente oggetto di backup.

8.5 Tutte le risorse di memorizzazione, diverse da quelle citate al precedente punto 8.4 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 in disponibilità personale come hard disk portatili o NAS[5] ad uso esclusivo. Tutte queste aree di memorizzazione non devono ospitare dati di interesse, poiché la sicurezza e la protezione contro la loro eventuale perdita non sono garantite; pertanto la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.

8.6 Nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, dell'utente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività delle strutture sia necessario accedere a documenti di lavoro presenti sui dispositivi o sulla share personali, l'utente può delegare, in accordo con il proprio Responsabile, a un altro dipendente della sua stessa struttura a sua scelta ("fiduciario") il compito di individuare e inoltrare al Responsabile della struttura a cui è assegnato i documenti rilevanti per lo svolgimento dell'attività lavorativa.

3 Le cartelle personali sono di dimensione limitata e uguale per tutti gli utenti, in quanto documenti e file di lavoro devono essere di norma memorizzati nelle cartelle condivise della propria struttura o gruppo di lavoro.

4 Qualora siano coinvolti dati personali, l'utente dovrà adottare tutte le precauzioni e le misure per garantire la sicurezza e l'immodificabilità del o dei file originali (salvataggio crittografato con password e impronta SHA-256)

5 Network Attached Storage

La delega si esprime come richiesta all'amministratore di sistema, da effettuarsi tramite il referente SIRe Asset, di temporanea abilitazione al fiduciario ad accedere ai dispositivi o alla share personale dell'utente.

Delle attività svolte dal referente SIRe e dal fiduciario deve essere informato l'utente interessato.

8.7 Qualora l'utente non abbia delegato un suo fiduciario, secondo quanto sopra specificato, in caso di straordinaria necessità ed urgenza, il Responsabile della struttura a cui è assegnato l'utente può richiedere, tramite il referente SIRe Asset, con apposita e motivata richiesta all'Amministratore del Sistema, di accedere alla share e/o ai dispositivi dell'utente assente, in modo di prendere visione delle informazioni e dei documenti necessari; di tale attività deve essere redatto apposito verbale e informato l'utente interessato.

8.8 E' consentito trasferire documenti elettronici dai sistemi informativi e strumenti dell'ente a/da dispositivi esterni (hard disk, chiavette usb, cd, dvd e altri supporti) nei casi previsti (DGR 1-7108 del 29 giugno 2018 recante: "Disposizioni in materia di accesso civico e di accesso civico generalizzato per le strutture della Giunta regionale del Piemonte" e DGR 8-854 del 23 dicembre 2019 "Disciplina per gli uffici della Giunta regionale relativa alle modalità di rilascio di documenti amministrativi e tariffario per il rimborso dei costi sostenuti dall'amministrazione regionale. Revoca DGR n. 39-4814 del 17.12.2001") e per temporanee esigenze di lavoro, al termine delle quali le copie devono essere cancellate.

8.9 Nei rapporti con soggetti esterni all'Amministrazione è consentito l'utilizzo di strumenti di condivisione file di grandi dimensioni sul cloud, fatto salvo il rispetto delle prescrizioni di cui al Regolamento Europeo 679/16 "General Data Protection Regulation", quando le caratteristiche dei file non ne consentono la gestione con gli ordinari strumenti a disposizione degli utenti. In questo caso, l'utente dovrà adottare tutte le precauzioni e le misure per garantire la sicurezza e l'immodificabilità del o dei file originali oggetto del trasferimento (salvataggio crittografato con password e impronta SHA-256). Gli strumenti utilizzabili sono quelli già preventivamente verificati e resi disponibili dall'Amministratore di sistema.

8.10 Con regolare periodicità (almeno una volta al mese), ciascun utente provvede alla pulizia delle cartelle su server, con cancellazione dei file obsoleti o inutili: particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

8.11 L'Amministratore di sistema si riserva la facoltà di negare o interrompere l'accesso alla rete ai dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica.

8.12 Per gli utenti che erogano la propria prestazione lavorativa in modalità di telelavoro o lavoro agile si applicano anche le disposizioni di cui ai relativi disciplinari.

9 Help Desk[6]

9.1 In caso di malfunzionamento di strumenti e/o servizi del sistema informativo regionale l'utente deve segnalarlo, in prima persona o tramite il referente SIRe Asset, al servizio di Help Desk.

9.2 Il servizio di Help Desk è raggiungibile mediante il numero telefonico interno 82888 (800282888 da rete pubblica) o mediante l'indirizzo mail hd_regione@csi.it.

9.3 A fronte della segnalazione telefonica il servizio di Help Desk cerca di formulare una diagnosi del malfunzionamento intervenendo direttamente per quanto possibile o inoltrando la richiesta di assistenza al supporto di secondo livello interessato.

9.4 Per ogni segnalazione registrata, il servizio di Help Desk è tenuto ad aprire un ticket di assistenza e darne visibilità all'utente. Lo stesso ticket verrà chiuso a fronte della risoluzione del problema e anche della chiusura deve essere informato l'utente originatore della segnalazione.

10 Regole applicabili all'utilizzo di internet mediante gli strumenti informatici dell'Ente[7]

10.1 La rete internet può e deve essere utilizzata dall'utente a supporto dell'attività lavorativa.

10.2 L'accesso ad internet dalla rete privata regionale avviene attraverso un servizio "proxy" ed è filtrato da un ulteriore servizio di sicurezza che inibisce l'accesso a siti potenzialmente malevoli e/o manifestamente inopportuni sulla base di una "black list" costantemente aggiornata. È possibile richiedere, attraverso il referente SIRe Asset lo sblocco dalla black list di siti erroneamente inseriti nella stessa.

10.3 È favorito l'uso, di norma attraverso l'interfaccia web, di strumenti di messaggistica istantanea e servizi di videoconferenza e collaborazione on line, per permettere una efficace e comoda comunicazione sia tra i colleghi, sia con interlocutori esterni all'Ente. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche e alle e-mail.

11 Utilizzo della posta elettronica istituzionale

11.1 Ad ogni utente viene fornito un account e-mail nominativo.

11.2 L'insieme degli indirizzi di posta nominativi costituisce la rubrica globale della Regione Piemonte ed è disponibile nella piattaforma di gestione della posta. Trattandosi di dati personali possono essere divulgati esclusivamente per fini istituzionali.

11.3 L'Ente fornisce, altresì, delle caselle di posta elettronica condivise associate a unità organizzative, uffici o gruppi di lavoro il cui utilizzo è da preferire rispetto alle e-mail nominative per le comunicazioni di tipo procedimentale. È compito del referente SIRe Asset richiedere la

6 I dettagli relativi al funzionamento del servizio di Help Desk sono disponibili alla relativa pagina pubblicata sulla Intranet regionale (link operativo solo per consultazione all'interno .della rete regionale).

7 Le regole 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 e s.m.i..

creazione e/o la eliminazione delle caselle di posta condivise e gestire le abilitazioni e/o disabilitazioni degli utenti alle stesse, definendone il relativo livello di delega.

11.4 L'utilizzo dell'e-mail deve essere finalizzato allo svolgimento delle proprie mansioni lavorative e alle comunicazioni relative alle stesse, conformemente al punto 7.1. Si ricorda che gli indirizzi delle caselle di posta elettronica forniti dall'Ente di norma non devono essere utilizzati, in particolare in modo massivo, per fini non connessi all'attività lavorativa. (ad esempio l'invito a partecipare ad eventi extra lavorativi).

11.5 È compito di ogni utente provvedere alla costante eliminazione delle mail non necessarie al fine di contenere le dimensioni degli archivi di posta. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell'allegato sulle cartelle di rete.

11.6 L'iscrizione a mailing-list o newsletter esterne con l'indirizzo fornito dall'Amministrazione è ammessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.

11.7 Allo scopo di garantire sicurezza alla rete, l'utente 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 contengono allegati con contenuto di tipo attivo come, ad esempio, *.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 opportuno contattare il referente SIRe Asset o l'Help Desk per una valutazione dei singoli casi.

11.8 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.

11.9 Nel caso fosse necessario inviare allegati "pesanti" (oltre ai 10 MB) è opportuno ricorrere alla compressione dei file originali in un archivio di formato .zip o equivalente e agli strumenti di pubblicazione di file disponibili nel sistema di posta. Per esigenze particolari, è consentito il ricorso agli strumenti cloud raggiungibili dalla rete dell'Ente, coerentemente a quanto disposto al punto 8.9.

11.10 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 criptazione con apposito software (archiviazione e compressione con password). La password di criptazione deve essere comunicata al destinatario possibilmente attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e comunque mai insieme 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.

11.11 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 avviso di assenza facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza oppure indicando un indirizzo email alternativo preferibilmente di tipo condiviso, del

tipo settore@regione.piemonte.it. Si rammenta che ciascun utente ha il diritto alla disconnessione e il diritto di non dover presidiare la propria casella di posta elettronica nel periodo di ferie, poiché le stesse sono destinate al recupero psico-fisico delle energie (cfr. L. 81/2017).

11.12 Nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, dell'utente, qualora per necessità delle strutture sia necessario accedere alla sua casella di posta, il titolare della casella di posta ha la facoltà di delegare un altro utente, denominato "fiduciario", per verificare il contenuto di messaggi e per inoltrare al Responsabile della propria struttura quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. La delega si esprime attraverso l'apposita funzione presente sull'interfaccia della mail istituzionale.

11.13 Nel caso non sia presente nemmeno il fiduciario, solo in casi di straordinaria necessità ed urgenza e per ragioni di sicurezza, il Responsabile della struttura a cui è assegnato l'utente assente potrà richiedere all'Amministratore di sistema di accedere alla sua casella di posta. Sarà compito del Responsabile della struttura assicurarsi che sia redatto un verbale attestante quanto avvenuto e che venga informato il lavoratore interessato.

11.14 La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti al servizio, possibilmente su autorizzazione del Responsabile della struttura competente. Per evitare violazioni della privacy per diffusione degli indirizzi di posta nonché che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo e indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn) se la tipologia del messaggio lo consente.

11.15 È consentito inviare messaggi di posta elettronica in nome e per conto di un altro utente solo su sua espressa autorizzazione formale o delega.

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

11.17 Nel caso in cui l'utente non presti più la sua attività lavorativa presso la Giunta Regionale del Piemonte, la casella di posta elettronica nominativa sarà disattivata appena l'ufficio incaricato della gestione delle credenziali di posta riceve l'informazione dalla procedura di Alerting (cfr. punto 6.3); contestualmente si provvederà alla cancellazione del contenuto "on line".

11.18 Prima della cessazione dal servizio, l'utente è tenuto ad impostare una risposta automatica che informa di tale cessazione e indica un indirizzo mail alternativo, preferibilmente di gruppo, cui rivolgersi per le tematiche precedentemente trattate dall'utente stesso. Se per esigenze lavorative sorgesse la necessità di accedere al contenuto di tale casella di posta, il Responsabile della struttura organizzativa a cui l'utente era assegnato potrà inoltrare, anche tramite il referente SIRe, motivata richiesta all'Amministratore di sistema.

11.19 In coerenza con il punto 8.8 non è prevista la possibilità di produrre copia delle caselle di posta per utenti non più in servizio presso l'Amministrazione. In ogni caso si informa che il contenuto delle caselle di posta elettronica cancellate potrà essere trattato dall'Ente, per il tramite dell'Amministratore di sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio. Le informazioni così raccolte saranno 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”.

Si informa che, ai sensi della normativa sull’archiviazione e conservazione degli atti amministrativi, dell'articolo 2214 del Codice civile e dell'articolo 22 del Dpr 600/73, per ottemperare legittime istanze di accesso agli atti ai sensi della L. 241/90 o accesso civico generalizzato (d.lgs 33/13) l’Ente deve conservare per dieci anni sui propri Server di Posta Elettronica tutti i messaggi di posta elettronica aventi rilevanza istruttoria o inerenti l’attività procedimentale e contrattuale.

L’Ente, per il tramite dell’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, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail.

12 Processo di abilitazione/disabilitazione alle procedure

12.1 Il Responsabile (Direttore/Dirigente) determina per ogni dipendente assegnato alla Struttura le abilitazioni e i profili da attribuire, modificare o revocare in coerenza con le funzioni e le singole attività per ciascuno di essi secondo le regole di liceità, correttezza e trasparenza, anche con riferimento alle corrette profilazioni sulla base del principio di accountability sancito dal Regolamento (UE) 2016/679. È richiesta pertanto ai responsabili delle strutture regionali una costante verifica di tipo organizzativo sulla necessità e attualità delle abilitazioni in capo ai dipendenti assegnati alla propria struttura.

12.2 I percorsi di abilitazione e disabilitazione devono essere “tracciabili” e veicolati, dal referente Sire Asset, attraverso gli strumenti messi a disposizione dall’Amministrazione, verso il “soggetto individuato”

La responsabilità delle attribuzioni e delle mancate cancellazioni è una responsabilità del dirigente.

12.3 Ogni qualvolta il “soggetto individuato” abiliti un dipendente ad una procedura/applicativo con il relativo profilo, deve essere dato riscontro al dirigente, ai referenti SIRe Asset della direzione e al dipendente abilitato. Si intende per “soggetto individuato” chi detiene la possibilità di attribuire ruoli/profili alle persone rispetto agli applicativi: il ruolo può essere in capo al CSI Piemonte e/o a altri funzionari dell’Ente in relazione allo specifico applicativo.

13 Utilizzo dei telefoni, fotocopiatrici, scanner e stampanti messi a disposizione dall’Ente.

13.1 L’utente è consapevole che tutti gli strumenti dati in uso sono Asset messi a disposizione dall’Ente per lo svolgimento dell’attività lavorativa.

13.2 Qualora venisse assegnato uno smartphone o cellulare, o anche la sola SIM, all’utente, quest’ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari, smartphone e/o SIM dell’Ente si applicano, a compendio delle regole definite dall’Ufficio competente, le

disposizioni sopra previste per gli altri dispositivi informatici e per l'accesso in rete, per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare si raccomanda il rispetto delle indicazioni per la protezione dell'accesso al dispositivo e per il corretto uso della navigazione in Internet e della posta elettronica (cfr. punti 10 e 11).

13.3 La stampa di documenti avviene, di norma, su dispositivi multifunzione disponibili all'interno delle sedi regionali e condivise mediante il dominio *regpient01*.

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

a) stampare documenti solo se strettamente necessario per lo svolgimento delle proprie funzioni operative;

b) prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, se possibile.

13.5 Sia per l'attività in ufficio sia nei casi di telelavoro e lavoro agile non è prevista l'assegnazione di dispositivi di stampa individuali.

13.6 Nel caso in cui si rendesse necessaria la stampa di informazioni riservate, l'utente dovrà utilizzare le apposite funzioni di stampa riservata, disponibili sui dispositivi multifunzione, per evitare la possibile perdita o divulgazione di tali informazioni a persone terze non autorizzate.

13.7 Non è consentita l'installazione di dispositivi di stampa di proprietà degli utenti sui PC messi a disposizione dall'Ente

14 Assistenza agli utenti e manutenzioni

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

a) verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale;

b) verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete;

c) richieste di aggiornamento software e manutenzione preventiva hardware e software.

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

14.3 L'accesso in teleassistenza sui PC della rete richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Amministratore di sistema, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.

14.4 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 disciplinare.

15 LOG di sistema

15.1 I log relativi all'uso del File System di dominio e della intranet, quelli relativi all'utilizzo di strumenti, reperibili nella memoria degli strumenti stessi ovvero sui server o sui router, nonché i file salvati o trattati su Server o strumenti, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di sistema, per esigenze di servizio, per la sicurezza del lavoro e per la tutela del patrimonio, ovvero quando la verifica sia conseguente a specifiche richieste delle autorità competenti.

Le informazioni registrate nei log dipendono dalla natura degli eventi tracciati e dalle finalità associate. Devono almeno permettere di:

- Imputare l'evento tracciato (azione o tentativo di azione sul sistema informatico) al proprio autore (persona fisica, attrezzatura tecnica, programma informatico, ecc.).
- Datare l'evento (grazie alla sincronizzazione degli orologi di sistema).
- Valutare l'evento in termini di: tipo di operazione (es. invio di una mail), parametri rilevanti dell'azione (es. destinatari della mail), risultato dell'operazione (es. successo o fallimento).

In nessun caso i messaggi di log possono contenere informazioni confidenziali come password o i corrispondenti hash, qualsiasi forma di autenticazione utente (es. chiavi pubbliche) o altra informazione la cui riservatezza deve essere preservata.

15.2 I controlli possono avvenire secondo le disposizioni previste al successivo punto 16 del presente Regolamento.

15.3 Le informazioni in possesso dell'Amministrazione regionale di cui al comma 1 potranno essere utilizzate, nei limiti di quanto previsto nel presente Disciplinare, per tutti i fini connessi al rapporto di lavoro e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.

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

16.1 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, esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e [...] previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali [...][8], può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori, 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 all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di

8 Cfr. art. 4,comma 1, L. 20 maggio 1970, n.300

modificazione di procedimenti tecnici destinati a controllare i movimenti[9] o la produttività dei lavoratori. I controlli devono essere effettuati nel rispetto del presente Disciplinare 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 Disciplinare 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.

16.2 L'uso degli strumenti informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato al precedente punto 15 del presente Disciplinare. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'utente, 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, 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 punti 17 e 18) e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli strumenti informatici.

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

17.1 Qualora, per le finalità qui sopra descritte, risulti necessario l'accesso agli strumenti e alle risorse informatiche e relative informazioni descritte al punto 6, 7, 8, 10 e 11, l'Amministratore di sistema si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

i 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 Disciplinare.

ii Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare l'Amministratore di sistema, potendo così accedere alle informazioni descritte al punto 15 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 dell'indirizzo IP dell'utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.

9 Vale disposto art. 4, comma 2, L.300/1970

iii 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 i. e ii., l'Amministratore di sistema potrà intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

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 dall'Amministratore di sistema 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).

18 Conservazione dei dati

18.1 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 al traffico telematico (log di sistema e del server proxy), la cui conservazione non sia necessaria, sono mantenute per 180 giorni dalla loro produzione.

18.2 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.

18.3 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.

Le misure di sicurezza implementate per proteggere i log, da problemi operativi o modifiche non autorizzate (volontarie o involontarie) garantiscono:

- la correttezza dei messaggi di log, sottoponendo a controllo i meccanismi di generazione dei log per ogni sistema IT;
- l'integrità dei messaggi di log, mediante meccanismi di cifratura durante la trasmissione degli stessi dalla fonte alla piattaforma di centralizzazione;
- la disponibilità dei messaggi di log: grazie a meccanismi di fault tolerance relativi al dimensionamento della memoria delle fonti di log;
- l'inalterabilità e l'accesso autorizzato ai messaggi di log: secondo il principio di Segregation of Duties e tramite meccanismi di controllo accessi alla piattaforma, consentiti solamente da rete IT;
- sul file system centralizzato, i log sono raccolti solo per la finalità di conservazione, secondo quanto stabilito dalle vigenti Leggi;
- l'accesso è consentito solo alle PDL degli specialisti di sicurezza.

19 Utilizzo dei Social Network

19.1 L'utilizzo a fini promozionali e commerciali di strumenti di tipo "social media", dei blog e dei forum, anche professionali, è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive e istruzioni operative al personale addetto alla comunicazione attraverso gli account istituzionali.

19.2 La partecipazione o consultazione dei social media durante l'orario di lavoro è consentita esclusivamente in casi di necessità lavorative o necessità di contatti attraverso messaggistica istantanea.

19.3 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, oltre che gli stessi utenti utilizzatori dei social media.

19.4 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 dipendente dell'Ente.

19.5 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 di competenza.

19.6 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 scritto 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 scritto/esplicito del Responsabile della Struttura di appartenenza , salvo in casi di manifestazioni pubbliche ad accesso libero.

19.7 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.

20 Pubblicazione e messa a disposizione

20.1 Il presente Disciplinare è stato redatto dal Gruppo di lavoro interdirezionale GDPR con il supporto del Responsabile per la protezione dei dati che è chiamato a garantire il coordinamento degli adempimenti.

20.2 La sua pubblicizzazione avverrà nelle seguenti forme: trasmissione per posta elettronica interna a tutti i Responsabili di Struttura e a tutti gli utenti, attraverso la intranet della Giunta regionale.

21 Sanzioni disciplinari

21.1 È fatto obbligo a tutti i dipendenti/collaboratori/utenti di osservare le disposizioni portate a conoscenza con il presente disciplinare.

21.2 L'inosservanza di quanto disposto nel presente documento dà luogo a responsabilità disciplinare qualora rientri in una delle infrazioni previste dal codice disciplinare.