

Deliberazione della Giunta Regionale 3 agosto 2026, n. 29-2942

Modifiche al Regolamento interno sull'utilizzo del lavoro agile per i dipendenti della Giunta regionale adottato con D.G.R. n. 8 - 6951 del 29.05.2023.



Seduta N° 181

Adunanza 03 AGOSTO 2026

Il giorno 03 del mese di agosto duemilaventisei alle ore 10:15 si è svolta la seduta della Giunta regionale in via ordinaria, in modalità mista, ai sensi della D.G.R. n. 1-8208 del 26 febbraio 2024 con l'intervento di Alberto Cirio Presidente, Maurizio Raffaello Marrone Vice Presidente e degli Assessori Paolo Bongioanni, Enrico Bussalino, Daniela Cameroni, Marina Chiarelli, Marco Gabusi, Marco Gallo, Matteo Marnati, Federico Riboldi, Andrea Tronzano, Gian Luca Vignale con l'assistenza di Roberta Mettola nelle funzioni di Segretario Verbalizzante.

DGR 29-2942/2026/XII

OGGETTO:

Modifiche al Regolamento interno sull'utilizzo del lavoro agile per i dipendenti della Giunta regionale adottato con D.G.R. n. 8 - 6951 del 29.05.2023.

A relazione di: Vignale

A relazione dell'Assessore Vignale:

Premesso che:

la Legge 7 agosto 2015 n. 124 "Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche" consente a ciascuna amministrazione, nell'ambito della propria autonomia organizzativa, di individuare modalità innovative, alternative al telelavoro, più adeguate rispetto alla propria organizzazione, ai fini della promozione nelle amministrazioni pubbliche della conciliazione dei tempi di vita e di lavoro e del miglioramento della qualità dei servizi erogati, fermo restando il rispetto delle norme e dei principi in tema di sicurezza sul luogo di lavoro, tutela della riservatezza dei dati e verifica dell'adempimento della prestazione lavorativa;

la legge 22 maggio 2017, n. 81, al capo II, disciplina quale modalità flessibile di esecuzione del rapporto di lavoro subordinato il "Lavoro Agile". Il lavoro agile è una modalità flessibile di esecuzione della prestazione lavorativa caratterizzata dallo svolgimento dell'attività lavorativa in parte all'interno dei locali aziendali e in parte all'esterno basata sulla flessibilità organizzativa e sulla volontarietà delle parti che sottoscrivono l'accordo individuale;

il CCNL Funzioni Locali sottoscritto il 23.02.2026 al Titolo VI, Capo I, ha disciplinato il lavoro agile stabilendo all'art. 63, comma 2, che "il lavoro agile è una modalità di esecuzione del rapporto di lavoro subordinato, disciplinato da ciascun Ente con proprio Regolamento ed accordo tra le parti...";

la D.G.R. n. 8-6951 del 29 maggio 2023 della Regione Piemonte "Legge 7 agosto 2015 n. 124 e

Legge 22 maggio 2017, n. 81. Approvazione Regolamento interno sull'utilizzo del lavoro agile per i dipendenti della Giunta Regionale ai sensi dell'art. 63, comma 2 del CCNL Funzioni Locali sottoscritto il 16 novembre 2022" ha approvato il Regolamento interno sull'utilizzo del lavoro agile per i dipendenti della Giunta Regionale;

il Regolamento interno sull'utilizzo del lavoro agile descriveva il lavoro agile come modalità flessibile di esecuzione del rapporto di lavoro subordinato, disciplinandone modalità, tempi e strumenti in coerenza con le disposizioni della Legge 22 maggio 2017, n. 81;

la direttiva del 29 dicembre 2023 del Ministro per la Pubblica Amministrazione ha fornito alle amministrazioni di cui all'art. 1, comma 2, del D. Lgs. n.165/2001, indicazioni in materia di lavoro agile definendolo come strumento organizzativo stabile volto alla conciliazione dei tempi di vita e di lavoro, e non come misura emergenziale adottata durante il periodo pandemico;

la direttiva ha richiamato che il lavoro agile si fonda sulla volontarietà delle parti che sottoscrivono l'accordo individuale e ha evidenziato l'esigenza che ciascuna amministrazione, attraverso specifiche indicazioni nell'ambito degli accordi individuali, definisca le misure organizzative necessarie affinché le previsioni della direttiva trovino concreta applicazione;

la D.G.R. 3-2182/2026/XII del 30 gennaio 2026 recante "Approvazione del Piano integrato di attività e organizzazione (PIAO) della Giunta regionale del Piemonte per gli anni 2026-2028, ai sensi del Decreto Legge n. 80 del 9 giugno 2021, convertito in Legge n. 113 del 6 agosto 2021", ha individuato un apposito punto 3.3 "Strategie e sviluppo di modelli innovativi di organizzazione del lavoro – Il lavoro agile" prevedendo che l'Amministrazione procedesse alla revisione della normativa interna per la disciplina del lavoro a distanza nella forma del lavoro agile;

Ritenuto, alla luce delle previsioni normative sopra citate e dell'esigenza di proporre un modello organizzativo basato su una maggiore autonomia e flessibilità nella gestione delle attività, opportuno di procedere a modificare il Regolamento interno sull'utilizzo del lavoro agile per i dipendenti della Giunta regionale, compresi i Dirigenti; le modifiche riguardano la previsione del lavoro agile per i Dirigenti (artt. 3, co. 1 e 13 co. 3), l'incremento del numero massimo di giornate fruibili su base annuale (art. 4, comma 4), la previsione di ulteriori ipotesi di deroga al limite massimo annuale (art. 13, comma 2) e la possibilità di ricorrere al lavoro agile in casi di interventi manutentivi straordinari o di situazioni imprevedute che determinino la necessità di ridurre od escludere l'ordinario accesso ad una o più sedi regionali, al fine di assicurare la continuità operativa e lo svolgimento delle attività istituzionali (art. 14, comma 3).

Dato atto che il Regolamento richiede che, nella scelta dei luoghi di svolgimento della prestazione lavorativa in modalità lavoro agile, debba essere garantita la presenza delle condizioni che assicurino la piena operatività della dotazione informatica, debbano essere adottate tutte le precauzioni e le misure idonee a garantire la più assoluta riservatezza sui dati e sulle informazioni che vengono trattate dal lavoratore e che debbano essere rispettate e applicate le direttive dell'amministrazione in materia di salute e sicurezza del lavoratore. A tal fine sono allegati al Regolamento, oltre al modello di richiesta di lavoro agile (allegato sub 1) e allo schema di accordo individuale (allegato sub 2 e sub 3), l'informativa sui rischi per la salute e sicurezza in modalità lavoro agile ai sensi dell'art. 22, L. n. 81/2017 e D. Lgs. n. 81/2008 s.m.i. (allegato sub 4) e il disciplinare della Regione Piemonte per l'utilizzo dei sistemi informatici (allegato sub 5).

Dato atto che è stato esperito il confronto con le OO. SS. ai sensi dell'art. 5 del CCNL Funzioni Locali del 16.11.2022 e che la proposta è stata trasmessa al CUG ai sensi dell'art. 57 del D. Lgs. n. 165/2001;

Dato atto altresì che, ai sensi dell'art. 7, comma 4), del CCNL per il triennio 2022-2024 "i criteri di priorità per l'accesso al lavoro agile ed al lavoro da remoto nonché l'individuazione dei casi in cui è possibile estendere il numero delle giornate di prestazione rese in modalità agile o da remoto" sono oggetto di contrattazione collettiva integrativa e che, di conseguenza, l'art. 13 del Regolamento allegato è stato oggetto di sottoscrizione da parte dell'Amministrazione e delle OO.SS. in data 31 luglio 2026.

Ritenuto pertanto, alla luce di quanto sopra illustrato, di modificare e sostituire il regolamento di cui

alla D.G.R. n. 8 - 6951 del 29 maggio 2023 della Regione Piemonte, come da allegato alla presente deliberazione quale parte integrante e sostanziale.

Vista la Legge 7 agosto 2015 n. 124;

vista la Legge 22 maggio 2017 n. 81;

visto il CCNL Funzioni Locali 2022-2024 del 23.02.2026 per il personale del Comparto e del 12.02.2026 per i Dirigenti;

vista la D.G.R. n. 8-6951 del 29 maggio 2023 della Regione Piemonte;

vista la direttiva del 29 dicembre 2023 del Ministro per la Pubblica Amministrazione;

vista la D.G.R. D.G.R. 3-2182/2026/XII del 30 gennaio 2026 della Regione Piemonte;

Attestato che, ai sensi della DGR n. 8-8111 del 25 gennaio 2024 ed in esito all'istruttoria sopra richiamata, il presente provvedimento non comporta oneri contabili diretti né effetti prospettici sulla gestione finanziaria, economica e patrimoniale della Regione Piemonte, in quanto le modifiche al Regolamento interno sull'utilizzo del lavoro agile per i dipendenti della Giunta regionale hanno carattere meramente normativo;

Attestata la regolarità amministrativa del presente provvedimento ai sensi della DGR n. 8-8111 del 25 gennaio 2024.

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

delibera

- di approvare le modifiche al Regolamento interno sull'utilizzo del lavoro agile per i dipendenti della Giunta regionale di cui alla D.G.R. n. 8 - 6951 del 29 maggio 2023 come meglio dettagliate in premessa e, conseguentemente, di approvare il nuovo testo del Regolamento interno, con i relativi allegati (sub. 1, 2, 3, 4 e 5, descritti in premessa), unitamente alla presente deliberazione per farne parte integrante e sostanziale, con decorrenza a far data dal 1° settembre 2026;

- di riservarsi di apportare al Regolamento interno sull'utilizzo del lavoro agile per i dipendenti della Giunta regionale i necessari adeguamenti in conformità a quanto previsto dalla contrattazione collettiva nazionale;

- 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 contabili diretti né effetti prospettici sulla gestione finanziaria, economica e patrimoniale della Regione Piemonte, come in premessa attestato.

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 co.1 del D.lgs. 33/2013.

Allegati

Sono parte integrante del presente provvedimento gli allegati riportati a seguire ¹, archiviati come file separati dal testo del provvedimento sopra riportato:

- | | | |
|----|--|---|
| 1. | DGR-2942-2026-All_1-REGOLAMENTO_INTERNO_LAVORO_AGILE.pdf |  |
| 2. | DGR-2942-2026-All_2-Allegato_1_Modello_di_richiesta_di_lavoro_agile.pdf |  |
| 3. | DGR-2942-2026-All_3-
Allegato_2_Schema_di_Accordo_individuale_lavoro_agile_(comparto).pdf |  |
| 4. | DGR-2942-2026-All_4-
Allegato_3_Schema_di_Accordo_individuale_di_lavoro_agile_(dirigenza).pdf |  |
| 5. | DGR-2942-2026-All_5-
Allegato_4__Informativa_sui_rischi_per_la_salute_e_sicurezza_in_modalità_lavoro_a_gile.pdf |  |
| 6. | DGR-2942-2026-All_6-
Allegato_5_Disciplinare_della_Region_Piemonte_per_l'utilizzo_dei_sistemi_informatici.pdf |  |

Allegato

1 L'impronta degli allegati rappresentata nel timbro digitale QRCode in elenco è quella dei file pre-esistenti alla firma digitale con cui è stato adottato il provvedimento

REGOLAMENTO INTERNO SULL'UTILIZZO DEL LAVORO AGILE PER I DIPENDENTI DELLA GIUNTA REGIONALE

Art. 1 Definizione

1. Ai fini del presente Regolamento interno (di seguito denominato Regolamento) si intende per "Lavoro agile" una modalità flessibile di esecuzione della prestazione lavorativa per processi e attività di lavoro, connotata anche dallo svolgimento di parte dell'attività lavorativa all'esterno della sede di lavoro, anche senza precisi vincoli di orari o di luogo, entro i soli limiti di durata del tempo di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione collettiva, e nel rispetto delle fasce di operatività di cui all'art. 7, comma 7, del presente Regolamento.

Art. 2 Finalità e principi generali

1. Il lavoro agile risponde alle seguenti finalità:

- introdurre nuove soluzioni organizzative che favoriscano lo sviluppo di un modello gestionale improntato alla flessibilità organizzativa per incrementare l'efficienza e l'efficacia dell'azione amministrativa;
- promuovere una visione dell'organizzazione del lavoro ispirata ai principi della flessibilità e dell'autonomia, responsabilizzando il personale e favorendo relazioni fondate sulla fiducia e sul lavoro di squadra;
- ottimizzare la diffusione di tecnologie e di competenze digitali, anche attraverso un'analisi dei processi ed una sempre maggiore digitalizzazione degli archivi e delle pratiche;
- facilitare le pari opportunità e le misure di conciliazione dei tempi di vita e di lavoro;
- promuovere la mobilità sostenibile tramite la riduzione degli spostamenti casa-lavoro-casa, nell'ottica di una politica ambientale sensibile alla diminuzione del traffico urbano in termini di volumi e di percorrenza;
- implementare misure strategiche di welfare aziendale finalizzate al benessere organizzativo del personale e all'age management.

2. Lo svolgimento della prestazione lavorativa in modalità agile viene regolamentata nel rispetto dei principi di cui alla Legge n. 81/2017, articoli da 18 a 23, e delle disposizioni del CCNL Funzioni Locali 2022-2024 del 23.02.2026 per il personale del Comparto e del 12.02.2026 per i Dirigenti; in particolare viene garantito il principio per il quale al lavoratore agile compete un trattamento economico e normativo non inferiore a quello complessivamente applicato nei confronti dei lavoratori che svolgono le medesime mansioni esclusivamente all'interno dell'amministrazione, nel rispetto dei contratti collettivi e integrativi vigenti.

3. E' garantito il diritto alla formazione, all'informazione, all'esercizio dei diritti sindacali e l'inclusione nei processi di misurazione e valutazione della performance, secondo il vigente sistema per la Performance dell'Ente e le disposizioni contrattuali collettive e integrative applicabili e, tenuto conto delle attività assegnate, nell'ambito della modalità agile di svolgimento della prestazione lavorativa, attraverso l'accordo individuale.

Art. 3 Destinatari

1. La prestazione lavorativa in modalità agile può essere resa da tutti i dipendenti a tempo indeterminato e determinato, anche in regime di tempo parziale. Per il personale dirigente, l'attività lavorativa in modalità agile è svolta secondo quanto previsto dall'art. 13, comma 3.

2. La valutazione della richiesta di autorizzazione allo svolgimento della prestazione lavorativa in modalità agile, così come la definizione dei contenuti dell'accordo individuale con il dipendente, compete al Dirigente Responsabile. L'autorizzazione per i titolari di posizione organizzativa è di competenza del Dirigente Responsabile sentito il Direttore della Direzione di appartenenza. Tutti gli accordi individuali sono sottoscritti dal Dirigente Responsabile.

3. La modalità di lavoro agile è esclusa per i dipendenti titolari di un contratto di lavoro da remoto.

4. La modalità di lavoro agile è esclusa di norma nel periodo di prova previsto contrattualmente. Il Dirigente Responsabile della struttura di appartenenza può autorizzare

lo svolgimento dell'attività in lavoro agile al dipendente in costanza del periodo di prova previsto contrattualmente, previa valutazione della capacità di organizzazione autonoma dell'attività lavorativa assegnata.

5. La modalità di lavoro agile è esclusa nelle giornate in cui i dipendenti svolgono attività che richiedono necessariamente la presenza. In particolare:

- attività che prevedono ricevimento in presenza di pubblico;
- attività svolte dal personale addetto alla portineria, alla custodia e allo svolgimento di mansioni di autista;
- attività a tempo pieno di gestione degli archivi non dematerializzati.

6. La modalità di lavoro agile viene invece valutata caso per caso per:

- attività complesse di segreteria;
- attività che prevedono istruttorie tecniche multisettoriali e/o con soggetti esterni all'Amministrazione Regionale;
- attività che precludano la funzionalità della struttura di appartenenza e la qualità del servizio offerto;
- attività che per ragioni organizzative, anche temporanee, è necessario siano svolte in presenza.

Art. 4

Criteri per l'applicazione e modalità di accesso

1. Il Dirigente Responsabile, prima di autorizzare lo svolgimento della prestazione lavorativa in modalità agile, deve valutare la sussistenza delle seguenti condizioni:

- la mancanza di lavoro arretrato accumulato ancora da smaltire e, qualora ce ne fosse, la preventiva predisposizione di un idoneo e documentabile piano di smaltimento;
- la garanzia dell'invarianza dei servizi resi all'utenza.

2. Il Dirigente Responsabile deve garantire un'adeguata rotazione del personale autorizzato al lavoro agile, garantendo il presidio dell'ufficio.

3. La domanda di autorizzazione al lavoro agile, redatta sull'apposito modulo allegato, deve essere indirizzata dal dipendente al Dirigente Responsabile della struttura di appartenenza e, per conoscenza, a lavoroagile@regione.piemonte.it.

4. La prestazione lavorativa svolta in modalità agile può essere resa per un numero massimo di 60 giornate su base annua per unità di personale con rapporto di lavoro a tempo pieno e a tempo parziale orizzontale. Nel caso di rapporto di lavoro a tempo parziale verticale il numero di giornate da svolgere in modalità agile è riproporzionato, in relazione non solo al numero di giorni in cui è articolata la prestazione lavorativa, ma anche del monte ore settimanale. In caso di mobilità fra Direzioni o fra Settori, il numero di giornate in lavoro agile, riferite al dipendente interessato, può essere rimodulato in relazione a quanto previsto dall'art. 3, commi 5 e 6.

5. La prestazione lavorativa in modalità agile può essere svolta fino ad un massimo di due giorni a settimana, nel rispetto del limite complessivo di 60 giorni annuali. Per specifiche esigenze (familiari o di organizzazione lavorativa) il numero massimo di giorni può essere elevato a 3 la settimana, sempre nel limite massimo di 60 giorni annuali.

6. L'Amministrazione si riserva di richiedere la presenza in sede del dipendente, in qualsiasi momento, per prevalenti esigenze di servizio, che di fatto impediscano di rendere la prestazione lavorativa in modalità agile, con un preavviso, di norma, di 24 ore e, comunque, con comunicazione che deve pervenire in tempo utile per la ripresa del servizio.

7. Il dipendente deve rendicontare i risultati conseguiti e le attività svolte, secondo modalità e criteri definiti dall'Ente e dal Dirigente Responsabile.

Il Dirigente responsabile esercita, altresì, funzioni di controllo sull'applicazione della presente disposizione, verificando, se necessario, il rispetto dei criteri stabiliti.

Art. 5 **Accordo individuale**

1. L'accordo individuale, redatto secondo apposito modello allegato al presente Regolamento, definisce i seguenti contenuti minimi, concordati dal Dirigente Responsabile e dal dipendente, sulla base delle esigenze organizzative, delle caratteristiche delle attività da svolgere e degli obiettivi:

- data di inizio e durata dell'accordo individuale (non superiore ai 24 mesi);
- descrizione delle attività da svolgere in modalità agile;
- modalità di svolgimento della prestazione lavorativa in modalità agile anche con riferimento alle attività delle schede "Piani di Lavoro" del dipendente e agli ulteriori obiettivi

- specifici che possono essere assegnati nel corso dell'anno;
- indicazione del giorno/dei giorni in cui la prestazione viene effettuata in modalità agile;
 - indicazione dei luoghi (massimo 2) in cui verrà svolta l'attività, tali da garantire la protezione dei dati trattati, ai sensi dell'art. 10 del presente Regolamento;
 - ipotesi di recesso, risoluzione e mancato rinnovo dell'accordo individuale;
 - ipotesi di giustificato motivo del recesso;
 - le fasce di operatività e i tempi di riposo del lavoratore;
 - le modalità di esercizio del potere direttivo e di controllo del datore di lavoro;
 - l'impegno del lavoratore a rispettare le prescrizioni indicate nell'informativa sui rischi per la salute e sicurezza in modalità lavoro agile ricevuta dall'amministrazione;
 - riferimento al Regolamento sul lavoro agile nella Regione Piemonte e agli altri allegati all'accordo individuale, che il dipendente con la sottoscrizione dichiara di accettare e di rispettare.

2. Il testo dell'accordo individuale, con i relativi allegati, sottoscritto dal dipendente e dal Dirigente Responsabile, viene trasmesso al Settore competente in materia di gestione giuridica del personale per opportuna conoscenza. In caso di lavoro agile svolto dai Dirigenti viene sottoscritto apposito accordo in forma semplificata; la fruizione delle giornate avviene con preventiva comunicazione al Direttore della struttura di appartenenza.

Art. 6

Luogo di lavoro

1. Fermo restando che la sede di lavoro resta invariata ad ogni effetto di legge e di contratto, il lavoro agile può essere svolto in luoghi diversi dalla propria abitazione purché i luoghi prescelti rispondano a requisiti di idoneità, nel rigoroso rispetto delle indicazioni fornite dall'Amministrazione in materia di protezione dei dati e di salute e sicurezza sul luogo di lavoro.

2. Nelle giornate di lavoro agile i/le dipendenti utilizzano spazi chiusi pubblici o privati; il dipendente avrà cura di svolgere la propria attività lavorativa in postazioni che garantiscano la necessaria riservatezza delle attività, evitando che soggetti esterni all'Amministrazione regionale possano facilmente venire a conoscenza di dati o notizie riservate.

3. E' necessario fornire un'indicazione dei luoghi dove è resa la prestazione lavorativa, al fine della corretta copertura INAIL in caso di infortuni sul lavoro. Eventuali infortuni sul lavoro devono essere immediatamente comunicati alle strutture di appartenenza per le necessarie denunce.

4. I luoghi di lavoro individuati dal lavoratore per lo svolgimento del lavoro agile devono consentire di rientrare in sede nelle ipotesi di cui all'art. 4, comma 6, e all'art. 7, comma 6. In ogni caso il lavoro agile non può essere svolto all'estero.

Art. 7 **Rilevazione lavoro agile - Articolazione oraria**

1. L'orario di svolgimento dell'attività in lavoro agile viene rilevato tramite l'utilizzo della procedura di rilevazione delle presenze - assenze utilizzando l'apposita funzione (cd. "bollatrice virtuale"), nel rispetto dell'orario minimo previsto dalla tipologia oraria di ciascun dipendente e dalle fasce di attività.

2. Per effetto della distribuzione flessibile del tempo di lavoro, nelle giornate di lavoro agile non sono riconosciute prestazioni di lavoro straordinario né eccedenza oraria e recupero di permessi, prestazioni di lavoro in turno notturno, festivo o feriale non lavorativo che determinino maggiorazioni retributive, missioni, lavoro disagiato, lavoro svolto in condizioni di rischio.

3. Per le giornate di attività in lavoro agile i buoni pasto sono erogati in ottemperanza agli specifici obblighi previsti dalle disposizioni normative e contrattuali vigenti.

4. Nelle giornate di lavoro agile il dipendente, oltre ai giustificativi a giornata ed alle ferie ad ore, può fruire nelle fasce di operatività, ove ne ricorrano i relativi presupposti, dei permessi orari previsti dai contratti collettivi o dalle norme di legge. Nel caso di trasferte e/o sopralluoghi, il dipendente può completare l'orario giornaliero in lavoro agile.

5. Il dipendente che nelle giornate di lavoro agile, per sopraggiunti ed imprevisti motivi personali, si trovi nella condizione di impossibilità assoluta a rendere la prestazione di lavoro deve darne tempestiva comunicazione al proprio dirigente e coprire l'assenza giornaliera con gli istituti previsti dal vigente CCNL.

6. Nel caso in cui il dipendente nelle giornate di lavoro agile non sia in grado di rendere la prestazione lavorativa per problemi di connessione o altri problemi legati al luogo di svolgimento del lavoro agile deve tempestivamente avvisare il proprio dirigente e rientrare in sede, completando la propria prestazione lavorativa fino al termine del proprio orario ordinario di lavoro.

7. Nelle giornate di lavoro agile per il dipendente valgono le seguenti regole:

a) fascia di attività: all'interno della fascia 7.30 – 20.30 il dipendente definisce autonomamente l'orario di lavoro giornaliero, tenuto conto degli obiettivi assegnati e dei carichi di lavoro, nel rispetto delle disposizioni del presente Regolamento. In tale fascia il dipendente deve, in particolare, rispondere a comunicazioni, partecipare a riunioni e collaborare con colleghi o utenti;

b) fascia di operatività: l'orario di lavoro di cui alla lettera precedente deve comprendere le fasce orarie comprese fra le ore 10.00 e le ore 12.00 e fra le ore 14.00 e le ore 15.30;

c) fascia di disconnessione: 20.30 – 7.30 (11 ore consecutive di riposo ai sensi dell'art. 7 del D.Lgs. n. 66/2003); in tale fascia il lavoratore non eroga alcuna prestazione lavorativa.

8. Il comportamento del dipendente in servizio che, contattato non risponde per più volte e non provvede a richiamare, può essere valutato ai fini disciplinari.

9. Qualora il dipendente svolga l'attività in lavoro agile per più di sei ore consecutive deve, analogamente a quanto richiesto per lo svolgimento dell'attività in presenza, effettuare le pause previste dalla normativa vigente.

Art. 8

Dotazioni tecnologiche per lavoro agile

1. I dipendenti devono disporre di idonea dotazione tecnologica per lo svolgimento della prestazione lavorativa in forma agile, costituita da personal computer e strumenti per il collegamento da remoto ai servizi applicativi.

2. La connessione dati è sempre a carico del dipendente, fermo restando che questa deve garantire capacità di banda adeguata all'utilizzo del servizio RDS (indicativamente 5Mbps bidirezionale); è preferibile l'uso di connessioni di tipo dati (linea fissa xDSL/Fibra o Router

Cellulare tipo "*saponetta*") e non ricorrere all'utilizzo della funzione di hot spot (o tethering) dello smartphone in quanto potenzialmente interrompibili dall'arrivo di chiamate vocali.

3. L'utilizzo di strumenti informatici personali è consentito nel rispetto delle disposizioni del disciplinare per l'utilizzo dei sistemi informatici, che si applicano anche al lavoro agile. I dispositivi utilizzati devono essere dotati di sistema operativo supportato e regolarmente aggiornato. La connessione al sistema informativo dell'Ente con dispositivi personali è consentita solo attraverso la piattaforma RDS che garantisce l'indipendenza tra le risorse remote della rete regionale e quelle locali del dispositivo utilizzato.

4. In caso di necessità di supporto tecnico o in presenza di problematiche di sicurezza informatica che impediscano o ritardino sensibilmente lo svolgimento dell'attività lavorativa, anche in ordine a rischi di perdita o divulgazione di informazioni dell'Amministrazione, il dipendente è tenuto a darne immediata informazione al proprio responsabile e all'assistenza informatica, inviando una mail a hd_region@csi.it. Qualora le suddette problematiche dovessero rendere impossibile la prestazione lavorativa, il dipendente può essere richiamato in sede.

Art. 9 Monitoraggio

1. La prestazione di lavoro agile deve garantire il mantenimento di un livello qualitativo e di risultati non inferiore a quello del lavoro in sede.
2. L'attività svolta in lavoro agile, analogamente a quanto previsto per l'attività lavorativa in sede, è oggetto di valutazione da parte del Dirigente Responsabile.
3. I Dirigenti Responsabili verificano l'attività prestata dal dipendente ed il raggiungimento dei risultati attesi, anche confrontandosi con il dipendente stesso.

Art. 10 Obblighi di custodia e riservatezza

1. Nell'esecuzione della prestazione lavorativa in modalità agile, il dipendente è tenuto a garantire la riservatezza dei dati e delle informazioni trattate, persistendo il divieto di farne uso e/o comunicazione al di fuori delle finalità per le quali è autorizzato al trattamento dei

dati.

2. Il dipendente è tenuto a partecipare alle specifiche iniziative di formazione organizzate dall'Amministrazione in materia di modalità operative del lavoro agile, aspetti di salute e sicurezza sui luoghi di lavoro e dei rischi connessi all'utilizzo dei dispositivi tecnologici, alle misure di sicurezza anche comportamentale sul corretto utilizzo e sulla tutela delle informazioni, dei beni o materiali della Regione Piemonte e alle previsioni normative in materia di privacy e tutela dei dati personali. In particolare, il dipendente è tenuto a segnalare tempestivamente ogni fatto che rilevi in tema di violazione della riservatezza dei dati trattati.

Art. 11 Sicurezza sul lavoro

1. La Regione Piemonte garantisce, ai sensi del decreto legislativo 9 aprile 2008, n. 81, la salute e la sicurezza del lavoratore in coerenza con l'esercizio dell'attività di lavoro in modalità agile e consegna al singolo dipendente un'informativa scritta con indicazione dei rischi generali e dei rischi specifici connessi alla particolare modalità di esecuzione della prestazione lavorativa. Il dipendente è tenuto a rispettare e ad applicare correttamente le direttive dell'Amministrazione e deve prendersi cura della propria salute e sicurezza, in linea con le disposizioni dell'art. 20 del D. Lgs. n. 81/08, comma 1.

2. La Regione Piemonte non risponde degli infortuni verificatisi a causa della mancata diligenza del lavoratore nella scelta di un luogo non compatibile con quanto indicato nell'Informativa.

Art. 12 Recesso e mancato rinnovo

1. Durante il periodo previsto per lo svolgimento del lavoro agile, ciascuna delle parti può, con adeguato preavviso, non inferiore a 30 giorni, recedere dall'accordo di lavoro agile, motivato se ad iniziativa dell'ente. Resta fermo quanto previsto dall'art. 19 – comma 2 – della Legge 81/2017 nel caso di lavoratori disabili ai sensi dell'articolo 1 della legge 12 marzo 1999, n. 68.

2. Costituisce giusta causa di recesso la modifica delle attività tale da rilevare ai sensi

dell'art. 3 del presente Regolamento.

3. Nel caso in cui, in occasione del monitoraggio sulle attività svolte in lavoro agile, emergano due situazioni di significativa criticità in relazione agli aspetti qualitativi e quantitativi dell'attività svolta in modalità agile, il Dirigente Responsabile lo comunica, per iscritto, al Direttore della Direzione di appartenenza che, congiuntamente al Dirigente stesso, convoca il lavoratore; in relazione all'andamento del colloquio il Dirigente Responsabile, può disporre il rientro alle ordinarie modalità di prestazione lavorativa in presenza, a far data dal primo giorno lavorativo utile successivo alla comunicazione stessa.

4. Qualora, in corso di vigenza dell'accordo, il dipendente cambi struttura di assegnazione l'accordo in essere perde automaticamente efficacia e occorre procedere, ove il dipendente lo richieda, ad una nuova valutazione della sussistenza delle condizioni legittimanti l'applicazione del lavoro agile; lo stesso vale nel caso di modifica del contratto di lavoro (trasformazione da part time a full time e viceversa, da part time orizzontale a part time verticale).

Art. 13

Ulteriori ipotesi di lavoro agile

1. Il limite di cui all'art. 4, comma 4, del presente Regolamento può essere aumentato nei seguenti casi:

- a) in presenza di specifiche prescrizioni del medico competente;
- b) in attesa di concessione del lavoro da remoto in caso di pratica già istruita con parere favorevole dal Settore competente in materia di gestione giuridica del personale, in presenza di figli fino al compimento di 16 anni, età dell'obbligo scolastico;
- c) su richiesta del Dirigente Responsabile del dipendente, previa autorizzazione del Direttore della Direzione di appartenenza.

2. Possono essere stipulati accordi di lavoro agile che prevedono come limite massimo annuale 75 giorni in uno dei casi seguenti:

- a) in presenza di figli fino al compimento di 16 anni;
- b) la considerevole durata del tragitto casa – lavoro che supera i 60 minuti di viaggio con i mezzi

pubblici/auto o i 30 km di distanza; ai fini del calcolo si tiene conto delle proiezioni effettuate dagli applicativi più diffusi;

c) per i dipendenti con età superiore ai 60 anni;

d) per coloro che non possiedono più i requisiti previsti per l'accesso al lavoro da remoto per un periodo massimo pari ad un anno dalla scadenza dell'accordo.

3. La prestazione lavorativa in modalità agile per il personale dirigente, secondo quanto previsto dall'art. 5, comma 2, è consentita per n. 12 giornate annue, salvo parere contrario del Direttore di appartenenza. L'attestazione della presenza in servizio avviene con l'inserimento di apposito codice nell'applicativo di gestione delle presenze/assenze indicante l'orario di inizio e fine dell'attività lavorativa.

E', inoltre, consentita, per ulteriori temporanee esigenze valutabili da parte del Direttore competente che ne definisce le modalità.

Art. 14 **Disposizioni finali**

1. Il mancato rispetto di quanto previsto nel presente Regolamento costituisce violazione dei doveri di comportamento ed è valutabile ai fini disciplinari.

2. Per tutto quanto non previsto nel presente Regolamento trovano applicazione i contratti collettivi applicati alla Regione Piemonte, i regolamenti e le disposizioni interne di servizio e le norme di legge in materia di lavoro agile.

3. In casi di interventi manutentivi straordinari o di situazioni impreviste che determinino la necessità di ridurre od escludere l'ordinario accesso ad una o più sedi regionali, il Direttore competente potrà disporre, per l'insieme dei dipendenti interessati, l'effettuazione dell'attività in lavoro agile senza specifica sottoscrizione dell'accordo individuale, senza che tali giornate siano computate nei limiti previsti dal presente Regolamento e nel rispetto, ove applicabili, delle altre disposizioni ivi previste.

Costituiscono allegati della presente disciplina i seguenti documenti:

1. Modello di richiesta di lavoro agile;
2. Schema di Accordo individuale di lavoro agile (comparto);
3. Schema di Accordo individuale di lavoro agile (dirigenza);
4. Informativa sui rischi per la salute e sicurezza in modalità lavoro agile ai sensi dell'art. 22 L. n. 81/2017 e D. Lgs. n. 81/2008 s.m.i.;
5. Disciplinare della Regione Piemonte per l'utilizzo dei sistemi informatici.

**Al Direttore/Dirigente Responsabile
del Settore**

e p.c. lavoroagile@regione.piemonte.it

Domanda di autorizzazione allo svolgimento della prestazione lavorativa in modalità agile

Il/la sottoscritto/a _____
in servizio presso _____

con rapporto di lavoro

- full-time
- part time verticale: _____
- part-time orizzontale: _____

CHIEDE

di poter accedere alla modalità di “lavoro agile” per lo svolgimento delle proprie attività

SI IMPEGNA

ad attenersi alle disposizioni impartite dall'Amministrazione per lo svolgimento del lavoro agile;

ad utilizzare le apparecchiature in conformità alle istruzioni e alle disposizioni ricevute;

a concordare preventivamente con il Dirigente Responsabile l'attività e la/le giornata/e della prestazione in modalità lavoro agile;

a svolgere l'attività in lavoro agile nel rispetto dei criteri di idoneità, sicurezza e riservatezza e in un luogo rispondente ai requisiti minimi stabiliti nell'informativa sui rischi per la salute e sicurezza in modalità lavoro agile ai sensi dell'art. 22 L. 81/2017 e del D. Lgs. 81/2008 s.m.i.;

ad adottare tutte le precauzioni necessarie a garantire la salvaguardia e lo svolgimento dell'attività in condizioni di sicurezza custodendo con massima cura tutte le informazioni;

a garantire la riservatezza dei dati e delle informazioni trattate, persistendo il divieto di farne uso e/o comunicazione al di fuori delle finalità per le quali è autorizzato al trattamento dei dati;

a svolgere la propria attività lavorativa in postazioni che garantiscano la necessaria riservatezza delle attività, evitando che soggetti esterni all'Amministrazione regionale possano facilmente venire a conoscenza di dati o notizie riservate.

Luogo e data,

Firma del Dipendente

ACCORDO INDIVIDUALE PER LA PRESTAZIONE DI LAVORO AGILE

Con il presente accordo individuale, tra la Regione Piemonte, in persona di (nome e cognome), Direttore/Dirigente del Settore _____ e la/il dipendente _____ matricola n. _____ categoria _____ in servizio _____ presso _____ la Direzione _____ Settore _____ con tipologia di contratto (t. ind/ t. det -full time/ part time) _____

Vista la delibera di Giunta di approvazione del Regolamento Interno sull'utilizzo del lavoro agile per i dipendenti della Giunta regionale

si conviene quanto segue:

La/il dipendente _____ è ammessa/ammesso a svolgere la prestazione lavorativa in modalità agile, fuori dalla sede abituale di lavoro, nei termini e alle condizioni di seguito indicate e in conformità alle prescrizioni stabilite nel Regolamento sopra richiamato.

Art. 1

Avvio – durata – recesso

La/il dipendente a decorrere dal _____ e fino al _____ svolgerà la propria prestazione di lavoro anche in modalità agile.

Ognuna delle parti potrà recedere dal presente accordo con un adeguato preavviso, non inferiore a 30 giorni, motivato se ad iniziativa dell'ente.

Nel caso di lavoratori disabili ai sensi dell'art. 1 della legge 12 marzo 1999 n. 68 il termine di preavviso del recesso da parte del datore di lavoro non può essere inferiore a novanta giorni.

In presenza di un giustificato motivo ognuna delle parti potrà recedere dal presente accordo senza preavviso a decorrere dal giorno successivo alla comunicazione alla controparte.

Qualora la/il dipendente cambi struttura di assegnazione o nel caso di modifica del contratto di lavoro (trasformazione da part time a full time e viceversa, da part time orizzontale a part time verticale), l'accordo in essere perde automaticamente efficacia.

Costituisce giusta causa di recesso la modifica delle attività tali da non poter essere svolte in modalità agile.

Art. 2

Svolgimento del rapporto di lavoro

La prestazione lavorativa in lavoro agile è svolta per n. 1/2 giorni per settimana, di norma il _____ (indicazione del/dei giorno/i), presso _____ (indirizzo prioritario), ed eventualmente presso _____ (altro indirizzo). Lo svolgimento di lavoro agile in sede diversa da quanto indicato nel presente accordo deve essere preventivamente comunicato al Dirigente.

Per specifiche esigenze (familiari o di organizzazione lavorativa) il numero massimo di giorni può essere elevato a 3 a settimana, sempre nel limite massimo di 60 giorni annuali; la richiesta e l'autorizzazione vengono comunicate tramite mail.

La programmazione delle giornate lavorative in modalità agile deve essere concordata preventivamente con il Dirigente, tenuto conto delle esigenze lavorative ed organizzative della struttura di appartenenza.

Il Dirigente può chiedere la presenza in sede della/del dipendente in qualsiasi momento, per prevalenti esigenze di servizio, che di fatto impediscano di rendere la prestazione lavorativa in modalità agile, con un preavviso di norma di 24 ore e, comunque, con comunicazione che deve pervenire in tempo utile per la ripresa del servizio.

Art. 3

Attività lavorative, modalità di esecuzione e monitoraggio

La/il dipendente svolge in lavoro agile le seguenti attività, coerenti con il Piano di lavoro annuale:

- 1) _____
- 2) _____
- 3) _____
- 4) _____

Art. 4

Orario di lavoro

L'orario di svolgimento dell'attività in lavoro agile viene rilevato tramite l'utilizzo della procedura di rilevazione delle presenze - assenze utilizzando l'apposita funzione - cd. "bollatrice virtuale" -, nel rispetto dell'orario minimo previsto dalla tipologia oraria di ciascun dipendente e dalle fasce di operatività.

Nelle giornate di lavoro agile valgono le seguenti regole:

- a) fascia di attività: all'interno della fascia 7.30 – 20.30 il dipendente definisce autonomamente l'orario di lavoro giornaliero, tenuto conto degli obiettivi assegnati e dei carichi di lavoro, nel rispetto delle disposizioni del Regolamento interno. In tale fascia il dipendente deve, in particolare, rispondere a comunicazioni, partecipare a riunioni e collaborare con colleghi o utenti;
- b) fascia di operatività: l'orario di lavoro di cui alla lettera precedente deve comprendere le fasce orarie comprese fra le ore 10.00 e le ore 12.00 e fra le ore 14.00 e le ore 15.30;
- c) fascia di disconnessione: 20.30 – 7.30 (11 ore consecutive di riposo ai sensi dell'art. 7 del D.Lgs 66/2003); in tale fascia il lavoratore non eroga alcuna prestazione lavorativa.

Qualora la/il dipendente svolga l'attività in lavoro agile per più di sei ore consecutive deve effettuare le pause previste dalla normativa vigente.

Il dipendente che nelle giornate di lavoro agile, per sopraggiunti ed imprevisti motivi personali, si trovi nella condizione di impossibilità assoluta a rendere la prestazione di lavoro deve darne tempestiva comunicazione al proprio dirigente e coprire l'assenza giornaliera con gli istituti previsti dal vigente CCNL.

Art. 5 **Strumenti di lavoro**

Al fine di rendere possibile lo svolgimento della prestazione lavorativa il/la dipendente deve disporre di idonea dotazione tecnologica, costituita da personal computer e strumenti per il collegamento da remoto ai servizi applicativi.

La connessione dati è sempre a carico della/del dipendente, fermo restando che questa deve garantire capacità di banda adeguata all'utilizzo del servizio RDS (indicativamente 5Mbps bidirezionale); è preferibile l'uso di connessioni di tipo dati (linea fissa xDSL/Fibra o Router Cellulare tipo "*saponetta*") e non ricorrere all'utilizzo della funzione di hot spot (o tethering) dello smartphone in quanto potenzialmente interrompibili dall'arrivo di chiamate vocali.

L'utilizzo di strumenti informatici personali è consentito nel rispetto delle disposizioni del disciplinare per l'utilizzo dei sistemi informatici, che si applicano anche al lavoro agile.

I dispositivi utilizzati devono essere dotati di sistema operativo supportato e regolarmente aggiornato.

La connessione al sistema informativo dell'Ente con dispositivi personali è consentita solo attraverso la piattaforma RDS che garantisce l'indipendenza tra le risorse remote della rete regionale e quelle locali del dispositivo utilizzato.

In caso di necessità di supporto tecnico o in presenza di problematiche di sicurezza informatica che impediscano o ritardino sensibilmente lo svolgimento dell'attività lavorativa, anche in ordine a rischi di perdita o divulgazione di informazioni dell'Amministrazione, il dipendente è tenuto a darne immediata informazione al proprio responsabile e all'assistenza informatica, inviando una mail a hd_regione@csi.it. Qualora le suddette problematiche dovessero rendere impossibile la prestazione lavorativa, il dipendente può essere richiamato in sede.

Il dipendente ha l'obbligo di utilizzare e custodire gli strumenti di lavoro affidatigli con la massima cura e diligenza e nel rispetto delle norme in materia di salute e sicurezza sul lavoro.

Art. 6

Luogo di lavoro e sicurezza

La/il dipendente garantisce che i luoghi prescelti rispondano a requisiti di idoneità, nel rigoroso rispetto delle indicazioni fornite dall'Amministrazione in materia di protezione dei dati e di salute e sicurezza sul luogo di lavoro.

Il lavoratore si impegna:

- ad osservare le misure di prevenzione, protezione e comportamentali, impartite dal Datore di Lavoro nel documento "*Informativa sui rischi per la salute e sicurezza in modalità lavoro agile*" ai sensi dell'art. 22 L. n. 81/2017 e del D. Lgs. n. 81/2008 s.m.i.;
- a prestare la dovuta attenzione per evitare che si producano situazioni pericolose o si verifichino infortuni;
- a non adottare condotte che possano generare rischi per la propria salute e sicurezza o per quella di terzi, sospendendo eventualmente la propria attività nel caso rilevi situazioni critiche.

Art. 7

Protezione e riservatezza dei dati

La/il dipendente è tenuto a rispettare le normative comunitarie e nazionali sulla riservatezza e protezione dei dati in suo possesso e/o disponibili sul sistema informatico dell'Amministrazione, secondo le procedure stabilite dalla stessa, della cui corretta e scrupolosa applicazione il lavoratore è responsabile.

A tal fine il lavoratore è tenuto:

- ad adottare tutte le precauzioni necessarie a garantire la salvaguardia e lo svolgimento delle attività in condizioni di sicurezza custodendo con massima cura tutte le informazioni;
- a garantire la riservatezza dei dati e delle informazioni trattate, persistendo il divieto di farne uso e/o comunicazione al di fuori delle finalità per le quali è autorizzato al trattamento dei dati;

- a svolgere la propria attività lavorativa in postazioni che garantiscano la necessaria riservatezza delle attività, evitando che soggetti esterni all'Amministrazione regionale possano facilmente venire a conoscenza di dati o notizie riservate;
- a partecipare alle specifiche iniziative di formazione organizzate dall'Amministrazione in materia di modalità operative del lavoro agile, aspetti di salute e sicurezza sui luoghi di lavoro e dei rischi connessi all'utilizzo dei dispositivi tecnologici, alle misure di sicurezza anche comportamentale sul corretto utilizzo e sulla tutela delle informazioni, dei beni o materiali della Regione Piemonte e alle previsioni normative in materia di privacy e tutela dei dati personali. In particolare, la/il dipendente è tenuto a segnalare tempestivamente ogni fatto che rilevi in tema di violazione della riservatezza dei dati trattati.

Art. 8

Inadempimenti del lavoratore e sanzioni disciplinari

La prestazione lavorativa in modalità agile non modifica il potere direttivo del Dirigente Responsabile, che viene esercitato con modalità analoghe a quelle applicate con riferimento alla prestazione resa presso i locali dell'Amministrazione

La/il dipendente è tenuto al rispetto del Codice disciplinare e del Codice di comportamento dei Dipendenti del ruolo della Giunta Regionale.

Per quanto non espressamente previsto nel presente accordo si rinvia al Regolamento per la disciplina del lavoro agile adottato dalla Giunta Regionale.

Allegati:

- Informativa sui rischi per la salute e sicurezza in modalità lavoro agile ai sensi dell'art. 22 L. n. 81/2017 e D. Lgs. n. 81/2008 s.m.i.;
- Disciplinare per l'utilizzo dei sistemi informatici allegato alla DGR n. 11-8790 del 17.06.2024.

Letto, confermato e sottoscritto

IL DIRIGENTE

IL DIPENDENTE

VISTO

IL DIRETTORE per le EQ _____



ACCORDO INDIVIDUALE PER LA PRESTAZIONE DI LAVORO AGILE (DIRIGENZA)

Con il presente accordo individuale, tra la Regione Piemonte, in persona di (nome e cognome), Direttore _____ e la/il Dirigente _____
_____matricola n. _____ Responsabile del Settore _____

Vista la delibera di Giunta di approvazione del Regolamento Interno sull'utilizzo del lavoro agile per i dipendenti e i dirigenti della Giunta regionale

si conviene quanto segue:

La/il Dirigente _____ svolgerà la prestazione lavorativa in modalità agile, fuori dalla sede abituale di lavoro, nei termini e alle condizioni di seguito indicate e in conformità alle prescrizioni stabilite nel Regolamento sopra richiamato.

Art. 1

Avvio – durata – recesso

La/il Dirigente svolgerà la propria prestazione di lavoro anche in modalità agile nei limiti di 12 giornate annue, secondo quanto previsto dall'art. 13, comma 3, del Regolamento citato presso (indirizzo prioritario) _____ o (indirizzo secondario) _____. Lo svolgimento di lavoro agile in sede diversa da quanto indicato nel presente accordo deve essere preventivamente comunicato al Direttore di appartenenza.

In presenza di un giustificato motivo ognuna delle parti potrà recedere dal presente accordo senza preavviso a decorrere dal giorno successivo alla comunicazione alla controparte.

Qualora la/il Dirigente cambi struttura di assegnazione l'accordo in essere perde automaticamente efficacia.

Art. 2

Svolgimento del rapporto di lavoro

La programmazione delle giornate lavorative in modalità agile deve essere concordata preventivamente con il Direttore di appartenenza, tenuto conto delle esigenze lavorative ed organizzative della Direzione.

Il Direttore può chiedere la presenza in sede della/del Dirigente in qualsiasi momento, per prevalenti esigenze di servizio, che di fatto impediscano di rendere la prestazione lavorativa in modalità agile, con un preavviso di norma di 24 ore e, comunque, con comunicazione che deve pervenire in tempo utile per la ripresa del servizio.

Art. 3

Orario di lavoro

L'orario di svolgimento dell'attività in lavoro agile viene rilevato tramite l'utilizzo dell'apposito codice inserito nell'applicativo di gestione delle presenze – assenze.

Il dipendente che nelle giornate di lavoro agile, per sopraggiunti ed imprevisti motivi personali, si trovi nella condizione di impossibilità assoluta a rendere la prestazione di lavoro deve darne tempestiva comunicazione al proprio Direttore e coprire l'assenza giornaliera con gli istituti previsti dal vigente CCNL.

Art. 4

Strumenti di lavoro

Al fine di rendere possibile lo svolgimento della prestazione lavorativa il/la Dirigente deve disporre di idonea dotazione tecnologica, costituita da personal computer e strumenti per il collegamento da remoto ai servizi applicativi.

La connessione dati è sempre a carico della/del Dirigente, fermo restando che questa deve garantire capacità di banda adeguata all'utilizzo del servizio RDS (indicativamente 5Mbps bidirezionale); è preferibile l'uso di connessioni di tipo dati (linea fissa xDSL/Fibra o Router Cellulare tipo "*saponetta*") e non ricorrere all'utilizzo della funzione di hot spot (o tethering) dello smartphone in quanto potenzialmente interrompibili dall'arrivo di chiamate vocali.

L'utilizzo di strumenti informatici personali è consentito nel rispetto delle disposizioni del disciplinare per l'utilizzo dei sistemi informatici, che si applicano anche al lavoro agile.

I dispositivi utilizzati devono essere dotati di sistema operativo supportato e regolarmente aggiornato.

La connessione al sistema informativo dell'Ente con dispositivi personali è consentita solo attraverso la piattaforma RDS che garantisce l'indipendenza tra le risorse remote della rete regionale e quelle locali del dispositivo utilizzato.

In caso di necessità di supporto tecnico o in presenza di problematiche di sicurezza informatica che impediscano o ritardino sensibilmente lo svolgimento dell'attività lavorativa, anche in ordine a rischi di perdita o divulgazione di informazioni dell'Amministrazione, il dipendente è tenuto a darne immediata informazione al proprio responsabile e all'assistenza informatica, inviando una mail a hd_region@csi.it. Qualora le suddette problematiche dovessero rendere impossibile la prestazione lavorativa, il dipendente può essere richiamato in sede.

Il Dirigente ha l'obbligo di utilizzare e custodire gli strumenti di lavoro affidatigli con la massima cura e diligenza e nel rispetto delle norme in materia di salute e sicurezza sul lavoro.

Art. 5

Luogo di lavoro e sicurezza

La/il Dirigente garantisce che i luoghi prescelti rispondano a requisiti di idoneità, nel rigoroso rispetto delle indicazioni fornite dall'Amministrazione in materia di protezione dei dati e di salute e sicurezza sul luogo di lavoro.

Il Dirigente si impegna:

- ad osservare le misure di prevenzione, protezione e comportamentali, impartite dal Datore di Lavoro nel documento *“Informativa sui rischi per la salute e sicurezza in modalità lavoro agile”* ai sensi dell'art. 22 L. n. 81/2017 e del D. Lgs. n. 81/2008 s.m.i.;
- a prestare la dovuta attenzione per evitare che si producano situazioni pericolose o si verifichino infortuni;
- a non adottare condotte che possano generare rischi per la propria salute e sicurezza o per quella di terzi, sospendendo eventualmente la propria attività nel caso rilevi situazioni critiche.

Art. 6

Protezione e riservatezza dei dati

La/il Dirigente è tenuto a rispettare le normative comunitarie e nazionali sulla riservatezza e protezione dei dati in suo possesso e/o disponibili sul sistema informatico dell'Amministrazione, secondo le procedure stabilite dalla stessa, della cui corretta e scrupolosa applicazione il lavoratore è responsabile.

A tal fine il Dirigente è tenuto:

- ad adottare tutte le precauzioni necessarie a garantire la salvaguardia e lo svolgimento delle attività in condizioni di sicurezza custodendo con massima cura tutte le informazioni;
- a garantire la riservatezza dei dati e delle informazioni trattate, persistendo il divieto di farne uso e/o comunicazione al di fuori delle finalità per le quali è autorizzato al trattamento dei dati;
- a svolgere la propria attività lavorativa in postazioni che garantiscano la necessaria riservatezza delle attività, evitando che soggetti esterni all'Amministrazione regionale possano facilmente venire a conoscenza di dati o notizie riservate;
- a partecipare alle specifiche iniziative di formazione organizzate dall'Amministrazione in materia di modalità operative del lavoro agile, aspetti di salute e sicurezza sui luoghi di lavoro e dei rischi connessi all'utilizzo dei dispositivi tecnologici, alle misure di sicurezza anche comportamentale sul corretto utilizzo e sulla tutela delle informazioni, dei beni o materiali della Regione Piemonte e alle previsioni normative in materia di privacy e tutela dei dati personali. In particolare, il dipendente è tenuto a segnalare tempestivamente ogni fatto che rilevi in tema di violazione della riservatezza dei dati trattati.

Art. 7

Inadempimenti del Dirigente e sanzioni disciplinari

La prestazione lavorativa in modalità agile non modifica il potere direttivo del Direttore della Direzione di appartenenza, che viene esercitato con modalità analoghe a quelle applicate con riferimento alla prestazione resa presso i locali dell'Amministrazione.

La/il Dirigente è tenuto al rispetto del Codice disciplinare e del Codice di comportamento dei Dipendenti del ruolo della Giunta Regionale.

Per quanto non espressamente previsto nel presente accordo si rinvia al Regolamento per la disciplina del lavoro agile adottato dalla Giunta Regionale.

Allegati:

- Informativa sui rischi per la salute e sicurezza in modalità lavoro agile ai sensi dell'art. 22 L. n. 81/2017 e D. Lgs. n. 81/2008 s.m.i.;
- Disciplinare per l'utilizzo dei sistemi informatici allegato alla DGR n. 11-8790 del 17.06.2024.

Letto, confermato e sottoscritto

IL DIRETTORE

IL DIRIGENTE

INFORMATIVA SUI RISCHI PER LA SALUTE E SICUREZZA IN MODALITÀ LAVORO AGILE

art. 22 Legge n.81/2017 e D.lgs. 81/08 s.m.i.

Il presente documento vuole dare un'informativa per coloro che svolgeranno la propria attività lavorativa in modalità *lavoro agile (smart working)*.

L'informativa è predisposta e aggiornata a cadenza almeno annuale ai sensi dell'art. 22 della Legge n. 81/2017; è consegnata in copia anche ai RLS (Rappresentanti dei Lavoratori per la Sicurezza), poiché questa figura ha un ruolo specifico nel sistema di prevenzione per l'attuazione degli adempimenti previsti in materia di salute e sicurezza di tutela e rappresentanza dei lavoratori.

Anche il lavoratore che opera in modalità di lavoro agile si deve intendere come parte attiva della prevenzione e protezione della sua salute e sicurezza; è suo compito mettere in atto ogni comportamento utile a limitare i rischi derivanti dell'esecuzione della prestazione lavorativa al di fuori dei locali dell'Amministrazione, dove viene meno la possibilità da parte del Datore di Lavoro di verifica puntuale del rispetto dei principi ergonomici e tecnici di salute e sicurezza del lavoro.

Rev. Numero	Data emissione	Emessa da	Approvata da
00	DICEMBRE 2023	Servizio Prevenzione Protezione	Datore di lavoro
01	FEBBRAIO 2025	Servizio Prevenzione Protezione	Datore di lavoro

INDICE

INDICE.....	2
1. OBIETTIVO DELL'INFORMATIVA	3
2. AMBITO DI APPLICAZIONE	3
3. MISURE GENERALI PER IL LOCALE DESTINATO AL LAVORO AGILE	3
4. RISCHI SPECIFICI PER I LAVORATORI IN LAVORO AGILE	4
5. MISURE PREVENTIVE E PROTEZIONI DA ADOTTARE	4
6. RESPONSABILITÀ DEL LAVORATORE IN LAVORO AGILE	6

1. OBIETTIVO DELL'INFORMATIVA

L'obiettivo di questa informativa è di sensibilizzare i lavoratori sui rischi legati al lavoro agile e sulle precauzioni da adottare per prevenire infortuni e problemi di salute.

2. AMBITO DI APPLICAZIONE

Questa informativa si applica a tutti i lavoratori che svolgono attività lavorative a distanza, tramite l'uso di strumenti informatici (PC fisso, laptop, ecc.), in modalità di lavoro agile.

3. MISURE GENERALI PER IL LOCALE DESTINATO AL LAVORO AGILE

Le attività lavorative non possono essere svolte in locali tecnici o locali non abitabili (ad es. soffitte, seminterrati, rustici, box); mentre risulta necessaria un'adeguata disponibilità di servizi igienici, acqua potabile e presenza di impianti a norma (elettrico, termoidraulico, ecc.) adeguatamente mantenuti.

ILLUMINAZIONE

- Il locale deve prevedere adeguata illuminazione **naturale diretta** con idonea superficie finestrata che possa essere schermata allo scopo di evitare fenomeni di abbagliamento o riflessi (tendaggi).
- Il locale deve prevedere adeguata **illuminazione artificiale** (generale e localizzata) per evitare abbagliamenti diretti, riflessi e/o proiezioni di ombre.

AERAZIONE

- Il locale deve prevedere **adeguate condizioni microclimatiche** (temperatura, umidità e velocità dell'aria); inoltre, è opportuno garantire il **ricambio dell'aria** naturale o con ventilazione meccanica.
- Se presenti **impianti** di condizionamento, gli stessi devono essere a norma e regolarmente **manutenuti**.

IMPIANTO ELETTRICO

- L'impianto elettrico deve essere privo di parti visibili **danneggiate e/o fissate male**.
- Le parti attive dell'impianto (es. conduttori di fase o di neutro) non devono essere accessibili direttamente (ad esempio perché danneggiato l'isolamento).
- I componenti dell'impianto ed i luoghi che li ospitano devono essere **asciutti, puliti** e non produrre scintille, odori di bruciato e/o fumo.
- **Non devono essere accumulati, depositati o accostati materiali infiammabili** a ridosso dei componenti dell'impianto per evitare un possibile innesco di incendi.
- I cavi di alimentazione e le eventuali prolunghe di collegamento devono essere collocati in modo da **minimizzare il pericolo di inciampo**.

4. RISCHI SPECIFICI PER I LAVORATORI IN MODALITÀ LAVORO AGILE

Il lavoro agile non è esente da rischi.

I principali rischi per la salute e la sicurezza derivano da fattori legati all'ambiente domestico di lavoro, all'uso improprio di attrezzature, e a problematiche legate alla postura.

Ecco i principali rischi da considerare.

- **Rischi ergonomici:** una cattiva postura dovuta a una sedia scomoda o a una scrivania non regolata può causare, nel tempo, dolori muscolari e disturbi al sistema muscoloscheletrico, come dolori alla schiena, al collo, ai polsi e alle spalle.
- **Affaticamento visivo:** l'uso prolungato di schermi di computer senza pause adeguate può provocare astenopia (affaticamento degli occhi), visione offuscata e mal di testa.
- **Rischi legati all'uso di dispositivi tecnologici:** l'uso improprio di computer, smartphone e altri dispositivi elettronici può comportare lesioni da sovraccarico (come la sindrome del tunnel carpale o altre problematiche alle mani e alle braccia) se non utilizzati correttamente.
- **Rischi da incidenti domestici:** l'ambiente domestico non sempre è progettato per l'attività lavorativa e può comportare pericoli fisici come scivolamenti, incidenti domestici (es. cavi non protetti).
- **Rischi comportamentali.**

5. MISURE PREVENTIVE E PROTEZIONI DA ADOTTARE

Per ridurre al minimo i rischi associati al lavoro agile, l'Ente raccomanda di seguire le seguenti misure preventive.

POSTAZIONE DI LAVORO ERGONOMICA

Utilizzare una scrivania di altezza adeguata e una sedia ergonomica, che permetta una postura corretta, con schienale che supporti la schiena e piedi ben appoggiati a terra.

IL PIANO DI LAVORO DEVE ESSERE

- stabile e avere una superficie a basso indice di riflessione;
- di altezza sufficiente per permettere l'alloggiamento e il movimento degli arti inferiori per cambiamenti di posizione, nonché l'ingresso dei braccioli se presenti;
- lo spazio sul piano di lavoro deve consentire un appoggio degli avambracci davanti alla tastiera nel corso della digitazione;
- il mouse o qualsiasi dispositivo di puntamento in dotazione alla postazione di lavoro deve essere posto sullo stesso piano della tastiera, in posizione facilmente raggiungibile e deve disporre di uno spazio adeguato al suo uso, di dimensioni sufficienti a permettere una disposizione flessibile dello schermo, della tastiera, dei documenti e del materiale accessorio;
- di altezza tale da consentire all'operatore in posizione seduta di avere l'angolo braccio-avambraccio a circa 90°;
- di profondità tale da assicurare una adeguata distanza visiva dallo schermo.

LA SEDIA DI LAVORO DEVE

- essere stabile e permettere all'utilizzatore libertà nei movimenti, e una posizione comoda;
- fornire un adeguato supporto alla regione dorso-lombare dell'utilizzatore, adeguato alle sue caratteristiche, con altezza e inclinazione della seduta e dello schienale regolabili in maniera indipendente per assicurare anche un buon appoggio dei piedi;
- essere salda contro slittamento e rovesciamento, dotato di basamento a 5 punti di appoggio (razze).

LA TASTIERA DEVE

- essere indipendente e separata nei PC fissi, è facilmente regolabile, dotata di meccanismo di variazione della pendenza per consentire al lavoratore di assumere una posizione confortevole e tale da non provocare l'affaticamento delle braccia e delle mani;
- avere una superficie opaca per evitare riflessi. I simboli dei tasti devono presentare un sufficiente contrasto e devono essere leggibili dalla normale posizione di lavoro.

IL MOUSE O QUALSIASI DISPOSITIVO DI PUNTAMENTO DEVE ESSERE

- indipendente e separato in modo che sia possibile regolare la posizione.

LO SCHERMO DEVE ESSERE TALE CHE

- la risoluzione garantisca una buona definizione, una forma chiara, una grandezza sufficiente dei caratteri e, inoltre, uno spazio adeguato tra essi;
- l'immagine sia stabile, esente da farfallamento, tremolio o da altre forme di instabilità;
- la brillantezza e/o il contrasto di luminanza tra i caratteri e lo sfondo dello schermo siano facilmente regolabili e adattabili alle condizioni ambientali;
- sia orientabile ed inclinabile liberamente per adeguarsi facilmente alle esigenze dell'utilizzatore.

NEL CASO DI UTILIZZO DEL COMPUTER PORTATILE

- **Utilizzare una tastiera e un mouse o altro dispositivo di puntamento esterni nonché di un idoneo supporto che consenta il corretto posizionamento dello schermo.**
- Sistemare lo schermo su idoneo supporto che consenta il corretto posizionamento in altezza (spigolo superiore dello schermo deve trovarsi poco più in basso dell'orizzontale che passa per gli occhi dell'operatore e ad una distanza degli occhi pari a circa 50-70 cm).

NORME COMPORTAMENTALI

- distogliere periodicamente lo sguardo dal video e fissare oggetti lontani, al fine di ridurre l'affaticamento visivo;
- si raccomanda di effettuare **pause con cambio di attività per almeno 15 minuti ogni 2 ore** di utilizzo continuativo del videoterminale;
- durante le pause ed i cambiamenti di attività previsti, è opportuno dedicarsi ad attività che NON richiedano un intenso impegno visivo;
- **assumere una postura corretta di fronte al monitor con i piedi ben poggiati al pavimento e la schiena poggiata allo schienale della sedia nel tratto lombare, regolando allo scopo l'altezza della sedia e l'inclinazione dello schienale;**
- evitare di tenere lo schienale inclinato in avanti o lavorare con il tronco flesso e preferire inclinazione dello schienale verticale o leggermente all'indietro;

- evitare irrigidimenti delle dita e del polso durante la digitazione e l'utilizzo del mouse e, per quanto possibile, posizioni di lavoro fisse per tempi prolungati;
- evitare di esporsi a correnti d'aria fastidiose che colpiscano una zona circoscritta del corpo (ad es. la nuca, le gambe);
- curare la pulizia della tastiera e della superficie del video;
- ogni qualvolta sia necessario, collocare davanti a sé oggetti che richiedono una maggiore attenzione visiva, evitando frequenti spostamenti laterali di occhi e testa;
- in base alla statura, se necessario per mantenere un angolo di 90° tra gamba e coscia, utilizzare un poggiapiedi con un oggetto di dimensioni opportune.

ATTREZZATURE DI LAVORO

- le apparecchiature elettriche ed elettroniche, i dispositivi di connessione elettrica temporanea utilizzati, devono essere **marcate CE** (con etichetta che riporti il nome del costruttore e l'indicazione della tensione (Volt), corrente (Ampere) o la potenza massima (KW) assorbita);
- le apparecchiature elettriche ed elettroniche, i dispositivi di connessione elettrica temporanea utilizzati devono essere **integre**, prive di parti attive accessibili (es. conduttori di fase o di neutro dei cavi di alimentazione), che non emettano scintille, fumo e/o odore di bruciato;
- le apparecchiature elettriche ed elettroniche, i dispositivi di connessione elettrica temporanea utilizzati devono essere collocate in modo da poter **smaltire il calore prodotto** (non coprire le ventole e le aperture libere) e in ogni caso da non utilizzare quando tale produzione conduca a eccessivo riscaldamento;
- le spine dei dispositivi di connessione elettrica temporanea devono essere inserite in **prese compatibili** e completamente in esse, in modo da garantire anche in questo caso un contatto certo.

6. RESPONSABILITÀ DEL LAVORATORE IN LAVORO AGILE

Il lavoratore in modalità lavoro agile ha la responsabilità di:

- individuare per l'esecuzione del lavoro agile, luoghi che non prevedano un'esposizione a rischi diversi e ulteriori a quelli previsti durante la sua prestazione nel luogo di lavoro abituale.
- **evitare comportamenti che possano generare rischi per la sua salute e sicurezza o per quella di terzi e evitare ogni luogo, ambiente, situazione e circostanza che possa comportare un pericolo per la sua salute e la sua sicurezza o per quella di terzi.**
- adottare comportamenti sicuri, come evitare posture scorrette, fare pause frequenti e prendersi cura del proprio benessere psicologico.
- seguire le indicazioni contenute in questa informativa e a segnalare tempestivamente eventuali problematiche o difficoltà, al fine di garantire il proprio benessere e la sicurezza sul posto di lavoro.
- fornire dettagliata e tempestiva comunicazione all'Amministrazione in caso di infortunio, secondo le modalità individuate nel contratto.

Deliberazione della Giunta Regionale 17 giugno 2024, n. 11-8790

Modifiche al nuovo disciplinare per l'uso degli strumenti informatici adottato con D.G.R. n. 2-5456 del 03.08.2022.



Seduta N° 462

Adunanza 17 GIUGNO 2024

Il giorno 17 del mese di giugno duemilaventiquattro alle ore 16:00 in via straordinaria, in modalità telematica, ai sensi della D.G.R. n. 1-4817 del 31 marzo 2022 si è riunita la Giunta Regionale con l'intervento di Alberto Cirio Presidente, Fabio Carosso Vice Presidente e degli Assessori Elena Chiorino, Marco Gabusi, Luigi Genesio Icardi, Matteo Marnati, Vittoria Poggio, Marco Protopapa, Andrea Tronzano con l'assistenza di Guido Odicino nelle funzioni di Segretario Verbalizzante.

Assenti, per giustificati motivi: gli Assessori

Chiara CAUCINO - Maurizio Raffaello MARRONE - Fabrizio RICCA

DGR 11-8790/2024/XI

OGGETTO:

Modifiche al nuovo disciplinare per l'uso degli strumenti informatici adottato con D.G.R. n. 2-5456 del 03.08.2022.

A relazione di: Cirio

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 generale sulla protezione dei dati (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";

L'art. 5 del citato 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.

Dato atto che:

all’esito dell’attività istruttoria e preparatoria svolta dal gruppo di lavoro interdirezionale – denominato “GDPR”, istituito con D.D. 3 aprile 2019, n. 74 della Direzione regionale “Segretariato Generale”, è stata approvata la D.G.R. n. 2-5456 del 03.08.2022 avente ad oggetto “Nuovo disciplinare per l’uso degli strumenti informatici. Revoca della D.G.R. n. 2-12269 del 05-10.2009”;

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;

con D.D. 9 maggio 2023, n. 247 del Settore “Organizzazione” della Direzione della Giunta regionale il gruppo di lavoro sopra richiamato è stato integrato prevedendo il coinvolgimento della Direzione della Giunta regionale, della Direzione Competitività del Sistema regionale e del Settore regionale Trasparenza e Anticorruzione, affinché prosegua la sua attività quale presidio per le strutture dell’Ente per quel che concerne gli adempimenti continuativi, lo studio e l’approfondimento degli aspetti normativi, organizzativi e procedurali connessi con gli aspetti applicativi del Regolamento generale sulla protezione dei dati;

il gruppo di lavoro, nell’ambito della sua attività di studio e approfondimento, ha rilevato la necessità di procedere ad un parziale aggiornamento del suddetto disciplinare per l’uso degli strumenti informatici, allo scopo di renderlo maggiormente coerente con il principio di responsabilizzazione (accountability) previsto dal Regolamento (UE) 2016/679 che impone al titolare del trattamento di adottare misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al Regolamento UE (art. 24 Regolamento UE);

tale aggiornamento riguarda, più nel dettaglio, la disciplina dei tempi di conservazione dei file di *log* di sistema (paragrafi 15.4 e 18.1 del disciplinare), ossia dei file generati da un software che contengono informazioni dettagliate sulle operazioni, attività e modelli di utilizzo di un sistema. Al paragrafo 15.4, in particolare, viene introdotta una tabella che dettaglia i tempi di conservazione per ogni sistema oggetto di tracciatura in coerenza con il principio di responsabilizzazione previsto dal Regolamento (UE) 2016/679, mentre al paragrafo 18.1, per esigenze di coordinamento, si introduce un richiamo espresso a tale tabella;

tale aggiornamento, di cui all’allegato alla presente deliberazione, modifica e sostituisce il testo del disciplinare per l’uso degli strumenti informatici adottato con D.G.R. n. 2-5456 del 3 agosto 2022 e verrà reso noto a tutti i dipendenti con le forme più efficaci ed immediate attraverso la diffusione sulla intranet aziendale ed ogni altro mezzo idoneo.

Dato atto che il disciplinare come modificato è stato oggetto di valutazione in sede di comitato dei direttori il 11.06.2024 ai sensi dell’art 9 della l.r. 23/2028 e s.m.i.

Dato atto che il disciplinare, così come modificato, è stato oggetto di informativa alle Organizzazioni Sindacali e alla RSU Categorie.

Ritenuto pertanto, alla luce di quanto sopra illustrato, di modificare e sostituire il disciplinare di cui alla dgr. n. 2-5456 del 3 agosto 2022, come da allegato alla presente deliberazione parte integrante e sostanziale.

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 “Codice in materia di protezione dei dati personali” ;

visto il D.lgs. 82/2005 “Codice dell’amministrazione digitale”;

viste le “Linee guida del Garante per posta elettronica e internet” in Gazzetta Ufficiale n. 58 del 10 marzo 2007;

vista la legge regionale n. 23 del 28 luglio 2008 “Disciplina dell’organizzazione degli uffici regionali e disposizioni concernenti la dirigenza ed il personale”;

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

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”;

vista la deliberazione di Giunta regionale n. 2-5456 del 3 agosto 2022 “Nuovo disciplinare per l’uso degli strumenti informatici. Revoca della D.G.R. n. 2-12269 del 05.10.2009”.

Attestato che, ai sensi della DGR n. 8-8111 del 25 gennaio 2024 ed in esito all’istruttoria sopra richiamata, il presente provvedimento non comporta oneri contabili diretti né effetti prospettici sulla gestione finanziaria, economica e patrimoniale della Regione Piemonte, in quanto la modifica al disciplinare per l’uso degli strumenti informatici, non aumentando i tempi di conservazione dei file di log di sistema sopra descritti, non implica l’esigenza di servizi aggiuntivi rispetto a quelli già in uso.

Attestata la regolarità amministrativa del presente provvedimento ai sensi della DGR n. 8-8111 del 25 gennaio 2024.

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

delibera

- di approvare le modifiche al disciplinare per l’uso degli strumenti informatici di cui alla DGR n. 2-5456 del 3 agosto 2022 come meglio dettagliate in premessa e, conseguentemente, approvare il nuovo testo del disciplinare, allegato alla presente deliberazione per farne parte integrante e sostanziale, che sostituisce l’allegato alla citata deliberazione;
- di dare atto che il presente provvedimento non comporta oneri contabili diretti né effetti

prospettici sulla gestione finanziaria, economica e patrimoniale della Regione Piemonte, come in premessa attestato.

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 co.1 del D.lgs. 33/2013.

Allegato

Sono parte integrante del presente provvedimento gli allegati riportati a seguire ¹, archiviati come file separati dal testo del provvedimento sopra riportato:

DGR-8790-2024-All_1-Disciplinare_strumenti_informatici_serv_infr_tecn_-
_Allegato_a_DGR.docx

1.



Allegato

¹ L'impronta degli allegati rappresentata nel timbro digitale QRCode in elenco è quella dei file pre-esistenti alla firma digitale con cui è stato adottato il provvedimento



**DISCIPLINARE PER L'UTILIZZO
DEI SISTEMI INFORMATICI**

Sommario

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 Pubblicazione e messa a disposizione.

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 (BYOD¹) 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:

1 Bring Your Own Device

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

1.1 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 suddetti 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'adeguata 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 Regionale²](#).

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

1.1 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.

3.1 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).

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

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 *regpiem01* e relativa password;
 - per i dipendenti dell'Ente la username coincide con la matricola;
 - per le altre persone abilitate ad accedere al dominio (collaboratori/organismi 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 Le credenziali di autenticazione relative ai diversi ambiti, consistono in:), 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 Infrastruttura di rete e File System – 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 Help Desk).

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, *regpiem01*, 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 Le credenziali di autenticazione relative ai diversi ambiti, consistono in:

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 accessibile esclusivamente dall'utente³;
- 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 privacy⁴, tra utenti di strutture diverse; i contenuti di questa cartella vengono automaticamente cancellati tutte le notti;

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)

- eventuali altre cartelle condivise, rese disponibili secondo specifica abilitazione (cfr. 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.).

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. L'accesso al dominio garantisce all'utente la disponibilità dei dispositivi multifunzione di stampa e delle seguenti share di rete (cartelle condivise su server): 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 NAS⁵ 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.

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/dai dispositivi esterni (hard disk, chiavette usb, cd, dvd e altri supporti) nei

5 Network Attached Storage

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 Desk⁶

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_region@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.

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).

10 Regole applicabili all'utilizzo di internet mediante gli strumenti informatici dell'Ente⁷

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 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 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.. 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).

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..

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 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..

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 crittazione con apposito software (archiviazione e compressione con password). La password di crittazione 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 crittati. 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 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.); 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 E' consentito trasferire documenti elettronici dai sistemi informativi e strumenti dell'ente a/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. 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" abilita 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/profilo 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 e Utilizzo della posta elettronica istituzionale).

13.3 La stampa di documenti avviene, di norma, su dispositivi multifunzione disponibili all’interno delle sedi regionali e condivise mediante il dominio *regpiem01*.

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

15.4 I sistemi oggetto di tracciatura e i relativi tempi di conservazione sono riportati nella tabella seguente:

Sistema oggetto di tracciatura	Tempo di conservazione dei log
Apparati VPN	180 giorni
CLI (Nivola)	180 giorni
Service Portal (Nivola)	180 giorni
Database (MySQL, Oracle, SqlServer, PostGreSQL)	180 giorni
Firewall	180 giorni
Server (LDAP, Unix, Windows)	180 giorni
Web Application Firewall	60 giorni
Content filter	7 giorni
Server DNS	180 giorni
Server proxy (navigazione internet utenti)	7 giorni
Server Proxy (applicativi)	180 giorni
Posta Elettronica (metadati)	7 giorni
Autenticazione SPID, CIE, CNS	24 mesi
Autenticazione con credenziali e con certificato di autenticazione	180 giorni
Servizio EDR (Apex One)[1]	90 giorni
Servizio EDR (Vision One)[2]	30 giorni

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 [...]», 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 modificazione di procedimenti tecnici destinati a controllare i

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

movimenti⁹ 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 LOG di sistema 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 LOG di sistema 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 procedurali 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), sono conservate secondo quanto indicato nella tabella di cui al paragrafo 15.4.

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.