CONSIGLIO REGIONALE DEL PIEMONTE - Deliberazione dell'Ufficio di Presidenza
Delibera n. 101/2021 - Cl. 6.6.2 del 17 giugno 2021
Oggetto: SOSTITUZIONE DELL'ALLEGATO 1 ALLA DELIBERAZIONE DELL'UFFICIO DI PRESIDENZA N. 273/2018 "ADEMPIMENTI IN ATTUAZIONE DEL REGOLAMENTO UE 2016/679 E DEL DECRETO LEGISLATIVO 196/2003. APPROVAZIONE DELLE ISTRUZIONI OPERATIVE, DELLE DISPOSIZIONI PROCEDURALI IN MATERIA DI INCIDENTI DI SICUREZZA E DI VIOLAZIONE DI DATI PERSONALI (DATA BREACH) E DELLE MISURE ADEGUATE DI SICUREZZA". (CG)

(omissis)

Vista la deliberazione dell'Ufficio di Presidenza n. 273/2018 "Adempimenti in attuazione del Regolamento UE 2016/679 e del Decreto Legislativo 196/2003. Approvazione delle istruzioni operative, delle disposizioni procedurali in materia di incidenti di sicurezza e di violazione di dati personali (Data Breach) e delle misure adeguate di sicurezza.";

Ritenuto necessario aggiornare l'**allegato 1** "Istruzioni operative ai sensi dell'articolo 32 del GDPR per l'utilizzo dei dispositivi informatici, dei servizi digitali e della gestione documentale nell'attività lavorativa. Disciplinare interno." parte integrante e sostanziale della deliberazione dell'Ufficio di Presidenza n. 273/2018 per adeguarlo all'introduzione di nuovi servizi informatici di supporto alle attività dell'Assemblea regionale e delle direzioni del Consiglio (sistemi di videoconferenza e remotizzazione delle postazioni di lavoro);

L'Ufficio di Presidenza, all'***unanimità dei presenti***,

D E L I B E R A

di adottare nuove dettagliate istruzioni operative contenute nell'**allegato 1** alla presente deliberazione, di cui costituiscono parte integrante e sostanziale, in completa sostituzione dell'allegato 1 della deliberazione dell'Ufficio di Presidenza n. 273/2018 e di dare mandato agli uffici di pubblicarle nella Intranet del sito istituzionale del Consiglio nonché di predisporre e notificare apposito ordine di servizio al personale.

CONSIGLIO REGIONALE DEL PIEMONTE

Sommario

Istruzioni operative ai sensi dell'articolo 32 del GDPR per l'utilizzo dei dispositivi informatici, dei servizi digitali e della gestione documentale nell'attività lavorativa. Disciplinare interno.

Giugno 2021

Adozione del disciplinare e sua efficacia

Il Disciplinare è stato redatto da apposito gruppo di lavoro inter direzionale e approvato con Deliberazione dell'UdP n. 273 del 28/12/2018 nella sua prima versione.

A giugno 2021 si rende necessario un aggiornamento, approvato con Deliberazione dell'UdP n. Xx, a seguito dell'introduzione di nuovi servizi informatici di supporto alle attività dell'Assemblea regionale e delle direzioni del Consiglio (sistemi di videoconferenza e remotizzazione delle postazioni di lavoro).

I dipendenti del Consiglio regionale del Piemonte saranno informati tramite apposita circolare e il Disciplinare sarà reso disponibile anche sulla intranet.

Il Disciplinare potrà essere aggiornato ogni qualvolta se ne presenti l'opportunità e di tali revisioni sarà data tempestiva comunicazione ai dipendenti.

Le disposizioni contenute nel Disciplinare si applicano a tutto il personale del Consiglio regionale del Piemonte, nonché a tutti i soggetti che utilizzano strumenti informatici e servizi digitali o documentali del Consiglio (in particolare, garanti, Corecom, gruppi consiliari, uffici di comunicazione, borsisti, consulenti, tecnici in presidio). Le disposizioni sono rivolte a chiunque effettui trattamento di dati personali, anche nell'ambito di progetti didattici e per periodi limitati di tempo.

E' responsabilità di chiunque applicare e rispettare puntualmente le disposizioni del presente Disciplinare.

Il contenuto del presente documento costituisce ordine di servizio, pertanto la mancata ottemperanza a quanto disposto nel presente documento integra, oltre ad eventuali altri profili di responsabilità civile, penale ed erariale, anche un'ipotesi di violazione disciplinare.

Riferimenti normativi

- Codice dell'Amministrazione Digitale D. Lgs. 82/2005 e s.m.i.
- Regolamento UE 679/2016 (GDPR- General Data Protection Regulation), di seguito "GDPR", decreto legislativo 196/2003, così come modificato e integrato dal decreto legislativo 101/2018
- DUP n. 113 del 22 maggio 2018
- DUP n. 185 del 17 dicembre 2020
- DUP n. 49 del 25 marzo 2021

Principi generali

Il Disciplinare è adottato per assicurare la funzionalità e il corretto impiego dei personal computer portatili o fissi, dei dispositivi elettronici aziendali in generale, della posta elettronica, di internet e di tutti i servizi digitali da parte del personale: a tale fine, definisce le modalità d'uso di tali strumenti nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali.

Le disposizioni e le prescrizioni qui indicate si affiancano e integrano quelle già previste nel contratto di lavoro e, in generale, nelle disposizioni pattizie o regolamentari vigenti.

Le regole che disciplinano l'utilizzo del personal computer, dei dispositivi elettronici aziendali, della posta elettronica, di internet e di tutti i servizi digitali si conformano, pertanto, ai principi generali sanciti dal Regolamento Europeo 679/2016 e dal decreto legislativo 196/2003, così come modificato e integrato dal decreto legislativo 101/2018:

a) «liceità, correttezza e trasparenza». Liceità indica che ogni trattamento deve trovare fondamento in un'idonea base giuridica. I fondamenti di liceità del trattamento di dati personali sono indicati all'articolo 6 del GDPR: consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Correttezza allude alla lealtà e alla buona fede che il titolare deve osservare in tutte le fasi del trattamento dei dati.

Trasparenza significa invece garantire la piena consapevolezza all'interessato circa il soggetto che tratta i suoi dati e le modalità con cui li tratta. Lo strumento per dare attuazione a tale principio è l'informativa: l'informativa è una comunicazione rivolta all'interessato che ha lo scopo di informare il cittadino, anche prima che diventi interessato, sulle finalità e le modalità dei trattamenti operati dal titolare del trattamento.

b) «limitazione della finalità»: i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;

c) «minimizzazione dei dati»: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

d) «esattezza»: i dati devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

e) «limitazione della conservazione»: i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato;

f) «integrità e riservatezza»: i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali).

Disposizioni relative all'utilizzo dei dispositivi informatici

I dispositivi informatici costituiscono la postazione di lavoro degli utenti dei servizi digitali del Consiglio, sono rappresentati da personal computer portatili o fissi, tablet e smartphone, e dai programmi su di essi installati: le postazioni sono strumenti di lavoro e contengono dati riservati e informazioni personali di terzi ai sensi della normativa sulla privacy.

Vanno pertanto utilizzati e conservati con diligenza e cura, attenendosi alle prescrizioni fornite dal datore di lavoro e nel rispetto delle indicazioni da questo fornite.

Le impostazioni delle postazioni informatiche e dei relativi programmi installati sono predisposte dagli addetti informatici incaricati sulla base di criteri e profili decisi dall'Amministrazione consiliare, in funzione della qualifica dell'utente, delle mansioni cui questo è adibito, nonché delle decisioni e della politica di utilizzo di tali strumenti stabilita dall'Amministrazione consiliare stessa. L'utente non può modificarle autonomamente: può ottenere cambiamenti nelle impostazioni solo previa richiesta del Direttore della struttura di appartenenza al Settore Sistemi Informativi.

L'installazione sulle postazioni informatiche di sistemi operativi e programmi applicativi e, in generale, di software, avviene 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.

L'installazione di programmi da parte dell'utente non è consentita: in caso di necessità occorre rivolgersi, previa autorizzazione del proprio Direttore, al Settore Sistemi Informativi. In ogni caso tale installazione deve

avvenire senza aggirare divieti o restrizioni 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.

Tutti i software caricati sulle postazioni informatiche ed in particolare i software necessari per la protezione dello stesso o della rete, non possono essere disinstallati o in nessun modo manomessi dagli utenti.

L'accesso alle postazioni informatiche, ai programmi applicativi e alle varie funzionalità messe a disposizione degli utenti per lo svolgimento dell'attività avviene previa autenticazione, che consiste nella verifica dell'identità del dipendente attraverso l'uso di credenziali identificative nonché, quando richiesto dal sistema, di un certificato digitale.

Scelta, custodia, modifica e utilizzo delle password devono rispettare le seguenti prescrizioni:

- Al primo accesso ad un sistema e/o ad una banca dati, l'utente ha la responsabilità di cambiare la password assegnatagli;
- La password deve essere al minimo lunga otto caratteri, deve contenere una combinazione di lettere, numeri e caratteri speciali, deve essere differente dalle tre precedenti usate e non deve contenere riferimenti che possano ricondurre agevolmente al responsabile della stessa;
- L'utente è obbligato dal sistema a cambiare la propria password su base almeno trimestrale;
- L'utente ha la responsabilità di custodire con diligenza la propria password (ed i dispositivi fisici eventualmente in suo possesso). In nessuna circostanza l'utente è autorizzato a condividere le proprie credenziali di autenticazione con altri incaricati o terze persone.

Sono fatte salve tutte le prescrizioni ulteriori previste per il trattamento dei dati particolari o giudiziari.

In caso di furto o smarrimento delle credenziali, o comunque in tutti i casi in cui l'utente abbia fondati motivi di ritenere che ne possa essere stato fatto un utilizzo da parte di terzi, l'utente deve darne immediatamente informazione all'Amministrazione consiliare con contestuale denuncia all'autorità competente. Nel caso in cui l'utente abbia fondati motivi di ritenere che possa essere compromessa la riservatezza della password, o comunque che ne sia stato fatto un utilizzo indebito, deve immediatamente avvisare il Settore Sistemi Informativi (vedi paragrafo "Comportamento in caso di violazione della sicurezza").

In caso di allontanamento anche temporaneo dalla postazione informatica, l'utente deve evitare che persone estranee effettuino accessi non permessi, bloccandola.

Le credenziali di accesso degli utenti saranno disattivate nel caso in cui cessino il loro rapporto di lavoro, oltre che nei casi espressamente e tassativamente previsti dalla normativa.

Qualora sia necessario accedere a informazioni o documenti di lavoro presenti sulla postazione informatica del dipendente assente e unicamente per garantire l'operatività aziendale, il Direttore della struttura di appartenenza chiede per iscritto al Settore Sistemi Informativi di essere messo nelle condizioni di accedere alla postazione informatica stessa. Contestualmente, il Direttore deve informare il dipendente dell'avvenuto accesso, fornendo adeguata spiegazione e redigendo apposito verbale.

Per finalità di manutenzione e aggiornamento, gli incaricati del Settore Sistemi Informativi potranno accedere sia direttamente sia in remoto alla postazione informatica in via generalizzata. Resta inteso che per finalità di assistenza tali soggetti potranno accedere sia direttamente sia in remoto su richiesta del dipendente.

Dispositivi mobili

Particolare attenzione va posta verso i dispositivi mobili, per loro natura estremamente vulnerabili, sono veri e propri punti di accesso al sistema informativo del Consiglio; è fondamentale proteggerne l'accesso mediante gli strumenti messi a disposizione dal loro sistema operativo, cambiando regolarmente i codici.

La stessa cura deve essere prestata su dispositivi mobili personali sui quali siano possibili accessi a servizi digitali del Consiglio (es. la posta elettronica, le rubriche, ecc.): i dispositivi devono essere protetti da codici di accesso. In caso di smarrimento, furto o di utilizzo dei dispositivi da parte di soggetti non autorizza, occorre effettuare tempestivamente la segnalazione al Settore Sistemi Informativi (vedi paragrafo "Comportamento in caso di violazione della sicurezza").

Memorizzazione dei dati – archivi digitali

Al fine di garantire la disponibilità dei documenti di lavoro, l'utente potrà usufruire dell'area di rete individuale o di gruppo a ciò dedicata (dischi condivisi).

I supporti di memoria portatili e comunque riutilizzabili dovranno essere custoditi con la massima cura ed utilizzati adottando le necessarie cautele affinché soggetti estranei non possano venire a conoscenza dei documenti e delle informazioni ivi contenute.

Tutti i dispositivi elettronici aziendali sono forniti all'utente per lo svolgimento della sua attività lavorativa, nell'ambito delle mansioni a questo affidate. L'uso per fini personali è da considerare pertanto eccezionale e limitato, con esclusione dei dispositivi per i quali è esplicitamente regolamentato l'uso per fini personali.

Gli utenti dei servizi digitali del Consiglio regionale devono sempre utilizzare per la memorizzazione dei dati, gli appositi share di rete messi a disposizione dall'Ente (abilitati ai soli addetti) o i relativi database previsti dai progetti. In caso di necessità (anche solo temporanea) di mantenere per fini di lavorazione una copia delle informazioni offline (sul disco interno delle postazioni di lavoro, su chiavette USB, su hard disk esterni, su smartphone, tablet, ecc.), la copia locale deve essere cifrata ed eliminata al termine della lavorazione.

Non è consentito salvare dati e informazioni su strumenti cloud di archiviazione, gratuiti o a pagamento (es. Google Drive, Dropbox, ecc.), diversi da quelli messi a disposizione dal Consiglio regionale.

Utilizzo di internet e delle risorse di rete

La rete internet può e deve essere utilizzata dal dipendente a supporto all'attività lavorativa.

Al fine di ridurre il rischio di un utilizzo improprio di internet, quale ad esempio il caricamento o lo scaricamento di documenti non attinenti con l'attività lavorativa, la visione di siti internet non pertinenti con l'attività svolta, il collegamento a reti o forum comunque estranei alle mansioni del dipendente, si ricorda che:

- occorre prestare rispetto della normativa vigente in materia di protezione di diritti di proprietà intellettuale nell'acquisizione, riproduzione, condivisione di immagini, di musica, filmati, software;
- il Consiglio regionale utilizza sistemi e filtri automatici che prevengono determinate operazioni non attinenti all'attività lavorativa, bloccando l'accesso a predeterminate categorie di siti;
- i log di connessione alla posta elettronica e di navigazione in Internet degli utenti sono conservati per finalità di accertamento e repressione dei reati nel rispetto di quanto previsto dalla normativa vigente.

Si ribadisce che ogni utente è tenuto ad utilizzare Internet e le risorse di rete nel pieno rispetto delle leggi vigenti.

CONSIGLIO REGIONALE DEL PIEMONTE

Utilizzo della posta elettronica

La casella di posta elettronica istituzionale è uno strumento finalizzato esclusivamente allo scambio di informazioni nell'ambito dell'attività lavorativa.

Le comunicazioni via posta elettronica devono avere un contenuto espresso in maniera professionale e corretta nel rispetto della normativa vigente. I messaggi di posta elettronica devono contenere un avvertimento ai destinatari del seguente tenore letterale:

"Il presente messaggio, corredato degli eventuali allegati, contiene informazioni da considerarsi strettamente riservate e confidenziali. Ne è vietato l'uso improprio, la diffusione, la distribuzione o la riproduzione da parte di altre persone e/o entità diverse da quelle specificate. Qualora lo abbiate ricevuto per errore, vi preghiamo di distruggere il messaggio, comunicando l'errata ricezione tramite il reply all'indirizzo mittente."

Al fine di garantire continuità e accesso ai messaggi da parte dei soggetti autorizzati a condividere tali informazioni, si raccomanda l'utilizzo di caselle di posta elettronica istituzionali in comune, eventualmente affiancandole a quelle individuali.

Qualora sia necessario accedere a informazioni o documenti di lavoro presenti nella casella di posta elettronica del dipendente assente e unicamente per garantire l'operatività aziendale, il dipendente stesso può indicare e delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi ed a inoltrare al Direttore della struttura di appartenenza quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. In caso di assenza del fiduciario o di impossibilità di nomina dello stesso il Direttore deve chiedere per iscritto al Settore Sistemi Informativi, di essere messo nelle condizioni di accedere alla casella di posta elettronica in questione. Contestualmente, il Direttore deve informare il dipendente dell'avvenuto accesso, fornendo adeguata spiegazione e redigendo apposito verbale.

Nel caso in cui il dipendente non presti più la sua attività lavorativa presso il Consiglio regionale del Piemonte, la casella di posta elettronica sarà prontamente disattivata. Se sorge la necessità di prolungarne temporaneamente l'utilizzo da parte dell'Amministrazione consiliare, dovrà pervenire al Settore Sistemi Informativi richiesta scritta da parte del Direttore competente. Tale situazione espone a potenziali rischi di sicurezza in caso di violazione della casella di posta, deve dunque essere riservata a casi di effettiva necessità.

Qualora si verifichino anomalie nell'invio e ricezione dei messaggi di posta elettronica sarà cura dell'utente informare prontamente il Settore Sistemi Informativi.

Gli utenti dei servizi di posta elettronica e certificata sono tenuti ad adottare gli accorgimenti di seguito indicati, per garantire la riservatezza di eventuali comunicazioni personali, la continuità operativa dell'ente nonché l'eventuale esigenza giudiziaria di verifica che renda necessaria l'apertura dello strumento di posta:

- Se si ricevono mail da destinatari sconosciuti contenenti link o allegati sospetti occorre procedere alla segnalazione al settore Sistemi Informativi ed evitarne l'apertura, sino a completa verifica.
- La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.
- Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a queste indicazioni:
    - L'elenco dei destinatari deve essere digitato correttamente;
    - L'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile.
    - Nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio.

- In caso di invio di mail a soggetti esterni, si deve evitare di mandare in chiaro l'elenco degli indirizzi dei destinatari, occorre utilizzare opportunamente la funzione di invio in copia nascosta (ccn). Gli indirizzi mail sono dati personali, non possono essere divulgati impropriamente. Elenchi di indirizzi possono facilitare lo spam e attacchi malevoli sulle caselle di posta, oltre a divulgare impropriamente i dati personali.

- Nel caso di destinatari interni è preferibile mettere in chiaro i destinatari, per competenza oppure in conoscenza (ad eccezione delle convocazioni alle sedute istituzionali, dove è consigliato mettere in ccn i destinatari).

- Occorre prestare particolare attenzione all'uso della funzione 'Inoltra' che consente di inoltrare le mail, bisogna verificare il contenuto dei messaggi inoltrati e gli indirizzi mail presenti nella cronologia del testo; un uso inappropriato dell'inoltro delle mail potrebbe infatti facilitare la divulgazione di dati personali.

- Nell'invio delle comunicazioni via mail utilizzare abitualmente le caselle di posta elettronica condivise tra più lavoratori ovvero le caselle di posta di gruppo (eventualmente affiancandole a quelle individuali).

- In caso di prolungata assenza, utilizzare le funzionalità del sistema di posta per l'invio automatico di messaggi di risposta recanti le coordinate della casella di gruppo o del proprio responsabile a cui rivolgersi.

Ai fini della sicurezza della rete dell'ente, è necessario valutare l'affidabilità del mittente prima di accedere ai file allegati alla posta elettronica (non eseguire download di file eseguibili o documenti da siti Web o Ftp ambigui o comunque non conosciuti il cui indirizzo internet è inserito nel corpo della mail).
Al fine di ridurre il rischio di diffusione di mail contenenti malware vengono applicati alla mail in ingresso filtri di controllo delle estensioni di allegati (es .zip, .rar .exe, etc) e filtri di limitazione anti-spam.

Con l'occasione si rammenta che il contenuto dei messaggi inviati deve essere espresso in maniera professionale e corretto e quindi non deve contenere espressioni che possano rivelarsi offensive, razziste, sessiste, discriminatorie o volgari.

Piattaforme di collaboration e video conference

Alle riunioni che si svolgono da remoto si applicano le ordinarie disposizioni sul segreto d'ufficio e sul diritto alla protezione dei dati personali.

Le piattaforme di collaboration offrono strumenti per un supporto dell'attività lavorativa a distanza sia in tempo reale (es video conferenza, condivisione e modifica di documenti tra più persone nello stesso momento) che in modalità asincrona (es. uno spazio cloud per memorizzare condividere file).

Il Consiglio regionale dispone attualmente della piattaforma Cisco webex, che mette a disposizione uno strumento di videoconferenza e di condivisione in tempo reale di documenti.

Gli strumenti di collaboration, quando vengono impiegati per condividere documenti, video o immagini, devono essere utilizzati nel rispetto delle regole di comportamento indicate nel disciplinare al fine di garantire la riservatezza e in generale la sicurezza delle informazioni che possono transitare sulle stesse ma anche la tutela del segreto professionale, di marchi e del know-how dell'ente.

In particolare, in relazione alla funzionalità di collaborazione in tempo reale è vietato effettuare snapshot o attivare la registrazione delle call al di fuori dei casi necessari ed espressamente autorizzati dai partecipanti.

E' consentito, durante l'esecuzione delle call, l'uso delle funzioni di offuscamento delle sfondo o la disattivazione della telecamera. Le regole suindicate si applicano anche nel caso in cui vengano utilizzati strumenti di collaboration non aziendali come Skype, Zoom, Google Meet.

Tali strumenti non aziendali sono consentiti per la partecipazione a riunioni con l'esterno convocate da altri enti, ma per le riunioni interne deve essere utilizzata la piattaforma Cisco Webex.

In caso di utilizzo delle videoconferenze per la gestione delle sedute istituzionali occorre attenersi al Regolamento interno del Consiglio regionale e alle norme di comportamento deliberate dall'Ufficio di Presidenza.

Il fornitore dei sistemi è stato nominato responsabile del Trattamento.

Disposizioni per la gestione di documenti cartacei

Per quanto riguarda la documentazione cartacea presente negli uffici occorre attenersi alle seguenti istruzioni, volte ad assicurare la protezione dei dati personali.

Stampe e fotocopie

Il Consiglio regionale ha adottato un sistema di protezione delle stampanti multifunzione, che consentono di fare scansioni, fotocopie e stampe.

Ogni utente è dotato di un codice di accesso personale, che consente di evitare improprie diffusioni di informazioni personali.

E' vietato condividere con soggetti terzi il codice di accesso personale alle stampanti multifunzione.

Documenti negli uffici (scrivanie e armadi)

Per quanto riguarda l'eventuale documentazione cartacea, compresi i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento dei dati personali, soprattutto in caso di dati particolari, gli atti e i documenti dovranno essere conservati dai soggetti incaricati, esclusivamente per la durata del trattamento. Inoltre, verificare che tutti i dati raccolti siano effettivamente necessari.

Non lasciare mai documentazione sulle scrivanie oltre l'orario d'ufficio o in caso di assenza (pausa pranzo, riunione, ecc.).

Al termine del procedimento, conservare la documentazione negli archivi ad accesso selezionato e annotare il nome dei soggetti ammessi in appositi registri.

Conservare i dati idonei a rilevare lo stato di salute o in generale i dati particolari separatamente da ogni altro dato personale trattato.

Chiudere l'ufficio a chiave qualora non si abbia a disposizione un armadio munito di serratura.

Depositare le chiavi degli armadi e/o dei locali ove sono custoditi dati personali in luogo sicuro.

Effettuare la trasmissione e la comunicazione dei dati personali mediante posta, all'interno o all'esterno dell'Ente, per mezzo di supporti cartacei o magnetici, riposti in buste o pacchi chiusi. Nel caso si tratti di dati particolari, indicare sulla busta o sul pacco ovvero sul documento accompagnatorio la dicitura "dati particolari".

Comportamento in caso di violazione della sicurezza

La violazione è definita all'art. 4 par. 12 GDPR come *"la violazione di sicurezza che comporta accidentalmente in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati"* (data breach).

Non appena si viene a conoscenza di una violazione dei dati personali, al momento del verificarsi del fatto o della sua scoperta, il dipendente deve attivare apposita procedura di segnalazione, che prevede immediata comunicazione scritta e inviata con posta elettronica al settore sistemi informativi che provvederà a condividere la comunicazione con il tema sicurezza del Consiglio regionale (rif. Processo di gestione dei Data breach del Consiglio).

Gli eventi che possono comportare un data breach possono essere ad esempio:

- Data Exfiltration (copia o trasferimento non autorizzati di dati)
- Ransomware/Malware
- Distruzione accidentale archivio digitale
- Smarrimento, furto di PC o server
- Smarrimento, furto di dispositivo mobile (smartphone, USB KEY, CD/DVD HD, etc.)
- Smarrimento, furto o distruzione di un archivio cartaceo
- Divulgazione impropria di dati personali (ad esempio elenchi massivi di indirizzi mail)
- Indisponibilità di dati esposti su siti web o servizi applicativi

A fronte della segnalazione di un evento che può comportare il data breach, viene attivata la procedura di gestione del Consiglio.

Controlli effettuati dall'Amministrazione consiliare

L'Amministrazione consiliare si riserva di effettuare controlli per verificare il rispetto del Disciplinare. Nel caso di tali controlli il presente Disciplinare costituisce preventiva e completa informazione nei confronti dei dipendenti.

Gli eventuali controlli generali ed estesi atti a verificare condotte non conformi al presente Disciplinare avverranno preliminarmente su dati aggregati e anonimi riferiti all'intera struttura lavorativa ovvero al Settore o alla Direzione qualora il Settore, per caratteristiche intrinseche alla struttura organizzativa, non offrisse garanzie di completa anonimità della verifica. Nel caso vengano rilevate anomalie o irregolarità, dovrà essere inviato un avviso generalizzato ai dipendenti che richiami questi ultimi all'utilizzo corretto degli strumenti elettronici aziendali, nel rispetto della normativa vigente e dei diritti dei terzi, con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Se le anomalie o le irregolarità dovessero persistere, si procederà ad avvisare le autorità competenti.

Qualora venga constatata la violazione del presente Disciplinare, l'Amministrazione consiliare potrà irrogare le sanzioni applicabili previste dai contratti collettivi vigenti, nel rispetto delle procedure stabilite dagli stessi contratti.

L'Amministrazione consiliare, effettua attività di monitoraggio e verifica dell'efficacia delle protezioni predisposte sulle postazioni informatiche rispetto ad aggressioni esterne o interne senza che siano necessarie

preventive ulteriori informative. Le risultanze di tali attività di monitoraggio e verifica dovranno essere utilizzare soltanto in modo proporzionato e pertinente alle finalità e alla natura delle stesse vigente, di effettuare specifici controlli ad hoc nel caso di segnalazione di attività che abbiano causato danno all'Amministrazione stessa, che ledano diritti di terzi o che siano illegittime.

Inoltre, si rammenta che i dati relativi all'utilizzo della posta elettronica e di internet sono conservati conformemente a quanto previsto dalla normativa vigente.