REGIONE DEL VENETO

giunta regionale

Direzione ICT e Agenda Digitale

Regole per l'uso delle risorse ICT e dei dispositivi di telefonia mobile della Giunta regionale

Misure organizzative, tecniche e comportamentali

Versione 4.2

INDICE

Premessa

Le risorse ICT *(Information and Communications Technology*) costituiscono un bene dell'Amministrazione regionale e come tale va salvaguardato e protetto accuratamente.

La protezione di tale bene richiede un'analisi complessiva del contesto che, oltre agli aspetti prettamente tecnici, abbracci le prassi ed i comportamenti adottati dagli utilizzatori delle risorse ICT.

L'efficacia delle misure a protezione delle risorse ICT non può prescindere dal coinvolgimento attivo dell'utente finale quale elemento fondamentale inserito in un sistema organico basato su misure organizzative e tecniche dove in generale l'utente - o meglio il suo comportamento - rappresenta l'elemento più debole dell'intero sistema.

Nessuna misura di protezione è efficace senza il coinvolgimento dell'utente finale che deve adottare comportamenti conformi alle istruzioni ricevute, evitando azioni che (anche involontariamente) possano pregiudicare la sicurezza dei sistemi e/o dei dati.

Tutte le risorse ICT che l'Amministrazione regionale mette a disposizione degli utenti - così come definite nei successivi paragrafi - devono essere impiegate ai soli fini lavorativi in modo efficiente ed appropriato, evitando gli abusi.

Il presente documento aggiorna, con le regole d'uso nello stesso contenute, le "*Regole comportamentali per gli Utenti nell'uso delle risorse ICT dell'Amministrazione regionale"* già approvate con DGR n. 1480 del 16/10/2018 e descrive i criteri e le regole che disciplinano l'assegnazione e l'uso dei dispositivi di telefonia mobile di proprietà dell'Amministrazione regionale.

Finalità

Scopo del presente documento è preservare le risorse ICT dell'Amministrazione e fornire agli utenti le indicazioni circa il loro corretto ed appropriato uso, nel rispetto della normativa vigente in materia.

L'Amministrazione, in particolare, intende perseguire i seguenti obiettivi:

- ridurre l'esposizione alle minacce e ai rischi per la loro sicurezza, per salvaguardare la disponibilità, l'integrità, la confidenzialità dei dati e la continuità operativa dei servizi informatici;
- garantire il rispetto della normativa vigente in materia;
- garantire l'integrità e la disponibilità dei beni materiali dell'Amministrazione regionale;
- esplicitare le regole per la corretta fruizione del servizio di gestione della telefonia mobile erogato dalla Direzione ICT e Agenda digitale, definendone le caratteristiche, i criteri di assegnazione dei dispositivi di telefonia mobile e le modalità operative adottate da quest'ultima.

Ambito di applicazione

Il presente documento è rivolto agli "Utenti" così come definiti nel paragrafo "Definizioni".

Ciascun Utente, in base al proprio ruolo di semplice Utilizzatore di risorse ICT e di *persona autorizzata al trattamento* oppure di "delegato" di cui alla DGR n. 596/2018, è chiamato ad attenersi alle regole contenute nel presente documento.

Tali regole inoltre sono rivolte anche ai soggetti con mansioni tecniche come, ad esempio, gli amministratori di sistema, gli amministratori di rete, gli amministratori di banche dati, i gestori di servizi, ecc.

Le regole che disciplinano l'uso delle risorse ICT dell'Amministrazione regionale sono declinate sui versanti organizzativo, tecnologico-procedurale e comportamentale. Esse sono volte al perseguimento degli obiettivi di cui al paragrafo "Finalità", precisando al riguardo che:

- la **confidenzialità** o **riservatezza** riguarda la conoscibilità e fruibilità delle informazioni ai soli soggetti autorizzati;
- l'**integrità** è relativa alla completezza ed inalterabilità delle informazioni;
- la **disponibilità** concerne l'accessibilità ed usabilità delle informazioni nel tempo da parte dei soggetti autorizzati.

1. Misure organizzative

La Giunta regionale con DGR n. 596 del 08/05/2018 e s.m.i a seguito del mutato quadro normativo europeo in materia di privacy, per quanto riguarda i trattamenti di dati personali effettuati dalle strutture della Giunta regionale, ha ridefinito le misure organizzative/tecniche volte ad assicurare il rispetto del Regolamento n. 2016/679/UE, *General Data Protection Regulation* (GDPR), fornendo contestualmente nuove istruzioni per i trattamenti di dati personali e costituendo un Gruppo di Lavoro con compiti operativi, di gestione, supporto, analisi e soluzione dei problemi in materia di applicazione del Regolamento stesso.

Pertanto, per quanto attiene all'organizzazione privacy, si rinvia, alla citata DGR n. 596/2018, ricordando che, ai sensi della stessa, *«sono delegati tutti i Dirigenti in servizio presso l'Amministrazione regionale, ognuno per la parte di propria competenza, al trattamento di dati personali effettuato nello svolgimento dell'incarico ricevuto».*

Gestione degli incidenti informatici

Per "incidente informatico" s'intende un qualsiasi "imprevisto" rispetto al normale funzionamento in un sistema o più in generale di una infrastruttura informatica come ad esempio un malfunzionamento – incidentale o accidentale – di tipo hardware o software, un attacco informatico o un accesso non autorizzato ad un sistema che possa causare effetti negativi alla riservatezza, integrità o disponibilità dei dati contenuti.

L'utente è chiamato a segnalare tempestivamente al ***Call Center*** ogni incidente informatico o situazione anomala che potrebbe far presagire l'insorgere di un incidente, affinché l'operatore del ***Call Center*** possa avviare quanto prima il processo di classificazione e di risposta all'incidente stesso allo scopo di minimizzarne gli eventuali impatti negativi.

Inoltre, qualora l'incidente sia di una certa entità o estensione e riguardi il patrimonio informativo e di conoscenza detenuto dall'Amministrazione oppure i servizi o le applicazioni informatiche regionali, l'utente dovrà segnalare l'evento al Direttore della struttura regionale di riferimento/appartenenza, al Direttore della Direzione ICT e Agenda Digitale e, per conoscenza, al Data Protection Officer.

Gestione dei "data breach"

Per gli incidenti i cui effetti possono essere la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (cd. "***data breach***"), l'utente provvede tempestivamente a segnalare la situazione al ***Call Center*** per l'espletamento delle

verifiche di cui al punto precedente "*Gestione degli incidenti informatici*" e contestualmente segnala al "*Delegato*" al trattamento (Direttore della struttura regionale di riferimento/appartenenza) le violazioni ai dati personali rilevate e/o gli incidenti informatici che ha rilevato e che possono avere un impatto significativo sui dati personali.

Ricevuta la segnalazione il "*Delegato*" al trattamento si attiverà procedendo secondo le prescrizioni contenute nelle "*Istruzioni per i trattamenti di dati personali"* approvate con DGR n. 596/2018. Pertanto ogni Delegato, non appena venuto a conoscenza di un *data breach,* effettuerà una prima necessaria istruttoria, volta a verificare i presupposti della presunta violazione. A tal fine sarà opportuno tener traccia del percorso logico e delle motivazioni che hanno condotto ad effettuare le scelte in ambito privacy, sulla base del test di autovalutazione disponibile sul sito del Garante Privacy (https://servizi.gpdp.it/databreach/s/self-assessment) e poi, se nel caso, compilando - per le parti di propria competenza - il modulo editabile predisposto sulla base di quello del Garante Privacy e reso disponibile al seguente al link:

https://www.regione.veneto.it/web/informatica-e-e-government/informativa_privacy

Il predetto Delegato, valutati i rischi per i diritti e le libertà delle persone fisiche, avviserà - qualora ritenuto necessario - tempestivamente la Direzione ICT e Agenda Digitale ed il Data Protection Officer, chiedendo supporto e trasmettendo loro il citato modulo (*compilato con le informazioni disponibili*), per il seguito di competenza.

A sua volta, come previsto dalla succitata DGR n. 596/2018 il Direttore della Direzione ICT e Agenda Digitale, sulla base degli esiti della predetta istruttoria del Delegato, ricevuto il modulo anzidetto, dopo aver chiesto eventuali ulteriori informazioni e/o integrazioni (se ritenute necessarie) al Delegato mittente, effettuerà la notifica al Garante per la Protezione dei dati personali del *data breach,* per conto del Titolare del trattamento. Al fine di dar seguito a detta notifica, si dovrà procedere tramite procedura informatizzata, resa disponibile dal GDPD nel proprio sito internet, entro 72 ore dal momento in cui ne è venuto a conoscenza e senza ingiustificato ritardo.

Qualora le violazioni ai dati personali riguardino un servizio erogato in "cloud" da un "*service provider*" esterno, attivato direttamente dal "*Delegato*" al trattamento, la segnalazione potrà pervenire direttamente dal "*service provider*" stesso.

In tal caso, il "*Delegato*" al trattamento, una volta raccolte dal "*service provider*" del servizio interessato tutte le informazioni necessarie, ne darà comunicazione alla Direzione ICT e Agenda Digitale.

Qualora le violazioni ai dati personali ovvero gli incidenti informatici siano rilevati "direttamente" dalla Direzione ICT e Agenda Digitale nello svolgimento della propria attività istituzionale, la medesima

Struttura si occuperà dell'espletamento degli adempimenti conseguenti, informandone contestualmente il Data Protection Officer.

2. Misure tecnologiche e procedurali

Il Regolamento n. 679/2016/UE (GDPR) con l'introduzione dei principi di "*privacy by design*" e di "*privacy by default*" ha prescritto la necessità di configurare ogni trattamento dei dati prevedendo fin dall'inizio (ossia in fase di progettazione: *by design*) le garanzie indispensabili al fine di soddisfare i requisiti previsti dalla normativa e tutelare i diritti degli interessati, tenendo conto sia del contesto complessivo ove avviene il trattamento dei rischi per i diritti e le libertà degli interessati.

"*Privacy by design*" significa che già in fase di progettazione del trattamento dei dati dev'essere prevista l'implementazione di misure atte a garantire la tutela dei diritti e le libertà degli interessati, tenuto conto del contesto complessivo.

"*Privacy by default*" significa che le misure tecniche e organizzative sono per impostazione predefinita (*by default*, appunto) quelle che garantiscono la tutela dei dati trattati, ossia quelle che garantiscono di trattare solo i dati personali necessari per ogni specifica finalità del trattamento.

Per effetto della DGR n. 596/2018 ciascun "*Delegato*" al trattamento dei dati assume, per i procedimenti di propria competenza, le responsabilità attribuite al titolare del trattamento ed in particolare la messa in atto di adeguate misure tecniche e organizzative volte a garantire che i dati siano trattati nel rispetto del Regolamento n. 679/2016/UE *(GDPR)*.

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

Come conseguenza dell'applicazione del principio di responsabilizzazione dei soggetti titolari del trattamento contenuto nel Regolamento n. 679/2016/UE (GDPR), ciascun "*Delegato"* al trattamento ha il compito di decidere le modalità, le garanzie ed i limiti del trattamento dei dati personali in relazione alla propria realtà e alle caratteristiche peculiari della stessa.

Il "*Delegato*" al trattamento ha altresì il compito di individuare e mettere in atto adeguate misure di sicurezza in relazione alla reale situazione contingente.

Qualora le Strutture per esigenze particolari intendessero procedere autonomamente all'acquisto di nuove soluzioni software, dovranno preventivamente comunicarlo alla Direzione ICT e Agenda Digitale per una

valutazione di competenza. Le suddette strutture dovranno prevedere nei contratti d'appalto l'obbligo di rispettare le "*Linee guida per lo sviluppo delle applicazioni informatiche secondo gli standard regionali*" (Reference Architecture) approvate dalla Direzione ICT e Agenda Digitale, nonché le clausole di "responsabilità esterna" e di "amministrazione dei sistemi", in attuazione del Provvedimento Generale del Garante dei dati personali del 27/11/2008 (in materia di Amministratori di Sistema), come modificato con successivo Provvedimento Generale del 25/06/2009.

Si fa presente che la protezione dei dati fin dalla progettazione e protezione per impostazione predefinita costituisce il metodo ordinario di lavoro della Direzione ICT e Agenda Digitale.

La Direzione ICT e Agenda Digitale adotta misure tecniche/organizzative in sintonia con i principi di cui al Regolamento n. 679/2016/UE (GDPR) ed in particolare con quanto prescritto all'art. 25.

Qualora nell'implementare nuove soluzioni software la Direzione ICT e Agenda Digitale - a seguito di opportuna valutazione - opti per il ricorso a "*servizi in cloud*", l'individuazione dei relativi "*service provider*" avverrà dopo attenta analisi di mercato dei fornitori in grado di offrire servizi con elevate garanzie per la protezione dei dati ed in particolare nel pieno rispetto del Regolamento n. 679/2016/UE (GDPR).

Dati in "cloud"

Con il termine "*cloud computing*", o semplicemente "*cloud*" (nuvola), s'intende sinteticamente un insieme di tecnologie e di modalità di fruizione di servizi informatici che permette agli utenti di accedere e utilizzare da remoto funzionalità hardware e software attraverso una connessione Internet.

Le società che offrono questi servizi sono dette "fornitori di servizi cloud ("*service provider*") ed in genere addebitano un costo per i servizi di "*cloud computing*" in base al loro utilizzo.

Uno dei principali vantaggi connessi all'utilizzo del **"***cloud computing*" consiste nella corresponsione di un canone a fronte delle risorse effettivamente utilizzate.

Esistono diversi tipi di servizi in "*cloud*" (*Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS), e *Software as a Service* (SaaS)) e diversi modelli di "*cloud*" (pubblico, privato, community e ibrido).

In generale il ricorso al "*cloud computing*" non è privo di rischi specialmente per quanto riguarda la "privacy" sebbene i "*service provider*" affermino che i dati critici siano mascherati o crittografati e che solo gli utenti autorizzati abbiano accesso ai dati nella loro interezza.

Qualora le Strutture per esigenze particolari intendessero procedere autonomamente all'acquisto di "*servizi in cloud*", dovranno preventivamente comunicarlo alla Direzione ICT e Agenda Digitale per una valutazione di competenza. Il "*Delegato*" al trattamento, salvo motivate ragioni, deve rivolgersi a fornitori di servizi cloud la cui infrastruttura sistemistica sia localizzata nel territorio dell'Unione Europea dove l'applicazione delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche risulta omogenea ed in grado di garantire un elevato livello di protezione dei dati personali.

L'individuazione del *"service provider"* da parte del "Delegato" al trattamento deve avvenire dopo un'analisi di mercato sui fornitori di servizi cloud in grado di offrire servizi con elevate garanzie per la protezione dei dati rispettando pienamente le prescrizioni del Regolamento n. 679/2016/UE (GDPR).

Sicurezza delle postazioni di lavoro (PdL)

Le postazioni di lavoro, "fisse" o "mobili", assegnate agli utenti utilizzatori, vengono fornite dalla Direzione ICT e Agenda Digitale corredate del software di base e degli applicativi standard necessari allo svolgimento della prestazione lavorativa nel rispetto delle vigenti misure in ambito di sicurezza informatica.

Le PdL sono altresì configurate seguendo le best practices ritenute più idonee a garantire e mantenere la sicurezza del software di base e la protezione dei dati in esse contenuti.

Agli utenti utilizzatori verrà assegnato un profilo di "**non amministratore**" (bassi privilegi), secondo il principio del "privilegio minimo", al fine di salvaguardare maggiormente la sicurezza delle PdL impedendo l'avvio e l'esecuzione di malware o limitandone la capacità di diffondersi attraverso la rete dell'intero sistema informativo regionale.

Eventuali necessità operative di modifica della configurazione prevista di default, dovranno essere richieste al Call center regionale e tracciate tramite ticket per una adeguata valutazione.

Crittografia

Al fine di proteggere i dati contenuti nelle PdL regionali, è implementata (ove tecnicamente fattibile) la funzionalità nativa di crittografia del disco fisso (Bitlocker) che permette, in caso di furto o manomissione della PdL, di proteggere i dati contenuti all'interno della stessa rendendoli indecifrabili.

La chiave utilizzata per la cifratura dei dati è conservata centralmente presso i sistemi di Regione del

Veneto e consiste in una combinazione numerica univoca legata ai componenti hardware della PdL stessa (scheda madre, ram, cpu, disco, etc).

I supporti rimovibili di archiviazione (supporti USB o Hard Disk portatili) in uso sulle PdL regionali e contenenti dati personali o informazioni riservate, dovranno essere altresì sottoposti al processo di cifratura al fine di garantirne la riservatezza dei dati stessi chiedendo ove necessario un supporto al Call Center di Regione del Veneto.

Clean desk Policy

L'applicazione di una Clean Desk Policy (politica di scrivanie e computer puliti) permette di migliorare la protezione e la riservatezza delle informazioni sensibili e di ridurre la minaccia di un incidente di sicurezza allorché le informazioni vengano lasciate incustodite, la cui diffusione potrebbe causare gravi conseguenze anche economiche e danni reputazionali.

La politica delle scrivanie e dei computer puliti deve essere estesa a tutti i documenti, le note, i post-it nonché ai computer portatili, ai tablet, agli smartphone ed ai supporti di memoria rimovibili come dischi esterni, chiavette USB, CD, DVD.

Durante le assenze prolungate ed a fine giornata i PC portatili, gli smartphone, i tablet ed anche i supporti di memoria rimovibili che possano contenere informazioni sensibili devono essere riposti in luogo sicuro.

A fine giornata ciascuno dovrà provvedere altresì alla pulizia della propria scrivania rimuovendo e riponendo in un luogo sicuro tutta la documentazione cartacea contenente informazioni sensibili, provvedendo alla sua distruzione appena non più necessaria.

Coloro che organizzano una riunione sono altresì responsabili di verificare che a fine della stessa non venga lasciato alcun documento contenente informazioni sensibili nella sala dove si è svolta la riunione, assicurandosi di cancellare le lavagne, eliminare i fogli mobili e svuotare i cestini dai documenti eventualmente presenti.

Sicurezza delle applicazioni software

Nell'ambito delle attività di progettazione, implementazione, sviluppo, selezione e utilizzo di nuove soluzioni software da parte delle Strutture regionali dev'essere garantita l'osservanza:

- delle *"Linee guida per lo sviluppo del software sicuro nella pubblica amministrazione"* emanate da

AgiD per la sicurezza ICT delle Pubbliche Amministrazioni, aventi lo scopo di fornire indicazioni sulle misure da adottare in ciascuna componente della Mappa del Modello strategico del Piano Triennale;

- di quanto previsto dalla DGR n. 3176 del 27/10/2009 (*Sistema Informativo della Regione del Veneto: approvazione degli Standard Regionali Informatici e mandato alla Direzione Sistema Informatico per il loro governo e aggiornamento)* che definisce gli "standard regionali" per la conduzione dei progetti, la stesura della documentazione e le modalità di produzione del software. Tali standard sono aggiornati e pubblicati nella rete intranet regionale;
- dei principi di "*privacy by design*" e "*privacy by default*" durante tutto il ciclo di vita delle applicazioni "*web-based*", nonché il rispetto delle best practices emesse dall'Organizzazione internazionale *"Open Web Application Security Project (OWASP)"*;
- un'attività di Vulnerability Assessment / Web Application Penetration Test (WAPT) al fine di identificare eventuali vulnerabilità o misconfigurazioni di sicurezza dell'applicazione stessa sulla base dei riferimenti/lavori maggiormente riconosciuti dal settore (es. OWASP Top 10, CWE/SANS Top 25, OWASP Web Security Testing guide).

Nel caso di applicazioni da acquistare sul mercato (c.d. applicazioni «COTS» *"Commercial Off-the-Shelf component"),* le strutture regionali dovranno prendere in considerazione le "Linee guida sull'acquisizione e riuso di software per la Pubblica amministrazione" di AgID e Team per la Trasformazione digitale (Gazzetta ufficiale, serie generale n.119 del 23 maggio 2019), che attuano gli articoli 68 e 69 del **Codice** dell'**Amministrazione Digitale** (**CAD**).

La valutazione comparativa prevista all'articolo 68 del CAD e delle suddette linee guida prevedono che le PA effettuino una valutazione comparativa tecnico economica prima di acquistare software, motivando le proprie scelte e privilegiando le soluzioni open source, incluse quelle messe in riuso dalle altre amministrazioni. Lo sviluppo di nuovo software o l'acquisto di licenze di software proprietario dovrà essere quindi motivato.

Sicurezza della rete e dei server

La Direzione ICT e Agenda Digitale configura la Rete Telematica dell'Amministrazione per contribuire alla protezione dei server, che dovranno essere collocati su sottoreti dedicate all'interno del Data Center regionale o in Cloud e con strumenti e livelli di protezione perimetrali (ad es. *firewall, IPS/IDS, Web Application Firewall*, ecc.) adeguati in base al livello di classificazione assegnato ai dati ospitati nei server medesimi.

Per ragioni di sicurezza, nonché di gestione centralizzata dei "backup/restore" e dei log di accesso ai dati, sistemi ed applicazioni, **non è consentita** l'installazione, configurazione e gestione in proprio di Server presso le strutture regionali dislocate sul territorio.

L'accesso con privilegi amministrativi ai sistemi informatici regionali ospitati nel Data Center e in Cloud, dovrà avvenire per mezzo di un sistema di Privileged Access Management (PAM) al fine di garantire un livello maggiore di protezione e monitoraggio degli accessi nonché il ciclo di vita delle identità amministrative stesse.

Sicurezza della navigazione Internet

L'accesso ad Internet attraverso le risorse ICT e il sistema informativo regionale, deve essere utilizzato in modo strettamente pertinente allo svolgimento della propria attività lavorativa in maniera appropriata, diligente e rispettosa dei principi di seguito esposti, secondo le regole adottate in conformità alle "*Linee guida del Garante per posta elettronica e internet*" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007 e con DGR n. 863 del 31 marzo 2009 "*Approvazione disciplina per l'utilizzo di posta elettronica, internet, telefoni e fax all'interno di Regione del Veneto*" alla quale si rinvia.

Al fine di facilitare l'Utente nel rispetto delle regole di navigazione, l'Amministrazione provvede alla configurazione di blocchi attraverso l'utilizzo di 'blacklist' pubbliche in continuo aggiornamento e di filtri nella navigazione internet che vadano a prevenire il rischio di un utilizzo improprio della rete stessa.

L'Amministrazione si riserva inoltre di applicare per singoli Utenti o per Gruppi, politiche di navigazione personalizzate in base alle mansioni assegnate o eventuali specifiche esigenze lavorative.

Conservazione

I sistemi informatici sono stati programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- l'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;

- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

Strumenti ammessi per lo scambio di dati

Per ragioni di sicurezza, lo scambio di dati nell'ambito della propria attività lavorativa può avvenire soltanto attraverso gli strumenti messi a disposizione dalla Direzione ICT e Agenda Digitale e qui di seguito elencati:

- strumenti di "web collaboration" documentale in cloud acquisiti o attivati da Regione del Veneto;
- cartelle condivise su file server NAS (Network Attached Storage) associati alla struttura regionale o tematica lavorativa (*Es. \\GruppodiLavoro-XX*);

Per lo scambio di file con utenti esterni al dominio regionale, nel rispetto delle policy di riservatezza dell'Ente regionale, viene messo a disposizione uno strumento che potrà ospitare i dati solo per il tempo necessario all'esecuzione del loro download.

Il suddetto elenco potrebbe subire delle variazioni dovute all'evoluzione dei prodotti o alla sostituzione tecnologica degli stessi.

Non è consentita la condivisione diretta di cartelle e file tra le PdL utilizzando la funzione nativa del sistema operativo.

Accesso ai dati contenuti nelle risorse ICT

Cessazione del rapporto di lavoro

Ogni dipendente/collaboratore prossimo alla cessazione del rapporto di lavoro dovrà provvedere alla cancellazione e/o salvataggio delle email e dei file contenenti eventuali dati personali che lo riguardano all'interno delle risorse ICT assegnate, entro l'ultimo giorno lavorativo utile, pena la perdita dei medesimi a seguito di cancellazione da parte della Direzione ICT e Agenda Digitale.

Qualora l'Amministrazione regionale avesse la necessità di recuperare informazioni e documenti relativi

alle attività lavorative svolte, contenute nelle risorse ICT del dipendente cessato e fosse stata impossibilitata a recuperare le medesime dal lavoratore, è necessario adottare la procedura seguente.

Il Direttore della struttura interessata dovrà presentare richiesta alla Direzione ICT e Agenda Digitale di accesso ai contenuti predetti, assumendosi la responsabilità di tale accesso. La Direzione ICT e Agenda Digitale, procederà garantendo adeguate misure tecniche e redigendo un verbale dell'attività svolta. Il Direttore della struttura interessata dovrà dare preventiva notizia al lavoratore medesimo (se in vita), consentendo a quest'ultimo di proporre le sue osservazioni. In ogni caso dovrà essere tutelata la riservatezza e la dignità del lavoratore.

In ipotesi di Utenti cessati, qualora non sia pervenuta alcuna richiesta nelle modalità predette, si procederà alla cancellazione e alla conseguente distruzione definitiva dei contenuti delle risorse ICT ad essi assegnati a partire dal 61° giorno dalla data di cessazione. Verranno conservati solo i contenuti di 'proprietà' dell'Utente cessato ma esplicitamente già condivisi all'interno di repository in cloud (es. lettere, fogli di calcolo, moduli, presentazioni, siti internet).

Sospensione del rapporto di lavoro

In ipotesi di sospensione del rapporto di lavoro si rinvia a quanto descritto al punto precedente "*Cessazione del rapporto di lavoro*". Resta fermo il fatto che in caso di sospensione del lavoratore i dati contenuti nelle risorse ICT verranno preservati.

Gestione delle Utenze

Gli Utenti ricevono dal gestore del servizio delle credenziali individuali e univoche che devono essere mantenute riservate e custodite con cura da parte dell'utilizzatore stesso e non devono essere cedute a terzi.

Le credenziali personali, laddove già utilizzate, non possono essere assegnate ad altri Utenti, neppure in tempi diversi e qualora non utilizzate da almeno tre mesi vengono temporaneamente disabilitate dal sistema.

Il gestore può, a fronte di particolari situazioni, sospendere o disabilitare le credenziali rilasciate (ad es. la Direzione Organizzazione e Personale disabilita tempestivamente le credenziali del personale regionale andato in pensione).

Ogni password, nel rispetto dei parametri imposti dalla "Password policy" regionale, dev'essere associata esclusivamente ad un unico soggetto identificato e preventivamente censito sui sistemi del gestore.

Autenticazione utenti

L'accesso ai servizi e agli applicativi erogati da Regione del Veneto deve avvenire previa procedura di autenticazione mediante *nome utente* e *password* fornite dall'amministrazione e laddove il sistema lo consenta è fatto d'obbligo l'utilizzo della Multifactor Authentication (MFA) ad esempio la combinazione di nome utente, password e codice usa e getta.

L'accesso a servizi in cloud o di terze parti **non integrati** con i sistemi di autenticazione regionali o nazionali (es. SPID, CIE, CNS), deve avvenire mediante l'utilizzo di password diverse da quelle utilizzate per l'accesso ai sistemi regionali, al fine di evitare che eventuali data breach ai danni dei servizi in cloud o terze parti, possano costituire un rischio per la sicurezza e riservatezza dei dati e delle informazioni del sistema informativo regionale.

Autorizzazione e profilatura utenti

Gli Utenti, precedentemente autenticati, devono essere autorizzati dal Gestore (responsabile) del servizio circa l'ambito di accesso/conoscenza del Patrimonio Informativo dell'Amministrazione e le operazioni che su di esso possono eseguire.

Sarà cura del Direttore della struttura in cui opera l'Utente chiedere al Gestore (responsabile) del servizio di assegnare e/o modificare i diritti di accesso al servizio medesimo, in base alle mansioni assegnate e svolte dall'Utente.

Cessazione utenza regionale

In caso di cessazione dell'utenza regionale e dei collaboratori (per quiescenza, licenziamento, trasferimenti definitivi, cessazione definitiva del rapporto contrattuale), ci si richiama al Provvedimento del Garante Privacy del 04/12/2019 [9215890] il quale dispone che il datore di lavoro, dopo la cessazione del rapporto di lavoro debba rimuovere gli account di posta elettronica aziendali riconducibili a persone identificate o identificabili "*in un tempo ragionevole commisurato ai tempi tecnici di predisposizione delle misure, previa disattivazione degli stessi e contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del titolare del trattamento, provvedendo altresì ad adottare misure idonee ad impedire la visualizzazione dei messaggi in arrivo durante il periodo in cui tale sistema automatico è in funzione*".

Nei casi in cui il dipendente di cui si tratta sia stato assegnato in comando ad altra Amministrazione o si trovi in stato di aspettativa programmata per un periodo superiore ad almeno **60 giorni**, la casella di posta elettronica non verrà cancellata bensì disabilitata temporaneamente, su richiesta della Direzione

Organizzazione e Personale alla Direzione ICT e Agenda Digitale.

Ciò varrà altresì con riferimento a tutte le altre fattispecie contrattuali in cui il rapporto di lavoro non incorra in cessazione definitiva.

Gli Enti e le Società che in forza di contratti o convenzioni operano presso la Regione del Veneto sono tenute a richiedere tempestivamente la cessazione di utenze/credenziali dei loro collaboratori non più in servizio per l'Amministrazione regionale.

Utenti "Amministratori di Sistema"

In attuazione del Provvedimento Generale del Garante dei dati personali del 27/11/2008 (in materia di Amministratori di Sistema), come modificato con successivo Provvedimento Generale del 25/06/2009, tutti gli Utenti regionali che sovrintendono alla manutenzione, gestione della sicurezza e protezione dei dati delle risorse informatiche regionali vengono nominati e incaricati dalla Direzione ICT e Agenda Digitale come "Amministratori di Sistema" (AdS) e sono tenuti al rispetto delle misure tecniche ed organizzative atte alla periodica verifica delle attività compiute.

Gli incaricati esterni che hanno in gestione i sistemi di Regione del Veneto, dovranno essere individuati dall'azienda di appartenenza in qualità di Responsabile del trattamento, sulla base delle conoscenze e competenze di tipo tecnico, delle capacità relazionali e del grado di affidabilità e consapevolezza delle mansioni che andranno a svolgere. Tali risorse dovranno essere comunicate preventivamente alla Direzione ICT e Agenda Digitale ed aggiornate con cadenza annuale o sulla base di ogni evenienza.

I log di accesso di ciascun AdS deve essere registrato e conservato per almeno 6 mesi, con caratteristiche di completezza, integrità ed inalterabilità e deve comprendere anche i riferimenti temporali, la descrizione dell'evento e del sistema coinvolto.

Modalità di utilizzo e gestione delle caselle di posta elettronica "personali" ed "istituzionali"

La casella di posta elettronica regionale individualizzata con nome e cognome "personale", è legata all'account di dominio dell'utente con cui ne condivide la password. L'accesso a tali caselle è consentito secondo le seguenti modalità:

- a mezzo desktop tramite la modalità nativa dello strumento (browser web o client desktop);
- a mezzo dispositivo mobile di Regione Veneto, non personali, previa configurazione degli stessi da parte del supporto tecnico.

In entrambi i casi è abilitata l'autenticazione multifattore sulle impostazioni di sicurezza della casella stessa.

Le caselle di posta elettronica "**istituzionali**" (email condivise) non sono legate ad un account di dominio e pertanto vi si potrà accedere esclusivamente dalla propria casella "personale" tramite la modalità "*delegato*", ovvero senza la conoscenza della password di accesso.

Ad ogni Utente viene assegnato un determinato spazio in cloud per la memorizzazione dei messaggi di posta elettronica e/o dei file necessari allo svolgimento della propria attività lavorativa.

Esaurite le risorse messe a disposizione, l'Utente potrà ricevere o spedire messaggi solo dopo aver liberato spazio sufficiente attraverso la cancellazione dei messaggi di posta o la rimozione dei file memorizzati dallo spazio in cloud relativo.

I messaggi di posta elettronica cancellati potranno essere ripristinati dalla Direzione ICT e Agenda Digitale con cadenza giornaliera fino al limite tecnico temporale impostato dal fornitore del servizio stesso.

Nel caso in cui per il sistema di posta vengano adottate soluzioni tecniche diverse da quelle attualmente in uso presso l'Amministrazione regionale, l'individuazione delle relative istruzioni e il coordinamento delle attività correlate è demandata al Direttore della Direzione ICT e Agenda Digitale.

Si pone inoltre in evidenza quanto segue:

- l'email regionale deve essere utilizzata nel rispetto di quanto prescritto con DGR n. 863 del 31 marzo 2009 "Approvazione disciplina per l'utilizzo di posta elettronica, internet, telefoni e fax all'interno di Regione del Veneto" alla quale si rinvia;

- i messaggi di posta elettronica scambiati devono avere un impatto trascurabile sull'infrastruttura

informatica e telematica, per esempio riducendo l'eventuale presenza di allegati allo stretto necessario per espletare le necessità;

- l'utente deve cancellare i messaggi non più utili.

Si rammenta inoltre che al fine di contrastare il fenomeno dello "spamming" (ricezione di posta indesiderata) devono essere applicate le regole seguenti:

- cercare di limitare al massimo la diffusione dell'indirizzo email regionale su qualsiasi tipologia di risorsa Internet;
- non rispondere mai alle mail degli spammer, nemmeno per rimuovere il proprio nominativo dalla loro lista;
- non inviare o inoltrare catene telematiche. Se si dovessero ricevere messaggi di tal tipo non si devono in alcun caso attivare gli allegati di tali messaggi;
- utilizzare la funzionalità di segnalazione mittente, messaggio indesiderato o SPAM.

Indicazioni sulle annotazioni da inserire in calce alle email "personali" ed "istituzionali"

Come disposto nel citato "Disciplinare per l'utilizzo di Posta elettronica, internet, Telefoni e fax all'interno di Regione del Veneto" (Allegato alla DGR n. 863/2009), *"La Posta Elettronica, l'accesso alla rete Internet, i telefoni aziendali utilizzati dai Lavoratori, devono ritenersi normali strumenti di lavoro, forniti in dotazione dall'Amministrazione per lo svolgimento di attività lavorativa"*.

L'attuale sistema di posta elettronica è impostato in automatico per inserire in calce ai messaggi di posta inviati all'esterno del dominio regionale la seguente dicitura (sia in italiano che in inglese):

> *"Ai sensi del vigente D.Lgs. 196/2003 in materia di privacy e del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio si precisa che le informazioni contenute nel messaggio e negli eventuali allegati sono riservate esclusivamente al/ai destinatario/i indicato/i. Si invita ad astenersi dall'effettuare: inoltri, copie, distribuzioni e divulgazioni non autorizzate del presente messaggio e degli eventuali allegati. Nel caso di erroneo recapito, si chiede cortesemente a chi legge di dare immediata comunicazione al mittente e di cancellare il presente messaggio e gli eventuali allegati. Informazioni aggiuntive nella sezione **Privacy** del sito internet: www.regione.veneto.it"*

In aggiunta a ciò, al fine di addivenire ad una maggiore omogeneizzazione visiva della posta elettronica e in un'ottica di trasparenza e miglioramento del servizio reso alla cittadinanza, ciascun utente regionale dovrà inserire in firma ai messaggi inviati i propri dati identificativi *(logo regionale, nome e cognome,*

carica, struttura di riferimento, telefono fisso dell'ufficio) così come riportato nell'esempio seguente:

Nome Cognome
Direzione/Area di appartenenza
Direttore/Responsabile/Funzionario UO di appartenenza
tel. 041.xxx.xxx
email: nome.cognome@regione.veneto.it

Archiviazione della posta elettronica delle Segreterie degli Assessorati della Giunta regionale

In ordine alla necessità di archiviazione della posta elettronica delle Segreterie degli Assessorati della Giunta regionale, in seguito agli avvicendamenti conseguenti alle competizioni elettorali, risulta opportuno puntualizzare che a fronte della cessazione di ciascun Assessore, la relativa casella di posta istituzionale verrà mantenuta attiva fino all'insediamento del successore e per un periodo comunque non eccedente i **60 giorni** dalla sua cessazione.

Il nuovo Responsabile di Segreteria dell'Assessore, sarà temporaneamente abilitato da parte della Direzione ICT e Agenda Digitale, all'accesso alla precedente casella di posta elettronica istituzionale, al fine di consentire l'evasione di eventuali incombenze pendenti alla scadenza del precedente mandato.

Accesso remoto ai servizi regionali

L'accesso remoto ai servizi e agli applicativi regionali non esposti su rete internet è consentito solo ed esclusivamente agli utenti autorizzati previo l'utilizzo della piattaforma di Desktop Virtuale fornita dalla Direzione ICT e Agenda Digitale o attraverso nuove evoluzioni tecnologiche che saranno dalla stessa implementate.

Ogni Utente potrà accedere alla piattaforma suddetta utilizzando le proprie credenziali di dominio regionali in abbinata ad un secondo fattore di autenticazione (MFA) generato da App Authenticator autorizzate dalla Direzione ICT e Agenda Digitale da installarsi sul dispositivo smartphone o tablet aziendale o personale.

Qualora l'accesso alla piattaforma di Desktop Virtuale avvenga da un dispositivo personale non fornito dall'Amministrazione, al fine di prevenire l'intrusione e la diffusione di virus nei sistemi e nelle reti aziendali, è altamente consigliato mantenere aggiornato il sistema operativo del dispositivo stesso con le

ultime patch di sicurezza installate, nonché avere attivo ed aggiornato un sistema di antivirus/antimalware.

L'accesso da remoto ai servizi web, macchine Linux/UNIX e Windows ospitate nel Data Center regionale, è consentito esclusivamente per esigenze tecniche verificate ed autorizzate dalla Direzione ICT e Agenda Digitale mediante l'utilizzo di una connessione VPN (Virtual Private Network) con l'autenticazione multifattore (MFA) e puntualmente configurata.

3. Misure comportamentali

Tutti gli Utenti devono utilizzare le risorse ICT fornite dall'Amministrazione in maniera diligente, in modo appropriato, efficiente, rispettoso e per motivi lavorativi.

Nell'uso degli strumenti di comunicazione di proprietà dell'Amministrazione (ad es. posta elettronica con desinenza"... *@regione. veneto.it* ", telefoni regionali, servizi di comunicazione telematica, ecc.) gli Utenti sono tenuti a mantenere la correttezza e la gentilezza comunemente conosciute col termine di "*netiquette*".

Gli Utenti, inoltre, devono utilizzare le risorse ICT solamente per fini professionali (in relazione alle mansioni assegnate) e per conto dell'Amministrazione, evitando l'uso per attività non pertinenti o personali (come ad esempio la registrazione a siti di e-commerce, social network, siti di giochi *on line*, etc.)

Particolare cautela dev'essere posta, inoltre, nell'utilizzo di reti wifi libere o non conosciute per accedere ai servizi regionali, dal momento che l'operazione di accesso a tali servizi comporta l'inserimento di credenziali le quali potrebbero essere facilmente carpite da malintenzionati/hacker.

Gli Utenti non devono eseguire copie (anche parziali) di software protetto da leggi sul diritto d'autore che sia installato sui dispositivi forniti in uso dall'Amministrazione.

Gli Utenti sono inoltre tenuti a:

a) modificare periodicamente la password di accesso ai sistemi con cadenza almeno trimestrale rispettando le policy imposte dal Gestore;

b) non consentire ai browser web o alle applicazioni di memorizzare le password o altre informazioni di accesso;

c) non condividere o divulgare le proprie password a terzi e non archiviarle nei dispositivi (fissi o mobili) salvo utilizzando strumenti quali "password manager" con crittografia avanzata;

d) presidiare le risorse ICT assegnate al fine di evitare l'accesso a soggetti terzi non autorizzati che possano trafugare informazioni riservate in esse contenute;

e) effettuare la disconnessione del proprio account dalle PdL eventualmente condivise con altri utenti;

f) bloccare i dispositivi connessi alla rete nel caso in cui non possano essere presidiati, anche quando ci si allontana per brevi periodi;

g) non trasportare le postazioni di lavoro "fisse" al di fuori delle sedi dell'Amministrazione, salvo specifica autorizzazione;

h) mettere in sicurezza le postazioni di lavoro "mobili" assegnate qualora vengano lasciate in ufficio al di fuori dell'orario lavorativo (es. mediante cavo di sicurezza o sotto chiave in armadio);

i) procedere sempre allo spegnimento della postazione di lavoro al termine della giornaliera prestazione lavorativa, salvo particolari esigenze di servizio autorizzate dal Direttore di struttura o per ulteriori esigenze tecniche richieste dalla Direzione ICT e Agenda Digitale.

Uso delle postazioni di lavoro (PdL)

Le postazioni di lavoro (PdL) assegnate, offrono agli Utenti grandi potenzialità produttive. Tuttavia, ogni strumento informatico collegato alla rete dell' infrastruttura regionale potrebbe rappresentare una fonte di rischio per la sicurezza e la continuità operativa sia per l'utente stesso che per tutte le risorse ICT ad esso collegate. La Direzione ICT e Agenda Digitale mette a disposizione adeguati e aggiornati strumenti di protezione sulle PdL al fine di scongiurare i sempre crescenti rischi informatici. Tali strumenti tuttavia, richiedono una sempre più marcata collaborazione e responsabilizzazione da parte dell'utilizzatore abituale della risorsa che dovrà attenersi alle disposizioni riportate nel presente documento. Per "*Utente abituale*" si intende l'assegnatario della PdL come risulta registrato nell'inventario delle risorse in gestione dalla Direzione ICT e Agenda Digitale.

Sulla base dei suddetti presupposti e secondo le consuete logiche di razionalizzazione delle risorse ICT, sarà fornita una sola risorsa per utente, identificata come Desktop (fisso) o Laptop (mobile). Nei casi in cui l'utenza richieda una risorsa PdL di tipo Laptop in aggiunta a una di tipo Desktop, verrà adottato il Desktop Replacement (un laptop che funge anche da Desktop tramite le Docking Station sulla scrivania

dell'utente ma facilmente trasportabile altrove).

Gli Utenti **devono** applicare in modo scrupoloso le seguenti norme comportamentali e le specifiche procedure di seguito descritte:

- collegare il dispositivo assegnato, con frequenza **almeno settimanale,** alla rete intranet dell'Amministrazione per scaricare gli aggiornamenti di sicurezza rilasciati dalla Direzione ICT e Agenda Digitale (patch, hot fix, aggiornamenti antivirus, etc); qualora il dispositivo risulti non aggiornato o non più conforme alle vigenti impostazioni di sicurezza, la Direzione ICT e Agenda Digitale si riserva di **valutare la disconnessione temporanea** della PdL dal dominio regionale nelle more del suo ripristino tramite l'apertura di un ticket tramite il Call Center.

- segnalare ogni movimentazione, variazione, aggiornamento o prossima quiescenza dell'utilizzatore abituale della PdL regionale. Tali comunicazioni dovranno essere formalizzate con l'apposito modulo "move" reperibile nella intranet regionale, quindi firmate o vistate dal Direttore di appartenenza e comunicate al Call Center. In caso di movimentazione tra Direzioni, la comunicazione dovrà essere vistata dal Direttore della struttura originaria che ne convalida l'uscita (le PdL sostanzialmente "seguono" l'utenza, salvo casi espressamente motivati);

- salvare i file necessari allo svolgimento della propria attività lavorativa nelle cartelle di rete contenute all'interno di uno spazio a gestione centralizzata adeguatamente configurato dalla Direzione ICT e Agenda Digitale (NAS, Cloud, etc) per garantire riservatezza, integrità e disponibilità dei dati in esso contenuti. I dati memorizzati nel disco locale della propria PdL non sono sottoposti automaticamente a backup e potrebbero essere persi irrimediabilmente in caso di guasto hardware o accidentale cancellazione. Si rimanda al paragrafo "*Gestione dei data breach*" per maggiori approfondimenti.

- non lasciare mai incustoditi in aree pubbliche o quando si è in viaggio i dispositivi informatici assegnati o comunque contenenti dati di lavoro (PdL, Hard Disk, USB key, etc.). Tali dispositivi, infatti, potrebbero essere soggetti a smarrimento, furto, distruzione o compromissione dei dati, tentativi di frode e/o accesso non autorizzato ovvero essere "infettati" da virus. Si rimanda al paragrafo "*Gestione dei data breach*" per maggiori approfondimenti.

- non disabilitare le impostazioni di sicurezza preventivamente impostate dalla Direzione ICT e Agenda Digitale;

- non inserire chiavette USB o periferiche di archiviazione di massa (Hard Disk portatili) di dubbia provenienza o trovate in luoghi pubblici;

- non mettere oggetti sopra la PdL che possono compromettere l'integrità o la sua regolare aerazione;
- tenere lontano da tutte le strumentazioni informatiche liquidi e/o alimenti e anche fonti magnetiche;
- non mantenere abilitati protocolli insicuri di comunicazione, come ad es. il bluetooth, oltre il tempo strettamente necessario.

Modifiche delle risorse ICT

Tutte le risorse ICT assegnate ai dipendenti (PC fissi, laptop, tablet, smartphone, etc.) sono da considerarsi come strumenti di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza dell'intero sistema informativo regionale.

Per tale motivo nessuna modifica *hardware* o manomissione è consentita sulle stesse da parte degli utilizzatori assegnatari.

Per quanto riguarda le modifiche *software,* gli Utenti utilizzatori delle risorse ICT non devono alterare la configurazione originaria del dispositivo ricevuto in uso (ad es. disinstallando, eseguendo o installando applicazioni che interferiscano sul funzionamento del dispositivo medesimo) al fine di non compromettere gli standard di sicurezza impostati dalla Direzione ICT e Agenda Digitale. Sono fatte salve le personalizzazioni a livello Utente che non abbiano conseguenze negative sulla funzionalità e la sicurezza dei dispositivi stessi, nonché sui dati in essi contenuti.

Qualsiasi software non autorizzato sarà considerato come una violazione delle policy regionali sulla sicurezza informatica e l'assegnatario della PdL sarà individuato come responsabile per eventuali danni causati dall'applicativo non autorizzato al sistema informatico di Regione Veneto o alla riservatezza, integrità e disponibilità dei dati personali di cui l'Ente è titolare o responsabile.

Eventuali richieste di installazione di software aggiuntivo a quello in dotazione, dovranno essere rivolte al Call Center il quale ne provvederà all'installazione (previa verifica della disponibilità delle relative licenze) qualora il software risulti già tra quelli autorizzati dalla Direzione ICT e Agenda Digitale, altrimenti lo stesso Call Center provvederà ad inoltrare la richiesta agli uffici di competenza per le verifiche del caso.

Smarrimento/furto delle risorse ICT

Nei casi di smarrimento, furto o grave manomissione dei dispositivi assegnati o del loro contenuto, gli Utenti devono segnalare tempestivamente l'accaduto, entro 12 ore ai soggetti di seguito indicati:

- *Call Center* dell'Assistenza informatica, per l'eventuale blocco dell'uso delle risorse ICT;
- Direttore della Direzione ICT e Agenda Digitale, per la valutazione su eventuali azioni sul blocco o ripristino dei dati ad esso associati;

La Struttura in cui si è verificato il fatto di presunto reato, provvederà a redigere una relazione degli accadimenti rilevati, con la descrizione dei danni subiti, eventualmente ricostruiti anche dalle testimonianze che invierà tempestivamente, e comunque non oltre le 24 ore dal fatto, con nota protocollata alla:

- Direzione Gestione del Patrimonio, per la valutazione su eventuali azioni a tutela della proprietà regionale e sul ripristino dei danni subiti al patrimonio;
- Direzione Acquisti e AA.GG. per l'attivazione delle opportune coperture assicurative a tutela delle proprietà regionali in virtù delle polizze stipulate.

Il Dirigente della Direzione Acquisti e AA.GG., o suo delegato, per i fatti accaduti all'interno della provincia di Venezia, provvederà, entro le 48 ore successive agli eventi, o alla loro scoperta, a presentare formale denuncia alla Polizia Giudiziaria (Polizia di Stato, Carabinieri, etc.) competente per territorio. Per i fatti accaduti al di fuori della provincia di Venezia, sarà invece il Dirigente regionale della sede in cui si è verificato l'evento a provvedere alla presentazione della denuncia alla Polizia Giudiziaria competente per territorio.
Nel caso in cui si presupponga con l'accaduto una perdita di riservatezza, integrità e/o disponibilità dei dati personali contenuti all'interno del dispositivo smarrito o rubato, si rimanda al paragrafo "**Gestione dei data breach**" per una corretta gestione dell'evento.

4. Gestione della telefonia mobile

La struttura regionale a cui compete il servizio di telefonia mobile è la Direzione ICT e Agenda Digitale che, anche attraverso il supporto fornito dal Gestore di telefonia mobile, svolge le seguenti attività:

- monitoraggio e controllo della spesa telefonica;
- individuazione e classificazione delle diverse tipologie di dispositivi, dei relativi accessori e dei servizi di telefonia mobile annessi;
- attivazione, disattivazione, MNP e sospensione delle "*SIM card*";
- consegna, configurazione, personalizzazione, assistenza e manutenzione secondo le clausole contenute nel contratto di affidamento del servizio di telefonia mobile al Gestore del servizio stesso;
- aggiornamento tecnologico dei dispositivi di telefonia mobile;
- ritiro dei dispositivi di telefonia mobile;
- gestione del rapporto contrattuale con il Gestore di telefonia mobile.

Dispositivi di telefonia mobile assegnabili

La Direzione ICT e Agenda Digitale procede all'assegnazione dei dispositivi di telefonia mobile in base alla disponibilità, al momento del ricevimento della richiesta, di terminali previsti per la categoria di appartenenza dell'Utilizzatore, come da contratto sottoscritto con il Gestore di telefonia mobile. Ciascuna assegnazione è vincolata al rispetto dei limiti di spesa previsti per l'erogazione del servizio di telefonia mobile.

Iniziative/Progetti che necessitano l'impiego di servizi di telefonia mobile

Le strutture regionali che intendono avviare iniziative/progetti che necessitano l'impiego di servizi e/o di dispositivi di telefonia mobile al di fuori delle dotazioni standard previste nel contratto sottoscritto con il gestore di telefonia mobile, devono inserire nel proprio budget di progetto i relativi costi da sostenere.

A titolo esemplificativo e non esaustivo, i costi relativi alla telefonia mobile da prevedere sono: l'acquisizione degli apparati, la loro gestione/manutenzione, i canoni, il traffico voce/dati, i servizi attivati, ecc.

La Direzione ICT e Agenda Digitale potrà fornire un supporto tecnico alle Strutture regionali che ne faranno richiesta.

Dispositivi di telefonia mobile utilizzati per monitoraggio e tele allarmi

L'assegnazione delle "*Sim Card*" e/o "*apparati mobili"* da utilizzare per i servizi di monitoraggio e/o di tele-allarme o per funzionalità analoghe, avviene secondo le modalità descritte al paragrafo *"Richiesta di assegnazione di dispositivi di telefonia mobile"*.

Il Direttore della Struttura regionale richiedente assume ogni responsabilità conseguente all'uso delle "*Sim Card*" e/o "*apparati mobili"* assegnate e - su richiesta della Direzione ICT e Agenda Digitale - dovrà fornire periodicamente l'elenco delle "*Sim Card*" e/o "*apparati mobili"* assegnate ed installate sui sistemi di monitoraggio e di tele-allarme.

Richiesta di assegnazione di dispositivi di telefonia mobile

Fermo restando quanto previsto ai paragrafi "*Dispositivi di telefonia mobile assegnabili"* e "*Iniziative/Progetti che necessitano l'impiego di servizi di telefonia mobile"*, la richiesta di assegnazione dei dispositivi di telefonia mobile da presentare alla Direzione ICT e Agenda Digitale deve avere una delle seguenti motivazioni:

- svolgimento di incarichi che richiedono la rintracciabilità dell'Utilizzatore;
- comprovate esigenze di reperibilità dell'Utilizzatore;
- attribuzione all'Utilizzatore di compiti in settori "critici", quali ad esempio: la sicurezza della popolazione, il presidio e monitoraggio del territorio e delle infrastrutture di proprietà regionale nonché l'organizzazione sanitaria;
- esigenza temporanea dell'Utilizzatore dovuta ad incarichi e/o missioni in Italia e/o all'estero;
- esigenza manifestata da una Struttura regionale della fornitura di "*SIM Card*" e/o "*apparati mobili"* necessarie per servizi di monitoraggio del territorio e/o servizi di "allarme" da installare su apparati di proprietà regionale;
- ulteriori esigenze oggetto di valutazione da parte delle Strutture di appartenenza.

La richiesta di assegnazione di dispositivi di telefonia mobile, indirizzata al Direttore della Direzione ICT e Agenda Digitale, pena il mancato accoglimento, deve:

- essere sottoscritta: dal Direttore di U.O. con il visto del Direttore di Direzione o dal Direttore di Area; oppure dal Direttore della Direzione o di Area di appartenenza dell'Utilizzatore o Assegnatore;
- indicare il cognome, il nome, il numero di matricola, il ruolo e/o il livello d'inquadramento nell'Organizzazione regionale del richiedente e, per i collaboratori, l'indicazione e la durata del rapporto contrattuale intrattenuto con l'Amministrazione regionale;

- indicare la motivazione della richiesta con una breve descrizione dell'attività e della durata di utilizzo del dispositivo;
- indicare la categoria e la classe di abilitazione del dispositivo previste ai paragrafi *"Categorie di dispositivi di telefonia mobile"* e *"Classi di abilitazione"*.

Categorie di dispositivi di telefonia mobile

I dispositivi di telefonia mobile forniti dal Gestore a seguito della sottoscrizione del contratto di affidamento del servizio di telefonia mobile appartengono alle seguenti categorie: ***Top***, ***Base***, ***Tablet*** e ***Modem Wi-Fi 4G/5G***.

Il criterio di assegnazione dei dispositivi di telefonia mobile adottato è il seguente:

a) Categoria ***Top*****:**

- Segretario Generale della Programmazione;
- Segretario della Giunta regionale;
- Direttore della Direzione del Presidente;
- Direttori d'Area ed equiparati.

b) Categoria ***Base*****:**

- Responsabile della Segreteria particolare del Presidente, della Segreteria particolare del Vice-presidente, delle Segreterie particolari degli Assessori e della Segreteria del Direttore della Presidenza;
- Direttore di Direzione, di Unità Organizzative e di Strutture di Progetto;
- dipendente o collaboratore dell'Amministrazione regionale;
- Assegnatore o Utilizzatore che abbia motivate esigenze ai sensi del paragrafo "*Richiesta di assegnazione di dispositivi di telefonia mobile"* del presente documento.

c) Categoria ***Tablet*****:**

- Segretario Generale della Programmazione;
- Segretario della Giunta regionale;
- Direttore della Direzione del Presidente;
- Direttori d'Area ed equiparati;
- dipendenti regionali (su autorizzazione dei rispettivi Direttori d'Area).

d) Categoria ***Modem Wi-Fi 4G/5G*****:**

- Assegnatore o Utilizzatore con motivate esigenze.

Classi di abilitazione

L'abilitazione delle utenze voce/dati all'estero, varia a seconda del paese:

- Naz+SEE
- Extra UE

Salvo specifiche richieste protocollate (a firma del Direttore U.O. con visto del Direttore di Direzione e/o Area; a firma del Direttore di Direzione e/o Area) le abilitazione Extra UE sono riservate alle seguenti nomine apicali:

- Segretario Generale della Programmazione;
- Segretario della Giunta Regionale;
- Direttore della Direzione del Presidente;
- Direttori d'Area ed equiparati;
- Responsabile della Segreteria particolare del Presidente, della Segreteria particolare del Vice-presidente, delle Segreterie particolari degli Assessori e della Segreteria del Direttore della Presidenza;
- Assegnatore o Utilizzatore con motivate esigenze.

I restanti Utilizzatori sono abilitati al traffico voce/dati Naz+SEE.

Eventuali temporanee abilitazioni al traffico voce/dati Extra UE, devono essere richieste preventivamente con congruo anticipo alla Direzione ICT e Agenda Digitale, secondo le modalità descritte al paragrafo *"Richiesta di assegnazione di dispositivi di telefonia mobile"*, indicando nella richiesta la destinazione ed il periodo di permanenza.

Aggiornamento tecnologico

Periodicamente la Direzione ICT e Agenda Digitale provvede all'aggiornamento tecnologico dei dispositivi di telefonia mobile, comunicando preventivamente alle Strutture regionali interessate il piano degli interventi.

Qualora, per cause imputabili all'Utilizzatore o Assegnatore entro i termini comunicati non sia possibile effettuare l'aggiornamento tecnologico, la responsabilità del mancato aggiornamento sarà in capo a quest'ultimo.

A seguito della comunicazione inviata dalla Direzione ICT e Agenda Digitale, i Direttori di Direzione devono far pervenire a quest'ultima gli elenchi di "Utenze" per servizi di monitoraggio del territorio e/o servizi di "allarme".

Nel caso di mancato aggiornamento imputabile all'Utilizzatore o Assegnatore ovvero di mancato invio degli elenchi di "Utenze" per servizi di monitoraggio del territorio e/o servizi di "*allarme*", trascorso un

congruo periodo di tempo la Direzione ICT e Agenda Digitale procede a disabilitare temporaneamente le "Utenze" fino a quando non avrà ricevuto riscontro.

L'aggiornamento tecnologico sarà effettuato dalla Direzione ICT e Agenda Digitale compatibilmente con le risorse e le tecnologie disponibili.

Responsabilità e modalità di utilizzo dei dispositivi

L'Utilizzatore o Assegnatore del dispositivo di telefonia mobile è custode del bene regionale dal momento della consegna fino alla sua restituzione. E' responsabile del suo corretto utilizzo e del rispetto di quanto previsto dal presente documento nonché del "*Disciplinare per l'utilizzo di: Posta Elettronica, Internet, Telefoni e Fax, all'interno di Regione del Veneto*" approvato con DGR n. 863 del 31/03/2009.

L'Utilizzatore o Assegnatore è tenuto a custodire con la diligenza del "buon padre di famiglia" il dispositivo ricevuto, onde evitare eventuali danni, smarrimenti o sottrazioni. L'Utilizzatore o Assegnatore non può cedere in uso a terzi, a nessun titolo, il dispositivo di telefonia mobile ricevuto.

L'Utilizzatore o Assegnatore deve servirsi del dispositivo ricevuto in modo responsabile ai fini del contenimento delle spese sostenute dall'Amministrazione regionale.

L'uso "collettivo" del dispositivo (nel senso: *"da parte di più utilizzatori"*) è consentito solo se richiesto dall'Assegnatore all'atto della richiesta di assegnazione presentata alla Direzione ICT e Agenda Digitale. E' in capo all'Assegnatore la responsabilità di vigilare sull'uso del dispositivo. I dispositivi assegnati devono essere restituiti alla Direzione ICT e Agenda Digitale, anche se non più utilizzabili.

Al fine di proteggere i dati che potrebbero essere contenuti sui dispositivi di telefonia mobile, nonchè evitare l'accesso ai servizi dell'Amministrazione regionale attraverso le App di posta elettronica, drive, messaggistica, ecc. installate di default dall'Ufficio Telefonia Mobile e su cui sono memorizzate le credenziali dell'Utilizzatore, è fatto obbligo l'inserimento di uno o più sistemi di blocco del dispositivo stesso (pin, segno grafico, riconoscimento del viso o impronta digitale).

L'Utilizzatore o l'Assegnatore a nessun titolo può trattenere i dispositivi, anche se sostituiti per aggiornamento tecnologico previsto contrattualmente con il Gestore del servizio di telefonia mobile in essere.

Salvo motivate richieste, da valutare a cura della Direzione ICT e Agenda Digitale, sui dispositivi assegnati non è consentito:

- installare qualsiasi tipo di software, se non preventivamente autorizzato dalla Direzione ICT e Agenda Digitale;

- modificare autonomamente le configurazioni e impostazioni di sistema senza la preventiva autorizzazione della Direzione ICT e Agenda Digitale;
- utilizzare *SIM card "diverse"* (nel senso: "*non assegnate dall'Amministrazione regionale*") con dispositivi assegnati e di proprietà dell'Amministrazione regionale.

La Direzione ICT e Agenda Digitale non fornisce assistenza tecnica ai dispositivi mobili personali anche se su di essi sono installate le "*Sim Card*" regionali.

Chiamate per uso personale

E' facoltà di ciascun Utilizzatore, stipulare un contratto personale con il fornitore del servizio di telefonia mobile regionale. Tale contratto personale consentirà all'Utilizzatore di evidenziare e pagare le proprie telefonate/SMS/MMS personali. Le modalità per la stipula del contratto con le relative tariffe sono esplicate all'interno del portale "Ufficio Telefonia Mobile" presente nella scheda Servizi dell'Intranet regionale.

L'Amministrazione regionale, non fornisce assistenza per le chiamate personali, in quanto l'Utilizzatore stipula un contratto personale con il fornitore del servizio di telefonia mobile regionale

Richiesta tabulati telefonici

La Direzione ICT e Agenda Digitale non fornisce tabulati telefonici.

Smarrimento/furto del dispositivo

In caso di smarrimento, furto accertato o grave manomissione dei dispositivi assegnati o dei loro contenuti, l'Utilizzatore o l'Assegnatore è tenuto ad attenersi a quanto indicato al paragrafo *"Smarrimento/furto delle risorse ICT"* per quanto concerne le modalità di presentazione della denuncia nonché a segnalare tempestivamente l'accaduto direttamente alla Direzione ICT e Agenda Digitale ovvero - qualora gli uffici dell'Amministrazione regionale fossero chiusi - all'assistenza del Gestore del servizio di telefonia mobile al fine di sospendere la "*SIM Card*".

Alla ricezione della comunicazione di cui sopra, la Direzione ICT e Agenda Digitale provvederà a contattare l'Utilizzatore/Assegnatore per il blocco dei dispositivi e per la sostituzione della *"SIM Card"*, provvedendo all'assegnazione di un nuovo dispositivo entro 15 giorni (previa disponibilità).

Smarrimento codice personale di accesso ai dispositivi di telefonia mobile

Nel caso di riscontrata impossibilità di accesso ai predetti dispositivi a causa dello smarrimento del codice personale di accesso, ciascun Utilizzatore/Assegnatore dovrà darne comunicazione scritta alla Direzione ICT e Agenda Digitale entro **7** gg dall'evento.

Successivamente gli addetti dell'ufficio Telefonia Mobile contatteranno l'Utilizzatore/Assegnatore per concordare un appuntamento per la restituzione del vecchio apparato e la contestuale consegna e configurazione di un nuovo apparato.

Rilevazione e verifica costi

La Direzione ICT e Agenda Digitale determina il budget di spesa annuale del servizio di telefonia mobile regionale, sulla base delle disponibilità economiche previste dal bilancio di competenza e, comunque, nel rispetto di quanto indicato nel contratto in essere con il Gestore di telefonia mobile.

Periodicamente la Direzione ICT e Agenda Digitale monitora i consumi ed il trend di spesa sostenuti dalle utenze appartenenti alle singole Strutture Regionali per verificarne la compatibilità con il budget di spesa.

Assistenza tecnica e manutenzione

L'assistenza e la manutenzione dei dispositivi, così come previste dal contratto sottoscritto con il Gestore di telefonia mobile sono garantite e prestate presso la sede della Direzione ICT e Agenda Digitale, esclusivamente su apparati e dispositivi assegnati da quest'ultima.

L'Utilizzatore o l'Assegnatore in caso di malfunzionamenti o guasti al dispositivo deve contattare la Direzione ICT e Agenda Digitale e, previo appuntamento, recarsi presso gli uffici di quest'ultima per avere assistenza ed effettuare i necessari interventi.

La Direzione ICT e Agenda Digitale non può prendere in carico i dispositivi mobili acquisiti dalle Strutture regionali in quanto non sono oggetto del contratto sottoscritto con il Gestore di telefonia mobile.

Restituzione dei dispositivi

La detenzione e l'uso dei dispositivi di telefonia mobile assegnati è giustificata dal mantenimento dei requisiti al momento della presentazione della richiesta alla Direzione ICT e Agenda Digitale (paragrafo *"Richiesta di assegnazione di dispositivi di telefonia mobile"*). A titolo esemplificativo e non esaustivo si intendono incompatibili all'ulteriore detenzione e/o uso dei dispositivi le seguenti situazioni:

- cessazione del rapporto di lavoro dipendente e/o della condizione di lavoratore come definita nel presente documento;

- comando "*in uscita*" o trasferimento del dipendente presso struttura diversa da quella che ha effettuato la richiesta di assegnazione;
- termine delle esigenze temporanee dovute ad incarichi e/o missioni in Italia e/o all'estero.

Qualora l'Utilizzatore o l'Assegnatore (trasferito presso una struttura regionale diversa da quella che ha richiesto l'assegnazione dei dispositivi) intenda mantenere la dotazione di telefonia mobile assegnata, entro e non oltre 15 giorni dalla data del trasferimento stesso, pena la disabilitazione dell'utenza, deve comunicarlo alla Direzione ICT e Agenda Digitale presentando formale richiesta secondo le modalità descritte al paragrafo *"Richiesta di assegnazione di dispositivi di telefonia mobile"* del presente documento.

Portabilità

Alla cessazione della condizione di lavoratore, come definita nel presente documento, qualora la struttura di appartenenza non esprima parere negativo, l'Utilizzatore può chiedere alla Direzione ICT e Agenda Digitale di mantenere la sola Utenza (cd. "portabilità" del numero), fermo restando la restituzione dell'apparato di telefonia mobile e dei relativi accessori.

Gli Utilizzatori provenienti da Enti diversi dall'Amministrazione regionale che assumono la condizione di lavoratore (come definita nel presente documento), possono chiedere alla Direzione ICT e Agenda Digitale di intestare la propria utenza all'Amministrazione regionale (cd. "*portabilità in entrata*") seguendo le modalità descritte al paragrafo *"Richiesta di assegnazione di dispositivi di telefonia mobile"* del presente documento.

Disposizioni particolari per i collaboratori ed il personale esterno

I dispositivi di telefonia mobile di proprietà regionale possono essere assegnati a collaboratori e/o personale "esterno" all'Amministrazione regionale, previa richiesta del Direttore della struttura regionale a cui quest'ultimi afferiscono e/o collaborano, secondo le modalità descritte al paragrafo *"Richiesta di assegnazione di dispositivi di telefonia mobile"* del presente documento. In tal caso l'Assegnatario è il Direttore della Struttura regionale competente, mentre l'Utilizzatore è il collaboratore o soggetto esterno.

La responsabilità dell'utilizzo dei dispositivi di telefonia mobile è in capo all'Utilizzatore, restando all'Assegnatario la responsabilità di vigilare sull'uso del predetto dispositivo.

5. Violazioni e tutela legale

L'eventuale violazione delle norme e/o delle buone regole di comportamento indicate nel presente documento può comportare responsabilità civile, penale e disciplinare.

6. Entrata in vigore, pubblicità ed aggiornamento

Le regole contenute nel presente documento entrano in vigore dalla data di adozione del provvedimento di approvazione.

Del presente Regolamento sarà fornita massima pubblicità mediante la diffusione sull'Intranet dell'Ente.

Il presente Regolamento sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi dell'Ente o in caso di mutazioni legislative.

Ogni variazione sarà prontamente comunicata agli utenti.

APPENDICE

Tipologia di Dati

Il patrimonio informativo e di conoscenza detenuto dall'Amministrazione si suddivide in due macro-aree:

- i dati personali;
- i dati (*riservati o non riservati*) diversi da quelli personali.

Le due fattispecie necessitano di trattamenti peculiari, fatte salve le più generali cautele e misure di sicurezza descritte a proposito dei dispositivi come più sopra indicato.

I dati personali

Per quanto riguarda i dati personali si rinvia alle citate "*Istruzioni per i trattamenti di dati personali*", approvate con DGR n. 596 del 08/05/2018.

Si ricorda, ad ogni modo, che all'atto della dismissione di supporti che contengano dati personali è necessario distruggere o rendere inutilizzabili (*cancellandone il contenuto*) i supporti medesimi, secondo quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 13/10/2008 sui "*Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali"* (doc. web n. 1571514).

I dati diversi da quelli personali

Fatto salvo il requisito dell'Integrità, i dati diversi da quelli personali sono classificati in base al livello di Confidenzialità (*Confidentiality*) come segue:

- dati riservati;
- dati non riservati.

La predetta classificazione è generalmente effettuata dal Direttore della struttura che genera o gestisce i dati medesimi.

Dati riservati

Appartengono a questa categoria i dati a cui siano collegati interessi giuridicamente rilevanti (come ad es. la proprietà industriale, il diritto d'autore e i segreti commerciali).

La gestione, trasmissione e condivisione dei dati riservati deve essere sottoposta a particolari cautele e misure, stabilite dal soggetto responsabile, al fine di preservare la confidenzialità dei dati medesimi.

L'eventuale manutenzione, effettuata da partner privati, sui sistemi ed apparati che ospitano dati riservati deve essere disciplinata, a livello contrattuale, prevedendo specifici obblighi di riservatezza a carico dei partner privati.

Dati non riservati

Appartengono a questa categoria: i dati il cui accesso e/o utilizzo non ha restrizioni (ad es. gli "*Open Data*", i dati oggetto di "accesso civico", ecc.).

Contesto normativo di riferimento

Il presente documento si inserisce nel seguente quadro normativo:

- Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- D.Lgs. n. 196 del 30/06/2003 *(c.d. Codice Privacy)*, adeguato al predetto Regolamento 2016/679/UE con D.Lgs. n. 101 del 10/08/2018;
- Provvedimenti del Garante per la protezione dei dati personali in materia di *"misure di sicurezza"*, in particolare con riguardo agli Amministratori di Sistema *(Provvedimento generale del 27/11/2008 e s.m.i)*;
- Linee guida del Garante per posta elettronica ed internet (Provvedimento del 10/03/2007);
- Misure Minime di Sicurezza ICT per la Pubblica Amministrazione" emesse in data 26/06/2016 da AgID;
- DGR n. 596 del 08/05/2018 che ha approvato le *"Istruzioni per i trattamenti di dati personali*;
- DGR n. 863 del 31/03/2009 che ha approvato il *"Disciplinare per l'utilizzo di: Posta Elettronica, Internet, Telefoni e Fax, all'interno di Regione del Veneto"*.
- DGR 3176 del 27 ottobre 2009 che definisce e approva gli Standard Regionali Informatici (SIRV) redatti dalla Direzione ICT a Agenda Digitale, dando mandato alla stessa per il loro governo e aggiornamento e vincolando tutte le strutture regionali al loro rispetto;
- DGR n. 1189 del 31 agosto 2021 che ha approvato la "Modifica della composizione del "Gruppo di Lavoro GDPR" di cui alla DGR n. 596 dell'8 maggio 2018. Regolamento 2016/679/UE del Parlamento Europeo e del Consiglio del 27 aprile 2016, "General Data Protection Regulation" (GDPR);

Definizioni

Le risorse ICT

Nel presente documento con il termine *"risorse ICT"* si intende:

- il patrimonio informativo in formato elettronico detenuto dall'Amministrazione regionale;
- i servizi informatici erogati direttamente o per conto dall'Amministrazione;
- le postazioni di lavoro "fisse" *(PC desktop e simili)* e "mobili" *(PC portatili e simili);*
- i dispositivi di telefonia mobile (smartphone, *tablet, modem 4G/5G)*;
- i software e gli strumenti di produttività e di collaboration in cloud;
- il software per l'accesso remoto alle risorse aziendali;
- i server, gli apparati ed in generale tutto il materiale hardware.

Gli Utenti

Il termine "Utenti" si riferisce ai seguenti soggetti:

- i direttori e i dipendenti, a qualsiasi titolo inseriti nell'organizzazione regionale, senza distinzione di ruolo e/o livello;
- i consulenti e i collaboratori dell'Amministrazione regionale, a prescindere dal rapporto contrattuale intrattenuto con la stessa;
- i dipendenti e i collaboratori di società che hanno un contratto in essere con l'Amministrazione regionale e che utilizzano le risorse ICT dell'Amministrazione medesima;
- gli ospiti dell'Amministrazione regionale, per l'eventuale uso delle risorse ICT dell'Amministrazione medesima *(ad es. rete wifi)*;
- il personale di Enti e di Agenzie regionali collegato alla rete dell'Amministrazione regionale, per quanto applicabile.

La telefonia mobile

Per lo specifico ambito della telefonia mobile si applicano le seguenti definizioni:

A. **Dispositivo di telefonia mobile**: "*smartphone*", "*tablet*", "*SIM card*", *"Modem 4G/5G"* ed eventuali accessori;
B. **Utenza**: informazioni tecniche di accreditamento *(credenziali)* con le quali il dispositivo di telefonia mobile è riconosciuto ed accettato sulla "rete mobile";
C. **Gestore di telefonia mobile**: soggetto affidatario dell'incarico del servizio di telefonia mobile

regionale da parte dell'Amministrazione regionale;

D. **Lavoratore**: dipendente o direttore/dirigente senza distinzione di ruolo e/o di livello, a qualsiasi titolo inserito nell'Organizzazione regionale;

E. **Assegnatore**: lavoratore che per il ruolo che riveste nell'Organizzazione regionale ha l'autorità di richiedere ed assegnare uno o più dispositivi di telefonia mobile;

F. **Collaboratore**: soggetto che concorre a svolgere l'attività lavorativa a prescindere dal rapporto lavorativo intrattenuto con l'Amministrazione regionale;

G. **Utente/Utilizzatore**: lavoratore o collaboratore che riceve in uso uno o più dispositivi di telefonia mobile;

H. **Naz+SEE**: "*SIM card*" abilitata al traffico voce/dati nazionale e al traffico voce/dati nei paesi che aderiscono allo Spazio Economico Europeo;

I. **Extra UE**: tutti i paesi che non aderiscono allo Spazio Economico Europeo;

J. **MNP:** Mobile Number Portability ovvero portabilità della numerazione mobile in ingresso e/o uscita dall'Amministrazione regionale.