REGIONE DEL VENETO

giunta regionale

Direzione ICT e Agenda Digitale

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

Misure organizzative, tecniche e comportamentali

a551ee1b

INDICE

a551ee1b

1 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. 1677 del 26/10/2016 e descrive i criteri e le regole che disciplinano l'assegnazione e l'uso dei dispositivi di telefonia mobile di proprietà dell'Amministrazione regionale.

2 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;
- DGR n. 596 del 08/05/2018 che ha approvato le *"Istruzioni per i trattamenti di dati personali*;

- 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);
- 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"*.

3 Definizioni

3.1 Le risorse ICT

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

- il patrimonio informativo in formato elettronico detenuto dall'Amministrazione regionale come definito al successivo paragrafo 7;
- 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;
- i software di messaggistica istantanea (come ad esempio "messenger" o similari);
- i server, gli apparati ed in generale tutto il materiale hardware.

3.2 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.

3.3 La telefonia mobile

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

a) **Dispositivo di telefonia mobile**: telefono cellulare, "smartphone", "tablet", "SIM card", "Internet Key" 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.

4 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.

5 Ambito di applicazione

Il presente documento è rivolto agli "Utenti" definiti ai precedenti paragrafi 3.2. e 3.3.

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.

6 Regole per l'uso delle risorse ICT

6.1 Introduzione

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 4, 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.

6.2 Misure organizzative

La Giunta regionale con DGR n. 596 del 08/05/2018, 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».*

6.2.1 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 ospitati.

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, l'utente dovrà segnalare l'evento al Direttore della struttura regionale di riferimento/appartenenza ed al Direttore della Direzione ICT e Agenda Digitale.

6.2.2 Gestione dei "databreach"

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. "**databreach**"), l'utente provvede a segnalare tempestivamente la situazione al **Call Center** per l'espletamento delle verifiche di cui al punto 6.2.1 e comunica al "Delegato" al trattamento (Direttore della struttura regionale di riferimento/appartenenza) le violazioni ai dati personali rilevate 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 personal*i"* approvate con DGR n. 596/2018, a cui si rinvia. Pertanto ogni Delegato, non appena venuto a conoscenza di un databreach, effettuerà una prima necessaria istruttoria e, valutati i rischi per i diritti e le libertà delle persone fisiche, avviserà tempestivamente la Direzione ICT e Agenda Digitale ed il Data Protection Officer.

A sua volta il Direttore della Direzione ICT e Agenda Digitale, sulla base degli esiti della predetta istruttoria del Delegato, comunicherà al Garante per la Protezione dei dati personali il databreach, per conto del Titolare del trattamento senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, informandone contestualmente il Data Protection Officer.

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, procederà secondo le prescrizioni sopra riportate contenute nelle "Istruzioni per i trattamenti di dati personali" approvate con DGR n. 596/2018.

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 della procedura sopra descritta.

6.2.3 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 del 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 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 dagli utilizzatori;
- gestione del rapporto contrattuale con il Gestore di telefonia mobile.

6.3 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 - ognuno per la parte 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), ferme restando le responsabilità in capo alla Direzione ICT e Agenda Digitale per quanto riguarda l'adozione, gestione ed implementazione delle soluzioni tecnico-informatiche atte a prevenire e contrastare i rischi connessi alla sicurezza informatica (cd. cyber-security) correlati alla protezione dei dati personali, con funzioni gestionali ed operative.

6.3.1 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.

La Direzione ICT e Agenda Digitale, su richiesta, può fornire supporto al "Delegato" al trattamento affinché possa identificare e valutare i possibili rischi insiti nel trattamento dei dati sia per gli interessati che per l'Amministrazione regionale e per prevedere le idonee misure tecnico-organizzative atte a garantire che i dati siano trattati nel rispetto del Regolamento n. 679/2016/UE (GDPR).

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.

Inoltre, la Direzione ICT e Agenda Digitale - su richiesta del "Delegato" al trattamento - può fornire supporto nell'individuare le idonee misure tecniche da adottare:

- nella progettazione, implementazione e sviluppo di nuove soluzioni software attraverso l'affidamento a fornitori esterni;
- nell'identificazione di "service provider" di servizi in "cloud" in grado di offrire garanzie circa il rispetto del Regolamento n. 679/2016/UE (GDPR).

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).

6.3.2 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.
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).

6.3.3 Autenticazione utenti

L'accesso a tutti i servizi deve avvenire previa procedura di autenticazione.
Gli Utenti devono essere identificati e ricevere dal gestore del servizio delle credenziali individuali, univoche e "robuste" (nome utente e password), le quali devono essere mantenute riservate e custodite con cura. Ogni password dev'essere associata esclusivamente ad un unico soggetto identificato.
Le credenziali, laddove utilizzate, non possono essere assegnate ad altri Utenti, neppure in tempi diversi. Le credenziali non utilizzate da almeno tre mesi sono disabilitate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

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).
Gli Utenti devono proteggere le credenziali memorizzate sugli smartphone, utilizzate per fruire dei servizi dell'Amministrazione regionale (ad es. posta elettronica, intranet, ecc.) e, nel caso di furto o smarrimento dello smartphone medesimo, sia esso personale o dell'Amministrazione

regionale, devono cambiare tempestivamente la "password del dominio" regionale.

6.3.4 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.

6.3.5 Sicurezza dei server

I gestori di server devono configurare i server medesimi conformemente agli standard di sicurezza e/o best practices (ad es. abilitare soltanto i servizi strettamente necessari, applicare sistematicamente le "pacth", ecc.) emessi da Enti ed Organizzazioni internazionali (ad es. International Standard Organization - ISO, National Institute of Standards and Technology - NIST, Sans Institute, ecc.)

Laddove le strutture si avvalgano di propri fornitori, dovranno prevedere nei contratti d'appalto l'obbligo di rispettare i predetti standard di sicurezza e, inoltre, dovranno prevedere 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.

6.3.6 Sicurezza delle applicazioni

Nell'attività di progettazione, implementazione, sviluppo, selezione e utilizzo di nuove soluzioni software da parte delle Strutture regionali dev'essere garantito il rispetto:

a) 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 pubblicati nella rete intranet;

b) dei principi di "privacy by design" e "privacy by default", implementando sia le misure a tutela della privacy nel corso del ciclo di vita delle applicazioni che, per le applicazioni "web-based", le best practices emesse dall'Organizzazione internazionale *"Open Web* Applica*tion Security Project (OWASP)"*.

Il rispetto delle medesime prescrizioni di cui ai precedenti punti a) e b) dev'essere altresì previsto, nei relativi contratti d'appalto, dalle strutture regionali che affidino a un fornitore l'incarico di sviluppare soluzioni software. Peraltro è necessario, con riferimento al precedente punto b, prestare analoga attenzione anche nel caso di applicazioni acquistate sul mercato (c.d. applicazioni «COTS» *"Commercial Off*-the-Shelf *component").*

6.3.7 Sicurezza della rete

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 e con strumenti e livelli di protezione (ad es. firewall, IPS, application firewall, ecc.) adeguati in base al livello di classificazione assegnato ai dati ospitati nei server medesimi.

6.3.8 Salvataggio e ripristino dei dati ("backup" e "restore")

Tutte le strutture regionali che presso le loro sedi hanno server gestiti in proprio devono definire ed implementare opportune procedure di "backup **"** e "restore*"*, al fine di garantire la disponibilità dei dati stessi, minimizzando l'impatto causato da eventuali incidenti e/o errori che dovessero verificarsi nella loro gestione.

6.3.9 Gestione dei "log file"

Tutte le strutture regionali che presso le loro sedi hanno server gestiti in proprio devono attivare un sistema di raccolta delle informazioni relative all'accesso ai dati, sistemi, reti ed applicazioni utilizzati dall'Amministrazione, 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.

6.3.10 Gestione delle caselle di posta elettronica ("e-mail")

Fatto salvo quanto previsto dal "*Disciplinare per l'utilizzo di Posta elettronica, internet, Telefoni*

e fax all'interno di Regione del Veneto" (Allegato alla DGR n. 863/2009) circa l'utilizzo del servizio di Posta Elettronica dell'Amministrazione, ad ogni Utente viene assegnato un determinato spazio per la memorizzazione sul server centrale di posta.
Esaurito il predetto spazio sul server, l'Utente potrà ricevere o spedire messaggi solo dopo aver liberato spazio sufficiente attraverso la cancellazione o lo "scarico" dei messaggi di posta.
Una copia di tutti i messaggi di posta elettronica "in arrivo" e in partenza, presenti sul server, è salvata con procedure di "backup" a cadenza giornaliera per un periodo di 21 giorni consecutivi.
Qualora l'Utente "scarichi" sulla propria postazione di lavoro ovvero cancelli i messaggi di posta ancora presenti sul server, tali messaggi non saranno oggetto di "backup".
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.

6.3.11 Gestione delle richieste di accesso al contenuto di risorse ICT

L'Amministrazione regionale in caso di Utenti deceduti, sospesi o cessati dal servizio, potrebbe avere la necessità di recuperare documenti importanti su risorse ICT, assegnate ai predetti Utenti, al fine di proseguire le attività in cui gli Utenti medesimi erano coinvolti.
In tali casi il Direttore della Direzione o dell'Area di afferenza dell'Utente assegnatario delle risorse ICT potrà chiedere al Direttore della Direzione ICT e Agenda Digitale di avere accesso, nel rispetto della riservatezza dell'Utente interessato e di eventuali terzi, alle suddette risorse ICT per estrarre dalle risorse medesime le informazioni indispensabili per proseguire l'attività lavorativa.

6.3.12 Telefonia mobile

6.3.12.1 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 della presentazione della richiesta della categoria di appartenenza prevista nel contratto sottoscritto con il Gestore di telefonia mobile (paragrafo 6.3.12.6). Ciascuna assegnazione è vincolata al rispetto dei limiti di spesa previsti per l'erogazione del servizio di telefonia mobile.

6.3.12.2 ***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 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.

6.3.12.3 Dispositivi di telefonia mobile utilizzati per monitoraggi e tele allarmi

L'assegnazione delle "Sim Card" da utilizzare per i servizi di monitoraggio e/o di tele-allarme o per funzionalità analoghe, avviene secondo le modalità descritte al paragrafo 6.3.12.5.

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

6.3.12.4 Motivazione della richiesta di assegnazione di dispositivi di telefonia mobile

Fermo restando quanto previsto ai paragrafi 6.3.12.1 e 6.3.12.2, la richiesta di assegnazione dei dispositivi di telefonia mobile da presentare alla Direzione ICT e Agenda Digitale deve avere una delle seguenti motivazioni:

a) svolgimento di incarichi che richiedono la rintracciabilità dell'Utilizzatore;

b) comprovate esigenze di reperibilità dell'Utilizzatore;

c) 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;

d) esigenza temporanea dell'Utilizzatore dovuta ad incarichi e/o missioni in Italia e/o all'estero;

e) esigenza manifestata da una Struttura regionale della fornitura di "SIM Card" necessarie per servizi di monitoraggio del territorio e/o servizi di "allarme" da installare su apparati di proprietà regionale.

6.3.12.5 Modalità di presentazione della richiesta di assegnazione di dispositivi di telefonia mobile

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 della Direzione 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 come previsto al paragrafo 6.3.12.4, 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 6.3.12.6 e 6.3.12.7.

6.3.12.6 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**, **Intermedia**, **Base**, **Tablet** e **Internet Key**.

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 **Intermedia:**

- 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;
- Posizione Organizzativa;
- Dipendente di categoria "D";
- Collaboratore dell'Amministrazione regionale;

c) Categoria **Base:**

- Altro dipendente o collaboratore dell'Amministrazione regionale;

d) Categoria **Tablet:**

- Segretario Generale della Programmazione;
- Segretario della Giunta Regionale;
- Direttore della Direzione del Presidente;
- Direttori d'Area ed equiparati.
- Direttore di Direzione (su autorizzazione adeguatamente motivata dei rispettivi Direttori d'Area).

e) Categoria **Internet Key:**

- Assegnatore o Utilizzatore che abbia motivate esigenze ai sensi del paragrafo 6.3.12.4 del presente documento.

6.3.12.7 Classi di abilitazione

Le abilitazioni del servizio di telefonia mobile si articolano nelle seguenti classi: **Top**, **Intermedia** e **Base**.

Il criterio di assegnazione delle classi di abilitazione adottato è il seguente:

a) Abilitazione **Top** con utenza voce/dati**:**

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

a551ee1b

Tale abilitazione consente di utilizzare i dispositivi sul territorio nazionale e anche all'estero prevedendo, in quest'ultimo caso, dei limiti di spesa per il traffico dati (soglie dispositive) oltre le quali viene bloccato il traffico stesso.

b) Abilitazione **Intermedia** con utenza voce/dati**:**
   - 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;

   Tale abilitazione consente di utilizzare i dispositivi solo sul territorio nazionale (salvo esigenze temporanee dovute ad incarico, missione o permanenza prolungata all'estero), con inibizione di tutti i servizi a pagamento se non preventivamente autorizzati per finalità istituzionali secondo le modalità descritte al paragrafo 6.3.12.5 del presente documento.

c) Abilitazione **Base** con utenza voce:
   - Posizione Organizzativa;
   - Dipendenti di categoria "D";
   - Altri dipendenti;
   - Collaboratori dell'Amministrazione.

   Tale abilitazione consente di utilizzare i dispositivi mobili nel territorio nazionale (salvo esigenze temporanee dovute ad incarico, missione o permanenza prolungata all'estero) con dei limiti di spesa e con inibizione di tutti i servizi a pagamento se non preventivamente autorizzati per finalità istituzionali, con le modalità descritte al paragrafo 6.3.12.5 del presente documento.

Eventuali temporanee abilitazioni di utilizzo all'estero dei dispositivi di telefonia mobile da parte di Lavoratori già in loro possesso (esigenze temporanee dovute ad incarichi e/o missioni all'estero), devono essere richieste preventivamente con

congruo anticipo alla Direzione ICT e Agenda Digitale, secondo le modalità descritte al paragrafo 6.3.12.5, indicando nella richiesta la destinazione ed il periodo di permanenza.

6.3.12.8 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.

6.4 Misure comportamentali

6.4.1 Uso delle risorse e fruizione del servizio "wi-fi"

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 (ad esempio esecuzione di programmi di intrattenimento, giochi on line, etc.)

Particolare cautela dev'essere posta nell'utilizzo di reti wifi gratuite per accedere alla Intranet e ai servizi di posta elettronica regionale, 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 fomiti in uso dall'Amministrazione.
Gli Utenti sono inoltre tenuti a:

a) sottoporre a scansione antivirus preventiva gli eventuali supporti mobili utilizzati (pendrive USB, CDROM/DVD, hard disk esterni, ecc.) prima di utilizzare le risorse negli stessi contenuti;
b) modificare periodicamente le password con cadenza almeno trimestrale;
c) presidiare le risorse ICT al fine di evitare l'accesso a soggetti terzi non autorizzati;
d) bloccare i dispositivi connessi alla rete nel caso in cui non si possano presidiare i dispositivi medesimi;
e) non trasportare le postazioni di lavoro "fisse" al di fuori delle sedi dell'Amministrazione, salvo specifica autorizzazione;
f) procedere allo spegnimento delle postazioni di lavoro "fisse", al termine dell'orario di lavoro, salvo particolari esigenze di servizio autorizzate dal Direttore di struttura o di riferimento.

6.4.2 Uso dei computer portatili

Fatte salve le regole generali indicate al punto precedente, l'utilizzo di computer portatili, all'esterno dei locali dell'Amministrazione regionale, deve essere oggetto di particolare cura ed attenzione da parte degli Utenti perché tale utilizzo rappresenta una fonte di rischi particolarmente rilevante in termini di sicurezza, sia delle risorse in sé sia dei dati nelle stesse contenuti.
Tali dispositivi, infatti, possono essere soggetti a smarrimento, furti, distruzione o compromissione dei dati, tentativi di frode e/o accesso non autorizzato ovvero essere *"infettati*" da virus o *"*codice malevole*"*.

Peraltro un'eventuale contaminazione da virus informatici potrebbe diffondersi e ripercuotersi all'intera rete informatica dell'Amministrazione, una volta che tali dispositivi siano collegati direttamente alla rete interna.

È necessario, pertanto, adottare ulteriori norme comportamentali nonché specifiche procedure (di seguito descritte) che gli Utenti sono chiamati ad applicare in modo scrupoloso, conformemente alle apposite indicazioni che saranno rese disponibili in internet dalla Direzione ICT e Agenda Digitale alla pagina http://www.regione.veneto.it/web/informatica-e-e-government/:

a) cifrare i dati (laddove possibile e previa analisi dei rischi/costi-benefici);
b) fare periodicamente delle copie di back-up dei dati e verificarle regolarmente;
c) attestarsi, con frequenza almeno settimanale, alla rete intranet dell'Amministrazione per scaricare gli aggiornamenti forniti dall'Amministrazione (patch, hot fix ed elenchi dei virus);
d) mantenere abilitato l'antivirus;
e) non disabilitare le impostazioni di sicurezza originariamente impostate dall'Amministrazione;
f) evitare di accedere e navigare in siti web "pericolosi" per la sicurezza informatica, a prescindere dal fatto che ciò avvenga al di fuori dell'orario di lavoro;
g) non mantenere abilitati protocolli insicuri di comunicazione, come ad es. il bluetooth, oltre il tempo strettamente necessario.

6.4.3 Modifiche delle risorse ICT

Per quanto riguarda le modifiche si devono distinguere:

a) modifiche hardware degli strumenti dell'Amministrazione: gli Utenti non devono intervenire sui dispositivi, togliendo, sostituendo od installando componenti hardware (ad esempio masterizzatosi CDROM/DVD, schede LAN, ecc.) senza autorizzazione della Direzione ICT e Agenda Digitale;
b) modifiche software: gli Utenti non devono modificare i parametri di configurazione dei dispositivi assegnati, salvo che ciò avvenga su precisa autorizzazione della Direzione ICT e Agenda Digitale. Sono fatte salve le personalizzazioni a livello Utente che non abbiano conseguenze negative sulla funzionalità dei dispositivi stessi. Gli Utenti, inoltre, 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) senza autorizzazione della Direzione ICT e Agenda Digitale.

6.4.4 Smarrimento/furto delle risorse ICT

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

a) Autorità Giudiziaria (sporgendo denuncia);
b) Call Center dell'Assistenza informatica, per l'eventuale blocco dell'uso delle risorse ICT;
c) Direttore della propria Struttura di appartenenza;
d) Direttore della Direzione ICT e Agenda Digitale, mediante comunicazione formale.

6.4.5 Telefonia mobile

6.4.5.1 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 ed è responsabile del suo corretto utilizzo e del rispetto di quanto previsto dal presente documento nonché del *<Disciplinare per l'utilizzo di: Posta Elett*ronica, 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 u*tilizzatori"*) è consentito solo se richiesto dall'Assegnatore all'atto della richiesta di assegnazione presentata alla Direzione ICT e Agenda Digitale (paragrafo 6.3.12.5).

E' in capo all'Assegnatore la responsabilità di vigilare sull'uso del dispositivo, anche mediante la procedura di cui al paragrafo 6.4.5.3. I dispositivi assegnati devono essere restituiti alla Direzione ICT e Agenda Digitale, anche se non più utilizzabili.

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.

6.4.5.2 *Chiamate per uso personale (uso "promiscuo")*

L'Amministrazione Regionale, nel rispetto di quanto previsto nel <<Disciplinare per l'utilizzo di: Posta Elettronica, Internet, Telefoni e Fax, all'interno di Regione del Veneto>> approvato con DGR n. 863 del 31 marzo 2009, consente agli utilizzatori di effettuare traffico telefonico "promiscuo" (anche per fini personali) con i dispositivi assegnati, anteponendo il codice indicato dal Gestore di telefonia mobile alle chiamate "voce" e sms.
L'uso "promiscuo" non è consentito nel caso di dispositivi:

- ad "uso collettivo" (paragrafo 6.4.5.1);
- assegnati a collaboratori e/o personale esterno (paragrafo 6.4.5.9).

Periodicamente la Direzione ICT e Agenda Digitale provvede a far addebitare nel cedolino stipendio del dipendente i costi delle telefonate effettuate per fini personali.
Previa "registrazione" sul sito del Gestore del servizio di telefonia mobile, ogni Utilizzatore dei dispositivi di telefonia mobile, può controllare il proprio "traffico in uscita", effettuato negli ultimi 180 giorni.

Il codice indicato dal Gestore di telefonia mobile alle chiamate "voce" e sms., da impiegare per il traffico "promiscuo", è attivo sul solo territorio nazionale e viene comunicato preventivamente dalla Direzione ICT e Agenda Digitale ad ogni eventuale cambiamento.

L'Utilizzatore che si trova all'estero può effettuare telefonate per fini personali senza anteporre il suddetto codice. Una volta rientrato in Italia, l'Utilizzatore dovrà richiedere alla Direzione ICT e Agenda Digitale il tabulato delle chiamate effettuate nel periodo indicato.
La Direzione provvederà a far addebitare sul cedolino stipendio dell'Utilizzatore le chiamate che quest'ultimo indicherà nel tabulato come traffico personale.

6.4.5.3 Richiesta tabulati telefonici

Previa motivata richiesta, la Direzione ICT e Agenda Digitale fornirà all'Utilizzatore i tabulati telefonici del "traffico in uscita", addebitato negli ultimi 180 gg. dalla data di ricezione della richiesta, con le ultime tre cifre del numero chiamato non visibili.
Allo stesso modo, la Direzione ICT e Agenda Digitale fornirà all'Assegnatore i medesimi tabulati relativi alle utenze ad uso "collettivo" e quelle assegnate a collaboratori e/o personale esterno.

6.4.5.4 Smarrimento/furto

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 6.4.4 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".

6.4.5.5 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.

La Direzione ICT e Agenda Digitale comunica a ciascun Direttore di Direzione l'elenco delle utenze di propria pertinenza che per 6 mesi consecutivi non hanno prodotto traffico al fine di verificare la loro effettiva necessità di utilizzo. Entro 15 giorni dalla data di ricevimento della comunicazione il Direttore di Direzione dovrà comunicare alla Direzione ICT e Agenda Digitale l'esito della verifica condotta pena la disabilitazione delle utenze medesime.

6.4.5.6 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.
Per garantire l'assistenza e la manutenzione dei dispositivi assegnati alle Segreterie della Giunta Regionale, è prevista, previo appuntamento, la presenza di personale tecnico presso la sede di Palazzo Balbi a Venezia.

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.

6.4.5.7 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 6.3.12.4). 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 il dispositivo di telefonia mobile assegnato, 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 6.3.12.5 del presente documento.

Nel caso di cessazione del rapporto di lavoro dipendente, entro e non oltre 15 giorni dalla data di cessazione l'Utilizzatore o l'Assegnatore deve restituire alla Direzione ICT e Agenda Digitale i dispositivi mobili assegnati. Decorso inutilmente il predetto termine la Direzione ICT e Agenda Digitale provvederà a disabilitare l'utenza e potrà avvalersi, nei confronti di quest'ultimi delle azioni legali necessarie per il recupero dei dispositivi stessi.

6.4.5.8 Portabilità

Alla cessazione della condizione di lavoratore, come definita nel presente documento, quest'ultimo 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 richiedere alla Direzione ICT e Agenda Digitale di intestare la propria utenza all'Amministrazione regionale (cd. "portabilità in entrata") seguendo le modalità descritte al paragrafo 6.3.12.5 del presente documento.

6.4.5.9 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 6.3.12.5 del presente documento. In tal caso l'Assegnatore 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'Assegnatore la responsabilità di vigilare sull'uso del predetto dispositivo, anche mediante la procedura descritta al paragrafo 6.4.5.3 del presente documento.

6.4.6 Violazioni e tutela legale

L'eventuale violazione delle norme e/o delle buone regole di comportamento può comportare l'applicazione in capo ai contravventori di sanzioni di tipo civile, penale e/o disciplinare.

7 Gestione dei dati

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

a) i dati personali;
b) 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.

7.1 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).

7.2 I dati diversi da quelli personali

Fatto salvo il requisito dell'Integrità, i dati diversi da quelli personali (definiti al precedente punto 7.1) sono classificati in base al livello di Confidenzialità (Confidentiality) come segue:

a) DATI RISERVATI
b) DATI NON RISERVATI

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

7.2.1 Dati riservati

Appartengono a questa categoria i dati a cui siano collegati interessi giuridicamente rilevanti (come ad es. la proprietà individuale, 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.

7.2.2 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.)