Regole Comportamentali per gli Utenti nell'uso delle risorse ICT dell'Amministrazione regionale

Regione del Veneto

AREA PROGRAMMAZIONE E SVILUPPO STRATEGICO

Direzione ICT e Agenda Digitale

Indice

1 Introduzione

Le risorse ICT (*Information and Communications Technology*) dell'Amministrazione Regionale sono dei beni di valore, da mantenere e proteggere accuratamente.

La protezione di tali risorse risulta complessa ed articolata e richiede un'analisi globale dei sistemi, del contesto, dei comportamenti e delle prassi.

Tuttavia nessuna misura di protezione risulta efficace senza il coinvolgimento attivo dell'Utente, il quale deve adottare comportamenti rispettosi delle istruzioni fornite, evitando azioni che possano pregiudicare la sicurezza dei sistemi e/o dei dati.

Il presente documento rappresenta una riedizione aggiornata delle "*Norme Comportamentali per gli Utenti nell'uso delle risorse informativo–informatiche dell'Amministrazione regionale***"**, approvate con DGR n. 199 del 27 febbraio 2014, abrogate e sostituite dalle presenti regole comportamentali.

Tutte le risorse ICT, fornite dall'Amministrazione Regionale agli Utenti, come definiti al paragrafo 1.1, devono essere utilizzate in modo appropriato, efficiente, rispettoso e per motivi lavorativi.

Sul tema si rinvia anche a quanto stabilito dal "*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.

1.1 Definizione delle risorse ICT

Le risorse ICT, messe a disposizione dall'Amministrazione Regionale, oggetto di tutela da parte del presente documento, sono:

- il patrimonio informativo di cui al paragrafo 3, detenuto dall'Amministrazione, in formato elettronico;
- i servizi informatici erogati dall'Amministrazione;
- le postazioni di lavoro "fisse" (PC desktop e simili) e "mobili" (PC portatili e simili);
- i dispositivi cellulari (*smartphone*);
- i software di comunicazione (tipo "*messenger*" e simili);
- *i server*, le apparecchiature e tutto il materiale *hardware* in generale.

1.2 Finalità del presente documento

Il presente documento si prefigge di tutelare le risorse ICT dell'Amministrazione e di fornire indicazioni agli Utenti circa il corretto ed appropriato uso delle stesse.

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

- ridurre i rischi relativi alle minacce di sicurezza informatica, preservando la disponibilità, integrità e confidenzialità dei dati e la continuità dei servizi erogati;
- garantire il rispetto della normativa in materia.

1.3 Contesto Normativo di riferimento

Questo documento fa riferimento al 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*", che sarà direttamente applicabile in tutti gli Stati dell'Unione europea a partire dal 25 maggio 2018;

- D.Lgs. 30 giugno 2003, n. 196 "*Codice in materia di protezione dei dati personali*", che contiene la disciplina rilevante in materia di privacy;
- 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 novembre 2008).
- "*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.

1.4 Ambito di applicazione del presente documento

Il presente documento si applica ai soggetti di seguito indicati e, per brevità, definiti "Utenti":

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

Le norme si rivolgono a differenti categorie di soggetti essendo destinate a disciplinare sia il comportamento di Utenti "meri utilizzatori" (fruitori di PC desktop, smartphone, PC portatili, ecc.), sia il comportamento di Utenti che svolgono mansioni tecniche (Amministratori di Sistema, Amministratori di Rete, gestori di banche dati, gestori di servizi, ecc.).

Ciascun Utente, in base al proprio profilo "base" o "evoluto", dovrà attuare le norme che sono allo stesso indirizzate e, nel caso di dubbi di applicazione delle stesse, rivolgersi alla Direzione ICT e Agenda Digitale.

2 Regole per il corretto uso delle risorse ICT

2.1 Premessa

Le regole sono declinate su tre versanti: organizzativo, tecnologico-procedurale e comportamentale.

Tutti gli interventi sono finalizzati a garantire la confidenzialità, l'integrità e la disponibilità delle informazioni dell'Amministrazione.

In particolare:

- 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.

La finalità è, altresì, quella di garantire l'integrità e la disponibilità anche dei beni materiali dell'Amministrazione regionale.

2.2 Soluzioni organizzative

Ciascun Responsabile del trattamento dei dati personali designa un ***Referente Privacy*** all'interno della propria struttura e segnala il nominativo alla Direzione ICT e Agenda Digitale.

Il predetto Referente disamina le questioni di privacy e tiene i contatti con la Direzione ICT e Agenda Digitale.

2.2.1 Gestione degli incidenti e databreach

Ogni incidente (ad es. malfunzionamento PC, indisponibilità dei servizi applicativi e di rete) deve essere segnalato in modo tempestivo al ***Call Center*** che raccoglierà le segnalazioni e avvierà il relativo processo di classificazione e risoluzione dell'incidente medesimo al fine di minimizzare gli eventuali impatti negativi sul normale svolgimento delle attività lavorative.

Nel caso l'incidente di una certa gravità riguardi il Patrimonio Informativo e di conoscenza detenuto dall'Amministrazione oppure le applicazioni informatiche, l'Utente dovrà avvisare anche il Direttore della struttura regionale di riferimento/appartenenza e il Direttore della Direzione ICT e Agenda Digitale.

Per gli incidenti che coinvolgano dati personali (cd. "***databreach***") il Garante per la Protezione dei dati personali è intervenuto con il documento: "*Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015*" [http://www.garanteprivacy.it - doc. web. 4129029].

Per ottemperare agli obblighi imposti da tale documento ogni Utente, una volta avvisato il ***Call Center***, segnala anche al proprio Direttore le violazioni o gli incidenti informatici che ha rilevato e che possono avere un impatto significativo sui dati personali. Il predetto Direttore/Responsabile dei dati avvisa la Direzione ICT e Agenda Digitale e, assieme a quest'ultima, comunica al Garante per la Protezione dei dati personali, entro 48 ore dalla conoscenza del fatto, dell'avvenuto incidente di ***databreach.***

2.2.2 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*), che devono essere mantenute riservate e custodite con cura. Ogni *password* deve 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.

2.2.3 Autorizzazione e profilatura degli 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.

2.2.4 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 Intitute*, ecc.)

Laddove le strutture si avvalgano di propri fornitori dovranno prevedere nei contratti di 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.

2.2.5 Sicurezza delle applicazioni

Le strutture che sviluppino applicazioni informatiche devono rispettare:

a) quanto previsto dalla DGR n. 3176 del 27 ottobre 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) l'approccio della "*privacy by design*", incorporando sia i principi e le misure a tutela della privacy nell'intero ciclo di vita delle applicazioni[1] che, per le applicazioni *web-based*, le *best practices* emesse dall'Organizzazione internazionale Open Web Application Security Project (OWASP);

> Il nuovo Regolamento (UE) 2016/679, al 78° "considerando" iniziale stabilisce che: " *in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della* ***protezione dei dati fin dalla progettazione*** *e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici*."

Le strutture che affidino ad un fornitore l'incarico di sviluppare applicazioni devono, pertanto, prevedere nei relativi contratti di appalto che siano rispettare le stesse prescrizioni di cui ai precedenti punti a) e b).

[1] Ad es. gli applicativi, di *default*, non devono consentire la conoscibilità delle informazioni a chiunque, ma devono consentire agli Utenti ambiti di operatività non eccedenti rispetto al profilo di appartenenza.

Sarebbe opportuno, con riferimento al precedente punto b), inoltre, prestare analoga attenzione anche nel caso di applicazioni acquistate sul mercato (c.d. applicazioni <<COTS>> "*Commercial Off-the-Shelf component*").

2.2.6 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.

2.2.7 Gestione della disponibilità (salvataggio e ripristino dei dati)

Tutte le strutture regionali che hanno presso le proprie sedi server gestiti in proprio devono prevedere un processo di "*backup*" e "*restore*" dei dati in modo da garantire la disponibilità dei dati, mitigando l'impatto causato da eventuali incidenti e/o errori che dovessero verificarsi nella gestione dei dati.

2.2.8 Gestione dei *log file*

Tutte le strutture regionali che hanno presso le proprie sedi 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.

2.2.9 Gestione delle caselle di posta elettronica

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*".

2.2.10 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 alle suddette risorse ICT per estrarre dalle risorse medesime le informazioni indispensabili per proseguire l'attività lavorativa.

2.3 Soluzioni comportamentali

2.3.1 Uso delle risorse e fruizione del wifi

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.).

Al fine di scongiurare i rischi derivanti dall'effetto "*bridge*" (ponte) tra la rete Intranet regionale ed altre reti, gli Utenti devono evitare di accedere dall'esterno della rete Intranet regionale ai servizi di posta elettronica (https://mailrve.regione.veneto.it) e/o al servizio web regionale (https://intranet.regione.veneto.it) e contemporaneamente ad altri siti Internet potenzialmente pericolosi.

Particolare cautela deve essere posta, inoltre, nella utilizzo di reti wifi gratuite per accedere alla Intranet e ai servizi di posta elettronica regionale dal momento che nell'accedere a tali servizi devono essere inserite le credenziali e che queste ultime 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 tenuti 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;
- modificare periodicamente le password, con le modalità previste dalle procedure indicate al punto 5 dell'Allegato B al D.Lgs. 196/2003 e con cadenza almeno trimestrale;
- presidiare le risorse ICT al fine di evitare l'accesso a soggetti terzi non autorizzati;
- bloccare i dispositivi connessi alla rete nel caso in cui non si possano presidiare i dispositivi medesimi;
- non trasportare le postazioni di lavoro "fisse" al di fuori delle sedi dell'Amministrazione, salvo specifica autorizzazione;
- procedere allo spegnimento delle postazione di lavoro "fisse", al termine dell'orario di lavoro, salvo particolari esigenze di servizio autorizzate dal Direttore di struttura o di riferimento.

2.3.2 Utilizzo di dispositivi cellullari e computer portatili.

Fatte salve le regole generali indicate al punto precedente, l'utilizzo di dispositivi cellullari e 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.

Per altro 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.

E' necessario, pertanto, adottare ulteriori norme comportamentali nonché specifiche procedure, di seguito descritte, che gli Utenti sono chiamati ad applicare in modo scrupoloso:

- cifrare i dati (laddove possibile e previa analisi dei rischi/costi-benefici);
- fare periodicamente delle copie di *back-up* dei dati e verificarle regolarmente;
- attestarsi, con frequenza almeno settimanale, alla rete intranet dell'Amministrazione per scaricare gli aggiornamenti forniti dall'Amministrazione (*patch*, *hot fix* ed elenchi dei virus);
- mantenere abilitato l'antivirus;
- non disabilitare le impostazioni di sicurezza originariamente impostate dall'Amministrazione;
- 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;
- non mantenere abilitati protocolli insicuri di comunicazione, come ad es. il *bluetooth*, oltre il tempo strettamente necessario.

2.3.3 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 masterizzatori 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.

Per quanto concerne i dispositivi cellullari e i computer portatili si rinvia a quanto indicato nel paragrafo precedente dedicato a tali dispositivi.

2.3.4 Smarrimento e 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.

3 Gestione dei Dati

Il patrimonio informativo e di conoscenza detenuto dall'Amministrazione si suddivide in due macroaree:

- 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.

3.1 I Dati personali

In questo paragrafo si vuole porre l'attenzione sugli aspetti di sicurezza relativi al trattamento di dati personali.

Ai fini della corretta applicazione delle indicazioni che seguono, si ritiene utile riportare di seguito la classificazione dei dati personali fatta dal legislatore.

Ai sensi dell'Art. 4 del D.Lgs. n.196/2003 ("Codice in materia di protezione dei dati personali"), è un "*dato personale*", qualunque informazione relativa a **persona fisica**, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

a) I dati personali devono essere trattati e protetti secondo quanto previsto dal D.Lgs. 30 giugno 2003 n.196.

b) Ai sensi dell'art. 31 del D.Lgs. 196/2003, i dati personali, oggetto di trattamento, devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

c) Specifiche misure di sicurezza (c.d. "misure minime" di sicurezza) sono prescritte dagli artt. 33-36 e Allegato B del D.Lgs. 196/2003 e, ai fini di questo documento, sono destinate ad Utenti diversi (gestore del servizio/sistema, direttore regionale/responsabile del trattamento, utente/incaricato del trattamento). Ad es. spettano al gestore del servizio gli obblighi in tema di autenticazione informatica; al Responsabile del trattamento la nomina degli Incaricati e l'aggiornamento periodico dell'ambito di trattamento consentito; agli Incaricati del trattamento attenersi alle istruzioni ricevute con la nomina e adottare le necessarie cautele per la segretezza della *password*.

d) 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 ottobre 2008 sui "*Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali*" (doc. web n. 1571514).

3.1.1 Dati sensibili e giudiziari

Tutti gli Utenti devono porre particolare attenzione nei trattamenti dei dati personali sensibili e giudiziari (definiti all'Art. 4 del D.Lgs. n.196/2003) in relazione alla confidenzialità dei dati.

Sono indicati alcuni comportamenti o regole minime da rispettare: *cifrare i dati memorizzati sui file/database o in fase di trasferimento; proteggere i canali di trasmissione; evitare l'invio con la posta elettronica di dati sensibili e giudiziari; recuperare tempestivamente i documenti stampati o ricevuti via fax che contengano dati sensibili o giudiziari per sottrarli alla vista di*

chi non è autorizzato; separare logicamente i dati "comuni" da quelli sensibili/giudiziari nei database, ecc.

I Direttori di struttura che intendano avvalersi di procedure automatizzate per la gestione dei dati sensibili e giudiziari devono assicurarsi che tali procedure rispettino i seguenti requisiti:

- requisiti di cui al comma 6 [2] dell'art. 22 del D.Lgs. 196/2003;
- requisiti, per quanto compatibili, dell'Allegato B del D.Lgs. 196/2003;

Laddove i Direttori per valutare le misure di sicurezza, volte a garantire la protezione dei dati sensibili e giudiziari, potranno richiedere la collaborazione della Direzione ICT e Agenda Digitale.

3.2 I dati diversi da quelli personali

Fatto salvo il requisito dell'Integrità, i dati diversi da quelli personali (definiti al precedente punto 3.1) sono classificati in base al livello di Confidenzialità (*Confidentiality*) come segue:

1. Dati riservati
2. Dati non riservati.

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

3.2.1 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.

3.2.2 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.)

Per i dati non riservati, il responsabile stabilisce le forme e modalità attraverso cui rendere disponibili e/o liberamente accessibili i dati, nel rispetto della normativa vigente.

4 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.

[2] "*I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità*." (Art. 22, comma 6, del D.Lgs. 196/2003).