Regione del Veneto

Norme comportamentali per gli Utenti nell'uso delle risorse informativo–informatiche dell'Amministrazione regionale

A cura della Direzione Sistema Informatico

Ufficio Privacy e Ufficio Sicurezza Informatica

ALLEGATOA alla Dgr n. 240 del 15 marzo 2011

Indice

1 INTRODUZIONE E NOTAZIONI PRELIMINARI 3

1.1 Definizione delle risorse informativo–informatiche 3

1.2 Finalità del presente documento 3

1.3 Contesto Normativo di riferimento 4

1.4 Ambito di applicazione del presente documento 4

2 REGOLE PER IL CORRETTO USO DELLE RISORSE INFORMATIVO-INFORMATICHE 4

2.1 Premessa 4

2.2 Soluzioni organizzative: Ufficio Sicurezza Informatica, Ufficio Privacy e Referenti Privacy presso le strutture regionali 5

2.3 Soluzioni tecnologico-procedurali 5
2.3.1 Gestione degli incidenti 5
2.3.2 Autenticazione Utenti 5
2.3.3 Autorizzazione e profilatura degli Utenti 6
2.3.4 Sicurezza dei server 6
2.3.5 Sicurezza delle applicazioni 6
2.3.6 Sicurezza della rete 7
2.3.7 Gestione della disponibilità (salvataggio e ripristino dei dati) 7
2.3.8 Gestione dei *log file* 7

2.4 Soluzioni comportamentali 7
2.4.1 Uso delle risorse 7
2.4.2 Utilizzo di “palmari”, computer e dispositivi portatili 8
2.4.3 Modifiche delle risorse informatiche 8
2.4.4 Furto e smarrimento delle risorse 9

3 GESTIONE DEI DATI 9

3.1 I Dati personali 9
3.1.1 Dati sensibili e giudiziari 10

3.2 I dati diversi da quelli personali 11
3.2.1 Dati riservati 11
3.2.2 Dati non riservati 12

4 VIOLAZIONI E TUTELA LEGALE 12

ALLEGATOA alla Dgr n. 240 del 15 marzo 2011

1 Introduzione e notazioni preliminari

Le risorse informativo–informatiche dell'Amministrazione Regionale sono un bene di valore, da mantenere e proteggere accuratamente.

In particolare, la protezione del patrimonio informativo in formato elettronico risulta articolata e complessa e richiede di essere considerata in modo specifico.

Soltanto con un'analisi globale dei sistemi, del contesto, dei comportamenti e delle prassi, è possibile valutare i rischi e definire adeguate misure di sicurezza sia dal punto di vista organizzativo che tecnico.

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

Il presente documento rappresenta un'evoluzione e miglioramento delle "*Norme Comportamentali per gli Utenti***"** e delle "*Linee Guida di Sicurezza Informatica***",** approvate con DGR n. 584 del 5 marzo 2004 che sono entrambe abrogate e sostituite dalle presenti norme comportamentali e linee guida.

Tutte le risorse informatiche, fornite dall'Amministrazione Regionale agli Utenti, come definiti al paragrafo 1.4, 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 informativo–informatiche

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

- il patrimonio informativo e di conoscenza detenuto dall'Amministrazione in formato elettronico;
- le applicazioni informatiche (*software*);
- le postazioni di lavoro "fisse" (PC desktop e simili);
- i Personal Computer "portatili" (compresi i *notebook* e simili);
- i cellulari tecnologicamente più avanzati ed i "palmari" (ad es. BlackBerry, iPhone, iPAQ e simili),
- gli strumenti per la comunicazione "*voice over ip*" o tipo "*messenger*";
- i server, le apparecchiature di rete e tutto il materiale *hardware* in generale.

1.2 Finalità del presente documento

Il presente documento si prefigge di tutelare le risorse informativo-informatiche dell'Amministrazione e di dare 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 delle leggi e normative vigenti in materia.

1.3 Contesto Normativo di riferimento

Questo documento fa riferimento al quadro normativo vigente ed in particolare a:

- 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,
- Documento Programmatico sulla Sicurezza (D.P.S.), il più importante documento in materia di privacy e sicurezza dei dati dell'Amministrazione, adottato annualmente dall'Amministrazione regionale (si veda l'ultimo DPS approvato).

1.4 Ambito di applicazione del presente documento

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

a) Dirigenti 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 partner dell'Amministrazione regionale che utilizzino risorse dell'Amministrazione regionale;
d) ospiti e persone a vario titolo presenti nei locali dell'Amministrazione, per quanto riguarda l'eventuale uso delle risorse informatiche e telematiche dell'Amministrazione regionale;
e) Enti e Agenzie regionali attestati sulla 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, BlackBerry, iPhone, 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 all'Ufficio Sicurezza Informatica e all'Ufficio Privacy, istituiti presso Direzione Sistema Informatico.

2 Regole per il corretto uso delle risorse informativo-informatiche

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: Ufficio Sicurezza Informatica, Ufficio Privacy e Referenti Privacy presso le strutture regionali

Gli Utenti in base alle proprie esigenze, in presenza di dubbi riguardanti la privacy, l'attuazione delle norme comportamentali o delle misure di sicurezza, potranno rivolgersi all'Ufficio Sicurezza Informatica o all'Ufficio Privacy, istituiti presso la Direzione Sistema Informatico.

I Dirigenti devono designare, all'interno della propria struttura, un Referente Privacy che approfondisca le questioni e che tenga i contatti con l'Ufficio Privacy.

In ogni caso è buona norma che le questioni di privacy siano preventivamente affrontate all'interno della struttura tra gli Utenti e il Referente Privacy.

2.3 Soluzioni tecnologico-procedurali

2.3.1 Gestione degli incidenti

Ogni incidente (es. malfunzionamento PC, indisponibilità dei servizi applicativi e di rete) deve essere segnalato al *Call Center* in modo tempestivo 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 Dirigente della struttura regionale di riferimento/appartenenza e il Dirigente della Direzione Sistema Informatico.

2.3.2 Autenticazione Utenti

L'accesso a tutti i servizi o informazioni che devono esser condivise in rete da un gruppo ristretto di persone deve avvenire esclusivamente dopo la procedura di autenticazione.

Gli Utenti devono essere identificati e ricevere dal gestore del servizio delle credenziali 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 Risorse Umane dovrà tempestivamente disabilitare le credenziali del personale regionale che sia cessato dal servizio e sospendere quelle del personale in aspettativa o comando esterno).

2.3.3 Autorizzazione e profilatura degli Utenti

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

Sarà cura del dirigente di struttura segnalare al gestore i diritti di consultazione o di modifica da attribuire all'Utente in base alle mansioni assegnate e svolte dall'Utente ed ogni conseguente variazione affinché ci sia coerenza tra i diritti e mansioni assegnati.

2.3.4 Sicurezza dei server

I gestori di server (comprese quindi tutte le strutture regionali che hanno presso le proprie sedi server gestiti in proprio), devono configurare i server medesimi secondo opportuni Standard di sicurezza o *best practices* (quali ad es. abilitare soltanto i servizi strettamente necessari ed applicare sistematicamente le "*pacth*") emessi da Enti ed Organizzazioni internazionali, quali - 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 ed inoltre dovranno prevedere clausole di responsabilità esterna e 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.

2.3.5 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);

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

Sarebbe opportuno, con riferimento al precedente punto b), inoltre, prestare analoga attenzione anche nel caso di applicazioni acquistate sul mercato (c.d. applicazioni "*off the shelf product*").

[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.

2.3.6 Sicurezza della rete

La Direzione Sistema Informatico deve configurare la Rete Telematica dell'Amministrazione per contribuire alla protezione dei server, che dovranno essere collocati su sottoreti dedicate e con di livelli di protezione adeguati in base al livello di classificazione assegnato ai dati ospitati nei server medesimi.

2.3.7 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 negativo di eventuali incidenti o errori che dovessero verificarsi nella gestione dei server.

2.3.8 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.

2.4 Soluzioni comportamentali

2.4.1 Uso delle risorse

Tutti gli Utenti devono utilizzare le risorse informatiche, 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 informatiche 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.) o altre attività estranee all'ambito istituzionale.

Al fine di scongiurare i rischi derivanti dall'effetto "*bridge*" (ponte) tra la rete Intranet regionale ed altre reti, gli Utenti devono evitare di:

- mantenere contemporaneamente aperte la connessione alla Intranet regionale e la connessione verso reti esterne (siti internet) non attendibili e/o sicure;
- non accedere dall'esterno della rete Intranet regionale ai servizi di posta elettronica (https://mail.regione.veneto.it/exchange) e/o al servizio web regionale (https://intranet.regione.veneto.it) e contemporaneamente ad altri siti Internet di cui non si abbia ragionevole certezza di sicurezza.

Gli Utenti non devono eseguire copie (anche parziali) del software installato sui dispositivi, senza preventiva autorizzazione, essendo lo stesso generalmente protetto da leggi sul diritto d'autore.

Gli Utenti, invece, 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 previste dal punto 5 dell'Allegato B al D.Lgs. 196/2003 e con cadenza almeno trimestrale;
- presidiare le risorse informatiche 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 dirigente di struttura o di riferimento.

2.4.2 Utilizzo di "palmari", computer e dispositivi portatili

Fatte salve le regole generali indicate al punto precedente, l'utilizzo di "palmari", computer e dispositivi portatili all'esterno dei locali dell'Amministrazione 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 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, quindi, 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 (le statistiche indicano - ad es. - come pericolosi siti contenenti materiale pornografico o gioco d'azzardo);
- non mantenere abilitati protocolli insicuri di comunicazione, come ad es. il *bluetooth*, oltre il tempo strettamente necessario.

2.4.3 Modifiche delle risorse informatiche

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 Sistema Informatico,

b) modifiche *software*: gli Utenti non devono modificare i parametri di configurazione dei dispositivi assegnati, salvo che ciò avvenga su precisa autorizzazione della Direzione Sistema Informatico. Sono fatte salve le personalizzazioni a livello Utente che non abbiano conseguenze negative sulla funzionalità dei dispositivi. Gli Utenti, inoltre, non devono disinstallare, eseguire o installare applicazioni sui dispositivi senza autorizzazione della Direzione Sistema Informatico.

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

2.4.4 Furto e smarrimento delle risorse

Nei casi di smarrimento, furto accertato o grave manomissione dei dispositivi assegnati o del contenuto degli stessi, gli Utenti devono segnalare tempestivamente il fatto ai soggetti di seguito indicati:

- Dirigente della propria Struttura di appartenenza;
- Autorità Giudiziaria (sporgere denuncia);
- Direzione Sistema Informatico;
- *Call Center* dell'Assistenza informatica.

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, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Nella macroarea dei "dati personali" si definiscono "comuni" i dati diversi da quelli sensibili e giudiziari.

I "*dati sensibili*" sono i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale.

I dati personali idonei a rivelare lo stato di salute e la vita sessuale sono una ulteriore sottocategoria dei dati sensibili a cui la normativa riserva una tutela rafforzata nel trattamento (c.d. dati "supersensibili").

I "*dati giudiziari*" sono i dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi del codice di procedura penale.

Si definisce come "*trattamento*", qualunque operazione o complesso di operazioni, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati personali, anche se non registrati in una banca di dati.

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, dirigente 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 e l'adozione del DPS (integrativo); 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 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 Dirigenti 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 Dirigenti non siano in grado di valutare autonomamente le misure di sicurezza per garantire la protezione dei dati sensibili e giudiziari potranno richiedere la collaborazione all'Ufficio Sicurezza Informatica e all'Ufficio Privacy, istituiti presso Direzione Sistema Informatico.

Il trattamento con strumenti elettronici di dati sensibili e giudiziari richiede la redazione annuale del Documento Programmatico sulla Sicurezza (DPS) come previsto dal D.Lgs. 196/2003.

Per i dati gestiti a livello centralizzato dal Centro Sviluppo Servizi Territoriali (CSST) presso la Direzione Sistema Informatico, il DPS è predisposto da questa per l'approvazione successiva da parte della Giunta Regionale.

Per i dati sensibili e giudiziari, contenuti in server che risiedono presso le strutture regionali e non sui sistemi centralizzati della Direzione Sistema Informatico, le medesime strutture devono adottare entro il 31 marzo, ed aggiornare annualmente, un DPS integrativo del DPS proposto dalla Direzione Sistema Informatico.

L'obbligo di adozione del DPS resta a carico degli Enti e delle Agenzie regionali che fruiscano dei servizi di hosting e/o housing erogati dalla Direzione Sistema Informatico.

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 Dirigente della struttura che genera o gestisce i dati medesimi.

3.2.1 Dati riservati

Appartengono a questa categoria i dati la cui creazione e/o utilizzo è opportuno/necessario sia riservata ad un gruppo selezionato ed identificato di dipendenti/collaboratori dell'Amministrazione o di altre Pubbliche Amministrazioni o di partner privati.

In particolare, per ciascun dato riservato il soggetto responsabile dovrebbe gestire una *lista di distribuzione* con l'elenco dei soggetti cui è consentito l'accesso o l'impiego del dato medesimo.

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.

---

[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).

3.2.2 Dati non riservati

Appartengono a questa categoria: i dati il cui accesso e/o utilizzo non ha restrizioni.

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

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.