Comune di Udine
Dipartimento Affari Generali
Servizio Sistemi Informativi e Telematici

REGOLAMENTO
PER L'ACCESSO ED UTILIZZO DEI SISTEMI INFORMATIVI E DELLE RISORSE INFORMATICHE, TELEMATICHE E TELEFONICHE DELL'AMMINISTRAZIONE

(versione aggiornata al 15.06.2007)

Il testo del presente Regolamento è stato approvato con Deliberazione di Giunta Comunale n. ord. 271 del 19 giugno 2007.

INDICE:

PREMESSA

TITOLO I PARTE GENERALE
Art. 1 - Definizioni
Art. 2 - Oggetto del Regolamento
Art. 3 - Finalità del Regolamento
Art. 4 – Compiti del Servizio Sistemi Informativi e Telematici

TITOLO II SISTEMI INFORMATIVI
Art. 5 - Generalità
Art. 6 - Accesso
Art. 7 - Utilizzo
Art. 8 - Codici di Accesso (password)

TITOLO III RISORSE INFORMATICHE
Art. 9 - Generalità
Art. 10 - Accesso
Art. 11 - Utilizzo
Art. 12 - Assistenza Tecnica
Art. 13 - Stazioni di lavoro portatili
Art. 14 - Protezione Antivirus

TITOLO IV SERVIZIO DI POSTA ELETTRONICA
Art. 15 - Generalità
Art. 16 - Accesso
Art. 17 - Utilizzo

TITOLO V SERVIZIO DI RETE INTERNET
Art. 18 - Generalità
Art. 19 - Accesso
Art. 20 - Utilizzo

TITOLO VI SERVIZI DI RETE TELEFONICA FISSA E MOBILE
Art. 21 Generalità
Art. 22 Accesso alle Risorse di Rete Telefonica Fissa
Art. 23 Utilizzo delle Risorse di Rete Telefonica Fissa
Art. 24 Accesso alle Risorse di Rete Telefonica Mobile
Art. 25 Utilizzo delle Risorse di Rete Telefonica Mobile

TITOLO VII DISPOSIZIONI FINALI
Art. 26 - Responsabilità degli utenti

APPENDICE A - LEGISLAZIONE
APPENDICE B – DICHIARAZIONE DI PRESA VISIONE

PREMESSA

Negli ultimi anni le Risorse Informatiche, di Rete Telematica, di Rete Telefonica fissa e mobile che l'Amministrazione ha messo a disposizione dell'utenza per lo svolgimento della normale attività lavorativa, sono cresciute in misura considerevole in virtù di diversi fattori concomitanti, quali ad esempio:

- l'introduzione di nuovi software applicativi
- la capillare diffusione della posta elettronica per le comunicazioni interne ed esterne
- l'utilizzo crescente di Internet quale abituale strumento di lavoro per la ricerca di informazioni e l'accesso a banche dati "on-line"
- l'ampio utilizzo della telefonia mobile per le comunicazioni di servizio.

La diffusione dei citati strumenti e tecnologie ICT (Information & Communication Technology) ha incrementato di fatto la complessità gestionale dei Sistemi Informativi dell'Amministrazione, portando in primo piano numerosi problemi di carattere operativo aventi però importanti ripercussioni dal punto di vista delle responsabilità in capo al singolo utente finale e all'Ente.

Tra i problemi ricorrenti che attengono all'accesso ed all'utilizzo di sistemi e tecnologie ICT vi sono quelli legati alla sicurezza fisica e logica dei Sistemi Informativi automatizzati, quelli legati al trattamento delle informazioni da parte degli utenti, le problematiche legate alla proprietà intellettuale e diritto d'autore di banche dati e programmi informatici ed i temi specificatamente legati ai cosiddetti "computer crimes" (ovvero: crimini informatici).

I fattori legati all'alta diffusione delle stazioni di lavoro informatizzate ad uso individuale oppure al sempre più esteso utilizzo della rete Internet hanno comportato, per i gestori dei sistemi e tecnologie ICT, la necessità di tenere alto il livello di attenzione nei confronti dei possibili comportamenti che il singolo addetto potrebbe attuare nel momento dell'accesso e dell'utilizzo delle risorse ad egli assegnate per lo svolgimento del lavoro d'ufficio.

Molti dei problemi sopra accennati, possono essere affrontati e risolti dalle Amministrazioni sensibilizzando e formando opportunamente l'utenza sui temi afferenti il campo della cosiddetta "Informatica Giuridica", laddove si specificano le norme di legge che devono essere rispettate al fine di un corretto utilizzo delle Risorse Informatiche, Telematiche e Telefoniche costituenti i Sistemi Informativi di un Ente o Azienda.

Ai fini del presente Regolamento, si è voluto però dare un'accezione più ampia al termine "corretto" non limitandolo solo al concetto di utilizzo conforme alla normativa vigente, ma estendendolo alla necessità di perseguire, tramite adeguati comportamenti, un utilizzo efficiente ed efficace degli strumenti che l'Amministrazione mette a disposizione dell'utenza, con il fine ultimo di raggiungere una gestione ottimale dei sistemi informativi automatizzati.

Per esplicitare in maniera chiara i suddetti comportamenti, è stato preparato il presente testo di Regolamento Interno che disciplina le modalità di accesso e di utilizzo alle diverse risorse individuate nel seguito, richiamando i testi normativi vigenti, responsabilizzando l'utenza nei confronti di possibili comportamenti difformi dagli stessi ma anche richiamando alcuni esempi pratici di errato utilizzo delle risorse a disposizione.

Il Regolamento è strutturato in capitoli distinti a seconda della tipologia di risorsa in esame, al fine di facilitare la lettura all'utente e consentire un rapido accesso all'argomento desiderato.

TITOLO I
PARTE GENERALE

Art. 1 - Definizioni

Amministrazione (denominato anche: *Ente*): il Comune di Udine, con sede in Via Lionello 1, Udine.

Servizio Sistemi Informativi e Telematici (SSIT): la funzione organizzativa che è direttamente responsabile dell'acquisizione, della gestione operativa e dello sviluppo delle tecnologie informatiche, telematiche e telefoniche dell'Amministrazione ed alla quale è riconosciuto il ruolo di amministratore dello stesso.

Sistemi Informativi: tutte le banche dati ed i programmi informatici che costituiscono l'insieme delle risorse software acquisite su licenza da fornitori esterni o di proprietà dell'Amministrazione oppure disponibili tramite collegamenti interni o esterni all'Ente, installati su un qualunque sistema elaborativo server, client o di rete trasmissione dati su cui il SSIT ha responsabilità di acquisizione, gestione operativa e sviluppo.

Risorse Informatiche, Telematiche e Telefoniche: le attrezzature ed i dispositivi fisici come ad esempio:
- le stazioni di lavoro (personal computers), le workstations, le stampanti ad uso individuale e per gruppi di lavoro e accessori di informatica individuale
- le postazioni telefoniche fisse, gli apparati radiomobili cellulari, schede SIM, centralini telefonici ed accessori di telefonia
- gli apparati di rete trasmissione dati e le altre attrezzature facenti parte della rete trasmissione dati comunale, della rete telefonica fissa e di quella mobile
- i collegamenti dati e telefonici acquisiti tramite noleggio da fornitori esterni oppure di proprietà dell'Amministrazione.

Servizi di Rete Informatica, Telematica e Telefonica: i servizi disponibili tramite l'accesso alle Risorse Informatiche, Telematiche e Telefoniche dell'Amministrazione.
Sono esempi di servizi di Rete Informatica quelli relativi all'autenticazione degli Utenti per l'utilizzo di stampanti di gruppo oppure per l'accesso e l'utilizzo del sistema di Posta Elettronica o di Internet. Esempi di servizi di Rete Telematica sono invece quelli che permettono il collegamento delle stazioni di lavoro ai sistemi dipartimentali server anche da locazioni remote. Infine sono servizi di Rete Telefonica ad esempio quelli disponibili dai centralini telefonici (trasferimento di chiamata, deviazione ad altro numero, ecc) oppure dalla rete del gestore di rete telefonica mobile (segreteria telefonica, "dual-billing", ecc.).

Dirigente: Direttore Generale, Segretario Generale, Direttore di Dipartimento, Dirigente di Servizio, Responsabile di Unità Organizzativa.

Utente: la persona fisica, di norma identificabile nell'incaricato del trattamento dei dati ai sensi dell'Art. 4, comma 1, lettera h, del D.Lgs. 30 giugno 2003, n.196, che, previa espressa autorizzazione da parte del SSIT, ha accesso ed utilizza i Sistemi Informativi e le Risorse Informatiche, Telematiche e Telefoniche dell'Amministrazione.
Sono Utenti di norma:
- i dipendenti dell'Amministrazione
- gli amministratori dell'Ente
- il personale esterno con incarichi professionali assegnati dall'Amministrazione
- gli stagisti, i tirocinanti e gli addetti di società terze che prestano servizio o lavorano per conto dell'Amministrazione
- i tecnici informatici dipendenti di società fornitrici dell'Amministrazione

- tutti gli altri soggetti che, per periodi di tempo limitati o continuativi, hanno accesso e utilizzano a qualche titolo i Sistemi Informativi e le Risorse Informatiche, Telematiche e Telefoniche dell'Amministrazione.

Art. 2 - Oggetto del Regolamento

Con il presente Regolamento vengono definite le modalità di accesso e di utilizzo dei Sistemi Informativi, delle Risorse Informatiche, Telematiche e Telefoniche dell'Amministrazione.

Per quanto non espressamente specificato, il presente Regolamento deve essere interpretato secondo correttezza e buona fede.

In caso di dubbi interpretativi o necessità di ulteriori informazioni circa i contenuti o l'applicazione del presente Regolamento, gli Utenti sono invitati a rivolgersi immediatamente al SSIT inviando le proprie richieste o quesiti all'indirizzo ssi@comune.udine.it.

Art. 3 - Finalità del Regolamento

L'adozione del presente Regolamento è finalizzata a garantire prioritariamente:
- il rispetto delle leggi in materia di trattamento delle informazioni e dei dati trattati dagli utenti dei sistemi informativi, anche tenuto conto delle esigenze di tutela della privacy e della sicurezza del trattamento degli archivi informatici
- il rispetto delle leggi in materia di tutela giuridica dei programmi per elaboratore e delle banche dati
- il rispetto delle leggi in materia di crimini informatici.

Inoltre il presente Regolamento mira ad assicurare:
- la riservatezza delle informazioni trattate con i Sistemi Informativi dell'Amministrazione e la sicurezza nello scambio di informazioni da parte degli Utenti
- il corretto utilizzo delle Risorse Informatiche, Telematiche e Telefoniche da parte degli Utenti per lo svolgimento del lavoro d'ufficio al fine di garantire la massima efficienza nell'utilizzo delle Risorse stesse
- la massima disponibilità e continuità di servizio dei Sistemi Informativi dell'Amministrazione, nell'interesse degli Utenti e della collettività.

Art. 4 - Compiti del Servizio Sistemi Informativi e Telematici

Il Servizio Sistemi Informativi e Telematici (SSIT) si assume l'onere di:
- adottare tutti i dispositivi di sicurezza necessari per proteggere l'integrità fisica e logica dei sistemi ed apparecchiature informatiche, telematiche e telefoniche che ha in gestione
- implementare opportuni meccanismi di controllo e monitoraggio, anche a livello preventivo, atti ad evitare possibili intrusioni ai Sistemi Informativi ed alle apparecchiature informatiche, telematiche e telefoniche ovvero abusi nell'utilizzo delle stesse
- responsabilizzare e formare gli Utenti circa le conseguenze penali, civili ed amministrative connesse all'uso indebito o improprio degli strumenti informatici, telematici e telefonici.

Per raggiungere gli obiettivi sopra descritti il SSIT provvede alla redazione ed al continuo aggiornamento dei piani per la sicurezza informatica dell'Amministrazione, adottando le più recenti tecnologie disponibili sul mercato ICT al fine di implementare misure idonee a salvaguardia delle Risorse Informatiche, Telematiche e Telefoniche dell'Ente.

In particolare il SSIT si riserva la facoltà di accedere in un qualunque momento alle Risorse Informatiche, Telematiche e Telefoniche ai soli fini dell'espletamento di compiti di monitoraggio sulle Risorse stesse nonché ai fini della salvaguardia della sicurezza dei Sistemi Informativi dell'Amministrazione, nel rispetto della riservatezza dei dati personali di cui al D.Lgs. 30 giugno 2003, n.196.

TITOLO II
SISTEMI INFORMATIVI

Art. 5 – Generalità

I Sistemi Informativi utilizzati dagli Utenti costituiscono uno strumento di lavoro.

L'utilizzo dei Sistemi Informativi da parte degli Utenti è preceduto di norma dal preventivo rilascio da parte del SSIT di una specifica autorizzazione per l'accesso alle risorse informative (o banche dati) che compongono quel determinato sistema, e nell'autorizzazione all'utilizzo dei programmi informatici che permettono il trattamento delle informazioni e dei dati ivi contenuti.

Costituiscono esempi di risorse informative:
- le banche dati accessibili tramite collegamenti ai sistemi gestionali dell'Amministrazione, di norma memorizzate in elaboratori dipartimentali (server) gestiti dal SSIT, come ad esempio: il sistema di contabilità, del personale, dell'anagrafe comunale, di gestione degli atti formali, di protocollo, ecc.;
- le banche dati accessibili tramite collegamenti ai servizi di rete informatica interna gestiti dal SSIT, come ad esempio le diverse raccolte di fonti dati di carattere giuridico e normativo disponibili in rete su CD-ROM condivisi;
- le banche dati accessibili tramite collegamenti dedicati ai servizi di rete informatica gestiti da soggetti esterni (es. ANCI, Ministero dell'Economia, Motorizzazione Civile, ecc), anche via Internet;
- le banche dati memorizzate nella stazione di lavoro dell'Utente finale o su spazi di memorizzazione su server dipartimentali, anche condivisi, gestite da programmi informatici regolarmente autorizzati dal SSIT.

Costituiscono invece esempi di programmi informatici che permettono il trattamento delle informazioni contenute nelle banche dati sopra descritte:
- programmi emulatori di terminali video come OnNet, ecc
- programmi di produttività individuale come Word, Excel, Access, Lotus Notes, ecc
- altri programmi client specializzati o sviluppati ad hoc dai fornitori per usi particolari come AutoCAD, GeoMedia, WinRap, Methodica Trend, Sigma5, ecc.

L'Utente che accede ai Sistemi Informativi è responsabilizzato sul fatto che tutti i dati personali oggetto di trattamento contenuti negli archivi informatici degli stessi sono protetti ai sensi del D.Lgs. 30 giugno 2003, n. 196.

L'Utente inoltre è consapevole che le banche dati sono tutelate dalla normativa sul diritto d'autore di cui alla L. 22 aprile 1943, n. 633 e pertanto si impegna a non divulgarne i contenuti informativi al di fuori di motivi di servizio.

Sono altresì vietate ai sensi del D.Lgs. 6 maggio 1999 n.169 la riproduzione, la distribuzione, la comunicazione, totale o parziale, con qualsiasi mezzo e in qualsiasi forma delle banche dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore.

L'Utente è altresì responsabilizzato sul fatto che taluni comportamenti impropri attuati nell'accesso e nell'utilizzo dei Sistemi Informativi possono violare le norme in tema di criminalità informatica di cui alla L. 23 dicembre 1993, n. 547.

Art. 6 – Accesso

L'accesso ai Sistemi Informativi è riservato ai soli Utenti previo rilascio di opportuna abilitazione all'uso da parte del SSIT.

La concessione dell'abilitazione all'accesso di una specifica risorsa informativa o di utilizzo di programma informatico da parte di un Utente avviene di norma dietro presentazione al SSIT di una richiesta motivata da parte del Dirigente da cui l'Utente finale dipende.

Nella richiesta viene specificata la risorsa informativa ovvero il programma informatico per il quale viene chiesto l'accesso e l'utilizzo da parte dell'Utente.

Ogni abilitazione all'accesso di un sistema informativo viene assegnata esclusivamente per via nominale all'Utente finale.

Il SSIT, ricevuta la richiesta di accesso alla risorsa informativa, provvede di norma alle operazioni tecniche che permettono l'abilitazione all'uso della stessa, la relativa accoglibilità previa verifica di congruità tecnica ed organizzativa ed evadendo le richieste nel più breve tempo possibile, di norma nel rispetto dell'ordine di arrivo delle stesse e tenendo in debito conto le situazioni organizzative e le esigenze debitamente segnalate che impongono particolare urgenza.

Le operazioni tecniche di cui sopra possono consistere nella semplice abilitazione dell'Utente all'accesso ed utilizzo di una risorsa informativa effettuata dal personale tecnico del SSIT, nel rilascio di una credenziale di accesso personale ad uso esclusivo dell'Utente finale, nell'installazione sulla stazione di lavoro dell'Utente dell'opportuno programma informatico che permette l'utilizzo della risorsa informativa individuata, oppure in una combinazione di più azioni tra quelle sopra descritte.

L'elenco dei Sistemi Informativi ai quali un Utente ha diritto di accesso ed utilizzo viene trasmesso con cadenza annuale ad ogni Dirigente da cui egli dipende ai fini della verifica periodica di sussistenza della necessità di accesso ai Sistemi Informativi individuati.

L'Utente assegnatario di un'abilitazione all'accesso ad un qualunque sistema informativo sottoscrive la dichiarazione di presa visione ed accettazione delle norme contenute nel presente regolamento.

Art. 7 – Utilizzo

E' assolutamente vietato all'Utente divulgare ad altri Utenti informazioni relative ad una abilitazione di accesso personale ricevuta dal SSIT per l'accesso ed utilizzo delle risorse informative ad egli assegnate.

E' espressamente vietato all'Utente accedere in maniera non autorizzata a banche dati accessibili tramite collegamento ai servizi di rete informatica interna o esterna, compresa Internet, nonché di effettuare, o far effettuare da terzi, l'installazione di programmi informatici su qualunque tipo di elaboratore, in particolare sulle stazioni di lavoro assegnate agli Utenti.

Le predette attività di installazione dovranno essere oggetto di esplicita richiesta e saranno eseguite di norma dal personale tecnico del SSIT, salvo diversa esplicita autorizzazione da parte del SSIT stesso.

E' inoltre fatto divieto all'Utente di effettuare, o far effettuare da terzi, qualunque operazione di installazione o re-installazione di un qualunque prodotto software, anche facente parte della dotazione installata dal SSIT sulla stazione di lavoro oppure aggiuntivo rispetto ad essa. Sono altresì vietate tutte le modifiche tecniche che alterino in maniera sostanziale le funzionalità o le

caratteristiche di funzionamento di programmi informatici, di archivi informatici o di banche dati accessibili tramite collegamento ai servizi di rete trasmissione dati interna o esterna, compresa Internet.

Tutte le succitate attività di modifica della configurazione definita dovranno essere oggetto di richiesta e saranno eseguite di norma dal personale tecnico del SSIT, salvo diversa esplicita autorizzazione da parte del SSIT stesso.

E' inoltre espressamente vietato:

- distribuire o duplicare qualunque software soggetto a copyright non rispettando i termini contrattuali contenuti nella relativa licenza d'uso oppure software prodotto da terzi per conto dall'Amministrazione;
- distribuire, anche via Posta Elettronica, qualsiasi tipo di software che possa danneggiare o limitare le funzionalità dei Sistemi Informativi o delle Risorse Informatiche dell'Amministrazione, in particolare software virale.

L'Utente è consapevole che lasciare un elaboratore incustodito può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Per questo motivo viene suggerito all'Utente che, prima dello spegnimento fisico della stazione di lavoro utilizzata per l'attività lavorativa oppure in caso di assenze prolungate dall'ufficio, si proceda preventivamente allo scollegamento (logoff o logout) dalla Risorsa Informativa che egli stava utilizzando.

Art. 8 - Codici di Accesso (password)

L'accesso alle risorse informative viene protetto da apposite credenziali costituite da username e password alle quali si applica quanto previsto dall'Allegato B del D.Lgs. 30 giugno 2003 n.196.

L'Utente ha quindi l'esclusiva responsabilità di custodire la password, comunicata dal SSIT nella fase di abilitazione all'utilizzo della singola risorsa informativa da parte dell'Utente stesso, con la massima diligenza possibile e di non comunicarla o diffonderla a terzi.

Tutte le password di accesso ed abilitazione all'utilizzo delle risorse informative e dei programmi informatici componenti i Sistemi Informativi vengono rilasciate dal SSIT individualmente all'Utente utilizzatore dietro presentazione di richiesta da parte del Dirigente da cui l'Utente dipende.

Ogni Utente è tenuto a cambiare sollecitamente la password rilasciata inizialmente dal SSIT per l'accesso alla risorsa informativa al primo utilizzo della risorsa stessa e, successivamente, almeno ogni 6 mesi, pena la perdita di validità e la disattivazione della stessa; è obbligo dell'Utente chiedere altresì la sostituzione della password di accesso nell'eventualità in cui egli sospetti che essa abbia perso la necessaria segretezza.

Qualora un Utente venisse a conoscenza, anche in maniera fortuita, di password assegnate ad altro Utente, è tenuto a darne immediata notizia al SSIT ai fini della sollecita sostituzione.

Il SSIT indica come criterio generale di scelta delle password che le stesse vengano formate da almeno 8 caratteri, siano composte da lettere maiuscole/ minuscole e cifre numeriche, non utilizzino i caratteri speciali (& ^ % $ #), evitando parole riconducibili a termini di uso comune tratti dal dizionario, nomi propri o geografici e riferimenti agevolmente riconducibili all'Utente stesso (es. nome del coniuge o di familiari, luogo e data di nascita, ecc).

TITOLO III
RISORSE INFORMATICHE

Art. 9 – Generalità

Le Risorse Informatiche che vengono assegnate agli Utenti costituiscono uno strumento di lavoro.

L'insieme delle Risorse Informatiche a disposizione degli Utenti è suddiviso di norma in due categorie:

- Risorse assegnabili individualmente, cioè per via nominativa, al singolo Utente
- Risorse non assegnabili individualmente al singolo Utente, in quanto condivise nell'accesso e nell'utilizzo tra più Utenti.

Per Risorsa Informatica assegnabile nominalmente all'Utente, si intende ad esempio:

- la stazione di lavoro (denominata anche: personal computer o PC), costituita di solito dall'unità base elaborativa dotata di floppy disk, lettore/masterizzatore di CD/DVD, hard disk, video, tastiera e mouse
- la stampante eventualmente collegata alla stazione di lavoro di cui sopra
- gli eventuali altri dispositivi accessori esterni direttamente collegati alla stazione di lavoro (es. scanner, tavoletta grafica, ecc).

Per Risorsa Informatica non assegnabile nominalmente all'Utente ma a disposizione di gruppi di Utenti definiti dal SSIT, si intende ad esempio:

- una stazione di lavoro adibita a funzioni di sportello utilizzata a turno da diversi utenti;
- una stampante di gruppo collegata alla rete trasmissione dati comunale utilizzata da più Utenti
- uno spazio di memorizzazione su un sistema elaborativo dipartimentale (server) utilizzato da più Utenti che accedono e condividono le informazioni ivi contenute.

L'Utente è reso edotto che qualunque utilizzo delle Risorse Informatiche o comportamento da parte dell'Utente non strettamente inerente l'attività lavorativa può dare luogo a malfunzionamenti o disservizi sia nei confronti dell'utenza interna sia di soggetti e persone esterne, causando maggiori costi per l'Amministrazione e diseconomie nella gestione dei sistemi e delle attrezzature informatiche. Taluni utilizzi impropri delle Risorse Informatiche possono inoltre mettere a rischio la sicurezza informatica dei Sistemi Informativi dell'Amministrazione.

Art. 10 – Accesso

L'accesso alle Risorse Informatiche è riservato ai soli Utenti previa assegnazione delle stesse da parte del SSIT.

L'assegnazione di Risorse Informatiche ad un Utente avviene di norma dietro presentazione al SSIT di una richiesta motivata da parte del Dirigente da cui l'Utente dipende, oppure su iniziativa del SSIT nel caso di Risorse che rientrano in piani di sostituzione tecnologica di sistemi ed apparecchiature informatiche ormai obsolete.

Ogni Risorsa Informatica viene assegnata nominalmente a un Utente o, qualora si tratti di risorsa condivisa non assegnabile individualmente bensì ad un gruppo di Utenti, al Dirigente dal quale l'Utente dipende.

Il SSIT, ricevuta la richiesta di assegnazione della Risorsa, provvede all'assegnazione fisica della stessa sul posto di lavoro dell'Utente individuato, previa verifica di congruità tecnica ed organizzativa, tenendo conto di fattori quali:

- disponibilità di Risorse Informatiche a magazzino
- piani periodici di acquisizione di nuove attrezzature informatiche
- carichi di lavoro connessi alle attività tecnico-amministrative degli uffici del SSIT.

La comunicazione succitata indica altresì, in caso di riscontrata accoglibilità, i tempi previsti di evasione della richiesta medesima.

Tutte le richieste di assegnazione di Risorse Informatiche pervenute al SSIT vengono evase nel più breve tempo possibile, di norma nel rispetto dell'ordine di arrivo delle stesse e tenendo in debito conto le situazioni organizzative e le esigenze debitamente segnalate che impongono particolare urgenza.

L'elenco completo delle Risorse Informatiche in dotazione a ciascun Dipartimento e Servizio dell'Amministrazione viene trasmesso con cadenza annuale ad ogni Dirigente ai fini della verifica ai fini inventariali delle apparecchiature informatiche assegnate nominalmente agli Utenti o a gruppi di Utenti afferenti la stessa struttura organizzativa.

Ciascun Utente assegnatario di una Risorsa Informatica sottoscrive la dichiarazione di presa visione ed accettazione delle norme contenute nel presente Regolamento.

Art. 11 – Utilizzo

Non è consentito all'Utente la modifica delle caratteristiche fisiche impostate sulla Risorsa Informatica assegnata ad uso individuale né sulla Risorsa condivisa con altri Utenti.

In particolare, nel caso di stazione di lavoro, non è consentito all'Utente di provvedere, salvo la preventiva autorizzazione da parte del SSIT:

- all'installazione o alla rimozione di qualunque dispositivo interno o esterno all'unità base elaborativa o ad altre unità ad essa collegate al fine di modificare le caratteristiche tecniche o di funzionamento della stessa
- alla modifica di qualsiasi parametro di configurazione o di funzionamento relativo a caratteristiche tecniche dell'unità base elaborativa.

E' espressamente vietato all'Utente provvedere in via autonoma, cioè senza l'intervento da parte del personale tecnico del SSIT, allo spostamento fisico di una Risorsa Informatica, ovvero di parti e componenti della stessa, nell'ambito dello stesso ufficio, tra diversi uffici o tra le sedi dell'Amministrazione.

E' altresì severamente vietato all'Utente, in particolar modo se dipendente di società esterne, il collegamento anche temporaneo alla rete trasmissione dati comunale di sistemi ed apparecchiature informatiche di proprietà personale o aziendale, salvo la preventiva autorizzazione da parte del SSIT.

E' responsabilità dell'Utente provvedere affinché la stazione di lavoro assegnata ad uso individuale venga spenta ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.

L'Utente è consapevole che lasciare un elaboratore incustodito può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Per questo motivo viene suggerito all'Utente di attivare sulla stazione di lavoro ad uso individuale uno dei programmi salva

schermo (“screen saver”) forniti con il software installato dal SSIT, attivando la relativa password di sblocco, scelta nel rispetto di quanto indicato all’Art. 14 del presente Regolamento.

Non è consentita l'attivazione della password di accensione (altresì denominata “password di BIOS”) o di altro blocco fisico o logico su una Risorsa Informatica senza la preventiva autorizzazione da parte del SSIT.

Ogni Utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il SSIT nel caso in cui vengano rilevati dall’apposito software virus informatici sulla stazione di lavoro ad egli assegnata o nei casi di dubbia provenienza dei supporti.

I supporti rimovibili utilizzati per il trattamento delle informazioni (es. floppy disk, CD-ROM, ecc.) possono essere reimpiegati solamente quando le informazioni precedentemente contenute siano state cancellate in maniera definitiva; in caso contrario è responsabilità dell’Utente provvedere affinché gli stessi supporti vengano distrutti.

L’Utente è responsabilizzato sul fatto che, nel caso di restituzione in via definitiva di una stazione di lavoro, è suo preciso compito avvertire preventivamente il SSIT della eventuale presenza di archivi informatici contenenti dati personali, sensibili o riservati memorizzati nella stessa.

Art. 12 – Assistenza Tecnica

Tutti gli interventi di assistenza tecnica prestati da parte dei tecnici informatici appartenenti al SSIT o da parte di soggetti terzi debitamente autorizzati dal SSIT, attuati per la risoluzione di malfunzionamenti su Risorse Informatiche, possono essere eseguiti solamente con il consenso esplicito dell’Utente o con l’assenso del Dirigente da cui egli dipende. Qualora ciò non fosse possibile, il SSIT non si assume alcuna responsabilità per la mancata effettuazione dell’intervento stesso ed in particolare per ogni ritardo nelle attività lavorative dell’Utente derivato dal mancato intervento.

In particolare il tecnico informatico potrà accedere alle Risorse Informatiche assegnate all’Utente per fornire ausilio nella soluzione dei problemi tecnici da egli segnalati, anche remotamente mediante tecniche di telediagnosi (ad esempio visualizzando il contenuto dello schermo video della stazione di lavoro o il contenuto degli archivi), solamente se autorizzato come sopra precisato.

Art. 13 – Stazioni di lavoro portatili

L’Utente, qualora risulti assegnatario di una stazione di lavoro portatile (PC portatile), è responsabile della custodia della stessa sia durante gli spostamenti che durante l’utilizzo nel luogo di lavoro.

I PC portatili utilizzati anche per attività esterne all’Amministrazione (es. convegni, visite in azienda), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Alle stazioni di lavoro portatili si applicano le stesse regole di utilizzo previste per le stazioni di lavoro connesse di norma alla rete trasmissione dati comunale.

Art. 14 - Protezione Antivirus

Tutte le stazioni di lavoro assegnate agli Utenti sono protette contro il rischio di attacco al sistema informatico a opera di virus o altro software aggressivo di cui all’art.615 quinquies del codice

penale; la protezione si estende di norma anche ai sistemi dipartimentali (server) che ospitano informazioni e programmi utilizzati dagli Utenti ed al sistema di Posta Elettronica in uso presso l'Amministrazione.

La protezione avviene mediante l'utilizzo di idonei programmi installati sui sistemi la cui efficacia e aggiornamento sono verificati dal SSIT conformemente a quanto disposto dall'Allegato B del D.Lgs. 30 giugno 2003 n.196; ciononostante l'Utente è tenuto ad assumere comportamenti tali da ridurre al minimo tale rischio.

Non è consentito l'utilizzo di supporti di memorizzazione come floppy disk, CD-ROM, nastri magnetici o altro supporto di provenienza dubbia o ignota. In ogni caso qualunque dispositivo di memorizzazione di provenienza esterna all'Ente dovrà essere prudenzialmente verificato da parte dell'Utente mediante il programma antivirus prima del suo utilizzo.

Nel caso vi sia il sospetto della presenza di un virus informatico su un supporto di memorizzazione, quest'ultimo dovrà essere consegnato tempestivamente al SSIT per la successiva analisi e trattamento.

Nel caso in cui venga effettivamente rilevata dall'Utente la presenza di un virus su una stazione di lavoro dal programma software antivirus ivi installato, questi dovrà immediatamente:
- sospendere ogni elaborazione in corso senza spegnere la stazione di lavoro
- segnalare tempestivamente l'accaduto al servizio di Help Desk del SSIT.

TITOLO IV
SERVIZIO DI POSTA ELETTRONICA

Art. 15 – Generalità

La Posta Elettronica è un servizio di rete telematica disponibile per gli Utenti e costituisce uno strumento di lavoro che l'Amministrazione mette a disposizione degli stessi per migliorare la comunicazione interna ed esterna all'Ente.

Il servizio di Posta Elettronica dell'Amministrazione, permette la spedizione, la ricezione e l'inoltro di messaggi di testo o compositi tra i diversi Utenti dei Sistemi Informativi, ma può essere anche utilizzato per le comunicazioni da e verso l'esterno dell'Amministrazione tramite l'utilizzo della rete Internet.

Nel primo caso, a ciascun Utente abilitato all'utilizzo del servizio di Posta Elettronica viene assegnata dal SSIT una casella di posta elettronica nominativa.

Art. 16 – Accesso

L'accesso al servizio di Posta Elettronica è riservato ai soli Utenti, previa abilitazione da parte del SSIT.

L'abilitazione per l'accesso al servizio di Posta Elettronica ed il rilascio della relativa casella di posta elettronica, avviene di norma dietro presentazione al SSIT di una richiesta da parte del Dirigente da cui l'Utente dipende.

Con le modalità sopra descritte, il Dirigente può anche richiedere al SSIT l'attivazione di caselle di Posta Elettronica non nominative, cioè non destinate ad uso di Utenti bensì di carattere istituzionale (es. Sindaco, Assessore, generico Servizio o unità organizzativa, ecc), specificando la lista degli Utenti abilitati all'accesso ed utilizzo della stessa.

Il SSIT, ricevuta la richiesta di attivazione del servizio di Posta Elettronica per un Utente, provvede al rilascio di una credenziale di accesso ed alla creazione della casella di Posta Elettronica ad uso personale. Similmente, nel caso in cui la richiesta riguardi l'attivazione di una casella di Posta Elettronica istituzionale, il SSIT provvede alla creazione della stessa ed alle abilitazioni conseguenti.

L'Utente è responsabilizzato sul fatto che l'ID personale rilasciato dal SSIT per l'accesso ed utilizzo del sistema di Posta Elettronica è a tutti gli effetti assimilabile ad un'abilitazione di accesso dotata di password e come tale soggetta alle prescrizioni di cui agli Art. 12, 13 e 14 del presente Regolamento.

Art. 17 – Utilizzo

L'Utente si impegna ad utilizzare la casella di Posta Elettronica unicamente per scopi attinenti la propria attività lavorativa.

La dimensione massima di un singolo messaggio di Posta Elettronica in spedizione o in ricezione (compresi eventuali documenti allegati) è fissata a 5 Mb. La dimensione massima dello spazio di memorizzazione per tutti i messaggi di Posta Elettronica dell'Utente, contenuti cioè nelle cartelle dei messaggi arrivati, spediti, in bozza, ecc, è invece di 30 Mb.

Il SSIT si riserva di valutare dal punto di vista tecnico-organizzativo le eventuali richieste da parte degli Utenti di aumento delle dimensioni della casella di Posta Elettronica.

E' precisa responsabilità dell'Utente:
- non allegare ai messaggi di Posta Elettronica documenti troppo voluminosi
- tenere in ordine la casella di Posta Elettronica, curando periodicamente la dimensione della stessa (sia documenti arrivati che spediti), cancellando o archiviando i documenti inutili oppure obsoleti, soprattutto se dotati di allegati voluminosi

È espressamente vietato utilizzare il servizio di Posta Elettronica per:
- inviare, inoltrare o ricevere messaggi di carattere personale da altri Utenti o da corrispondenti terzi
- inviare o memorizzare messaggi interni o esterni di natura oltraggiosa, discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale o partitica
- partecipare a dibattiti, forum o mailing-list non aventi attinenza con l'attività lavorativa
- partecipare alle cosiddette "catene telematiche" (altresì denominate "catene di S. Antonio").

Il SSIT assicura la riservatezza dei contenuti delle caselle definite sul sistema di Posta Elettronica adottando opportune misure a garanzia della sicurezza informatica dei sistemi; resta però responsabilità dell'Utente curare la riservatezza della visione di comunicazioni contenute nella propria casella di Posta Elettronica, proteggendo opportunamente l'accesso indebito da parte di terzi alla stazione di lavoro come prescritto all'Art. 7 del presente Regolamento.

TITOLO V
SERVIZIO DI RETE INTERNET

Art. 18 – Generalità

La rete Internet è una risorsa informativa esterna che l'Amministrazione mette a disposizione degli Utenti per consentire la comunicazione con soggetti esterni, per la ricerca di informazioni sul web e per migliorare la qualità del lavoro svolto negli uffici comunali.

L'accesso e l'utilizzo del servizio di rete Internet è riservato esclusivamente per scopi attinenti l'attività lavorativa degli Utenti.

L'Utente è responsabilizzato sul fatto che taluni utilizzi impropri della rete Internet possono mettere a rischio la sicurezza informatica dei Sistemi Informativi.

Art. 19 – Accesso

L'accesso al servizio di rete Internet è riservato ai soli Utenti, previa abilitazione da parte del SSIT.

L'abilitazione per l'accesso al servizio di rete Internet avviene di norma dietro presentazione al SSIT di una richiesta da parte del Dirigente da cui l'Utente dipende.

Il SSIT, ricevuta la richiesta di attivazione del servizio di rete Internet per un Utente, provvede ad autorizzare lo stesso tramite apposita abilitazione dell'account utilizzato per usufruire i servizi di Rete Telematica dell'Amministrazione.

Art. 20 – Utilizzo

E' assolutamente vietata la consultazione e la navigazione sui siti della rete Internet per motivi diversi da quelli strettamente legati all'attività lavorativa svolta dall'Utente.

E' assolutamente vietato scaricare dalla rete Internet sulla stazione di lavoro assegnata all'Utente o su qualsiasi tipo di supporto di memorizzazione (es. hard disk o floppy disk della stazione di lavoro) qualunque tipo di contenuto digitale, ad eccezione di quello avente attinenza con l'attività lavorativa dell'Utente.

Per contenuto digitale scaricabile da Internet si intende, ad esempio:
- archivi o banche dati contenenti informazioni testuali, immagini, musica, video, anche se non soggetti a copyright
- programmi informatici, in particolare quelli eseguibili sulla stazione di lavoro assegnata all'Utente come ad esempio salva schermo o prodotti software anche su licenza, salvo esplicita autorizzazione da parte del SSIT.

E' tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ad uso personale, ivi comprese le operazioni di remote banking, acquisti on-line e simili.

L'Utente è responsabilizzato sul fatto che la registrazione, se non strettamente necessario, dei propri dati personali (ivi compreso l'indirizzo della casella di Posta Elettronica rilasciato dal SSIT), su siti Internet non sicuri non è raccomandabile per motivi di sicurezza informatica.

È vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche, le registrazioni in "guest-books" (anche utilizzando pseudonimi) e quant'altro in generale possa ricadere nella fattispecie di uso a scopi personali della rete Internet.

TITOLO VI
SERVIZI DI TELEFONIA FISSA E MOBILE

Art. 21 - Generalità

I Servizi facenti parte della Rete Telefonica dell'Amministrazione assegnabili agli Utenti vengono di norma erogati da Risorse strumentali appartenenti alla Rete Telefonica Fissa (tipicamente le postazioni telefoniche da tavolo) ed apparati di Rete Telefonica Mobile (apparati radiomobili cellulari).

Le Risorse di cui sopra vengono assegnate all'Utente in ragione dello svolgimento dell'attività lavorativa e delle funzioni a essa strettamente inerenti, in modo da rispondere all'interesse e alle esigenze dell'Amministrazione ed al miglioramento della qualità del lavoro e della produttività individuale.

In questo contesto, qualunque impiego di Risorse di Rete Telefonica Fissa o Mobile deve essere considerato ai soli scopi lavorativi e comunque in un quadro di corretto controllo della spesa corrente e miglioramento dell'efficienza interna dell'Amministrazione.

L'Amministrazione si conforma, per l'accesso ed utilizzo dei sistemi e delle apparecchiature di telefonia fissa e mobile, alle direttive approvate con D.P.C.M 11 aprile 1997 e ss.mm. e Dir.Min. 30 ottobre 2001.

Art. 22 – Accesso alle Risorse di Rete Telefonica Fissa

L'accesso alle Risorse di Rete Telefonica Fissa è riservato ai soli Utenti, previa assegnazione delle stesse da parte del SSIT.

L'assegnazione della Risorsa ad un Utente avviene di norma dietro presentazione di una richiesta motivata da parte del Dirigente da cui l'Utente dipende, che evidenzia anche le caratteristiche dell'apparecchio richiesto in considerazione del ruolo e delle funzioni svolte da parte dell'Utente.

Di norma ogni apparato di rete telefonica fissa viene assegnato nominalmente a un Utente oppure, qualora si tratti di Risorsa condivisa da più Utenti non assegnabile individualmente, al Responsabile dell'ufficio ovvero al Dirigente dal quale egli dipende.

Il SSIT, ricevuta la richiesta di assegnazione della Risorsa, effettua la verifica di fattibilità provvedendo di norma all'acquisizione ed assegnazione fisica della stessa sul posto di lavoro dell'Utente ed all'attivazione di una nuova utenza telefonica (numero interno).

Il SSIT provvede all'evasione delle richieste nel più breve tempo possibile di norma nel rispetto dell'ordine di arrivo delle stesse e tenendo in debito conto le situazioni organizzative e le esigenze debitamente segnalate che impongono particolare urgenza.

ART. 23 - UTILIZZO DELLE RISORSE DI RETE TELEFONICA FISSA

Pur ribadendo l'uso ai soli fini lavorativi dell'apparecchiatura telefonica, è consentito l'utilizzo in via eccezionale dello stesso anche ai fini privati purché tale utilizzo venga analiticamente documentato mediante autocertificazione prodotta al SSIT da parte dell'Utente assegnatario dell'apparato telefonico.

In ogni caso è espressamente vietato ad un Utente l'utilizzo ai fini privati di un apparato telefonico assegnato ad altro Utente.

A tutela dell'Amministrazione, il SSIT si riserva la facoltà di verificare dagli appositi tabulati telefonici forniti dalle apparecchiature di Rete Telefonica Fissa il flusso di traffico uscente da un apparato telefonico assegnato ad un Utente, anche dietro presentazione di richiesta motivata da parte del Dirigente da cui l'Utente dipende, assolvendo in tal modo alla funzione di controllo mirato rispetto all'utilizzo dell'apparecchio.

Il SSIT si riserva inoltre di effettuare d'ufficio tutti i controlli del caso qualora dall'esame del traffico telefonico relativo alle utenze attive venga rilevato uno scostamento significativo dalla media rilevata in precedenza.

Art. 24 – Accesso alle Risorse di Rete Telefonica Mobile

L'accesso ed utilizzo degli apparati radiomobili cellulari e/o schede SIM di servizio (di seguito nel presente articolo Risorsa) risponde ai seguenti criteri di base:

1. Particolare funzione ricoperta all'interno della struttura organizzativa dell'Ente;
2. Necessità di una reperibilità in via continuativa per motivi di servizio;
3. Funzioni svolte prevalentemente all'esterno delle sedi lavorative dell'Ente;
4. Indisponibilità o inopportunità di utilizzo di mezzi comunicativi diversi.

Ai fini dell'assegnazione dell'utenza radiomobile dovranno essere soddisfatti almeno due dei criteri sopra esposti.

L'assegnazione della Risorsa ad un Utente avviene di norma dietro presentazione di una richiesta da parte del Dirigente da cui l'Utente dipende. La richiesta, sulla base dei criteri sopra indicati, dovrà essere adeguatamente motivata e riportare le opportune necessarie indicazioni circa gli scopi e, ove opportuno, in relazione alle funzioni svolte dal dipendente.

Tuttavia, in virtù dei criteri base sopra esposti, l'assegnazione di una Risorsa può anche non essere effettuata per via nominativa ma avvenire nei confronti di un gruppo di Utenti finali.

In questo ultimo caso, l'Utente assegnatario della Risorsa è colui che viene individuato quale responsabile per il gruppo degli Utenti finali del richiedente.

Il SSIT provvede all'evasione delle richieste nel più breve tempo possibile, tenendo in debito conto le situazioni organizzative e le esigenze che impongono particolare urgenza, previa validazione della sussistenza delle condizioni indicate al primo paragrafo del presente articolo, alla verifica della disponibilità della Risorsa ed all'approvazione da parte della Direzione Generale.

I Dirigenti possono richiedere, sulla base dei criteri sopra enunciati, ed in presenza di esigenze di carattere temporanee e contingente, la concessione provvisoria di Risorse al termine della quale le stesse dovranno essere restituite al SSIT.

Le Risorse sono concesse in uso al dipendente, fino ad esplicita revoca.

Il Dirigente è tenuto a comunicare al SSIT sia il venir meno dei requisiti di assegnazione e uso della Risorsa indicati che la cessazione del rapporto di lavoro o il trasferimento del dipendente ad altro Ente e a restituire il materiale ricevuto in dotazione.

Nell'ipotesi di trasferimento ad altro ufficio dell'Amministrazione, l'eventuale permanere dei requisiti per l'assegnazione e l'uso della Risorsa per motivi di servizio, dovrà essere attestato dal Dirigente in cui è stato trasferito l'Utente.

Art. 25 – Utilizzo delle Risorse di Rete Telefonica Mobile

L'Utente è inoltre tenuto ad usare la massima diligenza nella custodia e nella conservazione della Risorsa assegnata e a segnalare al SSIT eventuali malfunzionamenti della stessa.

La risorsa assegnata nominalmente ad un Utente o gruppi di Utenti deve essere utilizzata ai soli fini dell'attività lavorativa.

E' precisa responsabilità dell'Utente assegnatario avvisare tempestivamente il SSIT l'eventuale furto o smarrimento della Risorsa, fornendo copia del verbale di denuncia o di smarrimento della Risorsa.

Se il furto o lo smarrimento avvengono in un momento in cui non è possibile comunicare con il SSIT, l'Utente dovrà contattare direttamente il gestore di telefonia al fine di bloccare la scheda SIM. In entrambi i casi è necessario successivamente far pervenire la regolare denuncia fornita davanti alle Autorità competenti al SSIT con le modalità sopra indicate. Le modalità per contattare il gestore di telefonia mobile saranno comunicate agli utenti dal SSIT.

L'Utente che utilizza la Risorsa è responsabile del suo corretto utilizzo dal momento dell'assegnazione fino alla revoca ovvero alla restituzione della stessa; qualora l'Utente assegnatario non coincida con l'Utente utilizzatore, come nel caso di assegnazioni di apparati e/o schede SIM ad uso di reperibilità del personale, è preciso compito del primo sensibilizzare opportunamente il responsabile affinché impartisca al gruppo degli utilizzatori finali le indicazioni per il corretto utilizzo dello strumento di lavoro.

L'utilizzo ai fini privati di un'utenza di Rete Telefonica Mobile assegnata nominalmente ad un Utente potrà avvenire mediante sottoscrizione di apposito contratto di dual-billing (letteralmente: doppia fatturazione) con il gestore del servizio, qualora ciò sia disponibile; tale sottoscrizione avviene dietro presentazione al SSIT di apposita richiesta di attivazione della modalità sopra esposta.

La modalità "dual-billing" permette di addebitare i soli costi relativi al traffico telefonico effettuato ad uso privato direttamente all'Utente finale assegnatario dell'utenza, separandoli dai costi addebitati all'Amministrazione causati dal traffico generato per l'utilizzo della Risorsa per ragioni di servizio. Per questo motivo l'attivazione della modalità "fatturazione separata" è riservata ai singoli Utenti cui è stata assegnata una Risorsa e non a gruppi di Utenti.

È in ogni caso espressamente vietato l'utilizzo ai fini privati della risorsa assegnata ad altro Utente.

A tutela dell'Amministrazione, il SSIT si riserva la facoltà di verificare dagli appositi tabulati telefonici forniti dal gestore dei servizi di Rete Telefonica Mobile il flusso di traffico generato da un'utenza assegnata ad un Utente, anche dietro presentazione di richiesta motivata da parte del Dirigente da cui l'Utente, o il gruppo di Utenti, dipende, assolvendo in tal modo alla funzione di controllo mirato rispetto all'utilizzo della Risorsa.

Il SSIT si riserva inoltre di effettuare d'ufficio tutti i controlli del caso qualora, dall'esame del traffico telefonico relativo alle utenze attive, venga rilevato uno scostamento significativo dalla media rilevata in precedenza.

TITOLO VII
DISPOSIZIONI FINALI

Art. 26 - Responsabilità degli Utenti

Ciascun Utente dei Sistemi Informativi ha la responsabilità di segnalare immediatamente al SSIT ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza riguardante le Risorse Informatiche, Telematiche e Telefoniche ad egli assegnate o comunque utilizzate.

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento costituisce illecito perseguibile disciplinarmente, fatte sempre salve le responsabilità civili e penali.

APPENDICE A

LEGISLAZIONE

Decreto legislativo 30 giugno 2003 n.196
Codice in materia di protezione dei dati personali (estratto)

Art. 2 (Finalità)
1. Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
2. Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui al comma 1 nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento.

Art. 4 (Definizioni)
1. Ai fini del presente codice si intende per:
a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, 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, anche se non registrati in una banca di dati;
b) "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;
c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;
d) "dati sensibili", 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, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
e) "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, 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 degli articoli 60 e 61 del codice di procedura penale;
f) "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
g) "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
h) "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
i) "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
l) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
m) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
n) "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
o) "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
p) "banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
q) "Garante", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.
[*omissis*]
3. Ai fini del presente codice si intende, altresì, per:
a) "misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
b) "strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
c) "autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
d) "credenziali di autenticazione", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica;
e) "parola chiave", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

f) “profilo di autorizzazione”, l’insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
g) “sistema di autorizzazione”, l’insieme degli strumenti e delle procedure che abilitano l’accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
[*omissis*]

Art. 15 (Danni cagionati per effetto del trattamento)
1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.
2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

Art. 31 (Obblighi di sicurezza)
1. I dati personali oggetto di trattamento sono 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.

ALLEGATO B
DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA
Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell’incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l’identificazione dell’incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell’incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell’incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l’autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell’incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all’incaricato ed è modificata da quest’ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l’identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all’incaricato l’accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l’accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l’autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell’incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l’incaricato dell’intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all’inizio del trattamento, in modo da limitare l’accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente**,** è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale**.**
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:
19.1. l'elenco dei trattamenti di dati personali;
19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
19.3. l'analisi dei rischi che incombono sui dati;
19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati
personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-*ter* del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro
trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Decreto legislativo 29 dicembre 1992 n. 518
Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore (estratto)

Art. 1
1. All'art. 1 della legge 22 aprile 1941, n. 633, è aggiunto il seguente comma:
"Sono altresì protetti i programmi per elaboratore come opere letterarie ai sensi della Convenzione di Berna sulla protezione delle opere letterarie ed artistiche ratificata e resa esecutiva con legge 20 giugno 1978, n. 399".

Art. 5
1. Dopo la sezione V del capo IV del titolo I della legge 22 aprile 1941, n. 633, è aggiunta la seguente sezione:
"Sezione VI - PROGRAMMI PER ELABORATORE
Art. 64- bis . - 1. Fatte salve le disposizioni dei successivi articoli 64- ter e 64-quater, i diritti esclusivi conferiti dalla presente legge sui programmi per elaboratore comprendono il diritto di effettuare o autorizzare:
a) la riproduzione, permanente o temporanea, totale o parziale, del programma per elaboratore con qualsiasi mezzo o in qualsiasi forma. Nella misura in cui operazioni quali il caricamento, la visualizzazione, l'esecuzione, la trasmissione o la memorizzazione del programma per elaboratore richiedano una riproduzione, anche tali operazioni sono soggette all'autorizzazione del titolare dei diritti;
b) la traduzione, l'adattamento, la trasformazione e ogni altra modificazione del programma per elaboratore, nonché la riproduzione dell'opera che ne risulti, senza pregiudizio dei diritti di chi modifica il programma;
c) qualsiasi forma di distribuzione al pubblico, compresa la locazione, del programma per elaboratore originale o di copie dello stesso. La prima vendita di una copia del programma nella Comunità Economica Europea da parte del titolare dei diritti, o con il suo consenso, esaurisce il diritto di distribuzione di detta copia all'interno della Comunità, ad eccezione del diritto di controllare l'ulteriore locazione del programma o di una copia dello stesso.
Art. 64- ter . - 1. Salvo patto contrario, non sono soggette all'autorizzazione del titolare dei diritti le attività indicate nell'art. 64- bis, lettere a) e b), allorché tali attività sono necessarie per l'uso del programma per elaboratore conformemente alla sua destinazione da parte del legittimo acquirente, inclusa la correzione degli errori.
2. Non può essere impedito per contratto, a chi ha il diritto di usare una copia del programma per elaboratore di effettuare una copia di riserva del programma, qualora tale copia sia necessaria per l'uso.
3. Chi ha il diritto di usare una copia del programma per elaboratore può, senza l'autorizzazione del titolare dei diritti, osservare, studiare o sottoporre a prova il funzionamento del programma, allo scopo di determinare le idee ed i principi su cui è basato ogni elemento del programma stesso, qualora egli compia tali atti durante operazioni di caricamento, visualizzazione, esecuzione, trasmissione o memorizzazione del programma che egli ha il diritto di eseguire. Gli accordi contrattuali conclusi in violazione del presente comma sono nulli.
Art. 64-quater . - 1. L'autorizzazione del titolare dei diritti non è richiesta qualora la riproduzione del codice del programma di elaboratore e la traduzione della sua forma ai sensi dell'art. 64- bis, lettere a) e b), compiute al fine di modificare la forma del codice, siano indispensabili per ottenere le informazioni necessarie per conseguire l'interoperabilità, con altri programmi, di un programma per elaboratore creato autonomamente purché siano soddisfatte le seguenti condizioni:
a) le predette attività siano eseguite dal licenziatario o da altri che abbia il diritto di usare una copia del programma oppure, per loro conto, da chi è autorizzato a tal fine;
b) le informazioni necessarie per conseguire l'interoperabilità non siano già facilmente e rapidamente accessibili ai soggetti indicati alla lettera a);
c) le predette attività siano limitate alle parti del programma originale necessarie per conseguire l'interoperabilità.
2. Le disposizioni di cui al comma 1 non consentono che le informazioni ottenute in virtù della loro applicazione:
a) siano utilizzate a fini diversi dal conseguimento dell'interoperabilità del programma creato autonomamente;
b) siano comunicate a terzi, fatta salva la necessità di consentire l'interoperabilità del programma creato autonomamente;
c) siano utilizzate per lo sviluppo, la produzione o la commercializzazione di un programma per elaboratore sostanzialmente simile nella sua forma espressiva, o per ogni altra attività che violi il diritto di autore.
3. Gli accordi contrattuali conclusi in violazione dei commi 1 e 2 sono nulli.
4. Conformemente alla convenzione di Berna sulla tutela delle opere letterarie ed artistiche ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, le disposizioni del presente articolo non possono essere interpretate in modo da consentire che la loro applicazione arrechi indebitamente pregiudizio agli interessi legittimi del titolare dei diritti o sia in conflitto con il normale sfruttamento del programma".

Art. 8
1. All'art. 161 della legge 22 aprile 1941, n. 633, è aggiunto, in fine, il seguente comma:
"Le disposizioni di questa Sezione si applicano anche a chi mette in circolazione in qualsiasi modo, o detiene per scopi commerciali copie non autorizzate di programmi e qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'esclusione funzionale dei dispositivi applicati a protezione di un programma per elaboratore".

Art. 10
1. Dopo l'art. 171 della legge 22 aprile 1941, n. 633, è inserito il seguente:

"Art. 171- bis . - 1. Chiunque abusivamente duplica a fini di lucro, programmi per elaboratore, o, ai medesimi fini e sapendo o avendo motivo di sapere che si tratta di copie non autorizzate, importa, distribuisce, vende, detiene a scopo commerciale, o concede in locazione i medesimi programmi, è soggetto alla pena della reclusione da tre mesi a tre anni e della multa da L. 500.000 a L. 6.000.000. Si applica la stessa pena se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale dei dispositivi applicati a protezione di un programma per elaboratore. La pena non è inferiore nel minimo a sei mesi di reclusione e la multa a L. 1.000.000 se il fatto è di rilevante gravità ovvero se il programma oggetto dell'abusiva duplicazione, importazione, distribuzione, vendita, detenzione a scopo commerciale o locazione sia stato precedentemente distribuito, venduto o concesso in locazione su supporti contrassegnati dalla Società italiana degli autori ed editori ai sensi della presente legge e del relativo regolamento di esecuzione approvato con regio decreto 18 maggio 1942, n. 1369.
2. La condanna per i reati previsti al comma 1 comporta la pubblicazione della sentenza in uno o più quotidiani e in uno o più periodici specializzati".

Decreto legislativo 6 maggio 1999, n. 169
Attuazione della direttiva 96/9/CE relativa alla tutela giuridica delle banche di dati (estratto)

Art. 1
1. Al secondo comma dell'articolo 1 della legge 22 aprile 1941, n. 633, sono aggiunte, in fine, le seguenti parole:
«, nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore.».

Art. 2
1. Dopo il numero 8) dell'articolo 2 della legge 22 aprile 1941, n. 633, è aggiunto il seguente:
«9) Le banche di dati di cui al secondo comma dell'articolo 1, intese come raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo. La tutela delle banche di dati non si estende al loro contenuto e lascia impregiudicati diritti esistenti su tale contenuto.».

Art. 4
1. Dopo la sezione VI del capo IV del titolo 1 della legge 22 aprile 1941, n. 633, è inserita la seguente:
«Sezione VII
BANCHE DI DATI
Art. 64-*quinquies*. - 1. L'autore di un banca di dati ha il diritto esclusivo di eseguire o autorizzare:
a) la riproduzione permanente o temporanea, totale o parziale, con qualsiasi mezzo e in qualsiasi forma;
b) la traduzione, l'adattamento, una diversa disposizione e ogni altra modifica;
e) qualsiasi forma di distribuzione al pubblico dell'originale o di copie della banca di dati; la prima vendita di una copia nel territorio dell'Unione europea da parte del titolare del diritto o con il suo consenso esaurisce il diritto di controllare, all'interno dell'Unione stessa, le vendite successive della copia;
d) qualsiasi presentazione, dimostrazione o comunicazione in pubblico, ivi compresa la trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma;
e) qualsiasi riproduzione, distribuzione, comunicazione, presentazione o dimostrazione in pubblico dei risultati delle operazioni di cui alla lettera b).
Art. 64-*sexies*. - 1. Non sono soggetti all'autorizzazione di cui all'articolo 64-quinquies da parte del titolare del diritto:
a) l'accesso o la consultazione della banca di dati quando abbiano esclusivamente finalità didattiche o di ricerca scientifica, non svolta nell'ambito di un'impresa, purché si indichi la fonte e nei limiti di quanto giustificato dallo scopo non commerciale perseguito. Nell'ambito di tali attività di accesso e consultazione, le eventuali operazioni di riproduzione permanente della totalità o di parte sostanziale del contenuto su altro supporto sono comunque soggette all'autorizzazione del titolare del diritto;
b) l'impiego di una banca di dati per fini di sicurezza pubblica o per effetto di una procedura amministrativa o giurisdizionale.
2. Non sono soggette all'autorizzazione dell'autore le attività indicate nell'articolo 64-quinquies poste in essere da parte dell'utente legittimo della banca di dati o di una sua copia, se tali attività sono necessarie per l'accesso al contenuto della stessa banca di dati e per il suo normale impiego; se l'utente legittimo è autorizzato ad utilizzare solo una parte della banca di dati, il presente comma si applica unicamente a tale parte.
3. Le clausole contrattuali pattuite in violazione del comma 2 sono nulle ai sensi dell'articolo 1418 del codice civile.
4. Conformemente alla Convenzione di Berna per la protezione delle opere letterarie e artistiche, ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, le disposizioni di cui ai commi 1 e 2 non possono essere interpretate in modo da consentire che la loro applicazione arrechi indebitamente pregiudizio al titolare del diritto o entri in conflitto con il normale impiego della banca di dati.».

Art. 5
1. Dopo il titolo Il della legge 22 aprile 1941, n. 633, è inserito il seguente:
«TITOLO II-bis
DISPOSIZIONI SUI DIRITTI DEL COSTITUTORE DI UNA BANCA DI DATI DIRITTI E OBBLIGHI DELL'UTENTE
Capo I
DIRITTI DEL COSTITUTORE DI UNA BANCA DI DATI
Art. 102-*bis*. - 1. Ai fini del presente titolo si intende per:
a) costitutore di una banca di dati: chi effettua investimenti rilevanti per la costituzione di una banca di dati o per la sua verifica o la sua presentazione, impegnando, a tal fine, mezzi finanziari, tempo o lavoro;
b) estrazione: il trasferimento permanente o temporaneo della totalità o di una parte sostanziale del contenuto di una banca di dati su un altro supporto con qualsiasi mezzo o in qualsivoglia forma. L'attività di prestito dei soggetti di cui all'articolo 69, comma 1, non costituisce atto di estrazione;
c) reimpiego: qualsivoglia forma di messa a disposizione del pubblico della totalità o di una parte sostanziale del contenuto della banca di dati mediante distribuzione di copie, noleggio, trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma. L'attività di prestito dei soggetti di cui all'articolo 69, comma 1, non costituisce atto di reimpiego.
2. La prima vendita di una copia della banca di dati effettuata o consentita dal titolare in uno Stato membro dell'Unione europea esaurisce il diritto di controllare la rivendita della copia nel territorio dell'Unione europea.

3. Indipendentemente dalla tutelabilità della banca di dati a norma del diritto d'autore o di altri diritti e senza pregiudizio dei diritti sul contenuto o parti di esso, il costitutore di una banca di dati ha il diritto, per la durata e alle condizioni stabilite dal presente Capo, di vietare le operazioni di estrazione ovvero reimpiego della totalità o di una parte sostanziale della stessa.
4. Il diritto di cui al comma 3 si applica alle banche di dati i cui costitutori o titolari di diritti sono cittadini di uno Stato membro dell'Unione europea o residenti abituali nel territorio dell'Unione europea.
5. La disposizione di cui al comma 3 si applica altresì alle imprese e società costituite secondo la normativa di uno Stato membro dell'Unione europea ed aventi la sede sociale, l'amministrazione centrale o il centro d'attività principale all'interno della Unione europea; tuttavia, qualora la società o l'impresa abbia all'interno della Unione europea soltanto la propria sede sociale, deve sussistere un legame effettivo e continuo tra l'attività della medesima e l'economia di uno degli Stati membri dell'Unione europea.
6. Il diritto esclusivo del costitutore sorge al momento del completamento della banca di dati e si estingue trascorsi quindici anni dal I' gennaio dell'anno successivo alla data del completamento stesso.
7. Per le banche di dati in qualunque modo messe a disposizione del pubblico prima dello scadere del periodo di cui al comma 6, il diritto di cui allo stesso comma 6 si estingue trascorsi quindici anni dal I' gennaio dell'anno successivo alla data della prima messa a disposizione del pubblico.
8. Se vengono apportate al contenuto della banca di dati modifiche o integrazioni sostanziali comportanti nuovi investimenti rilevanti ai sensi del comma 1, lettera a), dal momento del completamento o della prima messa a disposizione del pubblico della banca di dati così modificata o integrata, e come tale espressamente identificata, decorre un autonomo termine di durata della protezione, pari a quello di cui ai commi 6 e 7.
9. Non sono consentiti l'estrazione o il reimpiego ripetuti e sistematici di parti non sostanziali del contenuto della banca di dati, qualora presuppongano operazioni contrarie alla normale gestione della banca di dati o arrechino un pregiudizio ingiustificato al costitutore della banca di dati.
10. Il diritto di cui al comma 3 può essere acquistato o trasmesso in tutti i modi e forme consentiti dalla legge.

Capo II

DIRITTI E OBBLIGHI DELL'UTENTE

Art. 102-*ter*. - 1. L'utente legittimo della banca di dati messa a disposizione del pubblico non può arrecare pregiudizio al titolare del diritto d'autore o di un altro diritto connesso relativo ad opere o prestazioni contenute in tale banca.
2. L'utente legittimo di una banca di dati messa in qualsiasi modo a disposizione del pubblico non può eseguire operazioni che siano in contrasto con la normale gestione della banca di dati o che arrechino un ingiustificato pregiudizio al costitutore della banca di dati.
3. Non sono soggette all'autorizzazione del costitutore della banca di dati messa per qualsiasi motivo a disposizione del pubblico le attività di estrazione o reimpiego di parti non sostanziali, valutate in termini qualitativi e quantitativi, del contenuto della banca di dati per qualsivoglia fine effettuate dall'utente legittimo. Se l'utente legittimo è autorizzato ad effettuare l'estrazione o il reimpiego solo di una parte della banca di dati, il presente comma si applica unicamente a tale parte.
4. Le clausole contrattuali pattuite in violazione dei commi 1, 2 e 3 sono nulle.».

Art. 6

1. L'articolo 171-bis della legge 22 aprile 1941, n. 633, è così modificato:
a) dopo il comma 1, è aggiunto il seguente:
«1 -*bis*. Chiunque, al fine di trarne profitto, riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter è soggetto alla pena della reclusione da tre mesi a tre anni e della multa da lire un milione a lire dieci milioni. La pena non è inferiore nel minimo a sei mesi di reclusione e a lire tre milioni di multa se il fatto è di rilevante gravità ovvero se la banca di dati oggetto delle abusive operazioni di riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, estrazione o reimpiego sia stata distribuita, venduta o concessa in locazione su supporti contrassegnati dalla Società italiana degli autori ed editori ai sensi della presente legge e del relativo regolamento di esecuzione approvato con R.D. 18 maggio 1942, n. 1369»;
b) al comma 2, le parole: «al comma 1 » sono sostituite dalle seguenti: «ai commi 1 e 1-bis».

Legge 23 dicembre 1993 n. 547
Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica (estratto)

Art. 1
1. All'art. 392 del codice penale, dopo il secondo comma è aggiunto il seguente:
"Si ha, altresì, violenza sulle cose allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico".

Art. 2
1. L'art. 420 del codice penale è sostituito dal seguente:
"Art. 420. - (Attentato a impianti di pubblica utilità).-Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni.
La pena di cui al primo comma si applica anche a chi commette un fatto diretto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità, ovvero dati, informazioni o programmi in essi contenuti o a essi pertinenti.
Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema, la pena è della reclusione da tre a otto anni".

Art. 3
1. Dopo l'art. 491 del codice penale è inserito il seguente:
"Art. 491-bis. - (Documenti informatici).- Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente agli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli".

Art. 4
1. Dopo l'articolo 615-bis del codice penale sono inseriti i seguenti:
"Art. 615-ter. - (Accesso abusivo a un sistema informatico o telematico). - Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.
La pena è della reclusione da uno a cinque anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in essi contenuti.
Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici d'interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.
Art.615-quater. - (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici). Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a un anno e con la multa sino a lire 10 milioni.
La pena è della reclusione da uno a due anni e della multa da lire 10 milioni a 20 milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617-quater.
Art. 615-quinquies. - (Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico). -Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi un esso contenuti o a esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire 20 milioni".

Art. 5
1. Nell'art. 616 del codice penale, il quarto comma è sostituito dal seguente:
"Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza".

Art. 6
1. Dopo l'art. 617-ter del codice penale sono inseriti i seguenti:

"Art. 617-quater. - (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche). - Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo d'informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.
Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:
1) in danno di un sistema informatico o telematico utilizzato dallo stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri e con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
3) da chi esercita anche abusivamente la professione di un investigatore privato.
Art. 617-quinquies. - (Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche) .- Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.
La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617-quater.
Art. 617 sexies. - (Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche). - Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro armi.
La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617-quater".

Art. 7
1. Nell'art. 621 del codice penale, dopo il primo comma è inserito il seguente:
"Agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi".

Art. 8
1. L'art. 623-bis del codice penale è sostituito dal seguente:
"Art. 623-bis. - (Altre comunicazioni e conversazioni).- Le disposizioni contenute nella presente sezione, relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano a qualunque altra trasmissione a distanza dei suoni, immagini o altri dati".

Art. 9
1.Dopo l'art. 635 del codice penale è inserito il seguente:
"Se ricorre una o più delle circostanze di cui al secondo comma dell'art. 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni".

Art. 10
1. Dopo l'art. 640 bis del codice penale è inserito il seguente:
"Art. 640-ter. - (Frode informatica). - Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità sui dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire 100 mila a 2 milioni.
La pena è della reclusione da uno a cinque anni e della multa da lire 600 mila a 3 milioni se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'art. 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.
Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante".

APPENDICE B

Dichiarazione di Presa Visione

Presa visione del Regolamento per l'utilizzo dei Sistemi Informativi, delle Risorse Informatiche, Telematiche e Telefoniche del Comune di Udine, approvato con Deliberazione di Giunta Comunale n. ord. _____ datata _____,

il/la sottoscritto/a _____,

appartenente al Dipartimento/Servizio/Società _____

nella sua qualità di Utente dei sistemi e delle risorse stesse, con la presente

DICHIARA

di averne inteso il significato e di impegnarsi ad accettare e rispettare le regole ivi contenute, sotto la propria responsabilità penale, civile e disciplinare.

In fede.

Udine, _____

Firma

_____