ASL DI BERGAMO	ISTRUZIONE	Cod. IOAGL06/1	P. 0/7

Titolo

REGOLAMENTO PER LA GESTIONE DEI DATI PERSONALI

COPIA

ISTRUZIONE OPERATIVA RELATIVA ALLA PG12

REVISIONE N. 1 DEL 26 APRILE 2004

EMESSO DA:
Il Responsabile Assicurazione Qualità
Dott.ssa Giuliana Mazzoleni

APPROVATO DA:
Responsabile del Servizio
Dott. Cesare Al. Infascelli

Titolo

REGOLAMENTO PER LA GESTIONE DEI DATI PERSONALI

DESTINATARI

Fermo restando che la normativa completa di riferimento è contenuta nel Codice per la protezione dei dati personali, approvato con Decreto legislativo 30/6/2003, n. 196, questo Regolamento è in modo particolare indirizzato a:

- *Responsabili del trattamento dei dati*
- *Amministratore di sistema*
- *Preposto alla conservazione delle password di accesso ai server*
- *Incaricati al Trattamento dei dati*
- Tutti i *dipendenti* preposti alla custodia della propria password, secondo le indicazioni fornite dal responsabile del trattamento dei dati a cui fanno riferimento

Nell'ASL di Bergamo, tali figure sono così individuate:

Responsabili del trattamento dati: sono i Responsabili di 1° e 2° livello, o loro delegati, appositamente individuati con nomina firmata per accettazione;

Amministratore di sistema: figura appositamente scelta fra il personale del Servizio Sistema Informativo Aziendale - "Information Technology – IT per intervenire in caso di problematiche relative agli *user id,* alle *password* e nella gestione delle misure di sicurezza adottate a tutela del sistema informativo aziendale;

Preposto alla conservazione delle password dei server: è un addetto del Servizio Sistema Informativo Aziendale - "Information Technology – IT incaricato di custodire ed aggiornare le password di accesso ai server dell'azienda

Incaricati al trattamento dei dati: sono i dipendenti individuati dai Responsabili, con nomina firmata per accettazione, per coadiuvare con gli stessi nel trattamento dei dati

TERMINI DI RIFERIMENTO

Al fine di rendere più chiara ed agevole la lettura si specificano qui di seguito i significati di alcuni fra i termini più ricorrenti usati dal legislatore.

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.

Ai fini della Tutela dei dati si intende, inoltre, per:

a) "comunicazione elettronica", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

b) "chiamata", la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;

c) "reti di comunicazione elettronica", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

d) "rete pubblica di comunicazioni", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

e) "servizio di comunicazione elettronica", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

f) "abbonato", qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura ditali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

g) "utente", qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

h) "dati relativi al traffico", qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

i) "dati relativi all'ubicazione", ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

l) "servizio a valore aggiunto", il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

m) "posta elettronica", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

Alle seguenti definizioni si intende dare il significato di:

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.

Circa le finalità del trattamento si intende per:

a) "scopi storici", le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;

b) "scopi statistici", le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;

c) "scopi scientifici", le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

REGOLE PER IL TRATTAMENTO DEI DATI

A) TRATTAMENTO SU SUPPORTO CARTACEO

1) Accesso ai dati

L'accesso ai dati personali è consentito esclusivamente al Responsabile del trattamento dei dati, ovvero alle persone dallo stesso incaricate. Queste ultime, se espressamente autorizzate, potranno visionare e, se del caso, prelevare esclusivamente i dati circa i quali hanno avuto incarico al trattamento, unicamente per lo specifico trattamento e per il tempo strettamente necessario allo stesso

Qualora il Responsabile o l'incaricato avesse necessità di archiviare temporaneamente i documenti cui si riferisce il trattamento, per quanto concerne i dati sensibili dovrà osservare le disposizioni previste nel seguente punto 3), 2° capoverso.

2) Accesso agli archivi

L'accesso agli archivi permanenti è consentito esclusivamente al Responsabile del trattamento dei dati, ovvero alle persone dallo stesso incaricate. Queste ultime, se espressamente autorizzate, potranno visionare e, se del caso, prelevare esclusivamente i dati circa i quali hanno avuto incarico al trattamento, unicamente per lo specifico trattamento e per il tempo strettamente necessario allo stesso.

Inoltre l'accesso all'archivio permanente dei dati sensibili dovrà essere controllato mediante:

a) registrazione di data e ora;

b) durata di permanenza nell'archivio.

In caso di accesso dell'incaricato all'archivio dati personali sensibili fuori dell'orario di lavoro, oltre alle disposizioni sopra riportate, sarà necessario effettuare la registrazione con l'espressa indicazione "fuori orario" e con la più precisa indicazione di data, ora e tempo di permanenza dell'incaricato nell'archivio.

3) Archiviazione temporanea dei dati sensibili

In caso di asporto dall'archivio, al fine di trattamento di dati personali sensibili, verificandosi la necessità di interruzione temporanea del trattamento stesso, i documenti contenenti i dati dovranno essere riposti e custoditi, per il tempo strettamente necessario all'interruzione, in apposite cassettiere, o armadi, o altro idoneo contenitore, muniti di serratura e rigorosamente chiusi a chiave. L'incaricato, sempre per il tempo strettamente necessario, custodirà la chiave a propria cura e sotto la propria responsabilità.

In caso di necessità di fotocopiatura o, comunque, di riproduzione dei documenti contenenti i dati personali sensibili ci si dovrà attentamente attenere a tutte le procedure soprariportate. Si dovrà, in particolare, osservare il massimo scrupolo per evitare che, durante la fase della duplicazione, i dati contenuti nei documenti possano in qualche modo venire a conoscenza di terzi non autorizzati.

B) TRATTAMENTO SU SUPPORTO MAGNETICO

1) Nomina dell'incaricato - Password

Il trattamento dei dati a mezzo di elaboratore è consentito solo ed esclusivamente all'incaricato , all'uopo nominato dal Responsabile del trattamento dati e munito di apposita password.

Le parole chiave potranno essere fornite solo all'incaricato del trattamento, esclusivamente e direttamente da parte del Responsabile, ovvero dagli amministratori di sistema individuati presso il Servizio Sistema Informativo Aziendale - "Information Technology – IT.

La gestione delle password è affidata ai singoli utenti, su indicazione del Responsabile del trattamento dei dati di riferimento.

Il Responsabile del trattamento dei dati deve:

a) verificare il corretto e diligente utilizzo della parola chiave;

b) informare gli incaricati del trattamento sui modi di selezione delle parole chiave e su come esse debbano essere custodite.

All'atto della consegna l'incaricato verrà ammonito delle responsabilità in ordine della tutela dei dati.

La modifica, da parte dell'interessato, della password avviene:

- per scadenza obbligatoria dei termini imposti dall'Amministratore del sistema
- per necessità del singolo utente.

In entrambi i casi gli obblighi del titolare della password varieranno a seconda delle indicazioni del proprio responsabile del trattamento dei dati di riferimento.

2) Codice di identificazione personale

Siccome i personal computer dell'Azienda sono, con rare eccezioni, tutti collegati in rete, i singoli *user id* assegnati e le rispettive password sono da considerarsi Codici Identificativi Personali di accesso alla rete.

Pertanto detta combinazione di user id e password non può essere assegnata a persone diverse neppure in tempi diversi.

Tale combinazione identificativa verrà disattivata nel caso di allontanamento definitivo dall'azienda del titolare.

3) Autorizzazione trattamento dati sensibili

L'incaricato del trattamento dei dati sensibili, qualora effettui il trattamento mediante elaboratori collegati in rete, dovrà essere previamente autorizzato dal Responsabile, sia singolarmente o per gruppi di lavoro.

Qualora l'incaricato dovesse provvedere all'interconnessione mediante reti con cui, in tutto o in parte, sia possibile collegarsi col mondo esterno usufruendo di reti di comunicazione e trasmissione, non esclusivamente privata , ma in ogni caso usufruibile da chiunque e pertanto definibili pubbliche, l'autorizzazione dovrà specificatamente prevedere quali elaboratori potranno essere utilizzati per detta interconnessione.

Ai dati sensibili sanitari, in particolare, potranno accedere i soli incaricati del trattamento, preposti caso per caso, alle specifiche fasi dell'attività sanitaria.

4) Custodia della parola chiave

Il Responsabile del sistema informativo sarà nominato per iscritto quale "Preposto alla custodia della password dei serve", mentre la custodia delle password dei singoli utenti viene gestita direttamente da questi su indicazione dei Responsabili del trattamento dei dati di riferimento.

Ciascun utente dovrà custodire le password ed i codici identificativi personali con il massimo scrupolo e la più totale riservatezza, ponendo in essere tutti gli accorgimenti atti ed idonei alla massima prevenzione di ogni possibile rischio di perdite, deterioramenti, sottrazioni o, comunque, conoscenza da parte di terze persone.

5) Programmi antivirus

Tutti gli elaboratori dedicati al trattamento dei dati personali, sensibili e non, che siano collegati in reti sia accessibili che non accessibili al pubblico, devono essere dotati di idonei programmi antivirus atti a prevenire in modo idoneo i fatti previsti nell'art. 615 quinquies Codice Penale, il quale espressamente sanziona la diffusione di programmi diretti a danneggiare il sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale o l'alterazione del suo funzionamento.

L'efficacia e l'aggiornamento di tali programmi antivirus deve essere sempre tenuta sotto controllo ed aggiornata.

In ogni caso l'aggiornamento deve avvenire al massimo ogni sei mesi ed è a cura del Servizio Sistema Informativo Aziendale - "Information Technology – IT.

***