

# **REGOLAMENTO PER IL TRATTAMENTO DEI DATI SENSIBILI E GIUDIZIARI**

**Approvato con Deliberazione C.C. n° 16 del 20/2/06**

## **ARTICOLO 1**

### **Oggetto del Regolamento**

Il presente Regolamento in attuazione del d.lg. 30 giugno 2003, n. 196, identifica i tipi di dati sensibili e giudiziari e le operazioni eseguibili da parte del Comune nello svolgimento delle proprie funzioni istituzionali.

## **ARTICOLO 2**

### **Individuazione dei tipi di dati e di operazioni eseguibili**

In attuazione delle disposizioni di cui agli artt. 20, comma 2, e 21, comma 2, del d.lg. 30 giugno 2003, n. 196, le tabelle che formano parte integrante del presente Regolamento, contraddistinte dai numeri da 1 a 8, identificano i tipi di dati sensibili e giudiziari per cui è consentito il relativo trattamento, nonché le operazioni eseguibili in riferimento alle specifiche finalità di rilevante interesse pubblico perseguite nei singoli casi ed espressamente elencate nel d.lg. n. 196/2003 (artt. 59, 60, 62-73, 86, 95, 98 e 112).

I dati sensibili e giudiziari individuati dal presente regolamento sono trattati previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi, specie nel caso in cui la raccolta non avvenga presso l'interessato.

Le operazioni di interconnessione, raffronto, comunicazione e diffusione individuate nel presente regolamento sono ammesse soltanto se indispensabili allo svolgimento degli obblighi o compiti di volta in volta indicati, per il perseguimento delle rilevanti finalità di interesse pubblico specificate e nel rispetto delle disposizioni rilevanti in materia di protezione dei dati personali, nonché degli altri limiti stabiliti dalla legge e dai regolamenti.

I raffronti e le interconnessioni con altre informazioni sensibili e giudiziarie detenute dal Comune sono consentite soltanto previa verifica della loro stretta indispensabilità nei singoli casi ed indicazione scritta dei motivi che ne giustificano l'effettuazione. Le predette operazioni, se effettuate utilizzando banche di dati di diversi titolari del trattamento, nonché la diffusione di dati sensibili e giudiziari, sono ammesse esclusivamente previa verifica della loro stretta indispensabilità nei singoli casi e nel rispetto

dei limiti e con le modalità stabiliti dalle disposizioni legislative che le prevedono (art. 22 del d.lg. n. 196/2003).

Sono inutilizzabili i dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali (artt. 11 e 22, comma 5, del d.lg. n. 196/2003).

### **ARTICOLO 3**

#### **Riferimenti normativi**

Al fine di una maggiore semplificazione e leggibilità del presente regolamento, le disposizioni di legge, citate nella parte descrittiva delle "fonti normative" delle schede, si intendono come recanti le successive modifiche e integrazioni.





**EVENTI CHE POSSONO GENERARE DANNI (All. B – 19.3)**

| <b>EVENTO</b>                  |   | <b>Descrizione evento ed impatto sulla sicurezza</b>  |
|--------------------------------|---|---|
| <b>Compartamento operatori</b> | E-A1  | Sottrazione di credenziali di autenticazione  |
|                                |   | <p><b>Descrizione:</b><br/>Le credenziali (userID/Password) possono essere sottratte al legittimo possessore con vari metodi, anche grazie alla negligenza nella conservazione da parte del possessore stesso.</p> <p><b>Impatto:</b><br/>Altri soggetti possono accedere alle banche dati protette con tali credenziali sostituendosi in tutto e per tutto al soggetto possessore delle stesse. Il sistema di protezione non può in principio sapere dell'occorrenza di tale furto.</p>  |
|                                | E-A2  | Errore materiale  |
|                                |   | <p><b>Descrizione:</b><br/>A causa di negligenza, scarsa conoscenza degli strumenti a disposizione o distrazione, gli addetti al trattamento possono compiere operazioni errate o specificare dati errati.</p> <p><b>Impatto:</b><br/>Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati.</p>  |
| E – A3                         | Comportamenti illegali conseguenti a minacce su operatori | <p><b>Descrizione:</b><br/>In conseguenza di pressioni di vario tipo (es. minacce, ricatti pressioni psicologiche) gli incaricati del trattamento possono compiere operazioni illecite sulla banca dati interessata all'evento.</p> <p><b>Impatto:</b><br/>Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati.<br/>In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.</p>  |
| E – A4                         | Comportamenti sleali e/o fraudolenti                      | <p><b>Descrizione:</b><br/>Con comportamento consapevole, derivate potenzialmente da vari fattori quali (risentimenti verso l'Ente, il perseguimento di fini personali, etc.) gli incaricati del trattamento possono compiere operazioni illecite sulla banca dati interessata l'evento.</p> <p><b>Impatto:</b><br/>Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati.<br/>In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.</p> |

| <b>EVENTO</b> | <b>Descrizione evento ed impatto sulla sicurezza</b> |
|---------------|--|
|---------------|--|

|                                |      |  |  |
|--------------------------------|------|--|--|
| Eventi relativi agli strumenti | E-B1 | Virus informatici                                      | <b>Descrizione:</b><br>Sul sistema su cui si trova la banca dati interessata all'evento o il software utilizzato per accedervi, può essere venirsi ad installare o essere semplicemente eseguito del software spurio del tipo "virus" informatico.   |
|                                |      |  | <b>Impatto:</b><br>Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.   |
|                                | E-B2 | Spamming   | <b>Descrizione:</b><br>Il sistema di posta utilizzato dagli incaricati del trattamento potrebbe essere obiettivo di invii di posta spuria generata anche con strumenti automatizzati. Tali messaggi possono contenere false notizie.   |
|                                |      |  | <b>Impatto:</b><br>Gli incaricati del trattamento possono erroneamente prendere in considerazione tali notizie ed operare interventi sulle banche dati non regolari.   |
|                                | E-B3 | Accesso da stazioni non autorizzate                    | <b>Descrizione:</b><br>Soggetti in possesso di credenziali di accesso al sistema, o intenzionati a sferrare un attacco informatico ad uno dei sistemi HW/SW da cui è possibile intervenire su una banca dato obiettivo, possono accedere al sistema individuato da una postazione non utilizzata in condizioni normali di operatività per accedere a tale sistema. |
|                                |      |  | <b>Impatto:</b><br>Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.   |
|                                | E-B4 | Intercettazione di informazioni transitanti sulla rete | <b>Descrizione:</b><br>Soggetti malintenzionati possono catturare, mediante vari sistemi fisici, parte delle informazioni che transitano sulla rete informatica dell'Ente. Ciò può avvenire in un qualunque tra il sistema utilizzato e il sistema HW/SW degli incaricati.   |
|                                |      |  | <b>Impatto:</b><br>Nei casi più gravi, mediante varie tecniche, si può giungere alla distruzione o manipolazione dei dati. In generale si può avere una sottrazione di dati da parte dei malintenzionati.  |
|                                | E-B5 | Malfunzionamento apparecchiature                       | <b>Descrizione:</b><br>I sistemi HW/SW con i quali vengono manipolati i dati oggetto dell'evento da parte degli incaricati, possono avere malfunzionamenti da cui possono derivare azioni reali sui dati parzialmente o totalmente diverse da quelle che si volevano operare.  |
|                                |      |  | <b>Impatto:</b><br>Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati.  |

|  |      |                         |  |
|--|------|-------------------------|--|
|  | E-B6 | Degrado apparecchiature | <p><b>Descrizione:</b><br/>I sistemi HW/SW con i quali vengono manipolati i dati oggetto dell'evento da parte degli incaricati, possono essere soggetti a degrado naturale conseguente all'uso o al solo funzionamento. Da ciò possono derivare azioni reali sui dati parzialmente o totalmente diverse da quelle che si volevano operare.</p> <p><b>Impatto:</b><br/>Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati.</p> |
|--|------|-------------------------|--|

| EVENTO                      |      |   | Descrizione evento ed impatto sulla sicurezza   |
|-----------------------------|------|---|---|
| Eventi relativi al contesto | E-C1 | Accesso non autorizzato a locali da cui si può accedere ai dati | <p><b>Descrizione:</b><br/>Un soggetto autorizzato allo scopo, può comunque accedere fisicamente ai locali presso dai quali è accessibile e manipolabile la banca dati interessata all'evento.</p>  |
|                             |      |   | <p><b>Impatto:</b><br/>Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati.<br/>In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.</p>                |
|                             | E-C2 | Sottrazione di strumenti contenenti dati e/o programmi          | <p><b>Descrizione:</b><br/>I sistemi HW/SW e/o i supporti di memorizzazione, nei quali sono immagazzinati i dati relativi alla banca dati interessata all'evento, possono venire sottratti illecitamente da parte di altri soggetti non aventi diritto di accedere a tale banca dati.</p> |
|                             |      |   | <p><b>Impatto:</b><br/>L'evento comporta la sottrazione, in modo illecito, di dati.</p>   |
|                             | E-C3 | Eventi distruttivi naturali/artificiali accidentali o volontari | <p><b>Descrizione:</b><br/>I sistemi HW/SW e/o i supporti di memorizzazione, nei quali sono immagazzinati i dati relativi alla banca dati interessata all'evento, possono essere interessati da eventi distruttivi di origine sia fortuita che dolosa.</p>                                |
|                             |      |   | <p><b>Impatto:</b><br/>Dall'evento può derivare la distruzione totale o parziale della banca dati.</p>  |

|  |      |                                 |   |
|--|------|---------------------------------|---|
|  | E-C4 | Guasto ai sistemi complementari | <p><b>Descrizione:</b><br/>I sistemi ausiliari necessari al corretto funzionamento degli apparati HW/SW con i quali viene trattata o che contiene la banca dati interessata all'evento possono avere malfunzionamenti in conseguenza di varie cause.</p> <p><b>Impatto:</b><br/>Dall'evento può derivare la distruzione totale o parziale della banca dati.</p> |
|--|------|---------------------------------|---|

**MISURE DI CONTRASTO DEI RISCHI (Al. B- 19.4)**

| Identificativo misura | Misura   | Descrizione estesa  | Tipologia misura | Periodicità controllo adozione |
|-----------------------|--|---|------------------|--------------------------------|
| M-01                  | Impianto di allarme  | Gli spazi interessati alla misura sono dotati di impianto di allarme in grado di rilevare e segnalare l'intrusione di soggetti non autorizzati.   | Fisica           | Annuale                        |
| M-02                  | Inferriate o blindature  | La via di accesso agli spazi è dotata di protezione fisica di tipo inferriate o blindature in grado di impedire l'accesso agli stessi senza la disponibilità della chiave riservata ai soli autorizzati   | Fisica           | Annuale                        |
| M-03                  | Serrature normali  | L'accessibilità agli spazi è legata alla utilizzazione di un'apposita chiave disponibile ai soli soggetti autorizzati   | Fisica           | Annuale                        |
| M-04                  | Armadi a parete ignifuga   | Armadi con pareti in grado di resistere al fuoco ed alle alte temperature per un tempo sufficiente a porre in sicurezza i dati contenuti prima del loro deterioramento  | Fisica           | Annuale                        |
| M-05                  | Estintori  | I locali/vani sono dotati di appositi estintori da utilizzarsi per l'estinzione delle fiamme in caso di incendio.   | Fisica           | Semestrale                     |
| M-06                  | Gruppo di continuità   | Il carico elettrico da proteggere è alimentato attraverso un gruppo statico di continuità in grado di erogare, senza interruzione, la potenza elettrica necessaria per un tempo sufficiente a porre in sicurezza il carico stesso.                                      | Fisica           | Annuale                        |
| M-07                  | Climatizzazione  | I locali/vani oggetto della protezione sono opportunamente climatizzati per poter assicurare il mantenimento di temperature operative compatibili durante l'anno.   | Fisica           | Semestrale                     |
| M-08                  | Parola chiave personale di accesso alla stazione di lavoro (pc, portatile, ecc.) | L'accesso alla risorsa fisica è assoggettato alla conoscenza di una parola chiave con le caratteristiche di cui alla regola 19.5 conosciuta dalla sola persona a cui è stato affidata da parte dell'Amministratore del sistema e poi modificata dallo stesso operatore. | Fisica           | Semestrale/trimestrale         |
| M-09                  | Parola chiave personale di accesso alla procedura informatica                    | L'accesso alla procedura informatica è assoggettato alla conoscenza di una parola chiave con le caratteristiche di cui alla regola 19.5 conosciuta dalla sola persona a cui è stato affidata da parte dell'Amministratore del sistema e poi modificata dallo            | Fisica           | Semestrale/trimestrale         |

|      |   |   |                   |   |
|------|---|---|-------------------|---|
|      |   | stesso operatore.   |                   |   |
| M-10 | Sistema di autorizzazione basato su profili       | Il modulo software utilizzato per il trattamento dei dati oggetto della misura di protezione è basato su un sistema di profilazione dell'utenza che prevede di differenziare le possibili operazioni di trattamento eseguibili dai vari utenti in base al profilo/i specifico/i ad essi assegnati.  | Fisica            | Annuale                                 |
| M-11 | Accesso mediante controllo dell'indirizzo di rete | L'accesso alla risorsa informatica alla rete cui è connessa avviene mediante il controllo dell'indirizzo di rete della stazione accedente; l'accesso viene consentito solo se tale indirizzo appartiene ad una lista predefinita di stazioni  | Logica            | Annuale                                 |
| M-12 | Logging   | L'accesso alla risorsa informatica in questione è assoggettato a tracciature delle operazioni effettuate con la registrazione di:<br>- epoca dell'operazione<br>- indirizzo di rete della stazione accedente (se definito)<br>- descrizione dell'operazione fatta<br>- identificativo dell'utente che compie l'operazione<br>Tali file di log sono accuratamente conservati per l'eventuale loro controllo. | Logica            | Semestrale                              |
| M-13 | Crittografia                                      | I dati sono crittografati mediante tecniche di cifratura adatte al livello di confidenzialità necessario in relazione alla natura dei dati in questione.  | Logica            | Annuale                                 |
| M-14 | Copia   | I dati o programmi sono copiati con regolarità su supporti fisici diversi che sono poi conservati in locali separati opportunamente protetti da accessi non autorizzati.  | Organizzati<br>va | Giornaliera/se<br>ttimanale/Me<br>nsile |
| M-15 | Copie multiple                                    | Le procedure di salvataggio sono effettuate producendo copie multiple che sono poi conservate in locali diversi ciascuno soggetti ad opportune restrizioni di accesso.  | Organizzati<br>va | Annuale                                 |
| M-16 | Filtraggi del traffico di rete                    | Il traffico di rete sviluppato attraverso la risorsa informatica è assoggettato ad opportuni controlli di congruità in termini di indirizzi e porte sorgenti e destinatarie sulla base di opportune tabelle (access list) pre-configurate in base al livello di protezione desiderato.  | Logica            | Annuale                                 |
| M-17 | Utilizzo firma digitale                           | L'accesso alla procedura informatica è assoggettato ad un sistema di riconoscimento forte basato sull'utilizzo di certificati digitali  | Logica            | Annuale                                 |

|      |   |  |                   |             |
|------|---|--|-------------------|-------------|
|      |   | <p>rilasciati da Certification authority riconosciuta.</p> <p>La utilizzabilità della chiave segreta, necessaria all'espletamento della procedura di autenticazione, è possibile da parte del soggetto autorizzato solo mediante la digitazione di un codice segreto (PIN = Personal Identification Number) conosciuto esclusivamente da lui stesso.</p> |                   |             |
| M-18 | Uso di smart-card                               | La chiave segreta necessaria per l'autenticazione forte da parte degli utenti autorizzati del servizio informatico è conservata su un dispositivo di sicurezza di tipo smart-card o equivalente.   | Fisica            | Annuale     |
| M-19 | Ingresso presidiato                             | I locali interessati alla misura sono dotati di servizio di portineria presidiata da personale addetto. Il personale addetto, mediante procedura di identificazione delle persone che accedono ai locali, può inibire l'accesso agli stessi. Tale inibizione di accesso può essere basata su fasce orario nell'arco della giornata lavorativa.           | Fisica            | Annuale     |
| M-20 | Informazione/formazione specifica sul rischio   | Gli incaricati del trattamento vengono resi edotti, in modo specifico e puntuale, degli eventi dannosi relativi a quella banca dati e sulle misure adottate per contrastare il rischio derivante. Vengono poi date istruzioni operative dettagliate sul come rendere operative le misure di contrasto del rischio.                                       | Organizzati<br>va | Annuale     |
| M-21 | Antivirus                                       | Sui sistemi interessati al trattamento dei dati in questione sono stati installati opportuni software di protezione dai virus informatici. Tali software sono costantemente aggiornati, in modo automatico, con frequenza almeno giornaliera. In certe situazioni il sistema provvede ad aggiornamenti più frequenti.                                    | Organizzati<br>va | Giornaliera |
| M-22 | Black list per posta elettronica (Antispamming) | Il sistema di smistamento della posta è stato configurato in modo da individuare siti mittenti che sono considerabili come emettitori di SPAM. Inoltre possono essere attivati, in caso di necessità, funzionalità di filtraggio del traffico in base a vari criteri.  | Organizzati<br>va | Mensile     |
| M-23 | Manutenzione risorse HW/SW                      | Sui sistemi HW/SW vengono attivate opportune azioni di manutenzione di tipo preventivo e correttivo al fine di poter prevenire il più possibile il manifestarsi dei guasti più ricorrenti ed evitare sospensioni di servizio conseguenti al verificarsi di tali guasti.  | Organizzati<br>va | Mensile     |



**CRITERI E PROCEDURE PER IL SALVATAGGIO ED IL RIPRISTINO DELLA DISPONIBILITA' DEI DATI (All. B – 19.5)**

| Descrizione archivi in relazione alla loro collocazione | Tipo e frequenza del salvataggio | Luogo di custodia delle copie | Struttura o persona incaricata del salvataggio | Pianificazione delle prove di ripristino  |
|---|----------------------------------|-------------------------------|--|---|
|   |                                  |                               | Sistema informativo                            | Non sono pianificate copie di ripristino a scadenze predeterminate, in quanto i ripristini effettivi vengono eseguiti giornalmente su richiesta degli interessati |
|   |                                  |                               |  |   |
|   |                                  |                               |  |   |
|   |                                  |                               |  |   |
|   |                                  |                               |  |   |
|   |                                  |                               |  |   |
|   |                                  |                               |  |   |
|   |                                  |                               |  |   |
|   |                                  |                               |  |   |
|   |                                  |                               |  |   |

**PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI (All. B – 19.6)**

| <b>Corso di formazione</b>  | <b>Descrizione sintetica</b>  | <b>Riferimento ai Responsabili o Incaricati</b>   | <b>Numero interessati</b> | <b>Calendario lezioni</b> |  |
|---|---|---|---------------------------|---------------------------|--|
| La privacy e il regime di trattamento di dati personali nella P.A | Analisi del contesto normativo e approfondimento del D.lgs 196/03 e del DPS dell'ente. I corsi sono finalizzati a istruire i destinatari su: i rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano e quindi sulle modalità per aggiornarsi alle misure minime adottate dal titolare | I corsi si rivolgono ai Responsabili per il trattamento dei dati , ai referenti, agli Incaricati del trattamento e a tutto il personale interessato con percorsi specifici legati alle suddette figure presenti nell' Ente. |                           |                           |  |

**TRATTAMENTI AFFIDATI ALL'ESTERNO (All. B – 19.7)**

| <b>Descrizione attività esternalizzata</b> | <b>Trattamento di dati interessati</b> | <b>Soggetto esterno</b> | <b>Descrizione impegni assunti per l'adozione delle misure</b> |
|--|--|-------------------------|--|
|  |  |                         |  |