

REGOLAMENTO COMUNALE PER IL TRATTAMENTO DEI DATI PERSONALI

(approvato con Deliberazione del Consiglio Comunale n. 4 del 19.01.2006)

Art. 1

Scopo del regolamento

1. Scopo del presente regolamento è garantire l'applicazione nel Comune del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, in seguito chiamato Codice) e delle altre disposizioni sulla protezione dei dati personali¹, in armonia con i principi giuridici che presiedono all'organizzazione e all'attività del Comune.

Art. 2

Titolarità e oggetto del trattamento di dati personali

1. Il Comune è il titolare² del trattamento³ dei dati personali gestiti per lo svolgimento delle proprie funzioni istituzionali, anche se non ancora registrati in una banca di dati⁴ o non soggetti a tale registrazione.

Art. 3

Contitolarità del trattamento di dati personali

1. La contitolarità del trattamento di dati personali avviene quando il Comune e altri soggetti pubblici, esclusi gli enti pubblici economici, ciascuno per lo svolgimento delle proprie funzioni istituzionali, gestiscono in comune il trattamento di dati personali condividendo i poteri decisionali, pur rimanendo autonomi e indipendenti gli uni dagli altri per quanto attiene la loro personalità giuridica.

2. I rapporti tra il Comune e i soggetti pubblici contitolari del trattamento di dati personali sono regolati dagli atti di costituzione e di modificazione di forme associative e dalle convenzioni stipulate dal Sindaco in esecuzione di deliberazioni del Consiglio comunale⁵.

Art. 4

Limiti al trattamento di dati personali da parte del Comune

1. Il Comune, nel trattamento di dati personali, si attiene alle seguenti regole:

1) effettua il trattamento soltanto se è necessario per lo svolgimento delle funzioni istituzionali⁶;

2) effettua il trattamento di dati ordinari, cioè diversi dai dati sensibili⁷ e dai dati giudiziari⁸, purché necessario per lo svolgimento di funzioni istituzionali, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente⁹;

¹ Art. 4, comma 1, lettera b), del Codice.

² Art. 4, comma 1, lettera f), del Codice.

³ Art. 4, comma 1, lettera a), del Codice.

⁴ Art. 4, comma 1, lettera p), del Codice.

⁵ Art. 42, comma 2, lettere c) ed e) del Dlgs 267/2000.

⁶ Art. 18, comma 2, del Codice.

⁷ Art. 4, comma 1, lettera d), del Codice.

- 3) effettua la comunicazione¹⁰ di dati personali ad altri soggetti pubblici nei seguenti casi¹¹:
- a) se è prevista da una norma di legge o di regolamento;
 - b) se risulti comunque necessaria per lo svolgimento di funzioni istituzionali del soggetto pubblico che ne abbia fatto richiesta motivata; in tal caso il Comune può iniziare la comunicazione al richiedente se siano trascorsi 45 giorni dalla comunicazione al Garante¹² dell'intenzione di effettuare l'operazione senza che il Garante abbia trasmesso una determinazione negativa; se la determinazione negativa del Garante perviene dopo 45 giorni, il Comune interrompe la comunicazione eventualmente iniziata¹³;
- 4) effettua la comunicazione di dati personali a privati e ad enti pubblici economici solo se prevista da una norma di legge o di regolamento¹⁴;
- 5) effettua la diffusione¹⁵ di dati personali, purché non idonei a rivelare lo stato di salute¹⁶, solo se prevista da una norma di legge o di regolamento¹⁷.
- 6) effettua il trattamento di dati sensibili se autorizzato da espressa disposizione di legge che specifichi¹⁸:
- a) i tipi dei dati che possono essere trattati;
 - b) le operazioni eseguibili;
 - c) le finalità di rilevante interesse pubblico perseguite;
- 7) effettua il trattamento di dati sensibili anche se esistono le seguenti condizioni:
- a) sia autorizzato da disposizione di legge che specifichi le finalità di rilevante interesse pubblico, ma non i tipi di dati e le operazioni eseguibili;
 - b) si sia dotato di apposito regolamento comunale¹⁹, sul quale il Garante abbia espresso parere favorevole²⁰;
- 8) effettua il trattamento di dati sensibili, anche in mancanza di espressa disposizione di legge, se esistono le seguenti condizioni²¹:
- a) il Garante, a richiesta del Comune, abbia individuato tra le attività demandate al Comune stesso, quelle che perseguono finalità di rilevante interesse pubblico;
 - b) si sia dotato di apposito regolamento comunale²², sul quale il Garante abbia espresso parere favorevole;
- 9) effettua il trattamento di dati giudiziari se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino²³:
- a) i tipi dei dati che possono essere trattati;
 - b) le operazioni eseguibili;
 - c) le finalità di rilevante interesse pubblico perseguite.
- 10) effettua il trattamento di dati giudiziari anche se esistono tutte le seguenti condizioni²⁴:

⁸ Art. 4, comma 1, lettera e), del Codice.

⁹ Art. 19, comma 1, del Codice.

¹⁰ Art. 4, comma 1, lettera l), del Codice.

¹¹ Art. 19, comma 2, del Codice.

¹² Art. 153 del Codice.

¹³ Art. 39 del Codice.

¹⁴ Art. 19, comma 3, del Codice.

¹⁵ Art. 4, comma 1, lettera m), del Codice.

¹⁶ Art. 22, comma 8, del Codice.

¹⁷ Art. 19, comma 3, del Codice.

¹⁸ Art. 20, comma 1, del Codice.

¹⁹ Art. 22 del Codice.

²⁰ Art. 20, comma 2, del Codice.

²¹ Art. 20, comma 3, del Codice.

²² Art. 22 del Codice.

²³ Art. 21, comma 1, del Codice.

²⁴ Art. 21, comma 2, del Codice.

a) sia autorizzato da disposizione di legge che specifichi le finalità di rilevante interesse pubblico, ma non i tipi di dati e le operazioni eseguibili;

b) si sia dotato di apposito regolamento comunale sul quale il Garante abbia espresso parere favorevole²⁵.

Art. 5

Consenso dell'interessato

1. Il Comune non deve chiedere il consenso dell'interessato al trattamento dei dati personali²⁶ né tale consenso può essere chiesto per legittimare trattamenti che non siano in linea con i requisiti stabiliti dalla normativa.

Art. 6

Notificazione

1. Allo stato attuale della legislazione²⁷, per effetto del provvedimento del Garante n. 1 in data 31 marzo 2004, il Comune è tenuto alla notificazione al Garante solo se intenda effettuare sondaggi di opinione che comportino la raccolta e la registrazione di dati sensibili in banche di dati gestiti con l'ausilio di strumenti elettronici.

Art. 7

Informativa

1. Quando i dati personali sono raccolti direttamente presso l'interessato, il Comune è tenuto a dare le informazioni previste dal Codice²⁸.

2. L'informativa è eseguita in uno dei seguenti modi:

a) con l'inserimento delle informazioni nelle lettere che contengono la richiesta di dati personali;

b) con l'inserimento delle informazioni nei bandi e negli avvisi pubblici che prevedono la fornitura di dati personali;

c) con l'inserimento delle informazioni nei moduli predisposti dal Comune per raccogliere dati personali;

d) con la messa a disposizione di fogli recanti le informazioni negli uffici aperti al pubblico dove si effettua la raccolta di dati personali;

e) mediante cartelli ben visibili esposti negli uffici, aperti al pubblico, dove si effettua la raccolta di dati personali;

f) oralmente dall'incaricato della raccolta quando essa avviene mediante interviste agli utenti dei servizi comunali.

3. Nell'informativa scritta possono essere omessi alcuni elementi, come le finalità del trattamento, la natura obbligatoria o facoltativa del conferimento dei dati, le conseguenze di un eventuale rifiuto di rispondere, quando tali elementi sono notori.

4. In ogni caso, l'informativa deve contenere il richiamo ai diritti dell'interessato²⁹, e l'indicazione del responsabile del trattamento e della titolarità del trattamento dei dati raccolti da parte del Comune.

²⁵ Art.21, comma 2, del Codice.

²⁶ Art. 18, comma 4, del Codice.

²⁷ Art. 37 del Codice.

²⁸ Art. 13 del Codice.

²⁹ Art. 7 del Codice.

Art. 8

Atti soggetti a pubblicazione

1. Gli atti comunali soggetti a pubblicazione mediante affissione all'albo pretorio e/o mediante manifesti e/o mediante giornali e bollettini e/o mediante inserimento nel sito *internet* istituzionale, sono redatti in modo da limitare al minimo indispensabile per la comprensione dell'atto l'esposizione di dati personali; non devono comunque contenere dati idonei a rivelare lo stato di salute³⁰.

2. Apposita informativa esposta all'albo pretorio, inserita nei manifesti, nei giornali, nei bollettini e nel *sito internet* rende noti i seguenti elementi:

1) disposizione di legge o di regolamento comunale che prevede la pubblicazione;

2) avvertenza che ogni ulteriore trattamento dei dati personali contenuti negli atti pubblicati, effettuato da soggetti pubblici e privati per esigenze non strettamente personali, è subordinato al consenso degli interessati³¹;

3) avvertenza che l'uso dei dati personali contenuti negli atti pubblicati, effettuato nell'esercizio della professione giornalistica, dovrà rispettare i limiti al diritto di cronaca posti a tutela della riservatezza, così come previsto dal relativo codice di deontologia professionale ex art. 136 del Codice.

Art. 9

Ripartizione delle competenze tra gli organi comunali

1. Le attribuzioni del Comune quale titolare del trattamento di dati personali sono esercitate dai suoi organi secondo la seguente ripartizione delle competenze:

1) il consiglio comunale:

a) emana le norme regolamentari in materia di protezione dei dati personali;

b) adotta, con la relazione revisionale e programmatica, le decisioni strategiche e formula gli obiettivi in materia di protezione dei dati personali;

c) stanZIA nel bilancio di previsione le risorse finanziarie necessarie per l'efficiente ed efficace esercizio dell'autonomia gestionale da parte dei responsabili interni del trattamento di dati personali;

d) delibera in ordine alle forme associative³² e ad altri rapporti con soggetti pubblici che comportano la contitolarità³³ del trattamento di dati personali;

2) la giunta comunale:

a) emana le norme regolamentari, in materia di ordinamento degli uffici e dei servizi, utili per garantire l'efficienza dell'apparato burocratico in relazione alla protezione dei dati personali;

b) assicura ai responsabili degli uffici e dei servizi, col piano esecutivo di gestione, le risorse necessarie all'adeguata protezione dei dati personali, anche ai fini, in carenza di professionalità interne, del supporto di specialisti esterni per la corretta gestione delle dotazioni *hardware* e *software*;

c) impartisce ai responsabili del trattamento di dati personali le direttive per l'affidamento di incarichi esterni di consulenza e di assistenza nonché per l'affidamento del trattamento di dati mediante contratto;

³⁰ Art. 22, comma 8, del Codice.

³¹ Art. 23 del Codice.

³² Artt. 31-34 del Dlgs 267/2000.

³³ Art. 4, comma 1, lettera f) del Codice.

3) il sindaco:

- a) rappresenta il Comune nei rapporti col Garante³⁴;
- b) notifica al Garante i trattamenti di dati personali quando la notifica è prescritta dalla legge e non è esclusa dal Garante, oppure è prescritta direttamente dal Garante³⁵.
- c) comunica al Garante l'intenzione di effettuare la comunicazione ad altri enti pubblici di dati personali necessaria per lo svolgimento di funzioni istituzionali, ma non prevista da una norma di legge o di regolamento³⁶;
- d) chiede al Garante le autorizzazioni che non rientrano tra quelle da lui rilasciate in via generale³⁷;
- e) designa, con proprio decreto, il segretario comunale e i responsabili dei settori quali responsabili³⁸ del trattamento dei dati personali gestiti dagli uffici di loro pertinenza;
- f) designa, con propria lettera, incaricati³⁹ del trattamento di dati personali, per un tempo e per operazioni determinati, gli amministratori comunali cui abbia rilasciato deleghe o conferito incarichi, o che abbiano ricevuto incarichi dal Consiglio, o che ne facciano richiesta per l'esercizio del loro potere di indirizzo e di controllo;
- g) designa, con proprio atto, incaricati del trattamento di dati personali, nei limiti delle necessità, gli addetti agli uffici di supporto agli organi di direzione politica⁴⁰;
- h) impartisce ai responsabili del trattamento, con propri decreti, opportune direttive e vigila sull'osservanza delle disposizioni in materia di trattamento di dati personali, ivi compreso il profilo della sicurezza;
- i) adotta e aggiorna, con propri decreti, su proposta del segretario comunale, il documento programmatico sulla sicurezza⁴¹;
- l) impartisce, con proprie circolari fondate sulla giurisprudenza, sulla dottrina e sulle pronunce del Garante, direttive agli uffici per la corretta applicazione della normativa sulla protezione dei dati personali;

4) il segretario comunale:

- a) coordina i responsabili dei settori ai fini dell'aggiornamento annuale del repertorio delle banche di dati personali (nonché delle raccolte di dati personali non registrati in banche di dati) trattati dal Comune, e delle liste degli incaricati del trattamento;
- b) coordina i responsabili dei settori in ordine agli accordi interni per il trattamento di dati personali gestiti da uffici appartenenti a più settori;
- c) coordina i responsabili dei settori in ordine alla formazione mirata alla protezione dei dati personali;

5) i responsabili dei settori:

- a) curano l'aggiornamento annuale del repertorio delle banche dei dati personali trattati dal Comune e delle raccolte informatizzate e cartacee di dati personali non registrati in banche di dati;
- b) nel mese di gennaio di ogni anno consegnano copie delle schede dei dati personali trattati dagli uffici di loro pertinenza, aggiornate al 31 dicembre, al Responsabile del Settore competente, che le utilizza per formulare la proposta di aggiornamento del documento programmatico sulla sicurezza.
- c) curano l'aggiornamento annuale delle liste degli incaricati;

³⁴ Art. 153 e segg. del Codice.

³⁵ Art. 37 del Codice.

³⁶ Artt. 19, comma 2, e 39, comma 2, del Codice.

³⁷ Art. 40 del Codice.

³⁸ Art. 4, comma 1, lettera g), del Codice.

³⁹ Art. 4, comma 1, lettera h), del Codice.

⁴⁰ Art. 90 del Dlgs 267/2000.

⁴¹ Art. 34, comma 1, lettera g), e Allegato B del Codice.

d) designano, con propri atti, gli incaricati del trattamento dei dati personali negli uffici di propria pertinenza, impartiscono loro le istruzioni necessarie, con particolare riguardo all'applicazione delle misure di sicurezza e all'informativa agli interessati; prescindono dalla designazione per gli addetti ad uffici per i quali la legge, o il regolamento comunale, o un ordine scritto di servizio stabiliscono esaurientemente l'ambito del trattamento di dati personali consentito⁴²;

e) possono designare, insieme ad altri responsabili, con atti a firma congiunta e sulla base di accordi interni, anche gli incaricati del trattamento quando i dati sono gestiti da uffici appartenenti a più settori;

f) adottano, nel rispetto delle direttive della Giunta, determinazioni a contrattare⁴³ e stipulano i relativi contratti per l'affidamento a terzi del trattamento dei dati comunali da effettuare sia all'interno sia all'esterno degli uffici comunali, in luoghi specificati dal contratto, e vigilano sul rispetto delle clausole contrattuali;

g) provvedono all'informativa agli interessati quando essa avviene con l'inserimento delle informazioni nei bandi e negli avvisi pubblici, con la messa a disposizione di fogli recanti le informazioni negli uffici aperti al pubblico e con cartelli ben visibili esposti negli uffici;

h) curano l'inserimento dell'informativa agli interessati nella modulistica comunale;

i) curano i rapporti con gli interessati che esercitano il diritto d'accesso⁴⁴;

l) predispongono il contenuto delle notificazioni e delle comunicazioni che sono sottoposte alla firma del Sindaco e inviate al Garante.

m) curano la formazione permanente degli incaricati in materia di protezione dei dati personali;

n) svolgono, per gli uffici di loro pertinenza, i compiti dell'amministratore di sistema, se questi non è stato nominato dal Sindaco;

o) curano l'istruttoria e predispongono il contenuto dei decreti del sindaco in materia di protezione dei dati personali;

Art. 10

L'amministratore di sistema

1. Il Sindaco può nominare, tra i dipendenti comunali a tempo indeterminato, o appositamente assunti a tempo determinato, o incaricati con rapporto di collaborazione coordinata e continuativa o con contratto di consulenza ad alta professionalità o specifica convenzione o avvalendosi di dipendenti di altri enti pubblici, un amministratore di sistema con i seguenti compiti:

a) sovrintendere alle risorse del sistema informatico e consentire a tutti gli utenti l'utilizzazione degli strumenti disponibili;

b) assicurarsi della qualità delle copie di *back-up* dei dati e della loro conservazione in luogo adatto e sicuro;

c) fare in modo che sia prevista la disattivazione dei codici identificativi personali (*user-id*), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancata utilizzazione dei codici identificativi personali per oltre sei mesi;

d) aggiornare almeno ogni semestre la procedura software contenente i dati relativi alla sicurezza;

e) informare il Sindaco nella eventualità che si siano rilevati dei rischi;

⁴² Art. 30, comma 2, del Codice.

⁴³ Art. 197 del Dlgs 267/2000.

⁴⁴ Art. 7 del Codice.

f) assistere il segretario comunale nella predisposizione del documento programmatico sulla sicurezza da presentare al sindaco in tempo utile;

g) segnalare al Sindaco tutte le informazioni per l'eventuale comunicazione al Garante del trattamento di ogni nuova base di dati non prevista già dalla legge;

h) predisporre, per ogni incaricato del trattamento e per ogni archivio, lo *user-id* utilizzato e assegnare la *password* che sarà subito modificata dall'incaricato;

i) revocare tutte le *password* non utilizzate per un periodo superiore a sei mesi;

l) revocare tempestivamente tutte le *password* assegnate a soggetti che su comunicazione scritta del responsabile del trattamento non sono più autorizzati ad accedere ai dati.

2. I compiti dell'amministratore di sistema, se non è stato nominato, sono espletati dai responsabili dei settori, con l'assistenza di esperti di informatica interni e/o esterni e devono essere descritti nel decreto del Sindaco con cui sono designati.

Art. 11

I responsabili esterni del trattamento

1. I compiti dei responsabili del trattamento di dati personali esterni alla struttura del Comune, siano essi soggetti pubblici o privati, che derivano la loro designazione da convenzioni deliberate dal Consiglio comunale⁴⁵ sono regolati dalle convenzioni stipulate dal Sindaco.

2. I compiti dei responsabili del trattamento di dati personali esterni alla struttura del Comune, che derivano la loro designazione da rapporti di natura contrattuale sono specificati nei contratti stipulati dai responsabili dei settori.

3. In ogni caso, il responsabile esterno deve dichiarare:

1) di essere consapevole che i dati che tratta nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del Codice per la protezione dei dati personali;

2) di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;

3) di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere;

4) di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il Comune in caso di situazioni anomale o di emergenze;

5) di riconoscere il diritto del Comune a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Art. 12

Incaricati esterni del trattamento

1. Coloro che, a qualsiasi legittimo titolo, non essendo dipendenti comunali o collaboratori coordinati e continuativi o collaboratori occasionali incaricati del trattamento di dati personali, accedono ai dati personali di qualsiasi tipo gestiti dal Comune, devono munirsi di una lettera firmata dal competente responsabile o dai competenti responsabili comunali del trattamento dove sono specificate le operazioni che sono autorizzati ad effettuare, il luogo, le modalità e la durata.

2. Gli incaricati esterni che provvedono alla installazione, alla sostituzione e all'aggiornamento di programmi o alla ricostruzione di archivi danneggiati devono effettuare la copia degli archivi prima dell'intervento e devono consegnarla al responsabile comunale;

⁴⁵ Art. 42, comma 2, lettera e) del Dlgs 267/2000.

essi devono impegnarsi per iscritto a non trattenere copie di archivi di dati comunali, sia per le operazioni effettuate all'interno che all'esterno della sede comunale.

Art. 13

Le misure di sicurezza in generale

1. Si intendono per misure di sicurezza i sistemi tecnici, organizzativi e logistici che garantiscono una effettiva protezione della sfera privata dell'interessato, in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento.

2. Il titolare, i responsabili e gli incaricati del trattamento di dati personali, ciascuno in relazione ai propri compiti, sono tenuti all'adozione di misure di sicurezza preventive, idonee a ridurre al minimo 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 raccolta⁴⁶.

Art. 14

Le misure minime di sicurezza

1. Le misure minime di sicurezza sono, tra le misure idonee, quelle espressamente prescritte dalla legge e che devono essere comunque adottate⁴⁷, altrimenti si incorre nel reato previsto dall'art. 169 del Codice.

2. Le misure minime di sicurezza prescritte dal Codice sono riportate nei seguenti allegati:

A - TRATTAMENTO CON STRUMENTI ELETTRONICI;

B - TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI.

Art. 15

Illeciti penali e amministrativi

1. Il trattamento illecito dei dati personali comporta speciali sanzioni penali e amministrative previste dal Codice e riassunte, rispettivamente, negli allegati C e D.

Art. 16

Responsabilità civile

1. Il trattamento di dati personali è considerato dalla legge attività pericolosa e quindi, ai sensi dell'articolo 2500 del Codice Civile, chiunque cagiona danno patrimoniale ad altri per effetto del trattamento di dati personali è tenuto al risarcimento, se non prova di aver adottato tutte le misure idonee ad evitare il danno⁴⁸.

2. Chiunque cagiona danno non patrimoniale ad altri per effetto del trattamento di dati personali è tenuto al risarcimento se il danno deriva da fatto penalmente rilevante⁴⁹ e comunque se i dati non siano:

a) trattati in modo lecito e secondo correttezza;

b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;

c) esatti e, se necessario, aggiornati;

⁴⁶ Art. 31 del Codice.

⁴⁷ Art. 33 del Codice.

⁴⁸ Art. 15, comma 1, del Codice.

⁴⁹ Art. 185, comma 2, del Codice Penale.

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati⁵⁰.

Art. 17

Repertorio delle banche dei dati personali

1. I responsabili del trattamento di dati personali tengono il repertorio dei dati personali trattati dagli uffici di loro pertinenza.

2. Per la formazione e il costante aggiornamento del repertorio utilizzano schede conformi al modello allegato al presente regolamento sotto la lettera E.

3. Il modello della scheda è utilizzato dai responsabili, opportunamente adattato, anche per il rilevamento dei dati personali non registrati in banche dati.

4. Nel mese di gennaio di ogni anno consegnano le copie delle schede, aggiornate al 31 dicembre, al Responsabile del Settore competente, che le utilizza per formulare la proposta di aggiornamento del documento programmatico sulla sicurezza⁵¹. La proposta è formulata dal Responsabile del Settore competente entro il mese di febbraio ed è approvata, con decreto del sindaco, entro il 31 marzo.

5. Se non è necessario l'aggiornamento del DPS il Sindaco conferma con decreto il documento dell'anno precedente.

⁵⁰ Art. 11 del Codice.

⁵¹ Art. 34, comma 1, lettera g), e Allegato B del Codice.

COMUNE DI BARBERINO DI MUGELLO

Provincia di Firenze

Allegato A al REGOLAMENTO DI ORGANIZZAZIONE PER IL TRATTAMENTO DEI DATI PERSONALI approvato con deliberazione del consiglio comunale n° ____ del

TRATTAMENTO CON STRUMENTI ELETTRONICI	
Art. 34 del Codice	Disciplinare tecnico in materia di misure minime di sicurezza allegato B al Codice
a) autenticazione informatica	<p>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.</p> <p>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.</p> <p>3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.</p>
b) adozione di procedure di gestione delle credenziali di autenticazione	<p>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.</p> <p>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.</p> <p>6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.</p> <p>7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.</p> <p>8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.</p> <p>9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.</p> <p>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.</p> <p>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.</p>
c) Utilizzazione di un sistema di autorizzazione	<p>12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.</p> <p>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 limi-</p>

	<p>tare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.</p> <p>14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.</p>
d) aggiornamento periodico dell'individuazione del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti informatici	<p>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.</p>
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici	<p>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.</p> <p>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.</p> <p>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.</p>
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi	<p>18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.</p> <p>21. [per i dati sensibili o giudiziari]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.</p> <p>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.</p> <p>23. [per i dati sensibili o giudiziari]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.</p>
g) tenuta di un aggiornato documento programmatico sulla sicurezza	<p>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:</p> <p>19.1. l'elenco dei trattamenti di dati personali;</p> <p>19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;</p> <p>19.3. l'analisi dei rischi che incombono sui dati;</p> <p>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;</p> <p>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;</p> <p>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;</p> <p>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;</p> <p>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.</p> <p>26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se do-</p>

	vuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari	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.
	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.

COMUNE DI BARBERINO DI MUGELLO

Provincia di Firenze

Allegato B al REGOLAMENTO DI ORGANIZZAZIONE PER IL TRATTAMENTO DEI DATI PERSONALI approvato con deliberazione del consiglio comunale n° ____ del

TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI	
Art. 35 del Codice	Disciplinare tecnico in materia di misure minime di sicurezza allegato B al Codice
a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative	27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
b) previsione di procedure per la conservazione di determinati atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti	28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.	29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

COMUNE DI BARBERINO DI MUGELLO

Provincia di Firenze

Allegato C al REGOLAMENTO DI ORGANIZZAZIONE PER IL TRATTAMENTO DEI DATI PERSONALI approvato con deliberazione del consiglio comunale n° ____ del _____

SANZIONI PENALI

Articolo del Codice	fattispecie	pena	annotazioni
167, comma 1	trattamento di dati personali in violazione degli articoli 18, 19, 23, 123, 126, 130 o in applicazione dell'articolo 129 del Codice	reclusione da 6 a 18 mesi (se dal fatto deriva un nocumento) oppure da 6 a 24 mesi (se il fatto consiste nella comunicazione o diffusione)	occorre il dolo specifico del fine di trarre per sé o per altri un profitto o di arrecare ad altri un danno; la condanna comporta la pubblicazione della sentenza
167, comma 2	trattamento di dati personali in violazione degli articoli 17, 20, 21, 22, commi 8 e 11, 21, 25, 26, 27 e 45 del Codice	reclusione da 1 a 3 anni (se dal fatto deriva un nocumento)	occorre il dolo specifico del fine di trarre per sé o per altri un profitto o di arrecare ad altri un danno; la condanna comporta la pubblicazione della sentenza
168	falsità nelle dichiarazioni e notificazioni rese al Garante	reclusione da 6 mesi a 3 anni	la condanna comporta la pubblicazione della sentenza
169	mancata adozione delle misure minime di sicurezza da parte di chiunque	arresto sino a 2 anni e ammenda da 10.000 a 50.000 € oppure ammenda di 12.500 € ed estinzione del reato se il colpevole si adegua tempestivamente alla prescrizione impartita dal Garante	si tratta di reato contravvenzionale
170	inosservanza di provvedimenti del Garante adottati ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), del Codice	reclusione da 3 mesi a 2 anni	la condanna comporta la pubblicazione della sentenza
171	violazione di norme in materia di lavoro (articoli 113, comma 1, e 114 del Codice)	sanzioni di cui all'art. 38 della legge 300/1970	la condanna comporta la pubblicazione della sentenza

COMUNE DI BARBERINO DI MUGELLO

Provincia di Firenze

Allegato D al REGOLAMENTO DI ORGANIZZAZIONE PER IL TRATTAMENTO DEI DATI PERSONALI approvato con deliberazione del consiglio comunale n° _____ del _____

SANZIONI CIVILI

Articolo del Codice	fattispecie	sanzione pecuniaria	annotazioni
161	omessa o inidonea informativa all'interessato prevista dall'art. 13 del Codice	da 3.000 a 18.000 € da 5.000 a 30.000 € nei casi dati sensibili o giudiziari o di trattamenti che presentano rischi specifici ai sensi dell'articolo 17 del Codice o comunque di maggiore rilevanza del pregiudizio per uno o più interessati	la pena può essere aumentata fino al triplo se risulta inefficace in ragione delle condizioni economiche del contravventore, pena facoltativa accessoria della pubblicazione in uno o più giornali
162	cessione di dati in violazione di quanto previsto dall'articolo 16, comma 1, lettera b), del Codice o di altre disposizioni in materia di trattamento	da 5.000 e 30.000 €	pena facoltativa accessoria della pubblicazione in uno o più giornali
162	comunicazione di dati sanitari in violazione dell'art. 84, comma 1, del Codice	da 500 e 3.000 €	
163	omessa o incompleta notificazione al Garante	da 10.000 a 60.000 €	pena accessoria della pubblicazione in uno o più giornali
164	omessa fornitura di informazioni o esibizione di documenti richiesti dal Garante	da 4.000 e 24.000 €	pena facoltativa accessoria della pubblicazione in uno o più giornali

COMUNE DI BARBERINO DI MUGELLO

Provincia di Firenze

Allegato E al REGOLAMENTO DI ORGANIZZAZIONE PER IL TRATTAMENTO DEI DATI PERSONALI approvato con deliberazione del consiglio comunale n° _____ del _____

COMUNE DI BARBERINO DI MUGELLO

Provincia di Firenze

CENSIMENTO DELLE BANCHE DI DATI PERSONALI

SCHEDA DI RILEVAZIONE

N°	denominazione banca dati

settore	ufficio
edificio	locale

responsabile del trattamento	incaricati del trattamento

giustificazione del trattamento	
fonte normativa (da specificare)	contratto (da specificare)
provvedimento del Garante (da specificare)	altro atto o provvedimento (da specificare)

interessati	
cittadini singoli famiglie convivenze amministratori comunali dipendenti comunali contribuenti affittuari fornitori	costruttori altre aziende commerciali associazioni e fondazioni professionisti altri (da specificare)

operazioni eseguibili	
raccolta	raffronto
registrazione	utilizzo
conservazione	interconnessione
organizzazione	blocco
elaborazione	comunicazione
modificazione	diffusione
selezione	cancellazione e distruzione
estrazione	

tipologia/e dei dati personali trattati o trattabili	
comuni sensibili	giudiziari
indicazione dei dati sensibili eventualmente trattati o trattabili	
origine razziale ed etnica convinzioni religiose, filosofiche o di altro genere opinioni politiche adesioni a partiti	adesioni a sindacati adesioni ad associazioni a carattere religioso, filosofico, politico o sindacale stato di salute vita sessuale
indicazione dei dati giudiziari eventualmente trattati o trattabili	
in materia di casellario giudiziale in materia di anagrafe delle sanzioni amministrative dipendenti da reato	relativi alle qualità di indagato o di imputato

contenitori dei documenti cartacei	
armadio con serratura (chiave estraibile)	locale accessibile solo con apposita chiave
shedario con serratura (chiave estraibile)	altri (da specificare)

mezzi elettronici impiegati			
elaboratore non in rete (enr)		server in rete geografica (srg)	
elaboratore in rete locale (eir)		modem (mod)	
server in rete locale (srl)		collegamento internet (int)	

annotazioni

data	firma del compilatore