Comune di Foggia

REGOLAMENTO DEL SISTEMA DI VIDEOSORVEGLIANZA

(Delib. C. C. del 22.02.2010 n. 19)

art. 01
Principi generali

1. Per tutto quanto non risulti dettagliatamente disciplinato nel presente documento, si rinvia a quanto disposto dal Codice in materia di protezione dei dati personali ed ai provvedimenti a carattere generale del Garante per la protezione dei dati personali approvato con D. Lvo 30.06.2003 n. 196.
2. A tal fine ed in applicazione alla disciplina codicistica, si intende per:
   a) "trattamento", tutte le operazioni o complesso di operazioni, svolte con l'ausilio dei mezzi elettronici o comunque automatizzati, 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, l'eventuale diffusione, la cancellazione e la distruzione dei dati;
   b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione identificati o identificabili, anche direttamente, e rilevati con trattamenti di immagini effettuati attraverso l'impianto di videosorveglianza;
   c) "titolare del trattamento", l'Ente Comune di Foggia, nelle sue articolazioni interne, cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali;
   d) "responsabile del trattamento", la persona fisica, legata da rapporto di servizio al titolare e preposto dal medesimo al trattamento dei dati personali;
   e) "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
   f) "comunicazione", il dare conoscenza dei dati personali a soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
   g) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
   h) "dato anonimo", il dato che, in origine, a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
   i) "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
   j) "banca dati", il complesso organizzato di dati personali formatosi presso la sala di controllo e trattato esclusivamente mediante riprese video che, in

relazione ai luoghi di installazione delle telecamere, riguardano i soggetti ed i mezzi di trasporto che transitano nell'area interessata.

3. Quanto sopra premesso, nel ricordare che il Garante per la protezione dei dati personali si è già espresso circa l'ammissibilità del trattamento di dati personali mediante sistemi di videosorveglianza, ai sensi dell'art. 13 del D. Lgs. n. 193/2003, si forniscono le seguenti informazioni:

art. 1
Ambito di applicazione

1. L'attività di videosorveglianza è svolta per le seguenti finalità: tutela del patrimonio, controllo del traffico, protezione civile e sicurezza pubblica, rispetto dell'ordinato e civile svolgimento delle attività commerciali, della circolazione e della convivenza dei cittadini, in concorso con le Centrali della Questura e dell'Arma dei Carabinieri; sono comunque quelle rispondenti alle funzioni istituzionali demandate all'ente, in particolare dal D. Lvo. 18.08.2000 n. 627, dal D.P.R. 24.07.1977 n. 616, dalla L. 07.03.1986 n. 65 sull'ordinamento della Polizia Municipale, nonché dallo Statuto e dai regolamenti comunali sanciti dalla L. 31.12.1996 n. 675 e disposizioni correlate, nonché dall'art. 54 del D. Lgs 18.08.2000 n. 267, come sostituito dall'art. 6 del D.L. n. 92/2008 convertito nella Legge n. 125/2008.
2. La possibilità di avere in tempo reale dati e immagini costituisce uno strumento di prevenzione e di razionalizzazione dei compiti che la Polizia Municipale svolge quotidianamente.
3. L'impianto di videosorveglianza, in estrema sintesi, ha lo scopo di:
   a) Identificazione, in tempo reale, di intasamenti e ostruzioni del traffico per consentire il pronto intervento della Polizia Municipale;
   b) Prevenzione di atti di vandalismo e danneggiamento agli immobili; in sostanza di tutela del patrimonio;
   c) Strumento attivo di protezione civile sul territorio;
   d) Ridurre il sentimento di insicurezza dei cittadini;
   e) Controllare determinate aree ad elevato rischio sicurezza.
4. Con questi scopi si vogliono tutelare le fasce più deboli della popolazione e cioè bambini. Giovani e anziani, garantendo quindi un certo grado di sicurezza negli ambiti circostanzi le scuole, i parchi e le piazze pubbliche, i percorsi a rischio sicurezza e contemporaneamente il patrimonio del Comune stesso e della cittadinanza.

art. 2
Costituzione del sistema

1. Il sistema, a regime, è costituito da tre centrali operative con funzioni di controllo e supervisione collocate una presso il Comando di Polizia Municipale, una presso la Questura e una presso il comando Provinciale dell'Arma dei Carabinieri, di un server per la registrazione delle immagini collocato presso la Centrale Operativa della Polizia Municipale e da un insieme di punti di ripresa costituiti da telecamere fisse e/o telecontrollabili.
2. Le immagini video riprese dalle telecamere sono trasmesse alle Centrali Operative tramite una infrastruttura di rete geografica di tipo proprietario dedicato esclusivamente a questo servizio, in fibra ottica e/o wireless, con trasmissione di tipo digitale ed encription dei dati. Il sistema non è collegato ad altri sistemi né ad alcuna rete pubblica di telecomunicazioni. Non è quindi accessibile da altre periferiche oltre alle Centrali Operative. Presso le Centrali Operative è possibile visualizzare le immagini di tutte le telecamere, brandeggiare (in orizzontale ed in

verticale) e zoomare le telecamere. In caso di necessità sarà anche possibile visualizzare le registrazioni delle telecamere stesse.

3. Mentre per il sistema di ripresa con telecamere "black box" che opera in maniera autonoma, in quanto provvisto di tutti gli apparati di funzionamento per la memorizzazione temporanea dei dati. I dati verranno trattati dal personale abilitato ai sensi del presente regolamento che provvederà allo scarico dei dati ed al trattamento degli stessi secondo la disciplina dettate dal presente regolamento e della normativa vigente.

art. 3
Modalità trattamento immagini

1. Il trattamento sarà effettuato con seguenti modalità: registrazioni su hard disk delle immagini video provenienti dalle telecamere dislocate sul territorio comunale**,** ovvero in caso di riprese con sistema black box, i dati rilevati verranno conservati su supporto ottico (DVD) per il tempo necessario dietro richiesta dell'Autorità Giudiziaria, per poi essere cancellati successivamente. I dati trattati interessano pertanto soggetti e/o mezzi di trasporto che transiteranno nell'area video sorvegliate.

art. 4
Conservazione immagini

1. Le immagini verranno conservate a regime per un massimo di 24 ore successive alla registrazione sul server di registrazione posizionato presso il Comando di Polizia Municipale di Foggia in via Manfredi, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nonché nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'Autorità Giudiziaria o di Polizia Giudiziaria.
2. Un eventuale allungamento dei tempi di conservazione sarà valutato come eccezionale e comunque in relazione alla necessità derivante da un evento già accaduto o realmente incombente, oppure alla necessità di custodire o consegnare una copia specificamente richiesta dall'Autorità Giudiziaria o di Polizia Giudiziaria, in relazione ad un'attività investigativa in corso, casi per i quali viene stabilito un termine massimo di settantadue (72).

art. 5
Sovrascrittura immagini

1. Il sistema impiegato è programmato in modo da operare al momento prefissato la sovrascrittura automatica delle immagini, con modalità tali da rendere non riutilizzabili i dati cancellati. In caso di cessazione di un trattamento, per qualsiasi causa, i dati personali saranno distrutti.

art. 6
Modalità raccolta dati

1. I dati personali oggetto di trattamento, trattati in modo lecito e secondo correttezza, sono:
   a) raccolti e registrati per le finalità di cui al precedente art. 1 e resi utilizzabili in altre operazioni del trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi, esatti e, se necessario aggiornati;
   b) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;
   c) conservati per un periodo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali dell'impianto, per le quali essi sono

stati raccolti o successivamente trattati ed in ogni caso pari al periodo di tempo stabilito dal precedente art. 4.

art. 7
Custodia dati

1. I dati personali oggetto di trattamento sono custoditi presso la sala di controllo del Comando di Polizia Municipale, dove è custodito il server con l'hard disk per la videoregistrazione digitale eventualmente anche presso le sale controllo della Questura e dei Carabinieri, che accedono al server come client.
2. Mentre i dati rilevati dal sistema " black box", verranno conservati su supporto ottico (DVD) per i tempo necessario dietro richiesta dell'Autorità Giudiziaria, per poi essere cancellati successivamente.
3. A questi locali può accedere, oltre il Sindaco in qualità di titolare del trattamento, o suo delegato, solo ed esclusivamente il responsabile e gli incaricati del trattamento, indicati ai successivi art. 11 e 12 istruiti sull'utilizzo dell'impianto e sul trattamento dei dati.
4. Previa presenza del responsabile del trattamento, o incaricato da Lui delegato, è ammesso l'accesso anche alla ditta autorizzata per eventuali interventi di manutenzione e/o ripristino del sistema.
5. La sala di controllo è sistematicamente chiusa a chiave, presidiata h24 ed è ubicata in locali non accessibili al pubblico nella parte adibita al controllo.
6. L'utilizzo di un sistema di videoregistrazione digitale impedisce la rimozione accidentale delle immagini registrate su supporti rimovibili su cui sono memorizzate le immagini.

art. 8
Comunicazione dati

1. I dati non saranno comunicati ad altri soggetti, né saranno oggetto di diffusione, salvo espressa richiesta dell'Autorità giudiziaria o della Polizia Giudiziaria in relazione ad un' attività investigativa in corso.
2. La comunicazione dei dati personali da parte del Comune di Foggia a favore di soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento.
3. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento delle funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'art. 39, comma 2 del D. Lgs 30.06.2003 n. 196.
4. Non si considera comunicazione la conoscenza dei dati personali da parte delle persone incaricate ed autorizzate per iscritto a compiere le operazioni del trattamento dal titolare o dal responsabile e che operano sotto la loro diretta autorità.

art. 9
Titolare trattamento dati

1. Il titolare del trattamento dei dati mediante visione e registrazione delle immagini della telecamere è il Comune di Foggia nella persona del Sindaco e legale rappresentante pro tempore.
2. Il titolare deve rispettare pienamente quanto previsto, in tema di trattamento dei dati personali, dalle leggi vigenti, ivi incluso il profilo della sicurezza per impedire appropriazioni o usi indebiti dei dati.

art. 10
Responsabile del trattamento dati

1. Il responsabile del trattamento, come da atto di nomina, documento agli atti è il Comandante della Polizia Municipale del Comune di Foggia, domiciliato in ragioni delle funzioni svolte in Foggia, presso il Comando di Polizia Municipale in via Manfredi.
2. Il responsabile procede al trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle presenti disposizioni.
3. Il responsabile del trattamento, dovrà attuare tutte le precauzioni di natura tecnica, procedurale ed organizzativa per garantire il rispetto di trattamento secondo la legge e le misure di sicurezza per impedire usi impropri dei dati.
4. In particolare, dovrà individuare gli eventuali settori di ripresa delle telecamere che possono insistere su aree private, ad elevato rischio di violazione della privacy, e procedere al loro oscuramento di ripresa.
5. Il responsabile vigila sull'utilizzo dei sistemi e sul trattamento delle immagini e dei dati in conformità agli scopi perseguiti dal Comune e alle altre disposizioni normative che disciplinano la materia ed in particolare alle eventuali disposizioni impartite dall'Autorità Garante per la protezione dei dati personali.
6. l responsabile custodisce le chiavi dell'armadio destinato alla conservazione delle registrazioni nonché le password per l'utilizzo del sistema.
7. Il responsabile della gestione e del trattamento impartisce idonee istruzioni atte ad evitare assunzioni o rilevamento di dati da parte delle persone autorizzate all'accesso per le operazioni di manutenzione degli impianti.
8. Il responsabile del trattamento potrà tenere un registro dell'impianto dove annotare gli accessi al sistema, i dati eventualmente assunti e quant'altro ritenga di annotare. Il tutto da lui sottoscritto.

art. 11
Incaricato trattamento dati

1. Incaricati del trattamento, come da atti di nomina, documenti agli atti, e quindi autorizzati ad utilizzare gli impianti e a visionare le registrazioni, nei casi in cui sia indispensabile per gli scopi perseguiti, sono soggetti di seguito individuati:
   a) Il Responsabile P.O. della Centrale Operativa, gli Ufficiali e gli Agenti di Polizia Giudiziaria in servizio effettivo presso la Centrale Radio Operativa del comando di Polizia Municipale.
2. Abilitati alla solo utilizzazione per la visione in diretta delle immagini trasmesse dalle telecamere di videosorveglianza, sono gli Ufficiali e il personale Agenti di P.G. in servizio presso il Comando, opportunamente addestrato a norma vigente del D. Lvo n. 196/2003, durante i servizi serali, notturni e festivi, impiegati come Operatori di Centrale.
3. Per eventuali centrali ubicate presso la Questura di Foggia e presso il Comando Provinciale dei Carabinieri, ogni organismo provvederà con atti autonomi a nominare i responsabili e gli incaricati del trattamento.
4. A ciascun incaricato verrà assegnata una password di accesso,della quale è responsabile per la custodia, conservazione e assoluta riservatezza.
5. Gli incaricati del materiale trattamento devono elaborare i dati personali ai quali hanno accesso, attenendosi scrupolosamente alle istruzioni del titolare o del responsabile.
6. Nello svolgimento dell'attività volta alla prevenzione dei crimini e tutela del patrimonio tramite il sistema di videosorveglianza, gli incaricati devono scrupolosamente osservare i principi di liceità, necessità e proporzionalità,

limitando i dettagli delle immagini alle reali necessità, predisponendo eventuali automatismi di ripresa (tour e/o preposizionamenti) avendo cura di evitare luoghi ed accessi privati, luoghi di lavoro, luoghi di culto, alberghi, ospedali, ecc..

7. Gli incaricati sono obbligati a non effettuare riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto attivato.
8. L'accesso alle immagini registrate deve essere effettuato esclusivamente in caso di eventi criminosi, di danni al patrimonio comunale o attività di Polizia Giudiziaria, dirette e delegate dall'Autorità Giudiziaria. In nessun caso, i dati trattati, devono essere diffusi o comunicati a terzi, salvo che si tratti di indagini giudiziarie o di polizia.
9. La mancata osservanza degli obblighi previsti al presente articoli comporterà l'applicazione di sanzioni disciplinari e, nei casi previsti dalla normativa vigente, di sanzioni amministrative oltre l'avvio degli eventuali procedimenti penali.

art. 12
Manutenzione impianto

1. Ai fini dell'efficienza e manutenzione degli impianti si avvarrà della collaborazione di Ditte nominate dall'Amministrazione Comunale, che svolgeranno prestazioni strumentali subordinate alle scelte del titolare del trattamento, con la collaborazione interna dei tecnici informatici del Settore – Comune di Foggia con prestazioni di manutenzione e ripristino, riferiti alla rete in fibre ottiche e wireless.

art. 13
Principi fondamentali D. Lgs. 196 del 30.06.2003

1. Nel rispetto dei principi fondamentali sanciti dal decreto Legislativo del 30.06.2003 n. 196, a tutela della riservatezza delle persone rispetto al trattamento dei dati personali, applicabile anche alle attività di videosorveglianza, ed in particolare di quello della pertinenza e non eccedenza dei dati trattati rispetto agli scopi perseguiti, le telecamere sono state installate in modo tale da limitare l'angolo visuale delle riprese, evitando quando non indispensabili come nell'ipotesi di cui al successivo punto, immagini dettagliate, ingrandite o dettagli non rilevanti.
2. E' comunque vietato divulgare o diffondere immagini, dati e notizie di cui si è venuti a conoscenza nell'utilizzo degli impianti,nonché procedere a qualsiasi ingrandimento delle immagini al di fuori dei casi regolati dal presente regolamento.
3. I dati raccolti per determinati fini (ad esempio ragioni di sicurezza, tutela del patrimonio) non possono essere utilizzati per finalità diverse o ulteriori (ad esempio pubblicità, analisi dei comportamenti di consumo) salvo esigenze di polizia e di giustizia.
4. E' vietato utilizzare le immagini che anche accidentalmente dovessero essere assunte per finalità di controllo anche indiretto sull'attività professionale dei dipendenti, secondo il disposto dell'art. 4 della Legge 20 maggio 1970 n. 300 (statuto dei lavoratori) e ferma restando la procedura prevista dal medesimo articolo.

art. 14
Modalità operative

1. Ove dovessero essere rilevate immagini di fatti identificativi di ipotesi di reato o di eventi rilevanti ai fini della sicurezza pubblica o della tutela ambientale e del patrimonio, l'incaricato del trattamento provvederà a darne immediata comunicazione agli organi competenti.
2. In tali casi, in deroga alla puntuale prescrizione delle modalità di ripresa di cui al precedente articolo, l'incaricato del trattamento procederà quando possibile agli ingrandimenti della ripresa delle immagini strettamente necessari e non eccedenti allo specifico scopo perseguito ed alla registrazione delle stesse su supporti ottici.
3. Dalla eventuale attività di duplicazione dei dati registrati su supporto ottico, dovrà redigere annotazione compilando apposito registro.
4. Alle informazioni raccolte ai sensi del presente articolo possono accedere solo gli organi di Polizia e l'Autorità Giudiziaria.
5. L'apparato di videosorveglianza potrà essere utilizzato anche in relazione ad indagini di Autorità Giudiziaria, di Corpi di Polizia o di organi di Polizia Municipale. Nel caso, in cui i Corpi e gli organi di Polizia, nello svolgimento di loro indagini, necessitino di avere informazioni ad esse collegate che possono essere contenute nelle riprese effettuate, possono farne richiesta scritta e motivata indirizzata al Responsabile della Gestione e del trattamento dei dati.

art. 15
Diritti dell'interessato

1. In ogni momento l'interessato potrà esercitare i suoi diritti nei confronti del titolare del trattamento, ai sensi dell'art. 7 del D. Lgs. n. 196/2003, in particolare, dietro presentazione di apposita istanza ha diritto:
   a) di conoscere l'esistenza di trattamenti di dati che possono riguardarlo;
   b) di essere informato sugli estremi identificativi del titolare e del responsabile oltre c) che sulle finalità e le modalità del trattamento cui sono destinati i dati;
   d) di ottenere, a cura del responsabile, senza ritardo e comunque non oltre 30 giorni dalla data di ricezione della richiesta;
   e) la conferma dell'esistenza o meno di dati personali che lo riguardano e la comunicazione in forma intelligibile dei medesimi dati, nonché l'indicazione della loro origine, della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa il trattamento;
   f) la richiesta non può essere inoltrata dallo stesso soggetto se non trascorsi almeno novanta giorni dalla precedente istanza, fatta salva l'esistenza di giustificati motivi;
   g) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   h) di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.
2. Per ciascuna delle richieste di cui sopra può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, secondo le modalità previste dalla normativa vigente.
3. Le suddette istanze possono essere trasmesse al titolare o al responsabile del trattamento, anche mediante lettera raccomandata, telefax o posta elettronica; costoro dovranno provvedere in merito entro e non oltre trenta giorni.

4. Quando la richiesta riguarda esercizio dei diritti di cui all'articolo 7, commi 1° e 2°, del D. Lgs. n.196/2003, la stessa può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.
5. Nell'esercizio dei diritti di cui all'articolo 7 del predetto decreto legislativo, l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi.
6. L'interessato può, altresì, farsi assistere da una persona di fiducia.
7. La richiesta può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.
8. Nel caso di esito negativo all'istanza di cui sopra, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente nei termini previsti.
9. I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
10. L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento.
11. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autentificata di un documento di riconoscimento dell'interessato.
12. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona legittimata in base ai rispettivi statuti od ordinamenti.

art. 16
Cartello presenza sistema

1. Il Comune di Foggia, in ottemperanza a quanto disposto dall'art. 13 del D. Lgs. n. 196 del 30.06.2003, ha provveduto ad affiggere un'adeguata segnaletica permanente all'accesso alla città e nelle aree in cui sono concretamente posizionate le telecamere attraverso appositi avvisi recanti la dicitura: "AREA/TERRITORIO VIDEOSORVEGLIATA/O – LA REGISTRAZIONE E' EFFETTUATA DALLA POLIZIA MUNICIPALE PER FINALITA' DI SICUREZZA E TUTELA DEL PATRIMONIO – ART. 13 DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (D. Lgs. n. 196/2003)", in cinque lingue inglese,francese, tedesco, spagnolo,arabo.

art. 17
Pubblicità attivazione del sistema

1. Il Comune di Foggia, nella persona del Responsabile del trattamento, si obbliga a comunicare alla comunità cittadina l'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di videosorveglianza, l'eventuale incremento dimensionale dell'impianto e l'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, con un anticipo di giorni dieci, mediante l'affissione di appositi manifesti informativi e/o altri mezzi di diffusione locale.

art. 18
Cessazione dati

1. In caso di cessazione, per qualsiasi causa, del presente trattamento i dati personali saranno distrutti.

art. 19
Provvedimenti attuativi

1. Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dagli artt. 141 e seguenti del D. Lgs. 30.06.2003 n. 196.
2. In sede amministrativa, il responsabile del procedimento ai sensi e per gli effetti degli artt. 4 e 6 della L. n. 241 del 07.08.1990 è il responsabile del trattamento dei dati personali così come individuato sopra.
3. Il presente regolamento viene pubblicato all'Albo Pretorio; copia dello stesso può essere richiesta presso il Responsabile dei Trattamenti dei dati.
4. Il medesimo potrà essere integrato o modificato con successivo provvedimento, in caso di variazione delle condizioni di applicazione.
5. Si allegano fac-simile richiesta ad accessi alle immagini di videosorveglianza con sintetica descrizione della relativa procedura, nonché l'allegato "B" del D. Lvo. n.196/2003.

FAC - SIMILE RICHIESTA DI ACCESSO A VIDEOREGISTRAZIONI

Il sottoscritto ..... , identificato tramite…….. ai sensi della vigente normativa in materia di privacy richiede di esercitare il diritto di accesso alle immagini video che potrebbero aver registrato dati personali a sé stesso afferenti. Per permettere di individuare tali immagini nell'archivio video, fornisce le seguenti informazioni:
1) Luogo o luoghi di possibile ripresa ……
……
……
……

2) Data di possibile ripresa
……

3) Fascia oraria di possibile ripresa (approssimazione di 30 minuti)
……

4) Abbigliamento al momento della possibile ripresa
……
……
……

5) Accessori (borse, ombrelli, carrozzine, animali al guinzaglio, altri oggetti)
……
……
……

6) Presenza di accompagnatori (indicare numero, sesso, sommaria descrizione degli stessi)
……
……
……

7) Attività svolta durante la possibile ripresa
……
……
……

Recapito (o contatto telefonico) per eventuali ulteriori approfondimenti
……

In fede.
(Luogo e data)..... .....

(firma)

……..

PARTE DA CONSEGNARE AL RICHIEDENTE

* In data …… alle ore …… il/la Sig./Sig.ra ……..ha avanzato richiesta di accesso a videoregistrazioni, ai sensi della vigente normativa in materia di privacy.

(Firma del ricevente la richiesta)

FAC - SIMILE RECLAMO

Al Responsabile trattamento dei dati

……

Il sottoscritto .....che aveva presentato in data……..…

presso ……...

una richiesta di accesso alle immagini video che potrebbero aver registrato miei dati personali presenta reclamo per i seguenti motivi ……..
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
Recapito (o contatto telefonico) per eventuali ulteriori approfondimenti

…….

In fede.

(Luogo e data).....

Firma

……

ALLEGATO "B" al decreto legislativo n. 196/2003

DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Artt. da 33 a 36 del codice)

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 e' 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 e' 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 e' prevista dal sistema di autenticazione, e' 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 e' 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 e' 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 e' 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 e' 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, e' 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 e' 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 e' 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.

Trattamenti senza l'ausilio di strumenti elettronici

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

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.
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.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari e' 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.