Regolamento per la disciplina delle modalità di trattamento dei dati personali. Istruzioni organizzative e tecniche

ART. 1
TITOLARE, RESPONSABILI E INCARICATI

Titolare del trattamento ai sensi dell'art. 28 del D.Lgs 196/03, d'ora in poi denominato Codice, è l'Università.
Responsabili del trattamento ai sensi dell'art. 29 del Codice sono:
- il Rettore relativamente ai dati trattati da: Segreteria del Rettorato, Servizio di Prevenzione e Protezione, Ufficio di collegamento Università impresa Industrial Liason Office, Servizio Stampa e Servizio di Radioprotezione;
- il Direttore Amministrativo, relativamente ai dati trattati dalle strutture afferenti allo staff della Direzione Amministrativa;
- i Dirigenti di Dipartimenti e Aree;
- il Direttore del Centro Universitario di Calcolo;
- i Presidi di Facoltà;
- i Direttori di Dipartimento;
- il Direttore della Sissis;
- il Direttore del Centro di Orientamento e Tutorato;
- i Direttori dei Centri interdipartimentali.

Ai Responsabili del trattamento compete l'attuazione delle misure di sicurezza sia logiche che fisiche previste dal Codice, dal Documento Programmatico per la Sicurezza dell'Ateneo e dal presente Regolamento.
L'individuazione di ulteriori responsabili, anche esterni, del trattamento dei dati dei quali è Titolare l'Università e la nomina degli stessi avviene con provvedimento del Rettore pro tempore.
I compiti dei responsabili del trattamento sono: operare, direttamente o a mezzo di incaricati individuati come di seguito specificato, il trattamento dei dati personali e di eventuali dati sensibili e giudiziari secondo il principio di pertinenza e non eccedenza dei dati stessi e conformandosi alle istruzioni di cui al presente regolamento e a quanto previsto dal Regolamento di Ateneo sul trattamento dati sensibili e giudiziari e dal Codice; adottare e rispettare le misure minime di sicurezza previste dal Codice nonché le ulteriori eventualmente individuate dal Titolare del trattamento ed indicate nel Documento Programmatico sulla Sicurezza aggiornato annualmente.
I responsabili individuano con proprio provvedimento formale i soggetti incaricati del trattamento con indicazione nominativa della persona fisica, del ruolo ricoperto e dell'ambito del trattamento consentito.
I trattamenti dei dati dei quali è Titolare l'Università possono essere legittimamente effettuati solamente dai soggetti incaricati: docenti, personale tecnico amministrativo e ogni altro soggetto anche non strutturato chiamato a svolgere funzioni che implichino i trattamenti suddetti.
Il Direttore del Centro Universitario di Calcolo pro tempore assume, altresì, la funzione di "Responsabile informatico d'Ateneo per il trattamento dei dati personali".

Il Responsabile Informatico d'Ateneo per il trattamento dei dati personali individua, in accordo con i responsabili del trattamento di cui all'art. 1 della relativa struttura, gli amministratori di sistema e provvede alla nomina degli stessi con provvedimento formale che dovrà essere trasmesso al Titolare per conoscenza.
Gli amministratori di sistema devono fornire idonea garanzia del pieno rispetto delle disposizioni in materia di corretto trattamento, compreso il profilo relativo alla sicurezza informatica, anche in considerazione delle responsabilità, di natura penale e civile, che possono derivare in caso di incauta o inidonea designazione.
I provvedimenti di nomina dovranno riportare la descrizione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
Gli Amministratori di sistema dovranno essere nominati in ragione di almeno uno ogni 50 unità di personale, per singola struttura.
Il Responsabile Informatico D'Ateneo per il trattamento dei dati personali cura, altresì, tutti gli adempimenti relativi al trattamento dei dati personali/sensibili/giudiziari effettuato con strumenti elettronici adottando le misure logiche ritenute necessarie per contrastare i rischi specifici dallo stesso individuati.
Il Responsabile Informatico d'Ateneo per il trattamento dei dati personali propone le modifiche da apportare al Documento Programmatico sulla Sicurezza dei dati Personali, in occasione della revisione annuale, rese necessarie dall'individuazione di nuovi e ulteriori rischi legati al trattamento elettronico dei dati, nonché dalle nuove risorse hardware e software in dotazione all'Ateneo, o comunque, acquisibili.
Presso il Centro Universitario di Calcolo sono costituiti i seguenti gruppi di lavoro, i cui componenti sono nominati dal Responsabile Informatico D'Ateneo:

1) Reti e sicurezza (connessioni in rete e sicurezza informatica);
2) RDBMS, Backup e Disaster Recovery (database, backup dei dati e ripristino dei sistemi);
3) Accesso al sistema Informativo (credenziali di accesso);
4) Sviluppo Applicazioni e gestione software applicativo (procedure applicative).

Le nomine avranno validità fino alla revoca delle stesse.
Tutti i soggetti incaricati devono evitare comportamenti che possano pregiudicare la riservatezza dei dati.

ART. 2
AMMINISTRATORI DI SISTEMA

Gli amministratori di sistema dovranno:
- assicurare la buona funzionalità di ciascun server e stazione di lavoro tramite aggiornamento del sistema operativo e protezione con tutti i sistemi disponibili (firewall, antivirus, etc.);
- accertarsi che non vi sia risorsa come server, router, switch indirizzabile, telecamera IP, bridge wireless, ponte ottico, etc. che non abbia un amministratore di sistema di riferimento e in caso contrario comunicarlo al Responsabile Informatico d'Ateneo; i telefoni e i router di backbone universitari VoIP hanno come amministratori di sistema di riferimento il personale afferente al "gruppo reti e sicurezza" del CUC;
- tenere un elenco scritto e sempre aggiornato che comprenda:

a) locale in cui si trova la risorsa informatica ed eventuale detentore di chiave con relativo recapito telefonico;
b) sistema operativo utilizzato (con il codice) ed eventuale numero di serie di ogni risorsa;
c) indirizzo IP e MAC;
d) eventuale nome mnemonico Internet (es. pc1.cuc.unipa.it);
e) nome e gruppo di lavoro Microsoft;
f) nome e cognome dell'utilizzatore;
g) ragione sociale dell'eventuale ditta manutentrice;
h) eventuale presenza di computer con funzioni di server;
i) eventuale connessione in rete non gestita dal gruppo reti e sicurezza costituito presso il CUC (ADSL, HDSL, CDN, wireless, ...);
- inviare, in occasione di ogni aggiornamento, l'elenco suddetto, via posta elettronica, al seguente indirizzo: *rete@unipa.it*;
- gestire le risorse informatiche presenti nelle aule didattiche con un piano di indirizzamento IP privato tipo 192.168.x.y con firewall e proxy server da utilizzare con username e password;
- accertarsi che non vengano utilizzate apparecchiature che consentano e/o facilitino l'intercettazione del traffico di rete (hub, software specifici di intercettazione, ..);
- conservare gli "access log" per almeno sei mesi in archivi immodificabili e inalterabili adottando sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici che devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica dell'integrità degli stessi con riferimenti temporali certi e la descrizione dell'evento che li ha generati.
Nel caso in cui si verifichi in rete wired una "duplicazione di indirizzo IP" l'amministratore di sistema deve immediatamente comunicarlo al Responsabile Informatico di Ateneo.
Nel caso in cui si verifichi un accesso a rete wireless con autenticazione non centralizzata (diversa da username e password relative alla posta elettronica) l'amministratore di sistema deve immediatamente comunicarlo al Responsabile Informatico di Ateneo.
Nel caso in cui si riscontri in rete la presenza di un DHCP server non autorizzato l'Amministratore di sistema deve immediatamente darne comunicazione al Responsabile Informatico di Ateneo;
Ogni piano di indirizzamento IP deve essere riferito ad un determinato Amministratore di Sistema; ciascun amministratore di sistema è tenuto, per la parte di propria competenza, ad aggiornare l'elenco degli utenti IP accedendo con le proprie credenziali all'indirizzo web http://netadmin.unipa.it.
Nel caso in cui all'interno di una struttura non si rinvenga la relativa professionalità, l'incarico di Amministratore di Sistema potrà essere conferito a persona fisica esterna all'Ateneo da parte del Direttore Amministrativo.

ARTICOLO 3
INTERVENTI FORMATIVI

La formazione e l'aggiornamento in materia di sicurezza dei dati personali degli operatori rientrano tra le misure di sicurezza espressamente previste dalla regola 19.6 dell'allegato B, disciplinare tecnico, al Codice.
Appositi interventi formativi, destinati a responsabili ed incaricati, verranno effettuati al momento dell'ingresso in servizio; ulteriori interventi di aggiornamento verrano organizzati in relazione a cambiamenti di mansioni, utilizzo di nuovi strumenti e modifiche normative.
Su iniziativa del Responsabile Informatico d'Ateneo, tutti gli amministratori di sistema e i componenti del CUC afferenti ai gruppi di cui all'art. 1 vengono annualmente avviati ad interventi formativi sulle politiche di sicurezza dei sistemi e delle reti di Ateneo (art. 34, Comma b).
Tutti gli interventi formativi sopra specificati vengono inseriti nel piano annuale delle attività formative del personale.

ART. 4
ISTRUZIONI OPERATIVE

Il trattamento di dati personali non deve essere effettuato se è possibile realizzare le singole finalità perseguite attraverso l'uso di dati anonimi.
I dati personali oggetto di trattamento devono essere pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti e 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 sono stati raccolti.
All'interessato o alla persona presso la quale sono raccolti i dati personali deve essere fornita verbalmente o per iscritto la cosiddetta informativa prevista dall'Art. 13 del Codice.
Al momento della raccolta dei dati non va richiesto il consenso dell'interessato.
In relazione all'acquisizione di dati dagli interessati presenti fisicamente, finalizzata ad adempimenti amministrativi, preceduta da un periodo di attesa all'interno di locali dell'Università, verranno adottati ordini di precedenza e sistemi di chiamata degli interessati che prescindano dall'individuazione nominativa; verranno altresì istituite apposite distanze di cortesia.
Relativamente al caso specifico dei dati indicati nella busta paga, viene stabilito che, nel rispetto del principio di pertinenza e non eccedenza, anche allo scopo di non rivelare delicati aspetti relativi a rapporti familiari o a provvedimenti giudiziari, non vengano riportate informazioni relative a pignoramenti, assegni alimentari e simili, ma vengano utilizzate diciture meno dettagliate che rendano ugualmente comprensibile la voce o codici identificativi; altresì, in caso di iscrizione a sindacato, nella voce della relativa trattenuta, non dovrà essere riportata l'indicazione del particolare sindacato al quale il dipendente è iscritto.
Per quanto attiene alla disciplina generale del trattamento dei dati sensibili e giudiziari si rimanda al relativo regolamento emanato con DR 6510 del 27 dicembre

2006.

ART. 5
TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI

Per i trattamenti effettuati con strumenti elettronici vengono stabilite le seguenti modalità.
Per il trattamento dei dati personali vengono rilasciate ad ogni singolo incaricato, a cura del Responsabile informatico di Ateneo, una o più utenze, ciascuna identificata con una username e una password; l'utenza consente l'individuazione dell'incaricato stesso. La password deve essere composta da almeno 8 caratteri, non deve contenere riferimenti facilmente riconducibili all'incaricato e deve essere modificata da quest'ultimo al primo utilizzo e almeno ogni sei mesi (tre in caso di dati sensibili e giudiziari).
L'incaricato deve adottare le cautele necessarie ad assicurare la segretezza della password e la diligente custodia di tutti dispositivi assegnatigli: PC, dispositivi USB, CD-ROM, floppy disk, etc.
Al fine di evitare accessi non consentiti e trattamenti non autorizzati, tutti i supporti su cui sono memorizzati i dati devono essere conservati in contenitori dotati di serratura, armadi o altro ricovero atto a garantirne l'inviolabilità.
Per assicurare la disponibilità dei dati in caso di prolungata assenza o impedimento dell'incaricato, lo stesso, dopo ogni modifica della password, deve consegnarla in busta chiusa e sigillata al proprio responsabile; le utenze non utilizzate per almeno sei mesi vengono disattivate dal Responsabile Informatico di Ateneo.
Gli incaricati non dovranno mai lasciare incustodita e accessibile la propria stazione di lavoro durante una sessione di trattamento; le password non possono essere riutilizzate, neanche in tempi diversi.
Il salvataggio dei dati trattati (backup) con strumenti informatici deve avvenire almeno settimanalmente ed, eventualmente, potranno essere concordati con il Responsabile Informatico di Ateneo sia la frequenza del backup che lo spazio disco necessario allo scopo.
Per tutto quanto al riguardo qui non stabilito, si rimanda al Documento Programmatico per la Sicurezza e all'allegato B al D.lgs. 196/2003.
L'Incaricato è responsabile per l'utilizzo di applicazioni informatiche e di elaborazioni effettuate attraverso l'utilizzo della propria utenza.
L'incaricato che rilevi nell'utilizzo del PC o di un'applicazione informatica un' anomalia che possa compromettere la sicurezza dei dati ne dà immediata comunicazione al Responsabile Informatico di Ateneo cui compete l'adozione delle misure tecniche necessarie alla risoluzione della stessa.
All'Incaricato è fatto divieto di installare programmi non attinenti le ordinarie attività lavorative senza il preventivo parere del Responsabile Informatico di Ateneo; è altresì fatto divieto di modificare le configurazioni hardware e software senza il succitato parere.
Nell'ambito delle misure minime di protezione previste dal Documento Programmatico per la Sicurezza e dal presente Regolamento possono essere adottati

differenti profili di utenza specificando il tipo di accesso ai dati (ad esempio: solo visualizzazione o anche modifica degli stessi).

ART. 6
PARTICOLARI MISURE DI SICUREZZA

Allo scopo di evitare i potenziali danni al sistema informativo dell'Ateneo e ai dati in esso contenuti, derivanti da un uso improprio della connessione alla rete Internet, tutti gli incaricati dovranno:

• Utilizzare la connessione in rete esclusivamente per lo svolgimento delle attività istituzionali;

• Comunicare formalmente al Responsabile Informatico di Ateneo l'utilizzo di eventuali ulteriori tipi di connessione (ADSL, HDSL, wireless o altro); in ogni caso, le apparecchiature collegate con provider esterni non possono essere collegate contemporaneamente in alcun modo alla rete universitaria;

• Adottare sistemi operativi che prevedano l'accesso con username e password e l'aggiornamento automatico dello stesso (non possono essere più utilizzati, per il collegamento in rete, sistemi operativi come Windows 95, 98, ME);

• Adottare sistemi antivirus che prevedano aggiornamenti automatici quotidiani e ad ogni riavvio del sistema;

• Utilizzare mail server dotati di sistema antivirus;

• Non diffondere messaggi di posta elettronica di provenienza dubbia;

• Non inviare messaggi con allegati di peso superiore a 50 MB;

nel caso di uso illegittimo della connessione alla rete Internet potranno trovare applicazione le disposizioni del codice penale di cui agli artt. : 615\ter "accesso abusivo ad un sistema informatico o telematico", 615\quater "detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici", 615\quinquies "diffusione di programmi diretti a danneggiare o interrompere un sistema informatico" nonché della legge 21\05\04 n. 128 che sanziona la condivisione e\o la fruizione di files relativi a un'opera cinematografica o assimilata protetta dal diritto d'autore.

ART. 7
TRATTAMENTI EFFETTUATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Relativamente ai trattamenti effettuati senza l'ausilio di strumenti elettronici viene stabilito che:

- nel caso in cui intervengano variazioni relativamente ai trattamenti consentiti a ciascun incaricato, venga coerentemente aggiornato il provvedimento di nomina specificando l'ambito del trattamento consentito;
- gli atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti devono essere utilizzati in modo che né terzi né altri incaricati possano avervi accesso, in modo da ridurre al minimo il rischio, anche accidentale, di perdita dei

dati e devono essere custoditi in armadi e schedari con serratura; laddove possibile, anche allo scopo di contrastare il rischio di distruzione, il documento cartaceo di particolare rilevanza deve essere riprodotto tramite scanner e la copia archiviata su supporto fisso o amovibile; i fascicoli del personale e in genere la documentazione riportante dati personali del personale dipendente devono essere custoditi in archivi ad accesso selezionato e limitato ad incaricati precedentemente individuati.

ART. 8
CARTELLINI IDENTIFICATIVI

Al fine di soddisfare l'esigenza fondamentale di trasparenza e ottimizzazione dei rapporti tra operatori e utenti dei servizi il personale d'Ateneo potrà essere dotato di cartellini identificativi recanti la fotografia, il nome, il cognome e la struttura di servizio di ciascun dipendente.
Il personale di front office delle segreterie dovrà essere obbligatoriamente dotato di cartellino con le informazioni di cui al comma precedente.

ART. 9
COMUNICAZIONE DI DATI

La comunicazione di dati personali ad altri soggetti pubblici è ammessa se prevista da norma di legge o regolamento. Se, comunque, necessaria per lo svolgimento di funzioni istituzionali, può essere effettuata dandone preventiva informazione all'Autorità Garante per la protezione dei dati personali, decorsi 45 giorni dall'informazione e salvo diversa determinazione del Garante.
La comunicazione di dati personali e identificativi a privati o enti pubblici economici e la loro diffusione sono ammesse esclusivamente se previste da norma di legge o regolamento.
La comunicazione di dati personali riguardanti studenti o laureati a privati o enti pubblici economici, rientrando l'agevolazione dell'inserimento di studenti e laureati e nel mondo del lavoro tra le finalità istituzionali dell'Università, è ammessa esclusivamente a tale scopo e previa sottoscrizione da parte dei destinatari dei dati stessi di un impegno a non utilizzarli per scopi commerciali e comunque diversi da quelli suddetti (Art. 19 comma 3 del Codice).
I dati suddetti possono, altresì, essere comunicati a soggetti pubblici e privati che perseguono finalità di interesse pubblico nell'ambito dell'istruzione superiore e del successivo inserimento nel mondo del lavoro per lo svolgimento di indagini statistiche ed esclusivamente a tale scopo.
In conformità a quanto su disposto, nell'informativa da fornire agli studenti all'atto dell'immatricolazione ai sensi dell'art. 13 del Codice, andrà specificato che tra i soggetti o le categorie di soggetti ai quali i dati degli studenti potranno essere comunicati, rientrano privati ed enti pubblici economici ai fini dell'avviamento al lavoro degli studenti stessi e dell'effettuazione di indagini statistiche.
Con particolare riferimento ai dati di cui è Titolare l'Università trattati dall'Istituto di

credito Cassiere, da nominare responsabile esterno del trattamento dei dati con provvedimento del Rettore, tale soggetto, laddove necessario per lo svolgimento delle funzioni di cui alla relativa convenzione stipulata con il Titolare, potrà effettuare comunicazione di tali dati anche a soggetti terzi.
Per quanto riguarda i trasferimenti di dati all'estero si rimanda al Titolo VII del Codice.

ART. 10
TRATTAMENTI DI DATI E RICERCA SCIENTIFICA

Il trattamento dei dati personali nell'ambito della ricerca statistica e scientifica deve essere effettuato nel rispetto di quanto previsto dal relativo codice deontologico pubblicato in G.U. n. 190 del 14/8/04.

ART. 11
COMUNICAZIONE E DIFFUSIONE DI DATI A FINI DI RICERCA SCIENTIFICA

Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico possono essere comunicati e diffusi anche a privati e anche per via telematica dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi con esclusione di quelli sensibili e giudiziari. Gli interessati possono opporsi per motivi legittimi.

ART. 12
Video sorveglianza

L'Università degli Studi di Palermo, nell'ambito dei propri fini istituzionali, al fine di garantire il regolare svolgimento delle attività didattiche di ricerca, nonché per garantire la sicurezza e l'incolumità di studenti, utenti, visitatori e di quanti accedono ai propri locali, per tutelare il proprio patrimonio mobiliare e immobiliare contro il rischio di furti e danneggiamenti e altresì per assicurare la sicurezza e la riservatezza dei documenti e dei dati personali in essi contenuti, può fare installare presso i locali e nelle aree dei quali è titolare sistemi di video sorveglianza.
Il trattamento dei dati personali effettuato mediante l'impianto di video sorveglianza nei locali dell'Ateneo deve essere svolto nel pieno rispetto dei diritti delle libertà fondamentali nonché della dignità delle persone con particolare riferimento alla riservatezza e all'identità personale;
I dati raccolti non possono essere utilizzati per finalità diverse da quelle sopra indicate e stabilite nell'apposito documento di certificazione delle scelte da redigersi a cura di ciascun responsabile del trattamento e non possono essere diffusi o comunicati a terzi.
Il trattamento dei dati personali acquisiti mediante gli impianti di video sorveglianza installati presso le strutture dell'Ateneo avviene nel rispetto delle prescrizioni del Codice nonché dei provvedimenti del Garante in materia ed è improntato a principi di liceità, necessità, proporzionalità e finalità.

Le immagini raccolte non devono essere in alcun modo impiegate come strumento di sorveglianza a distanza dei docenti, del personale tecnico amministrativo, degli studenti e degli altri utenti dell'Università sia con riferimento allo svolgimento dell'attività lavorativa che con riferimento alle proprie abitudini personali. A tale proposito è vietata l'installazione di videocamere in luoghi esclusivamente destinati allo svolgimento dell'attività lavorativa o altri quali, a mero titolo esemplificativo, toilette, spogliatoi, docce, armadietti, luoghi ricreativi; in particolare non potranno essere in alcun caso riprese le apparecchiature di rilevazione automatizzata della presenza del personale.
I programmi informatici dovranno essere configurati riducendo al minimo l'utilizzazione dei dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. In particolare, nel rispetto dei principi di pertinenza, non eccedenza e necessità sono da evitare riprese di dettaglio, quali primi piani delle persone, che non siano funzionali rispetto alle finalità istituzionali dell'impianto.
La durata della conservazione dei dati raccolti mediante gli impianti di videosorveglianza è limitata alle 24 (ventiquattro) ore lavorative. Le registrazioni effettuate nel pomeriggio del venerdì e nei giorni di sabato e domenica dovranno essere disponibili sino alle ore 24 del lunedì successivo. Lo stesso dovrà avvenire in corrispondenza dei periodi di chiusura prolungata delle strutture d'Ateneo, nei quali casi le registrazioni effettuate dovranno essere disponibili sino alle ore 24 del primo giorno successivo di apertura. Un eventuale prolungamento dei tempi di conservazione è ammesso nei casi in cui sia necessario custodire o consegnare il supporto contenente la registrazione specificatamente richiesto dall'Autorità Giudiziaria o di Polizia Giudiziaria in relazione ad attività investigative.
Il sistema impiegato deve essere programmato in modo da operare al momento prefissato – ove tecnicamente possibile – la cancellazione automatica da ogni supporto, anche mediante sovra registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.
La dislocazione delle telecamere risulta, al 31.01.2009, dall'allegato 1 realizzato con monitoraggio effettuato dal Servizio per la Privacy tramite somministrazione di apposito questionario a tutte le strutture d'Ateneo. Le eventuali modificazioni degli impianti esistenti nonché l'installazione di nuovi impianti potranno avvenire nel rispetto delle norme del presente regolamento, del Codice e dei provvedimenti dell'Autorità Garante in materia con contestuale comunicazione al Servizio per la Privacy.
In prossimità delle postazioni in cui sono state collocate le telecamere è affissa adeguata e visibile segnaletica permanente contenente l'informativa.
Responsabile del trattamento è il responsabile di cui all'art. 1 della struttura presso cui è stato installato l'impianto di video sorveglianza.
Il responsabile del trattamento svolge i seguenti compiti:
- Verifica che l'installazione e l'uso delle telecamere sia proporzionale al grado di rischio presente in concreto e che le stesse vengano utilizzate in modo da evitare

eccessi e ridondanze;
- Individua e nomina per iscritto gli incaricati addetti al trattamento dei dati raccolti mediante i sistemi di video sorveglianza impartendo loro, ancora per iscritto, le idonee istruzioni e ne da comunicazione alla Direzione Amministrativa;
- Verifica che la durata della eventuale conservazione delle immagini sia limitata alle ventiquattro ore successive alla rilevazione, fatti salvi i casi di chiusura prolungata delle strutture d'Ateneo per i quali si fa rinvio a quanto specificato nel punto 3 del presente articolo;
- Verifica che i sistemi di video sorveglianza siano stati installati e vengano usati nel rispetto della normativa sulla sicurezza dei dati personali e di altre disposizioni normative da osservare in caso di installazione di impianti audiovisivi;
- Verifica che, nelle immediate vicinanze delle telecamere posizionate, siano stati collocati dei supporti visibili con l'informativa;
- Adotta e rispetta le misure minime di sicurezza al fine di ridurre al minimo i rischi di distruzione, perdita, anche accidentale, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;
- Adotta i provvedimenti necessari per il tempestivo riscontro delle eventuali richieste di accesso ai dati raccolti mediante i sistemi di video sorveglianza e gli eventuali reclami degli interessati nel rispetto della normativa vigente e dei regolamenti d'Ateneo in materia di trattamento dei dati personali e di accesso agli atti amministrativi;
- Nel caso in cui l'installazione delle videocamere avvenga ad opera di un soggetto esterno acquisisce da quest'ultimo apposita relazione tecnica dell'intervento effettuato nonché attestazione di conformità dell'impianto alla normativa di riferimento;
- Documenta in un atto autonomo da conservare, le ragioni delle scelte effettuate con riferimento all'installazione e all'utilizzazione dell'impianto di video sorveglianza.

Gli incaricati al trattamento sono designati mediante atto formale dal responsabile e vengono scelti tra i soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.

Qualora, presso le strutture d'Ateneo, il servizio di vigilanza venga erogato da soggetti esterni, gli stessi dovranno essere nominati quali responsabili e/o incaricati "esterni" del trattamento dei dati personali raccolti mediante gli impianti di videosorveglianza con provvedimento del Direttore Amministrativo.

Il responsabile del trattamento informerà per iscritto le persone incaricate sulle loro responsabilità relative al trattamento e alla conservazione dei dati, alla loro protezione da eventi dannosi e agli altri obblighi di legge. Tali istruzioni dovranno essere aggiornate in caso di modifiche tecniche e normative.

L'accesso ai sistemi è consentito esclusivamente al titolare, al responsabile e agli incaricati di cui al precedente punto. Ciascuno di essi è dotato delle credenziali di autenticazione di cui è responsabile per la custodia, la conservazione e la assoluta riservatezza.

Il Titolare del trattamento, per il tramite dei responsabili, adotta preventivamente idonee misure di sicurezza al fine di proteggere i dati e ridurre al minimo i rischi di distruzione, perdita, anche accidentale, di accesso non autorizzato o trattamento non

consentito o non conforme alle finalità della raccolta.
L'interessato, dietro presentazione di apposita istanza, potrà:
- accedere esclusivamente ai dati che lo riguardano;
- richiedere informazioni circa le finalità, le modalità e la logica del trattamento;
- opporsi, motivatamente, in tutto o in parte al trattamento dei dati personali che lo riguardano, ancorchè pertinenti allo sopo della raccolta.
Le istanze devono essere trasmesse al Titolare (l'Università degli Studi di Palermo, in persona del Rettore pro tempore) o al responsabile del trattamento in forma scritta con allegato documento di riconoscimento.

ART. 13
DIRITTO DI ACCESSO AI PROPRI DATI DELL'INTERESSATO

In caso di richieste dell'interessato relative ai dati che lo riguardano in possesso dell'Università (art. 7 del Codice), le risposte dovranno essere fornite entro giorni 10 dal ricevimento dell'istanza.
Il riscontro a tali istanze, delle quali di seguito si riportano le varie tipologie, è subordinato, in taluni casi, al pagamento di un contributo spese:
- richiesta di ottenere conferma dell'esistenza di dati personali;
- richiesta di ottenere la comunicazione dei dati in forma intelligibile;
- richiesta di ottenere l'indicazione dell'origine dei dati;
- richiesta di conoscere le finalità del trattamento;
- richiesta di conoscere le modalità del trattamento;
- richiesta di conoscere la logica applicata al trattamento effettuato con l'ausilio di strumenti elettronici.
L'esercizio di diritti dell'interessato al di fuori dei casi su elencati quale, ad esempio, la richiesta di rettifica di dati errati in possesso dell'Università o la richiesta di opposizione al trattamento, non è subordinato al pagamento di alcun contributo.
Nei casi in cui non risulti confermata l'esistenza dei dati, il contributo da corrispondersi da parte del richiedente è pari a €. 10,00.
Nel caso in cui parimenti non risulti confermata l'esistenza dei dati, il presunto trattamento sia effettuato con strumenti elettronici e la risposta (negativa) sia data verbalmente, il contributo è pari a €. 2,50.
Il contributo spese non può essere richiesto quando i dati, cancellati o comunque non più reperibili , risultano essere stati trattati in precedenza.
Negli altri casi in cui, a seguito di una richiesta dell'interessato, risulta, invece, confermata l'esistenza di dati che lo riguardano, l'esercizio del diritto è gratuito, anche se l'interessato richiede la riproduzione dei dati su supporti di uso comune come floppy disk o CD ROM. Può essere richiesto un contribuito nella misura massima di €. 20,00 se viene richiesto specificamente di riprodurre i dati su supporti particolari di maggior costo.

ART. 14
ENTRATA IN VIGORE

Il presente regolamento sarà emanato con decreto del Rettore, affisso all'albo dell'Ateneo e pubblicato sul sito internet dello stesso.
L'entrata in vigore avverrà il giorno successivo a quello dell'affissione all'albo dell'Ateneo.

ART 15
NORMA DI RINVIO

Per quanto non espressamente previsto dal presente regolamento, si applicano le disposizioni previste dal D.Lgs 196/2003, le altre disposizioni legislative comunque attinenti e i provvedimenti del Garante in materia.