UNIVERSITÀ DEGLI STUDI DI PALERMO

AREA AFFARI GENERALI E LEGALI
Settore Affari Legali Generali. Privacy e trasparenza

Titolo I	Classe 3	Fascicolo /
N. 3537	del 20/01/2014	
UOR	CC	RPA

DECRETO N. 168/2014

IL RETTORE

Visto il D. Lgs. 196/03 codice in materia di protezione dei dati personali;
Visto il D. Lgs. 33/2013;
Visto il D. L. 9 febbraio 2012, n. 5 convertito con modificazioni dalla L. 4 aprile 2012, n. 35;
Visto il D.R. 2990 del 12 giugno 2006;
Visto il D.R. 2726 del 28 aprile 2009;
Visto lo Statuto d'Ateneo;
Visto il Decreto-legge 10 novembre 2008, n. 180

DECRETA

Viene emanato il regolamento per la disciplina delle modalità di trattamento dei dati personali. Istruzioni organizzative e tecniche che, di seguito, si riporta.

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 degli Studi di Palermo, nella persona del Rettore *pro tempore*. Il Titolare, prende le decisioni in ordine alle finalità, alle modalità di trattamento di dati personali ivi compreso il profilo della sicurezza.

I Responsabili del trattamento, ai sensi dell'art. 29 del Codice, sono individuati nei responsabili delle strutture in cui si articola l'Ateneo quali Rettorato, Direzione Generale, Aree Dirigenziali, Dipartimenti, Centri Interdipartimentali, Strutture di Raccordo, Poli Didattici, Uninetlab ed altre strutture di volta in volta individuate dal Titolare.
Ai Responsabili del trattamento compete l'attuazione delle misure di sicurezza, sia logiche che fisiche, previste dalla normativa vigente, dai Provvedimenti dell'Autorità Garante per la protezione dei dati personali (d'ora in poi denominato Garante) e dal presente Regolamento.
I compiti affidati al Responsabile del trattamento devono essere analiticamente specificati per iscritto nell'atto di nomina.
Il Titolare può designare con proprio provvedimento ulteriori Responsabili, anche esterni, per il trattamento dei dati dell'Università.
Nel caso in cui l'Università tratti dati personali di altro titolare, dovrà da quest'ultimo essere nominata responsabile esterno con apposito provvedimento.
Il Titolare esercita attività di vigilanza sul trattamento effettuato dal Responsabile esterno.
Il Responsabile esterno è tenuto a comunicare al Titolare la lista aggiornata dei propri incaricati al trattamento oggetto della nomina.
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 conformandosi alle istruzioni di cui al presente Regolamento e a quanto previsto dal Regolamento di Ateneo sul trattamento dati sensibili e giudiziari, dal Codice e dai Provvedimenti del Garante; adottare e rispettare le misure minime di sicurezza previste dal Codice, nonché le ulteriori eventualmente individuate dal Titolare del trattamento.
I responsabili individuano, con proprio provvedimento formale, i soggetti incaricati del trattamento specificando l'ambito del trattamento consentito. Tale provvedimento deve riportare l'indicazione nominativa della persona fisica, il ruolo ricoperto, il tipo di trattamento (con riferimento all'art. 4 del Codice), i compiti, la specificazione della banca dati e/o dell'archivio eventualmente utilizzati per il trattamento dei dati, la natura (sensibile e/o giudiziaria) dei dati trattati e l'ambito del trattamento consentito all'incaricato. In caso di revoca dell'incarico, sarà cura del responsabile del trattamento darne tempestiva notizia al Settore Affari legali generali. Privacy e trasparenza dell'Ateneo.
I trattamenti dei dati dei quali è Titolare l'Università possono essere legittimamente effettuati solamente dai soggetti incaricati: docenti, personale t.a.b. e ogni altro soggetto, anche non strutturato, chiamato a svolgere funzioni che implichino i trattamenti suddetti.
Tutti i soggetti incaricati devono evitare comportamenti che possano pregiudicare la riservatezza dei dati.
Il Dirigente dell'Area Servizi a Rete assume, altresì, la funzione di "Responsabile informatico d'Ateneo per il trattamento dei dati personali" tenuto conto anche delle indicazioni del CAD (Codice dell'Amministrazione Digitale).
Il Responsabile Informatico d'Ateneo per il trattamento dei dati personali individua (previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza), 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 AdS 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.
Nell'ambito delle strutture dell'Ateneo, gli AdS dovranno essere nominati in ragione di almeno uno ogni 70 unità di personale. Per le strutture con un numero di personale inferiore alle 70 unità si potrà procedere alla nomina di un amministratore di sistema di altra struttura. Al fine di ottimizzare l'attività degli AdS, il Responsabile Informatico d'Ateneo può nominare, per plessi che ospitano strutture, uffici, sezioni di dipartimento, ecc..., un AdS ogni 70 unità di personale (docente e T.A.B.).
Le nomine degli ADS, ove ve ne sia motivata ragione, potranno essere revocate dal Responsabile Informatico d'Ateneo.
Il Responsabile Informatico d'Ateneo per il trattamento dei dati personali cura, altresì, tutti gli adempimenti relativi al trattamento dei dati personali, sensibili e/o giudiziari effettuato con strumenti elettronici ai sensi del Codice e dall'Allegato B) Disciplinare tecnico in materia di misure minime di sicurezza, adottando le misure logiche ritenute necessarie per contrastare i rischi specifici dallo stesso individuati.
A tal fine, è compito del Responsabile Informatico d'Ateneo per il trattamento dei dati personali, valutare, anche ai fini della predisposizione di piani di privacy impact assessment, l'individuazione di possibili nuovi e ulteriori rischi legati al trattamento elettronico dei dati, derivanti dall'impiego di nuove risorse hardware e software in dotazione all'Ateneo, o comunque, acquisibili.

ART. 2
AMMINISTRATORI DI SISTEMA (ADS)

Gli Amministratori di Sistema (d'ora in poi AdS) dovranno:

- riferire al proprio Responsabile di struttura eventuali attività, in essere o da adottare, per mettere in sicurezza la propria struttura;
- operare secondo le direttive e procedure stabilite dal Responsabile Informatico di Ateneo per quanto concerne il corretto uso e funzionamento dei sistemi informativi di Ateneo, delle infrastrutture tecnologiche e l'implementazione di adeguate misure di sicurezza informatica;
- controllare, sotto il profilo tecnico, ogni sistema in rete e i servizi relativi alle strutture di sua competenza e riferire al Responsabile informatico di Ateneo per ogni violazione o sospetto di violazione della sicurezza informatica e/o al presente Testo Unico;
- adottare, compatibilmente con le risorse a sua disposizione, tutte le misure idonee per prevenire l'utilizzo illecito della rete e dei servizi di rete salvaguardando opportunamente le reti locali, i server e le postazioni di lavoro ed effettuando il monitoraggio delle proprie reti locali;
- svolgere attività di assistenza informatica del proprio bacino di utenza volta ad assicurare la connessione in rete di ciascuna stazione di lavoro e la buona funzionalità tramite aggiornamento del sistema operativo e la protezione delle stesse con quanto a disposizione;
- accertarsi che non vi sia risorsa come server, router, switch indirizzabile, telecamera IP, bridge wireless, ponte ottico, etc. che non abbia un responsabile di riferimento e, in caso contrario,

comunicarlo al Responsabile Informatico d'Ateneo; i telefoni VoIP e i router di backbone universitari hanno come AdS di riferimento il personale afferente all'Area Servizi a Rete;
- mantenere aggiornato, attraverso sistema http://netadmin.unipa.it, l'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 dall'Area Servizi a Rete (linee ADSL, HDSL, WiFi, etc.).

- 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 pubblico del tipo 147.163.x.y;
- accertarsi che non vengano utilizzate apparecchiature che consentano e/o facilitino l'intercettazione del traffico di rete (sonde, 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.
L'AdS responsabile del servizio netadmin.unipa.it verrà specificato in organigramma.

ART. 3
INTERVENTI FORMATIVI

La formazione del personale in materia di trattamento dei dati personali è considerata un'importante misura di sicurezza. Appositi interventi formativi, destinati a responsabili ed incaricati, verranno effettuati dall'Amministrazione al momento dell'ingresso in servizio; ulteriori interventi di aggiornamento verranno organizzati in relazione a cambiamenti di mansioni, utilizzo di nuovi strumenti e modifiche normative.
Su iniziativa del Responsabile Informatico d'Ateneo, tutti gli AdS di Ateneo e il personale afferente all'Area Servizi a Rete vengono annualmente avviati ad interventi formativi sulle politiche di sicurezza dei sistemi e delle reti di Ateneo.
Tutti gli interventi formativi sopra specificati vengono inseriti nel piano annuale delle attività formative del personale.

Gli interventi formativi dovranno anche essere rivolti al personale UNIPA/AOUP che tratta dati personali UNIPA e/o AOUP, individuati con provvedimento formale dal Rettore e dal DG dell'AOUP, secondo le modalità previste dal Regolamento per l'attività formativa del personale t.a.b. dell'Università degli Studi di Palermo.

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, delle credenziali di autenticazione (username e password) che consentono l'individuazione dell'incaricato stesso. La password deve essere composta da almeno 12 caratteri con almeno una lettera maiuscola e un numero, 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). Tali credenziali sono personali, non cedibili e utilizzabili

esclusivamente da chi è intestatario. L'incaricato è pienamente responsabile delle proprie attività e dei dati trasmessi e/resi pubblici ai sensi della vigente normativa.
L'incaricato deve adottare le cautele necessarie ad assicurare la segretezza della password e la diligente custodia di tutti dispositivi assegnatigli: PC, dispositivi USB, stampanti, scanner, 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 rinvia all'allegato B al D.lgs. 196/2003 e al Disciplinare d'Ateneo per l'utilizzo di internet e della mail approvato dal C.d.A. con deliberazione del 14 febbraio 2012.
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.
Nell'ambito delle misure minime di protezione predisposte dal Titolare possono essere adottati differenti profili di utenza specificando il tipo di accesso ai dati (ad esempio: solo visualizzazione o anche modifica degli stessi).
Per ulteriori e particolari misure di sicurezza da adottare per il trattamento di dati personali, effettuato con l'utilizzo di strumenti elettronici, si rinvia al Disciplinare sull'utilizzo della rete internet e della e-mail emanato con D.R. n. 249 del 02.04.2012.

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 che, per obsolescenza di prodotto, non prevedono aggiornamenti).
- Utilizzare mail server istituzionali @unipa.it.
- Non diffondere messaggi di posta elettronica di provenienza dubbia.

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 apparecchiature, dispositivi o programmi informatici diretti a danneggiare illecitamente un sistema informatico o telematico", art. 635 bis "danneggiamento di informazioni, dati e programmi informatici", art. 635 ter "danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità", art. 635 quater " danneggiamento di sistemi informatici e telematici", art. 635 quinquies "danneggiamento di sistemi informatici o telematici di pubblica utilità" nonché della legge 21\05\04 n. 128 che sanziona la condivisione e\o la fruizione di file protetti 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:

- 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;
- 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. Per tutto quanto al riguardo qui non stabilito, si rinvia all'Allegato B) 'Disciplinare tecnico in materia di misure minime di sicurezza' al Codice.

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 studenti 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 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.
L'accesso ai dati personali da parte delle strutture e dei dipendenti dell'Università, comunque limitato ai casi in cui sia finalizzato al perseguimento dei fini istituzionali, è ispirato al principio della circolazione delle informazioni, secondo il quale l'Università provvede all'organizzazione delle informazioni e dei dati a sua disposizione mediante strumenti, anche di carattere informatico, atti a facilitarne l'accesso e la fruizione anche presso le strutture didattiche e di ricerca.

Ogni richiesta d'accesso ai dati personali da parte delle strutture e dei dipendenti dell'Università, debitamente motivata, può essere soddisfatta con riferimento ai soli dati essenziali per svolgere attività istituzionali.

ART. 10
NOTIFICAZIONE DEL TRATTAMENTO

Con riferimento alla notificazione al Garante dei trattamenti di cui all'art. 37, comma 1, lettere da a) a f) del Codice, essa è effettuata dall'Università degli Studi di Palermo – per via telematica - preventivamente ed una sola volta, a prescindere dal numero delle operazioni da svolgere, nonché dalla durata del trattamento e può riguardare uno o più trattamenti con finalità correlate. Una nuova notificazione è richiesta anteriormente alla cessazione del trattamento o al mutamento di taluno degli elementi da indicare nella notificazione.
Al fine di consentire al titolare del trattamento di effettuare la dovuta notificazione, le strutture che intendono effettuare trattamenti di dati personali nelle ipotesi sopra elencate sono obbligate a darne tempestiva notizia all'Area Affari generali e legali- Settore Affari Legali generali. Privacy e trasparenza. Qualora la omessa o incompleta notificazione siano da imputare a colpa della struttura, sulla stessa graveranno le sanzioni amministrative che verranno irrogate dal Garante all'Università a fronte della violazione accertata.
Il Codice demanda al Garante il compito di individuare, tra i trattamenti di cui all'articolo sopra citato, quelli sottratti all'obbligo di notificazione purché non suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato nonché il compito di individuare ulteriori trattamenti in aggiunta a quelli elencati nella predetta disposizione. Il Garante con il provvedimento 1/2004 ha individuato i trattamenti di cui al comma 1 sottratti all'obbligo di notificazione.

ART. 11
PUBBLICAZIONE DI DATI SUL SITO ISTITUZIONALE

Con riferimento agli obblighi di pubblicazione e diffusione degli atti e dei documenti contenenti dati personali di cui al D. Lgs. 33/2013, l'Università contempera il diritto alla massima informazione con le esigenze derivanti dalla tutela della riservatezza e protezione dei dati personali disciplinata dal Codice e dai provvedimenti del Garante della Privacy, con particolare riferimento ai principi fondamentali in materia dettati dall'art.11 e seguenti del Codice (pertinenza, non eccedenza ed indispensabilità con riferimento alla finalità della pubblicazione).
Gli obblighi di pubblicazione dei dati personali diversi dai dati sensibili e dai dati giudiziari comportano la possibilità di una diffusione dei dati medesimi attraverso il sito istituzionale, nonché il loro trattamento secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca web ed il loro riutilizzo, nel rispetto dei principi sul trattamento dei dati personali.
Con riferimento ai dati di cui all'art. 26, comma 4, del D. Lgs. n. 33/2013, è esclusa la pubblicazione dei dati identificativi delle persone fisiche destinatarie dei provvedimenti di concessione di sovvenzioni, contributi, sussidi ed attribuzione di vantaggi economici, qualora da tali dati sia possibile ricavare

informazioni relative allo stato di salute ovvero alla situazione di disagio economico sociale degli interessati.
La pubblicazione nel sito istituzionale di dati relativi ai titolari di organi di indirizzo politico e di uffici o incarichi di diretta collaborazione, nonché a dirigenti titolari degli organi amministrativi è finalizzata alla realizzazione della trasparenza pubblica, che integra una finalità di rilevante interesse pubblico nel rispetto della disciplina in materia di protezione dei dati personali.
L'Università può disporre la pubblicazione sul proprio sito istituzionale di dati, informazioni e documenti che non ha l'obbligo di pubblicare, fermi restando i limiti e le condizioni espressamente previsti da disposizioni di legge, procedendo alla anonimizzazione dei dati personali eventualmente presenti.
Nei casi in cui è prevista la pubblicazione di atti o documenti diversi dai dati sensibili e dai dati giudiziari, l'Università provvede a rendere non intelligibili i dati personali non pertinenti rispetto alle specifiche finalità di trasparenza della pubblicazione.
Le notizie concernenti lo svolgimento delle prestazioni lavorative di chi opera presso l'Università e la relativa valutazione sono rese accessibili dall'Università. Non sono invece ostensibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione dal lavoro, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il predetto dipendente e l'amministrazione, idonee a rivelare taluna delle informazioni di cui all'articolo 4, comma 1, lettera d), del Codice.

ART. 12
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. 13
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. 14
VIDEOSORVEGLIANZA

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 videosorveglianza nei locali dell'Ateneo deve essere svolto nel pieno rispetto dei diritti e 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 non possono essere diffusi o comunicati a terzi. Il responsabile del trattamento può, se ritenuto opportuno, redigere un apposito documento sulla videosorveglianza che attesti le ragioni delle scelte e delle modalità di installazione e di utilizzo delle apparecchiature di videosorveglianza. Tale documento dovrà eventualmente essere esibito in occasione di visite ispettive oppure per l'esercizio dei diritti dell'interessato o di contenzioso.
Il trattamento dei dati personali acquisiti mediante gli impianti di videosorveglianza 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.
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 Settore Affari legali generali. Privacy e trasparenza.
In prossimità delle postazioni in cui sono state collocate le telecamere è affissa adeguata e visibile segnaletica permanente contenente l'informativa, che dovrà essere visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno.

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 al Settore Affari legali generali. Trasparenza e privacy.
- 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.
- 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 con l'informativa visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno.
- 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.
- Se ritenuto opportuno, 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 Rettore pro tempore.
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, ancorché pertinenti allo scopo 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. 15
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. 16
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 17
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."

Il Rettore
Prof. Roberto Lagalla