UNIVERSITÀ DEGLI STUDI DI PALERMO

La protezione dei dati personali
Attuazione del D. Lgs. 196/2003

MANUALE AD USO DEI RESPONSABILI

E DEGLI INCARICATI

Area Affari Generali e Legali
Settore Affari Legali Generali e Privacy

Indice degli argomenti

1. INTRODUZIONE

In ottemperanza alle disposizioni del D. Lgs 196/03 "Codice in materia di protezione dei dati personali", dei regolamenti d'Ateneo in materia di privacy e con riferimento alle attività svolte nell'ambito della Struttura universitaria di appartenenza, l'Incaricato dovrà effettuare i trattamenti di dati personali di propria competenza attenendosi scrupolosamente alle seguenti istruzioni e a ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal Responsabile del trattamento. Al fine di agevolare la consultazione del presente manuale si riportano, di seguito, le definizioni di alcuni dei termini più comunemente utilizzati contenute all'interno dell'art. 4 del D. Lgs. 196/03:

- **trattamento**: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, 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, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- **dato personale**: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- **dati identificativi**: i dati personali che permettono l'identificazione diretta dell'interessato;
- **dati sensibili**: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- **dati giudiziari**: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- **titolare"**: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- **responsabile**: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- **incaricati**: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- **interessato**: la persona fisica cui si riferiscono i dati personali.

I dati personali devono essere trattati in osservanza dei criteri di riservatezza, in modo lecito e secondo correttezza e per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati; inoltre, i dati devono essere trattai nel pieno rispetto delle misure minime di sicurezza (fisica e logica), custodendoli e controllandoli in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

1.1 PRINCIPALI RIFERIMENTI NORMATIVI E REGOLAMENTARI

In relazione all'organizzazione e alla pianificazione delle attività di trattamento dei dati, possono essere consultati i seguenti documenti:

- D. Lgs. 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali";
- Allegato B al D.Lgs. 196/03 "Disciplinare tecnico in materia di misure minime di sicurezza";
- Allegato A.4 al D.Lgs. 196/03 "Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici";
- Allegato A.2 al D.Lgs. 196/03 "Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici";
- Regolamento d'Ateneo per la disciplina delle modalità di trattamento dei dati personali. Istruzioni organizzative e tecniche, approvato con deliberazione del C.d.A. dell'Università degli Studi di Palermo del 14 novembre 2005;
- Regolamento d'Ateneo per il trattamento dei dati sensibili e giudiziari, approvato con deliberazione del CdA dell'Università degli Studi di Palermo del 27 gennaio 2006;
- Disciplinare sull'utilizzo della rete internet e della mail d'Ateneo, approvato dal CdA dell'Università degli Studi di Palermo nella seduta del 14 febbraio 2012.

1.2 LE MISURE MINIME DI SICUREZZA

Le misure minime di sicurezza (di cui agli artt. 33 – 36 e Allegato B al D Lgs. 196/03), di tipo fisico e logico, sono obbligatorie e sono distinte in funzione delle seguenti modalità di trattamento dei dati:

- **senza l'ausilio di strumenti elettronici** (es. dati in archivi cartacei o su supporto magnetico/ottico);
- **con strumenti elettronici** (PC ed elaboratori).

1.2.1 LA SICUREZZA FISICA

I dati personali, sia in forma cartacea che elettronica, devono essere protetti in modo da impedirne l'accesso a persone non autorizzate, con l'obiettivo di non violare la privacy rendendo pubblici dati di natura riservata e al tempo stesso di preservarne l'integrità.
La sicurezza fisica riguarda quelle misure adottate al fine di impedire l'accesso di persone non autorizzate ai dati (qualora siano archiviati su supporti cartacei) o ai dispositivi informatici utilizzati per il trattamento, l'elaborazione automatica e l'archiviazione dei dati stessi. Le misure di sicurezza fisica riguardano anche le procedure organizzative e gli strumenti adottati, al fine di garantire l'integrità e la conservazione dei dati, al fine di far fronte a eventi straordinari dovuti a cause naturali o provocati al fine di danneggiare l'Università.
Le misure da attuare richiedono l'ubicazione dei dati (cartacei o su supporti informatici) in locali protetti da serrature e ad accesso controllato.
I documenti cartacei devono inoltre essere archiviati in mobili protetti da serrature. La verifica della corretta adozione di quanto previsto dalle procedure da parte degli incaricati e la definizione delle procedure stesse è a carico dei Responsabili dei trattamenti.
Nel caso di trattamento informatico, devono essere attivate, se non già operative, procedure di controllo d'accesso alle sale in cui sono ubicati server e ai locali dove sono ubicati gli altri sistemi informatici utilizzati per il trattamento di dati personali.
I Responsabili del trattamento provvedono ad attuare le misure di protezione ad archivi contenenti

dati personali in modo da impedirne l'accesso a persone non autorizzate. Gli incaricati accedono ai dati personali secondo procedure definite ed evitano comportamenti che possano pregiudicare la riservatezza dei dati. Per esigenze specifiche chiedono indicazioni e direttive al Responsabile del trattamento dati di loro pertinenza.

1.2.2 LA SICUREZZA LOGICA

La sicurezza logica riguarda l'accesso ai dati personali trattati attraverso procedure informatiche e viene realizzata assicurando che gli accessi ai sistemi informativi avvengano secondo modalità predefinite, tali da garantire un elevato livello di sicurezza ed affidabilità. In particolare le misure di sicurezza logica mirano ad identificare gli utenti che accedono ai sistemi informatici adibiti al trattamento di dati, in modo tale da assicurare che soltanto gli incaricati autorizzati a compiere un determinato trattamento possano accedere ai dati di propria competenza. Tale identificazione avviene utilizzando un codice identificativo personale (username) associato univocamente ad ogni singolo incaricato ed una parola chiave (password).

1.3 NOMINA E REVOCA DEGLI INCARICATI

E' opportuno ricordare che il trattamento dei dati personali da parte di ciascun Incaricato va preventivamente autorizzato (con apposito provvedimento scritto) dal rispettivo Responsabile del trattamento (Direttore, Preside, Dirigente). Nel medesimo provvedimento, deve essere stabilito l'ambito di trattamento consentito. L'autorizzazione deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente ai fini dello svolgimento delle operazioni di trattamento proprie della struttura e riguarda esclusivamente l'ambito assegnato a ciascun Incaricato; chiunque, a vario titolo (strutturati e non) tratta dati personali all'interno della struttura deve essere preventivamente autorizzato. Il Responsabile del trattamento procederà alla revoca (sempre per iscritto) dell'autorizzazione in tutti i casi di perdita della qualità che consente all'Incaricato l'accesso ai dati personali (es. per trasferimento dell'Incaricato ad altro ufficio, per assegnazione ad altre attività, per cambio di mansioni, per estinzione del rapporto di lavoro/collaborazione con l'Ateneo). Per il conferimento, così come per la revoca, dell'incarico potranno essere utilizzati gli appositi moduli presenti all'interno della pagina web dell'Ufficio per la Privacy d'Ateneo. Essi dovranno riportare la firma del Responsabile e quella dell'Incaricato. Una copia dei provvedimenti (incarico e revoca) dovrà essere inviata all'Ufficio per la Privacy d'Ateneo.

2. TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

I dati personali archiviati su supporti di tipo magnetico e/o ottico devono essere protetti con le stesse misure di sicurezza previste per i supporti cartacei. Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.

2.1 CUSTODIA

I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (es. armadi, cassetti o classificatori chiusi a chiave). I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata e non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

2.2 COMUNICAZIONE

I dati personali non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento). Ogni comunicazione di dati personali a soggetti terzi e/o all'esterno dell'Università deve svolgersi nel pieno rispetto della normativa e dei regolamenti interni in materia di privacy.

2.3 DISTRUZIONE

L'eventuale distruzione di documenti contenenti dati personali deve essere effettuata in modo tale da rendere gli stessi documenti non più ricomponibili (sminuzzandoli o servendosi di distruggidocumenti) e nel pieno rispetto della normativa in materia di conservazione dei documenti pubblici. Con le medesime cautele, i dati personali che hanno esaurito lo scopo per il quale sono stati immagazzinati o raccolti in supporti magnetici od ottici devono essere cancellati, prima di riutilizzare detti supporti. Se ciò non è possibile, i supporti devono essere distrutti.

2.4 ULTERIORI ISTRUZIONI IN CASO DI TRATTAMENTO DI DATI SENSIBILI E/O GIUDIZIARI

Particolare attenzione dev'essere riservata ai documenti contenenti dati sensibili e/o giudiziari, i quali devono essere controllati e custoditi dagli incaricati in modo che non vi accedano persone prive di autorizzazione. Ad esempio, la consultazione di documenti/certificati per l'inserimento in procedure informatiche di gestione/amministrazione del personale di dati relativi a permessi sindacali, assenze per malattie etc., deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati in base alle presenti istruzioni. L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave. Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure farsi identificare e registrare su appositi registri.

3. TRATTAMENTI CON STRUMENTI ELETTRONICI

3.1 GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE

Il D.Lgs 196/2003 e relativi allegati prevedono che l'accesso alle procedure informatiche che consentono il trattamento di dati personali sia consentito agli Incaricati in possesso di "credenziali di autenticazione" che permettano il superamento di una procedura di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato (user-id) associato ad una parola chiave riservata (password). Gli Incaricati devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni:

- l'incaricato ha la responsabilità di custodire la propria password, non condividerla e non comunicarla ad altra persona;
- la password deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'Utente (nome, cognome, data di nascita ecc..);
- la password deve essere sostituita, a cura del singolo Incaricato, al primo utilizzo e

successivamente almeno ogni sei mesi (ogni tre mesi nel caso di trattamento di dati sensibili e/o giudiziari), così come previsto dal punto 5 del Disciplinare tecnico - All. B - allegato al D. Lgs. 196/2003);

- l'incaricato deve dare immediata informazione all'AdS di riferimento nel caso in cui abbia fondato motivo di ritenere che possa essere compromessa la riservatezza della password o che ne sia stato fatto un utilizzo indebito. Qualora l'incaricato venisse a conoscenza della password di altri, è tenuto a darne immediata notizia al S.I.A. e all'Amministratore di sistema.

3.2 PROTEZIONE DEL PC E DEI DATI

- I personal computer fissi e portatili acquisiti con fondi dell'Amministrazione e i programmi su di essi installati sono uno strumento di lavoro; contenendo anche dati e informazioni personali di terzi, detti strumenti devono essere utilizzati con diligenza e cura.
- Le impostazioni dei personal computer, nonché l'installazione di sistemi operativi e programmi applicativi, avviene di norma con il supporto degli AdS sulla base di criteri e profili decisi dall'Amministrazione e seguendo i necessari criteri di sicurezza. In ogni caso, l'uso dei programmi deve avvenire nel rispetto dei contratti di licenza che li disciplinano e delle specifiche prescrizioni di volta in volta fornite dall'Amministrazione.
- Tutti i PC devono essere dotati di password rispondenti alle normative di Ateneo e, ove possibile, va impostata anche la password di BIOS; inoltre, tutti i PC devono essere dotati di software antivirus aggiornato con cadenza almeno annuale e tale che si attivi automaticamente ad ogni avvio.
- Al termine delle attività di fine giornata che prevedono l'utilizzo della stazione di lavoro, questa deve essere spenta, assieme alle altre apparecchiature ad essa collegate (stampante, scanner, ..) prima di lasciare gli uffici, tranne che ciò non sia possibile per motivi legati ad attività di ricerca.
- Ciascun Incaricato deve prestare la massima attenzione nell'utilizzo di supporti di memorizzazione esterna (dispositivi usb, ecc.) e deve avvertire immediatamente l'AdS nel caso in cui vengano rilevati virus.
- Al fine di evitare accessi illeciti, deve essere sempre attivato il salva schermo con password.
- Sui PC devono essere installati, appena vengono resi disponibili (e comunque almeno annualmente), tutti gli aggiornamenti software necessari a prevenirne vulnerabilità e correggerne i difetti.
- Deve essere effettuato, con cadenza almeno settimanale un salvataggio di back-up di eventuali dati personali presenti unicamente sul proprio PC personale (cioè non accessibili tramite i sistemi informatici universitari).
- L'Incaricato non deve cedere a persone non autorizzate e non deve lasciare incustodita la propria postazione di lavoro, una volta superata la fase dell'autenticazione e/o dell'applicazione a cui si è avuto accesso.

3.3 CANCELLAZIONE DEI DATI DAI PC

I dati personali conservati sui PC devono essere cancellati in modo sicuro (es. formattando i dischi, con l'eventuale ausilio degli Amministratori di sistema) prima di destinare i PC ad usi diversi.
Nel caso di dismissione di apparecchiature elettroniche e con riferimento alla Circolare della Direzione Amministrativa del 18/12/2008, prot. n. 95911, devono essere adottate le misure di sicurezza prescritte dall'Autorità Garante con il Provvedimento del 13/10/2008 al fine di "adottare idonei accorgimenti e misure, anche con l'ausilio di terzi tecnicamente qualificati, volti a prevenire accessi non consentiti ai dati personali memorizzati"; in particolare:

- per quanto riguarda le misure tecniche preventive, i files devono essere protetti usando una password di cifratura, oppure i dati devono essere memorizzati su hard disk o su altri supporti magnetici usando sistemi di cifratura automatica al momento della scrittura;
- devono essere adottate misure tecniche di cancellazione sicura (si ricorda che, ai sensi del Provvedimento dell'Autorità Garante sopracitato, la cancellazione sicura delle informazioni su disco fisso o su altri supporti magnetici è ottenibile con programmi informatici di "riscrittura" che provvedono – una volta che l'utente abbia eliminato dei files dall'unità disco con i normali strumenti previsti dai sistemi operativi, ad es. con l'uso del "cestino" o con comandi di cancellazione" – a scrivere ripetutamente nelle aree vuote del disco. Si possono anche utilizzare sistemi di formattazione a basso livello degli hard disk o di "demagnetizzazione", in grado di garantire la cancellazione rapida delle informazioni).
- ai fini dell'eventuale smaltimento di rifiuti elettrici ed elettronici, si rende indispensabile adottare una delle misure prescritte dal Garante (si ricorda che ai sensi del Provvedimento dell'Autorità Garante, per la distruzione degli hard disk e di supporti magnetici non riscrivibili come cd rom e dvd, è consigliabile l'utilizzo di sistemi di punzonatura o deformazione meccanica o di demagnetizzazione ad alta intensità o di vera e propria distruzione fisica).

2.4 ULTERIORI ISTRUZIONI IN CASO DI TRATTAMENTO DI DATI SENSIBILI E/O GIUDIZIARI

Nel caso di trattamento di dati sensibili e/o giudiziari con strumenti elettronici, le password di accesso alle procedure informatiche che trattano dati sensibili e/o giudiziari devono essere sostituite, da parte del singolo incaricato, almeno ogni tre mesi. L'installazione degli aggiornamenti software necessari a prevenire vulnerabilità e correggerne i difetti dei programmi per elaboratori deve essere effettuato almeno semestralmente.

2.5 SUGGERIMENTI UTILI IN PRESENZA DI OSPITI O TERZI

- Fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali.
- Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e attivare il salvaschermo del PC .
- Non rivelare o fare digitare le password dal personale di assistenza tecnica.
- Non rivelare le password al telefono né inviarla via fax - nessuno è autorizzato a chiederle.
- Segnalare qualsiasi anomalia o stranezza al Responsabile.

2.6 GESTIONE DELLA POSTA ELETTRONICA

2.6.1 COMPITI E RESPONSABILITÀ

- L'incaricato è responsabile della propria casella di posta elettronica personale; responsabile delle caselle di posta elettronica di Struttura è il Responsabile della Struttura;
- L'incaricato è responsabile del proprio userid, della segretezza della relativa password e del contenuto dei messaggi inviati dalla propria casella; egli è responsabile di tutte le operazioni effettuate con la casella di posta elettronica relativa all'userid a lui associato.
- L'incaricato è responsabile delle eventuali conseguenze pregiudizievoli che un uso improprio del servizio da parte del proprio userid potrebbe comportare a terze persone, e ciò in riferimento alla vigente normativa in materia civile e penale.

- La password di accesso ai servizi di rete, compreso il servizio di posta elettronica, è strettamente personale ed in nessun caso va comunicata a terze persone, sia verbalmente che per iscritto. Qualora, per motivi tecnici, il personale del SIA, su richiesta dell'incaricato, abbia necessità di conoscere la password di accesso ai servizi di rete, questa dev'essere cambiarla immediatamente dopo l'intervento tecnico.

2.6.2. UTILIZZAZIONE DEL SERVIZIO

- Non inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
- Non inviare catene telematiche. Se si dovessero ricevere messaggi di tale tipo, si deve procedere all'immediata cancellazione. Non si devono, in alcun caso, aprire e/o scaricare gli allegati di tali messaggi.
- Limitatamente al rinnovo delle rappresentanze negli Organi Collegiali di Governo dell'Ateneo e del C.N.S.U., l'invio di messaggi per fini di comunicazioni elettorali è consentito su apposita autorizzazione del Direttore Amministrativo;
- Non inviare lo stesso messaggio a più di 200 (duecento) destinatari. Laddove le Strutture avessero la necessità di inviare comunicazioni ad una pluralità di destinatari, deve essere usato il gestore delle mailing list disponibile su apposito server del SIA. L'utilizzo di tale server è consentito ai singoli Utenti solo dietro autorizzazione scritta e motivata da parte del responsabile della Struttura di appartenenza.
- Non diffondere messaggi di provenienza dubbia.
- Per la trasmissione di comunicazioni all'interno dell'Università dovrà essere privilegiato l'uso della e-mail (ai sensi dell'art. 33, comma 1 lett. m) L. 18 giugno 2009 n. 69), prestando attenzione alla dimensione degli allegati (si richiama a tal proposito la Circolare del Direttore Amministrativo prot. n. 34731 del 18/05/2010 avente ad oggetto "comunicazioni mezzo e-mail").
- In caso di assenza prolungata programmata, si raccomanda al dipendente di attivare il sistema di risposta automatica ai messaggi di posta elettronica ricevuti indicando, nel messaggio di accompagnamento, le coordinate (anche elettroniche o telefoniche) di un collega o della struttura di riferimento da contattare in sua assenza e/o altre modalità utili di contatto della struttura organizzativa presso cui presta la propria attività lavorativa.
- Nell'ipotesi di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa l'interessato può delegare un altro utente ("fiduciario") il compito di verificare il contenuto di messaggi e inoltrare al responsabile dell'Area in cui presta servizio quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività deve essere informato il dipendente interessato alla prima occasione utile. Al termine dell'esigenza verificatesi all'utente interessato è fatto obbligo modificare la password di accesso.
- Qualora si verificassero anomalie nell'invio e ricezione dei messaggi di posta elettronica dovrà essere prontamente informato l'AdS di riferimento o il SIA.

4. ISTRUZIONI PER IL TRATTAMENTO DEI DATI PERSONALI EFFETTUATI MEDIANTEL'USO DI SISTEMI DI VIDEOSORVEGLIANZA.

4.1 PRINCIPI GENERALI

La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un

trattamento di dati personali (art. 4, comma 1, lett. b), del Codice).
È considerato dato personale, infatti, qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione.
Il trattamento dei dati attraverso sistemi di videosorveglianza deve essere fondato sui presupposti di liceità che il Codice prevede espressamente per i soggetti pubblici (svolgimento di funzioni istituzionali: artt. 18-22 del Codice).
Il trattamento dei dati dovrà avvenire nel rispetto del principio di necessità (art. 3 D.Lgs 196/2003), per cui ciascun sistema informativo ed il relativo programma informatico devono essere conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi (ad es., configurando il programma informatico in modo da consentire, per monitorare il traffico, solo riprese generali che escludano la possibilità di ingrandire le immagini e rendere identificabili le persone).
L'attività di videosorveglianza deve essere effettuata nel rispetto del c.d. principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonché nelle varie fasi del trattamento.
Tale attività deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite (art. 11, comma 1, lett. d) del Codice).

4.2 INFORMATIVA

Gli interessati devono essere sempre informati che stanno per accedere in una zona video sorvegliata. Il modello di informativa dovrà indicare il titolare del trattamento e la finalità perseguita ai sensi dell'art. 13, comma 3, del codice della privacy. Potrà essere utilizzato il modello semplificato indicato dall'autorità Garante riportato in allegato alle presenti istruzioni.
Il supporto con l'informativa:

- deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
- deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
- può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

Tale modello semplificato di informativa dovrà rinviare a un testo completo contenente tutti gli elementi di cui all'art. 13, comma 1, del Codice della Privacy, disponibile agevolmente senza oneri per gli interessati, con modalità facilmente accessibili anche con strumenti informatici e telematici (in particolare, tramite reti Intranet o siti Internet, affissioni in bacheche o locali, avvisi e cartelli agli sportelli per gli utenti, messaggi preregistrati disponibili digitando un numero telefonico gratuito).
In ogni caso il titolare, anche per il tramite di un incaricato, ove richiesto è tenuto a fornire anche oralmente un'informativa adeguata, contenente gli elementi individuati dall'art. 13 del Codice.
La violazione delle disposizioni riguardanti l'informativa di cui all'art. 13, consistente nella sua omissione o inidoneità (es. laddove non indichi comunque il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia), è punita con la sanzione amministrativa prevista dall'art. 161 del Codice della Privacy.

4.3 MISURE DI SICUREZZA DA APPLICARE AI DATI PERSONALI TRATTATI MEDIANTE SISTEMI DI VIDEOSORVEGLIANZA.

I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini (artt. 31 e ss. del Codice).
Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (se soggetto distinto dal titolare medesimo, nel caso in cui questo sia persona fisica).
Le misure dovranno essere rispettose dei principi che seguono:

A. in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;
B. laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
C. per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;
D. **la durata della conservazione dei dati raccolti è limitata alle 24 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 di 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 (art. 12 Regolamento d'Ateneo per il trattamento dei dati personali. Istruzioni Organizzative e tecniche.);
E. nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;
F. qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-ter del codice penale.

4.4 MODIFICHE AGLI IMPIANTI E ACCESSO AI SISTEMI.

Le eventuali modificazioni degli impianti esistenti nonché l'installazione di nuovi impianti potranno

avvenire nel rispetto delle norme del Regolamento cit., del Codice della Privacy e dei provvedimenti dell'Autorità Garante in materia con contestuale comunicazione all'Ufficio per la Privacy dell'Ateneo.
L'accesso ai sistemi è consentito esclusivamente al Titolare, al responsabile e agli Incaricati. Ciascuno di essi è dotato delle credenziali di autenticazione di cui è responsabile per la custodia, la conservazione e la assoluta riservatezza.

4.5 DIVIETO DI CONTROLLO A DISTANZA.

Nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa. Pertanto, è vietata l'installazione di apparecchiature specificatamente preordinate alla predetta finalità: non devono quindi essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul badge). Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro: in tali casi, ai sensi dell'art. 4 della l. n. 300/1970, gli impianti e le apparecchiature, "dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti" (v., altresì, artt. 113 e 114 del Codice; art. 8 l. n. 300/1970 cit.; art. 2 d.lg. n. 165/2001).
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, toilettes, spogliatoi, docce, armadietti, luoghi ricreativi; in particolare non potranno essere in alcun caso riprese le apparecchiature di rilevazione automatizzata della presenza del personale.
Il mancato rispetto di quanto sopra prescritto comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-ter, del Codice.
L'utilizzo di sistemi di videosorveglianza preordinati al controllo a distanza dei lavoratori o ad effettuare indagini sulle loro opinioni integra la fattispecie di reato prevista dall'art. 171 del Codice.
Sotto un diverso profilo, eventuali riprese televisive sui luoghi di lavoro per documentare attività od operazioni solo per scopi divulgativi o di comunicazione istituzionale, e che vedano coinvolto il personale dipendente, possono essere assimilati ai trattamenti temporanei finalizzati alla pubblicazione occasionale di articoli, saggi ed altre manifestazioni del pensiero. In tal caso, alle stesse si applicano le disposizioni sull'attività giornalistica contenute nel Codice (artt. 136 e ss.), fermi restando, comunque, i limiti al diritto di cronaca posti a tutela della riservatezza, nonché l'osservanza del codice deontologico per l'attività giornalistica ed il diritto del lavoratore a tutelare la propria immagine opponendosi, per motivi legittimi, alla sua diffusione (art. 7, comma 4, lett. a), del Codice).
Il trattamento dei dati posto in essere in violazione delle prescrizioni sopra riportate è, a seconda dei casi, illecito oppure non corretto, ed espone:

- all'inutilizzabilità dei dati personali trattati in violazione della relativa disciplina (art. 11, comma 2, del Codice);
- all'adozione di provvedimenti di blocco o di divieto del trattamento disposti dal Garante (art. 143, comma 1, lett. c), del Codice), e di analoghe decisioni adottate dall'autorità giudiziaria civile e penale;
- all'applicazione delle pertinenti sanzioni amministrative o penali (artt. 161 e ss. del Codice).

5. TRATTAMENTI EFFETTUATI PER FINALITA' DI PUBBLICAZIONE ON LINE

Il trattamento dei dati personali contenuti anche in atti e documenti amministrativi, effettuato ai fini della pubblicazione di questi ultimi sul sito istituzionale dell'Ateneo, è disciplinato dalla deliberazione dell'Autorità Garante per la protezione dei dati personali del 2 marzo 2011, pubblicata all'interno della G. U. n. 64 del 19/03/2011. In ottemperanza alle prescrizione del Garante, l'Ateneo di Palermo ha provveduto ad emanare due distinti provvedimenti (il primo del 22/12/2011, prot. n. 85415 e il successivo del 21/02/2012, prot. n. 13357, entrambi a firma del Direttore Amministrativo) e ha adottato le proprie Linee guida per quanto riguarda la materia specifica. Si forniscono di seguito, pertanto, alcuni suggerimenti di carattere generale rimandando ai provvedimenti di cui sopra per gli opportuni approfondimenti.

5.1 CAUTELE GENERALI

Previsioni normative: i dati possono essere messi in rete solo sulla base di una norma di legge o di regolamento che lo preveda. L'amministrazione può anche stabilire la diffusione delle informazioni personali nell'ambito del Piano triennale per la trasparenza. Nel pubblicare i dati, l'amministrazione deve rispettare i principi di necessità, proporzionalità e pertinenza. Rimane fermo il generale divieto di diffondere dati sulla salute.

Solo dati esatti e aggiornati: l'amministrazione deve mettere a disposizione solo dati esatti, aggiornati e proporzionati agli scopi per i quali sono messi on line. Occorre adottare misure in grado di ridurre il rischio di cancellazioni, modifiche, estrapolazioni delle informazioni. A tale scopo i file dovranno riportare "dati di contesto" (data di aggiornamento, periodo di validità, amministrazione, numero di protocollo). A tale fine il Garante della Privacy prescrive l'adozione di idonee misure per eliminare o ridurre il rischio di cancellazioni, modifiche, alterazioni o decontestualizzazioni delle informazioni e dei documenti resi disponibili tramite Internet indicando, tra i dati di contesto riportati all'interno del contenuto informativo dei documenti, delle fonti attendibili per il reperimento dei medesimi documenti. Un ulteriore accorgimento, la cui adozione viene però rimessa alla valutazione delle amministrazioni interessate, anche in relazione a specifiche categorie di documenti, è la sottoscrizione del documento pubblicato sul sito web con firma digitale o altro accorgimento equivalente, in modo da garantirne l'autenticità e l'integrità. Il rischio della decontestualizzazione è strettamente correlato alla possibilità che i contenuti informativi disponibili sul sito istituzionale siano accessibili mediante l'utilizzo di motori di ricerca esterni, ovvero siano reperibili attraverso la consultazione di siti dove sono ospitate copie dei medesimi contenuti informativi.

Cautele sui motori di ricerca esterni: è preferibile garantire la reperibilità dei documenti attraverso motori di ricerca interni al sito dell'amministrazione, utilizzando anche una specifica sezione del sito e limitando l'indicizzazione da parte dei motori di ricerca esterni. Tale modalità assicura un accesso coerente con la finalità per la quale i dati sono stati resi pubblici ed evita il rischio di manipolazione e di "decontestualizzazione" dei dati, cioè la estrapolazione arbitraria che rende incontrollabile il loro uso. A tale scopo, in relazione ai dati personali di cui si intende escludere la diretta individuabilità in Internet tramite motori di ricerca generalisti, è possibile utilizzare regole di accesso convenzionali codificate all'interno di uno specifico file di testo. Nel Provvedimento del 2 marzo 2011 il Garante fa riferimento, a titolo esemplificativo, all'inserimento di *metatag noindex* e *noarchive* nelle intestazioni delle pagine web o alla codifica di regole di esclusione all'interno di uno specifico file di testo - il file robots.txt - posto sul server che ospita il sito web configurato in accordo al *Robot Exclusion Protocol* (avendo presente comunque come tali

accorgimenti non siano immediatamente efficaci rispetto a contenuti già indicizzati da parte dei motori di ricerca Internet, la cui rimozione potrà avvenire secondo le modalità da ciascuno di questi previste). Resta impregiudicato l'utilizzo di strumenti idonei ad agevolare la reperibilità, all'interno del sito istituzionale dell'amministrazione, delle informazioni e dei documenti oggetto di divulgazione.

Tempi congrui di diffusione: i dati devono essere resi disponibili nei limiti temporali stabiliti dalle norme di settore. In mancanza di queste, occorre individuare congrui limiti temporali entro i quali mantenere on line i documenti. A questo scopo, secondo il Garante della Privacy, è possibile utilizzare sistemi di *web publishing* e Cms - *Content management systems* - in grado di attribuire, anche mediante l'utilizzo di parole-chiave (meta-dati), un intervallo temporale di permanenza della documentazione all'interno del sito istituzionale, consentendone una sua agevole rimozione, anche in forma automatica. In assenza di meccanismi automatizzati di gestione del termine di scadenza della medesima documentazione, andrebbero inoltre previste procedure di verifica della validità temporale e del requisito di disponibilità al pubblico delle informazioni ivi contenute, da programmare con cadenza periodica o in seguito ad un aggiornamento dell'informazione). La predetta congruità va commisurata alle esigenze sottese alle finalità di trasparenza, di pubblicità o di consultabilità di volta in volta perseguite, sempre che queste non abbiano carattere di permanenza (a titolo esemplificativo, il lasso temporale della pubblicazione sul sito istituzionale dei curricula dei dirigenti va commisurato al periodo di permanenza in servizio dell'interessato presso l'amministrazione, fermo restando il diritto di quest'ultimo di ottenere l'aggiornamento dei dati che lo riguardano). Tempi più circoscritti, invece, devono riguardare la disponibilità on line dell'atto o del documento pubblicato per finalità di pubblicità, avuto anche riguardo ai termini previsti dalla legge per l'impugnazione dei provvedimenti oggetto di pubblicazione. Trascorsi i predetti periodi di tempo specificatamente individuati, determinate notizie, documenti o sezioni del sito devono essere rimossi dal web o privati degli elementi identificativi degli interessati ovvero, in alternativa, laddove l'ulteriore diffusione dei dati sia volta a soddisfare esigenze di carattere storico-cronologico, gli stessi vanno sottratti all'azione dei comuni motori di ricerca, ad esempio, inserendoli in un'area di archivio consultabile solo a partire dal sito stesso o in un'area ad accesso riservato (si fa riferimento a sezioni del sito accessibili soltanto previa autenticazione informatica degli utenti).

Misure contro la duplicazione massiva di file: contro i rischi di riproduzione e riutilizzo dei file contenenti dati personali, devono essere installati software e sistemi di *alert* che consentono di riconoscere e segnalare accessi anomali (ad esempio per quantità rispetto a un determinato periodo di tempo) al fine di mettere in atto adeguate contromisure. Si può fare ricorso, ad esempio, ad accorgimenti consistenti nell'uso di firewall di rete in grado di riconoscere accessi che risultino anomali per numero rapportato all'intervallo di tempo di riferimento, oppure di filtri applicativi che, a fronte delle citate anomalie, siano in grado di rallentare l'attività dell'utente e di mettere in atto adeguate contromisure.

5.2 ATTI E DOCUMENTI ON LINE A FINI DI TRASPARENZA

Dipendenti pubblici: non si possono riprodurre sul web i dati sullo stato di salute, i cedolini dello stipendio, l'orario di entrata e di uscita, l'indirizzo privato, la e-mail personale.
Sono invece conoscibili da chiunque i livelli retributivi, i tassi di assenza, i risultati raggiunti, l'ammontare dei premi collegati alle performances, ma solo se in forma anonima o aggregata. Possono essere diffusi la retribuzione e i curricula di dirigenti, gli incarichi di collaborazione e consulenza, il ruolo dei dirigenti, i ruoli di anzianità e i bollettini ufficiali.

Beneficiari di contributi economici e agevolazioni: è possibile pubblicare gli elenchi dei soggetti cui sono stati erogati contributi, sovvenzioni, crediti, o riconosciute agevolazioni, sussidi o altri benefici. In tali elenchi possono essere riportati i dati identificativi (nome, cognome e data di nascita) omettendo invece di indicare il codice fiscale, le coordinate bancarie, le informazioni che descrivano le condizioni di indigenza e le informazioni sullo stato di salute.

5.3 ATTI E DOCUMENTI ON LINE A FINI DI PUBBLICITA' DEGLI ATTI

Concorsi e selezioni pubbliche: sono pubblicabili le graduatorie, gli esiti e i giudizi concorsuali, gli elenchi nominativi abbinati alle prove intermedie, gli elenchi degli ammessi alle prove scritte o orali. E' eccedente, invece, la pubblicazione del recapito telefonico, dell'indirizzo dell'abitazione, della e-mail, i titoli di studio, il codice fiscale, l'indicatore Isee, il numero dei figli disabili, i risultati dei test psicoattitudinali.
Graduatorie, elenchi professionali: per adempiere ad obblighi di pubblicità degli atti si possono pubblicare le graduatorie di mobilità professionale, l'inquadramento del personale, l'assegnazione di sede, i provvedimenti riguardanti la progressione di carriera, l'attribuzione di incarichi dirigenziali.

5.4 ATTI E DOCUMENTI ON LINE A FINI DI CONSULTABILITA'

Collocamento obbligatorio dei disabili: è lecito mettere a disposizione, ma solo a determinate categorie di soggetti legittimati e mediante accesso dedicato o con uso di username e password, gli elenchi di soggetti aventi diritto al collocamento obbligatorio, come i disabili appartenenti a r5categorie protette e i centralinisti telefonici non vedenti.

ALLEGATO 1


AREA
VIDEOSORVEGLIATA
La registrazione è effettuata da ..... per fini di .....
Art. 13 del Codice in materia di protezione dei dati personali (d.lg. n. 196/2003)


AREA
VIDEOSORVEGLIATA
La registrazione è effettuata da ..... per fini di .....
Art. 13 del Codice in materia di protezione dei dati personali (d.lg. n. 196/2003)