Inviata alla Giunta Regionale in data 26 MAR. 2009

Esecutiva per presa d'atto della Giunta Regionale in data _____

# Azienda per il Diritto agli Studi Universitari
# CHIETI

## SEDUTA del 9 marzo 2009

## Delibera n. 5

L'anno duemilanove il giorno nove del mese di marzo

alle ore 15,00 nella sede dell'Azienda per il Diritto agli Studi Universitari di Chieti, convocato nei modi e nei termini di legge, si riunisce il Consiglio di Amministrazione dell'Azienda con la Presidenza del dott. Massimiliano Pignoli e con l'intervento dei componenti:

| | P | A | | P | A |
|---|---|---|---|---|---|
| 1) Prof. Giandomenico PALKA (Vice Presidente) | X | | 5) Dott. Claudio PALMA (Componente) | X | |
| 2) Prof. Franco DI GIACOMO (Componente) | X | | 6) Dott. Ignazio RUCCI (Componente) | X | |
| 3) Dott. Giuseppe VISCO (Componente) | X | | 7) Sig. Francesco VERZELLA (Componente) | X | |
| 4) Dott. Angelo Lucio ROSSI (Componente) | X | | 8) Sig. Paolo RAIMONDI (Componente) | X | |

Assiste alla seduta, in qualità di Segretario e con parere consultivo il Direttore dell'Azienda per il Diritto agli Studi Universitari di Chieti, Avv. Teresa Mazzarulli.

Il Presidente, constatata la presenza del numero legale, dichiara validamente costituita la riunione del Consiglio di Amministrazione ed atta a deliberare sul seguente argomento posto all'ordine del giorno:

**Approvazione regolamento privacy.**

## IL CONSIGLIO DI AMMINISTRAZIONE

**VISTO** l'art.8 della Legge Regionale 6 dicembre 1994 n.91, che prevede che al Consiglio d'Amministrazione competa l'adozione di tutti gli atti necessari alla gestione dell'Azienda per il Diritto agli Studi Universitari di Chieti e Pescara;

**VISTO** il Decreto Legislativo 30 giugno 2003, n.196;

**VISTA** la legge 7 agosto 1990, n.241, della Legge 11 febbraio 2005, n.15 e del D.P.R. 184 del 12.4.2006;

**PRESO ATTO** della delibera n.28 del 3 maggio 2005 "DPS Documento Programmatico sulla Sicurezza dei dati personali", che sarà aggiornato nei termini previsti dalla legge, anche sulla base della regolamentazione specifica privacy, proposta con il presente atto;

**ESAMINATA** la proposta di Regolamento per il trattamento dei dati personali (Codice privacy) già trasmessa , a titolo informativo, alle Organizzazioni sindacali;

**ACQUISITO** il parere favorevole del Responsabile dell'Ufficio Affari Generali e del Personale in merito alla regolarità amministrativa del presente provvedimento con firma apposta sul presente atto;

**ACQUISITO** il parere favorevole del Direttore circa la legittimità del presente provvedimento

**CON VOTI unanimi,** palesemente espressi, nei modi e nelle forme di legge

## DELIBERA

per le motivazioni espresse in narrativa, che qui si intendono integralmente riportate:

1) di approvare il Regolamento per il trattamento dei dati personali (codice privacy) dell'Azienda per il Diritto agli Studi Universitari di Chieti e Pescara, composto da n.5 articoli e da n.2 allegati, ossia i moduli relativi alla nomina del Responsabile e dell'Incaricato del trattamento dei dati personali e/o sensibili, che costituiscono parte integrante e sostanziale dello stesso;
2) di sottoporre all'approvazione della Giunta Regionale il presente regolamento, ai sensi della Legge Regionale 6.12.1994, n.91;

Si attesta la regolarità tecnico/amministrativa del presente atto.

IL RESPONSABILE DELL'UFFICIO

Si attesta la regolarità contabile del presente atto.

IL RESPONSABILE DELL'UFFICIO

---

La presente deliberazione, previa lettura, è stata approvata e firmata a termine di legge.

IL SEGRETARIO
( Avv. Teresa Mazzarulli)

Azienda per il Diritto agli Studi Universitari

IL PRESIDENTE
(Dott. Massimiliano Pignoli)

---

Per copia conforme ad uso amministrativo.

*Chieti,*_____

IL SEGRETARIO
(Avv. Teresa Mazzarulli )

---

**CERTIFICATO DI PUBBLICAZIONE**

Si certifica che copia della presente deliberazione è stata pubblicata all'Albo Pretorio dell'Azienda per il Diritto agli Studi Universitari di Chieti il 16 MAR. 2009 e che vi rimarrà fino al 25 MAR. 2009

(per 10 giorni consecutivi), ai sensi dell'art. 13 del regolamento organizzativo dell'Azienda D.S.U.

*Chieti,* 16 MAR. 2009

Azienda per il Diritto agli Studi Universitari

IL SEGRETARIO
( Avv. Teresa Mazzarulli )

---

L'Ufficio proponente

_____

# AZIENDA PER IL DIRITTO AGLI STUDI UNIVERSITARI DI CHIETI E PESCARA

## Regolamento per il trattamento dei dati personali (Codice Privacy) Anno 2009

a cura del Responsabile Ufficio Affari Generali-Personale
dott.ssa Iginia De Lucia

**Ufficio Affari Generali-Personale**
Il Responsabile
Dott.ssa Iginia De Lucia

**Documento programmatico sulla sicurezza**

# Regolamento per il trattamento dei dati personali (Codice privacy)
## Anno 2009

### Introduzione

Il codice privacy per il trattamento dei dati personali, muovendosi nel solco normativo previsto dalle attuali disposizioni di legge , quali ad es. il Decreto Legislativo 30 giugno 2003 n.196, il Provvedimento del Garante per la protezione dei dati personali del 30 giugno 2005 e il D.Lgs 81/2008 , che in Italia regolamenta la sicurezza sui luoghi di lavoro, è lo strumento per mezzo del quale la Direzione dell'ADSU di Chieti, in qualità di titolare del trattamento, esplica la propria legittima competenza a:

- effettuare le scelte di fondo sulle modalità del trattamento sotto il profilo della sicurezza dei dati personali;
- esprimere la propria volontà in merito al trattamento dei dati personali a vari livelli, all'interno dell'Azienda.

Il legislatore , al fine di salvaguardare i diritti del cittadino e la sicurezza dei propri dati, ha imposto alle aziende precisi obblighi in materia di privacy, tra i quali quello di redigere annualmente uno specifico documento programmatico sulla sicurezza. Il tutto deve seguire lo standard ISO 27001/2005 che definisce le modalità da utilizzare per proteggere dati e informazioni da ogni possibile aggressione. I dati personali devono essere trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, specificatamente per lo svolgimento delle funzioni e delle mansioni assegnate. I dati devono essere esatti, aggiornati, pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti e trattati. Nei trattamenti è autorizzata solo l'esecuzione delle operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.

Per trattare correttamente i dati personali, nell'ambito di un'organizzazione aziendale, è necessario:

**1)**Custodire in modo riservato banche dati, contratti e comunque ogni documentazione raccolta nello svolgimento dell'attività lavorativa.

**2)**Adottare cautele organizzative per garantire che tutte le persone, con cui si collabora, siano informate sulle regole di riservatezza adottate per proteggere i dati ed impartire adeguate istruzioni per evitare abusi per negligenza, imprudenza o imperizia.

2

**3)**Verificare sempre l' origine dei dati utilizzati.

**4)**In caso di utilizzo dei dati, ricordarsi di verificare che la persona, che si contatta, abbia fornito il consenso ed accertarsi se sia necessario disporne per utilizzare correttamente i dati.

**5)**Informare prontamente la persona preposta al trattamento dei dati, qualora un interessato formuli un'istanza per l' esercizio dei suoi diritti.

**6)**Evitare di utilizzare liste di nominativi ed indirizzi quando non ne è certa la provenienza o il fornitore si è rifiutato di dichiarare per iscritto che l' uso dei dati è consentito, ai sensi della vigente normativa, esonerando da qualsiasi conseguenza derivante da tale uso.

**7)**Adottare tutte le misure di sicurezza informatiche previste dal sistema fornito dall'organizzazione in cui si opera, quando ci si connette alla rete predisposta per il collegamento alla banca dati.

**8)**Segnalare al proprio referente qualsiasi anomalia riscontrata nella qualità dei dati presenti nel data base utilizzato.

**9)**Adottare ogni precauzione nello svolgimento di attività che prevedono l'utilizzo di dati personali (invio di materiale per posta, e-mail o ricerche di mercato con strumenti di telemarketing), al fine di prevenire ogni forma, anche per mera negligenza o imperizia, di illecito utilizzo di dati personali.

**10)**Ferma restando la responsabilità del singolo utilizzatore del data base, attenersi alle istruzioni che sono state e che verranno impartite per garantire la corretta gestione dei dati stessi.
Ogni persona è titolare del diritto di disporre dei dati che la descrivono e che ne qualificano l'individualità. Quando si parla di privacy, quindi, oggi non si fa riferimento solo al diritto alla riservatezza, ma anche al diritto di scelta circa l'uso da parte di altri dei dati personali.

3

## Art.1 - Tipi di dati

Secondo la normativa vigente, il **dato personale** è qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. I codici identificativi, sia quelli ricavati da dati anagrafici (ad esempio il codice fiscale), che i codici univoci attribuiti a una persona in base a criteri predefiniti (ad esempio i codici cliente) sono dati personali.
Una categoria particolare di dati personali sono i **dati sensibili**. Si tratta dei 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. Questa tipologia di dati è sottoposta a un livello di protezione più elevato di quello previsto per i dati non sensibili.

| | |
|---|---|
| **Decreto legislativo 30 giugno 2003, n.196 e successive modifiche ed integrazioni**<br><br>**Nuovo codice in materia di protezione dei dati personali** | **Obiettivi**<br><br>• Incrementare la consapevolezza dell'importanza della privacy nelle attività quotidiane;<br>• Fornire i principi base del D.Lgs 196/03;<br>• Far conoscere le figure di riferimento del sistema privacy;<br>• Far emergere necessità specifiche delle singole strutture. |
| **Finalità (art.2,c.1 D.Lgs 196/03)**<br>Il D.L.gs del 30 giugno 2003, n.196(T.U. privacy)disciplina il trattamento dei dati personali, affinché lo stesso avvenga nel rispetto:<br>➢ dei diritti<br>➢ della dignità<br>➢ delle libertà fondamentali<br>**dell'interessato** in riferimento alla:<br>➢ riservatezza<br>➢ identità personale<br>➢ diritto alla protezione dei dati personali | **Applicabilità**<br><br>Si applica a tutti coloro che trattano dati personali, identificativi e sensibili. |

| Consenso | Casi di esclusione del consenso |
|---|---|
| 1. Il trattamento di dati personali, da parte di privati o di enti pubblici economici, è ammesso solo con il consenso espresso dell'interessato.<br>2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.<br>3. Il consenso è validamente prestato solo se espresso liberamente in forma specifica (cioè non prestato in modo generico) e documentata per iscritto, e se sono state rese all'interessato le informazioni, di cui all'art.13 del D.Lgs. n.196/2003;<br>4.Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili. | Il consenso **non è richiesto** quando:<br>**a)**i dati sono raccolti e detenuti in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;<br>**b)**è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato<br>**c)**riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;<br>**d)**è necessario per la salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo, nel caso in cui l'interessato non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere e volere. |

## Definizioni (art.4, D.lgs.196/03)

| Dati personali | Dati identificativi | Dati sensibili | Dati Giudiziari |
|---|---|---|---|
| Qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale | Dati personali che permettono l'identificazione diretta e certa di un soggetto, sia esso persona fisica, giuridica, ente o associazione (es.anagrafica, sesso) | 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 idonei a rivelare lo stato di salute e la vita sessuale. (Questi dati possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del garante). | Dati personali idonei rilevare provvedimenti concernenti:<br>- le pene<br>- le pene accessorie<br>- le misure alternative alla detenzione<br>- la liberazione condizionale<br>- dati che rivelino la qualità di imputato o indagato. |

Rispettare i principi fondamentali su elencati è importantissimo perché i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati. Quindi, rispettare questi principi permette di prevenire contestazioni che possono portare al blocco del trattamento dei dati.

5

## Art.2 - Trattamento dei dati personali: informativa e consenso

Per "**trattamento**" si intende qualunque operazione o complesso di operazioni, effettuate 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. Pertanto, qualsiasi operazione compiuta nei confronti dei dati personali costituisce "trattamento".La normativa disciplina anche i dati posti su supporti cartacei. Per tale motivo il concetto di trattamento comprende anche le operazioni che prescindono dall'utilizzo di strumenti elettronici. La regola che disciplina il trattamento dei dati è semplice, a parte le ipotesi già individuate di doverosità del trattamento (ad es. per l'espletamento dei doveri d'ufficio): ognuno ha diritto di essere informato e sapere per quali finalità e con quali modalità i dati sono raccolti e conseguentemente decidere se consentire o non consentire al trattamento.E' vietato il trattamento da parte di personale non autorizzato.La procedura di protezione dei dati personali è tutta racchiusa in questo meccanismo: chi intende trattare i dati ha l'obbligo di informare la persona cui si riferiscono i dati. Questa, sulla base delle informazioni ricevute, ha diritto di scegliere se permettere o vietare questo trattamento.

**Tipi di dati (D.Lgs.30.6.2003 n.196)**

| |
|---|
| **Dati personali**<br>Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. |
| **Dati identificativi**<br>I dati personali che permettono l'identificazione diretta dell'interessato. |
| **Dati sensibili**<br>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**<br>Dati personali idonei a rivelare provvedimenti di cui all'art.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. |

6

**Art.3 - Titolare del trattamento**

Tra i compiti che la Legge assegna al Direttore e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili delle proprie istruzioni e del trattamento di un'area di dati personali, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Nel caso dell'Azienda D.S.U., che giuridicamente fa capo al Direttore, il titolare del trattamento dei dati personali è lo stesso soggetto a cui fa capo, giuridicamente, l'attività. Il titolare del trattamento ha , inoltre, il compito di :

- designare i responsabili dei trattamenti dei dati personali e/o sensibili;
- impartire ai Responsabili le necessarie istruzioni per la corretta gestione e tutela dei dati personali, ivi compresa la salvaguardia della loro integrità e sicurezza. Le istruzioni ai responsabili dovranno essere impartite dal Titolare del trattamento dei dati, al momento della nomina;
- ricevere dai Responsabili designati annualmente una relazione sull'attività di loro competenza;
- aggiornare, entro il 31 marzo di ogni anno, il Documento Programmaticio sulla Sicurezza relativo alle strutture dell'ADSU.

**Responsabile del trattamento di dati personali**

Il Responsabile del trattamento dei dati personali e/o sensibili, ai fini della sicurezza, ha le seguenti responsabilità:

- promuovere lo sviluppo, la realizzazione ed il mantenimento dei programmi di sicurezza contenuti nel presente Documento Programmatico sulla Sicurezza dei Dati Personali;
- informare il Titolare del trattamento sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti;
- promuovere lo svolgimento di un continuo programma di addestramento degli Incaricati del Trattamento e mantenere attivo un programma di controllo e monitoraggio della corrispondenza con le regole di sicurezza.

Ciò premesso, nell'ambito delle Sue mansioni lavorative, ha la responsabilità della raccolta, registrazione, organizzazione, conservazione, consultazione, comunicazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, distruzione dei dati, che dovrà trattare in modo lecito, corretto, esatto e pertinente.

In ogni operazione di trattamento deve essere garantita la massima riservatezza ed, in particolare, è vietato comunicare e/o diffondere dati senza la preventiva autorizzazione del Titolare del trattamento.

In ogni operazione di trattamento deve essere garantita la massima riservatezza ed, in particolare, al Responsabile del trattamento è:

- vietato comunicare e/o diffondere dati senza la preventiva autorizzazione del Titolare;
- consentito l'accesso ai dati, limitatamente alle proprie mansioni;
- fatto obbligo di raccogliere il consenso degli interessati, in forma scritta o in forma orale, che dovrà essere preceduto dalla informativa;
- fatto obbligo di verificare, in caso di interruzione, anche temporanea del lavoro, che i dati trattati non siano accessibili a terzi non autorizzati.

**Incaricati del trattamento**

Gli Incaricati del trattamento dei dati personali sono identificati in tutti coloro che materialmente effettuano le operazioni di trattamento di dati personali e/o sensibili con specifico riferimento alla sicurezza. Essi hanno le seguenti responsabilità:

- svolgere le attività previste dai trattamenti secondo le prescrizioni contenute nel presente Documento Programmatico sulla Sicurezza e le direttive del Responsabile;
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del Responsabile del trattamento;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il Responsabile in caso di incidente di sicurezza che coinvolga dati personali e/o sensibili.

Non si configurano quali incaricati i soggetti che trattano esclusivamente dati statistici. Gli incaricati ricevono formale atto di nomina dai loro Responsabili del trattamento. Nell'atto scritto di designazione, i Responsabili devono prescrivere che gli Incaricati abbiano accesso esclusivamente ai soli dati personali e/o sensibili, la cui conoscenza sia strettamente necessaria per l'espletamento dell'attività, cui sono preposti.

Ciò premesso, nell'ambito delle mansioni lavorative, l' incaricato ha materialmente la responsabilità della raccolta, registrazione, organizzazione, conservazione, consultazione, comunicazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, distruzione dei dati, che dovrà trattare in modo lecito, corretto, esatto e pertinente.

In ogni operazione di trattamento deve essere garantita la massima riservatezza ed, in particolare, all'incaricato del trattamento è:

- vietato comunicare e/o diffondere dati senza la preventiva autorizzazione del Responsabile;
- consentito l'accesso ai dati, limitatamente alle proprie mansioni;
- fatto obbligo di raccogliere il consenso degli interessati, in forma scritta o in forma orale, che dovrà essere preceduto dalla informativa;
- fatto obbligo di verificare, in caso di interruzione, anche temporanea del lavoro, che i dati trattati non siano accessibili a terzi non autorizzati.

**Nomina e compiti dei Responsabili del trattamento dei dati**

La nomina dei Responsabili del trattamento dei dati dovrà essere notificata per iscritto ai soggetti individuati.

**Rapporti tra diritto di accesso e diritto alla riservatezza.**

L'accesso ai documenti sarà ammesso con le modalità di legge.

Per quanto riguarda i dati idonei a rivelare lo stato di salute o le abitudini sessuali, l'accesso a questi, contenuti in documenti amministrativi, è ammesso solo quando il diritto da tutelare, tramite istanza di accesso è di rango pari almeno al diritto alla riservatezza, ovvero consiste in un diritto alla personalità o in un altro diritto o libertà fondamentale o inviolabile (diritto alla difesa..)

I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato solo attraverso la consegna dei dati al medico di fiducia che, a sua volta li renderà noti all'interessato.

La documentazione sanitaria può essere ritirata dall'interessato o da persona diversa sulla base di una delega scritta e mediante consegna dei documenti in busta chiusa

**Rapporti con il Garante**
Ogni rapporto con il Garante (notificazioni, richieste di autorizzazione, comunicazioni) è di competenza del Titolare, il quale vi provvede tramite il Referente Privacy Aziendale; il Titolare deve inoltre provvedere al trattamento di taluni dati sensibili, qualora si rendano necessari ai sensi degli artt.39-110 del Codice Privacy.

**La banca dati** è qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

**Le tre componenti base per la protezione dei dati e la fiducia degli utenti sono:**

- **integrità** ossia la salvaguardia della esattezza dei dati, la difesa da manomissioni e da modifiche non autorizzate, il monitoraggio automatico degli accessi;
- **riservatezza** ossia la protezione delle informazioni tramite l'accesso solo agli autorizzati, la protezione delle trasmissioni, il controllo accessi;
- **disponibilità** ossia la garanzia per gli utenti della fruibilità dei dati delle informazioni e dei servizi, evitando la perdita o riduzione dei dati o dei servizi.

Tutto questo serve a salvaguardare :

- **il patrimonio aziendale;**
- **il Know how aziendale ossia l' abilità tecnica di gestione;**
- **l'attività aziendale;**
- **il nostro lavoro.**

9

**Art.4 - Responsabilità specifiche**

Tra i compiti che la Legge assegna al Direttore di un'Azienda e, nello specifico dell'Azienda per il Diritto agli Studi Universitari di Chieti e Pescara e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili delle proprie istruzioni e del trattamento di un'area di dati personali, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Nel caso dell'Azienda per il D.S.U., che giuridicamente fa capo al Direttore, il titolare del trattamento dei dati personali è lo stesso soggetto a cui fa capo, giuridicamente, l'attività.
Per poter progettare e quindi predisporre un funzionale piano di sicurezza è necessario "in primis" conoscere i rischi ai quali è esposto il proprio patrimonio informatico e, "in secundis" avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare.
I rischi presenti nell'Azienda per il Diritto agli Studi Universitari di Chieti, per quanto riguarda il patrimonio informatico, sono prevalentemente:

- Accessi non autorizzati;
- Effrazioni;
- Furti;
- Atti vandalici;
- Malfunzionamenti dovuti a guasti o sabotaggi;
- Malfunzionamenti dovuti ad eventi naturali (allagamenti, incendi...);
- Intercettazione.

L'importante è:
-acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informatico;
- avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare.

Per quanto riguarda poi il materiale cartaceo i rischi sono:

- Accesso non autorizzato;
- Modifiche deliberate o accidentali;
- Sottrazione;
- Distruzione;
- Scarsa consapevolezza del problema sicurezza;
- Distruzione, sottrazione ed alterazione ad opera di eventi naturali, azioni accidentali e comportamenti intenzionali.

Sulla base dei risultati conseguiti con l'analisi, di cui sopra, è possibile procedere alla predisposizione di un quadro esaustivo delle misure di controllo del rischio.
I sistemi di sicurezza adottati dall' Azienda D.S.U. devono basarsi sui seguenti punti fondamentali:

- sicurezza fisica;
- sicurezza logica;
- sicurezza organizzativa;
- gestione delle crisi.

**La sicurezza fisica** si realizza attraverso le opportune disposizioni per :

- controllo degli accessi;

10

- gestione delle chiavi;
- gruppo di continuità.

**La sicurezza logica** si realizza attraverso le opportune disposizioni per:

- sistemi di identificazione;
- sistemi di autenticazione;
- controlli antivirus.

**La sicurezza organizzativa** si realizza attraverso opportune disposizioni per:

- la gestione del personale;
- codici etici di comportamento;
- suddivisione incarichi;
- formazione e sensibilizzazione del personale.

**La gestione dell'emergenza** e delle crisi deve prevedere:

- procedure di backup;
- procedure di recupero dei dati;
- procedure di ripristino.

**Monitoraggio della posta elettronica e degli accessi ad Internet**

Al controllo della posta elettronica e degli accessi ad Internet dell'operato aziendale è applicato il principio di proporzionalità e non eccedenza e deve tener conto della legittima privacy e di altri interessi del dipendente. Tale controllo può essere disposto solo previa regolamentazione aziendale nella quale vengono indicate le finalità, le modalità e la cadenza di tale controllo e inoltre vengono indicati i criteri operativi di ogni attività di verifica dell'operato del singolo operatore e l'indicazione dei soggetti autorizzati al trattamento dei dati relativi. I dati devono essere raccolti per scopi specifici, espliciti e legittimi e non utilizzati in modo illecito. Il lavoratore deve essere adeguatamente informato sulla possibilità che vengano effettuati controlli.

**Art. 5 - Regole fondamentali per la protezione delle aree e dei locali interessati dalle misure di sicurezza.**

a) I locali e i contenitori nei quali sono archiviati e presso cui è possibile accedere ai dati devono essere sempre presidiati da personale autorizzato. In caso di assenza, anche temporanea, di idoneo presidio, i locali e i contenitori dei dati devono essere debitamente resi inaccessibili attivando i sistemi di chiusura disponibili. Qualora le chiusure siano deteriorate o mancanti è compito del responsabile dell'ufficio dare immediata comunicazione all'ufficio preposto alla manutenzione degli immobili. La gestione delle chiavi di accesso ai contenitori dei dati o all'ufficio, qualora detti contenitori ne fossero sprovvisti, deve essere effettuata a cura del responsabile dell'ufficio che provvederà a gestire un elenco di tutti i detentori delle chiavi e a mantenerlo aggiornato.

b) I responsabili degli Uffici sono incaricati del trattamento dei dati pervenuti, per cui devono mantenere un effettivo controllo sull'area di propria responsabilità.
- I visitatori occasionali devono essere accompagnati.
- Gli ingressi fuori orario devono essere controllati.

c) I locali nei quali sono archiviati dati personali devono essere sempre presidiati da personale autorizzato. In caso di assenza, anche temporanea del personale incaricato dei trattamenti dei dati i locali e i contenitori dei dati devono essere resi inaccessibili attivando i sistemi di chiusura disponibili. Qualora le chiusure siano deteriorate o mancanti, il responsabile del trattamento dei dati e gli incaricati del trattamento dei dati dell'ufficio sono tenuti a dare immediata comunicazione all'ufficio preposto alla manutenzione degli immobili.

d) Gli incaricati sono tenuti a fine giornata a non lasciare sulla scrivania e a riporre negli armadi tutta la documentazione contenente dati personali. I dati sensibili devono essere riposti in armadi chiusi e resi inaccessibili (es.in busta chiusa all'interno dei fascicoli).

e) Il materiale cartaceo contenente dati personali deve essere reso illeggibile prima dello smaltimento.

f) Il responsabile del sistema informatico mantiene un elenco, da aggiornare con cadenza almeno annuale, di tutte le attrezzature informatiche dei singoli uffici e della loro collocazione fisica.

g) L'accesso alla rete può avvenire esclusivamente tramite un processo di autenticazione che prevede un nome utente ed una password. Vengono attivati sistemi antintrusione ed antivirus che si aggiornano costantemente ed automaticamente al fine di minimizzare le possibilità di danno. Gli addetti all'informatica provvedono ad effettuare gli aggiornamenti importanti ai sistemi operativi ed ai software volti a garantire l'inviolabilità dei sistemi. In caso di danneggiamento dei dati o degli strumenti elettronici sono adottate idonee misure dirette a garantire il ripristino dell'accesso ai dati, in tempi certi e non superiori a sette giorni.

h) I responsabili degli uffici ai quali il presente documento e le sue successive revisioni verranno trasmessi, devono rendere noto a tutti i componenti dell'ufficio i contenuti del presente documento con particolare riferimento alle responsabilità.

12

**Allegato n.1**

**Prot.n.:**

**Chieti,**

Egr.Dott./Sig

**Oggetto:** Nomina quale **Responsabile** del trattamento dei dati personali e/o sensibili, ai sensi dell'art.30 del Decreto Legislativo del 30 giugno 2003, n.196

Ai sensi della normativa in oggetto e in qualità di Titolare - pro tempore - per il trattamento dei dati personali e/o sensibili, La nomino soggetto **Responsabile** del trattamento dei dati personali e/o sensibili, relativi all'Ufficio .....
Lei è autorizzata , nell'osservanza del regolamento aziendale, approvato con deliberazione del Consiglio d'Amministrazione n. del , ratificata dalla Giunta Regione Abruzzo con atto n. del ,a trattare i dati personali e/o sensibili, che attengono alle banche dati, censite presso l'Ufficio
Ciò premesso, nell'ambito delle Sue mansioni lavorative, così come definite dalle leggi vigenti, Le viene conferito l'incarico di responsabilità delle seguenti operazioni di trattamento , con l'avvertimento che dovrà operare osservando le direttive del Titolare del trattamento: raccolta, registrazione, organizzazione, conservazione, consultazione, comunicazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, distruzione.
Ai sensi dell'art.11 del Codice, in materia di protezione dei dati personali (Decreto Legislativo 30 giugno 2003, n.196), Lei si impegna a trattare i dati in modo lecito, secondo correttezza, in modo esatto e in modo pertinente.
In ogni operazione di trattamento deve essere garantita la massima riservatezza ed in particolare:
a) è vietato comunicare e/o diffondere i dati, senza la preventiva autorizzazione del Titolare del Trattamento;
b) l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni;
c) la fase di raccolta del consenso dovrà essere preceduta dalla informativa e dal consenso degli interessati, rilasciato in forma scritta o in forma orale;
d) in caso di interruzione, anche temporanea del lavoro, si dovrà verificare che i dati trattati non siano accessibili a terzi non autorizzati;
E' vietata la diffusione dei dati personali e/o sensibili, nel senso che Lei non comunicherà ad alcuna persona terza dati di tale natura, salvo che sia stato a ciò espressamente autorizzato dal Titolare della privacy, ossia dal Direttore dell'Azienda per il Diritto agli Studi Universitari di Chieti e Pescara.
Con la presente Ella è autorizzata a prendere visione del Documento Programmatico per la Sicurezza, una cui copia è depositata presso l' Ufficio Protocollo di questa ADSU ed Quale Responsabile Ella avrà cura di nominare gli incaricati del trattamento dei dati, cui materialmente è affidata l'esecuzione delle suddette operazioni.

Il Responsabile dell'Ufficio_____

Dott./sig._____

Data

Firma per accettazione

IdL/Modulo n.1 allegato Regolamento Privacy

13

**Allegato n.2**

**Prot.n.:** **Chieti,**

Egr.Dott./Sig

**Oggetto:** Nomina quale **Incaricato** del trattamento dei dati personali e/o sensibili, ai sensi dell'art.30 del Decreto Legislativo del 30 giugno 2003, n.196

Ai sensi della normativa in oggetto e in qualità di Responsabile - pro tempore - per il trattamento dei dati personali e/o sensibili, La nomino soggetto **Incaricato** del trattamento dei dati personali e/o sensibili, relativi all' Ufficio.....
Lei è autorizzata a trattare i dati personali e/o sensibili, che attengono alle banche dati, censite presso l' Ufficio.....
Ciò premesso, nell'ambito delle Sue mansioni lavorative, così come definite dalle leggi vigenti, Le viene conferito l'incarico di compiere materialmente le seguenti operazioni di trattamento , con l'avvertimento che dovrà operare osservando le direttive del Responsabile del trattamento: raccolta, registrazione, organizzazione, conservazione, consultazione, comunicazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, distruzione.
Ai sensi dell'art.11 del Codice, in materia di protezione dei dati personali (Decreto Legislativo 30 giugno 2003, n.196), Lei si impegna a trattare i dati in modo lecito, secondo correttezza, in modo esatto e in modo pertinente.
In ogni operazione di trattamento deve essere garantita la massima riservatezza ed in particolare:
a) è vietato comunicare e/o diffondere i dati, senza la preventiva autorizzazione del Responsabile del Trattamento;
b) l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni;
c) la fase di raccolta del consenso dovrà essere preceduta dalla informativa e dal consenso degli interessati, rilasciato in forma scritta o in forma orale;
d) in caso di interruzione, anche temporanea del lavoro, si dovrà verificare che i dati trattati non siano accessibili a terzi non autorizzati;
e) le proprie credenziali di autenticazione dovranno essere riservate.
E' vietata la diffusione dei dati personali e/o sensibili, nel senso che Lei non comunicherà ad alcuna persona terza dati di tale natura, salvo che sia stato a ciò espressamente autorizzato dal sottoscritto Responsabile Privacy.
Con la presente Ella è autorizzata a prendere visione del Documento Programmatico per la Sicurezza, una cui copia è depositata presso l' Ufficio Protocollo di questa ADSU.

Il Responsabile dell'Ufficio_____
Dott./sig._____

Data

Firma per accettazione

La presente copia è conforme all'originale in atti composta di n 14 fogli e n 14 facciate, è parte integrante e sostanziale della deliberazione n 5 del 9-3-09