



Il Regolamento di attuazione del Codice di tutela dei dati personali dell'Università degli Studi di Firenze

Aula Magna – 14 ottobre 2004

**“Nuove responsabilità organizzative del
titolare e azioni da intraprendere”**

Cristina Mugnai

Dirigente Area Servizi Informatici

Direttore Tecnico CSIAF



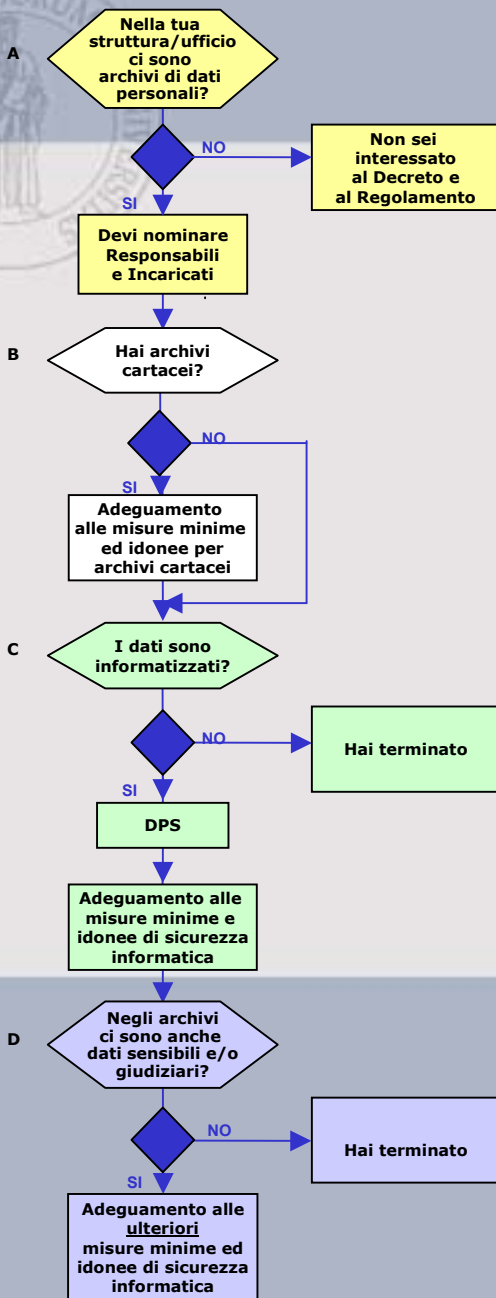
Titolare del trattamento c/o Università di Firenze (art. 3 del Regolamento)

Sono **titolari le strutture** che detengono dati personali, ovvero:

- le **unità amministrative**,
 - gli **uffici dirigenziali**, lo **SBA**, lo **CSIAF**,
 - gli **organismi di controllo**
-
- Le medesime strutture sono titolari anche dei dati personali dati in "hosting" a CSIAF ed a fornitori di servizi

Cosa devono fare i titolari?

A1. Censimento archivi dati personali



- **Cartacei** (es: archivi ufficio amministrativo, del personale, degli studenti e laureati, dei fornitori,....)
- **Informatizzati c/o struttura**
- **Informatizzati c/o CSIAF o altro fornitore di servizi**

Il censimento è obbligatorio (art.13 del Regolamento) entro xxxxxx (data ancora da definire) e va mantenuto aggiornato (art. 6 del Regolamento)

Chiunque inizi o cessi il trattamento di dati personali deve dare comunicazione scritta al titolare (art. 6 del Regolamento)

Rispondi a queste domande:

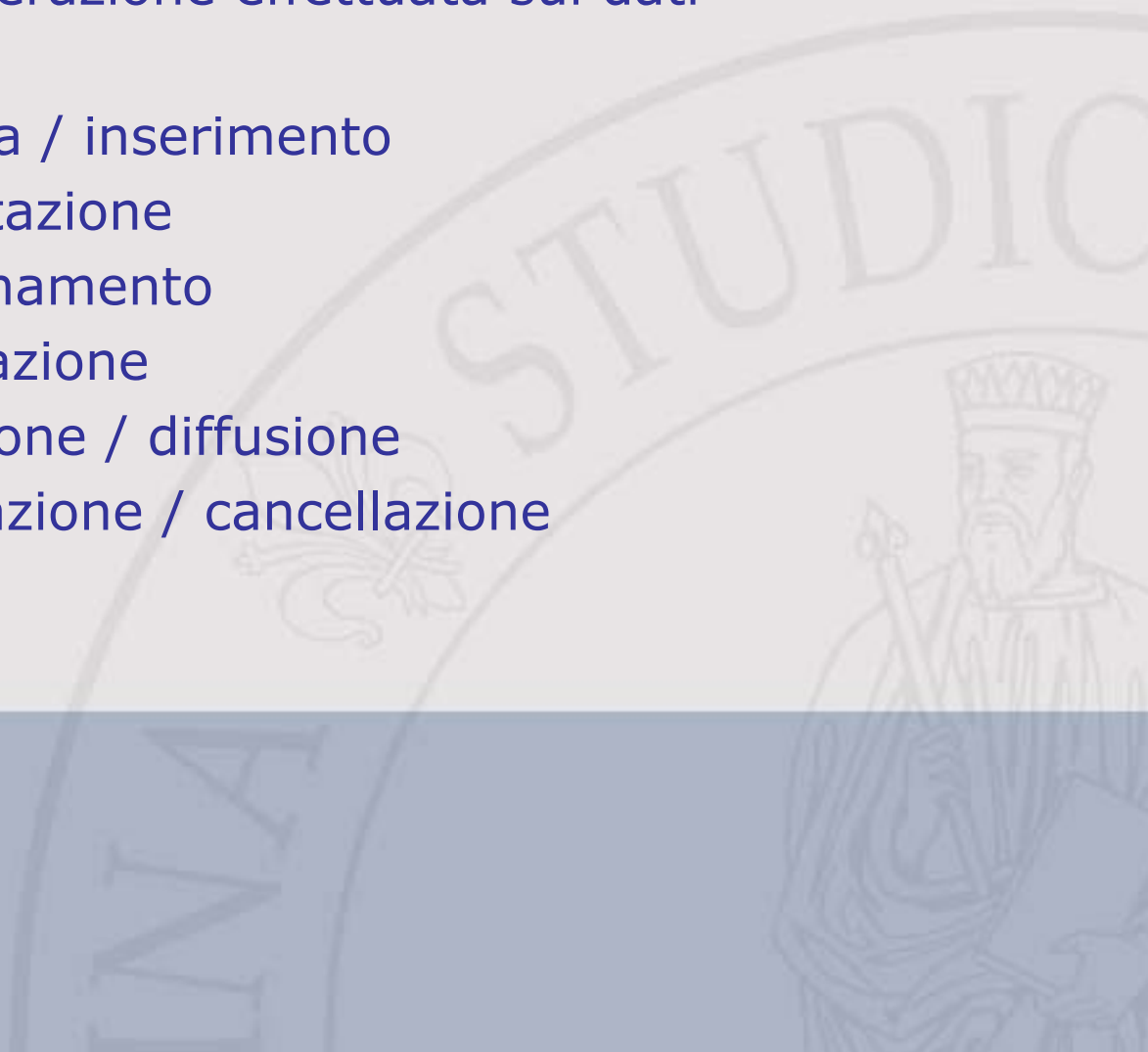
- È proprio necessario possederli?
- Sono necessari per lo svolgimento delle funzioni istituzionali? (art.18 c.2 del Decreto)



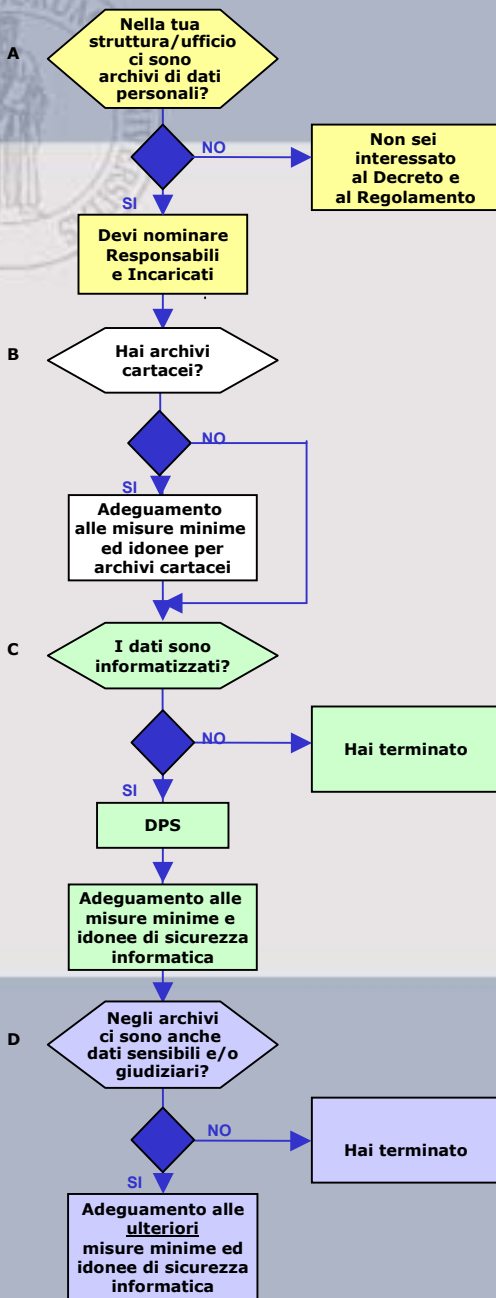
Cosa è un trattamento?

Qualunque operazione effettuata sui dati

Es: raccolta / inserimento
consultazione
aggiornamento
elaborazione
estrazione / diffusione
eliminazione / cancellazione



A2. Nomina responsabili trattamento (art. 29 del Codice e 3 del Regolamento)

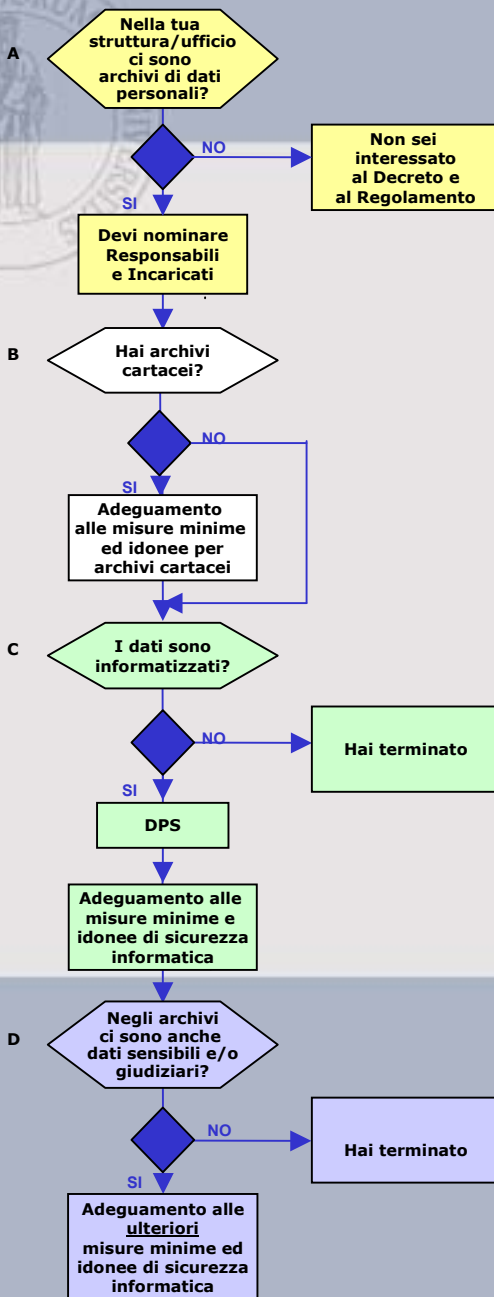


- **Responsabili del trattamento (opzionali)** sono coloro che sovrintendono alle operazioni di trattamento (es. responsabile di segreteria, ufficio, laboratorio, presidente CdS,...)
- Le **nomine** dei responsabili sono effettuate **per iscritto dal titolare all'interno della propria struttura** (un esempio sul [sito CSIAF](#))
- **CSIAF** può nominare i responsabili del trattamento **al di fuori della propria struttura, di concerto con i dirigenti di area ed i responsabili delle U.A. di riferimento**
- I **fornitori di servizi** che ospitano archivi della struttura sono designati **automaticamente** quali **responsabili del trattamento. Clausola nel contratto.**

Nella nomina è necessario specificare analiticamente i compiti

Il titolare deve vigilare tramite verifiche periodiche

A3. Nomina incaricati trattamento (art. 30 del Codice e 3 del Regolamento)

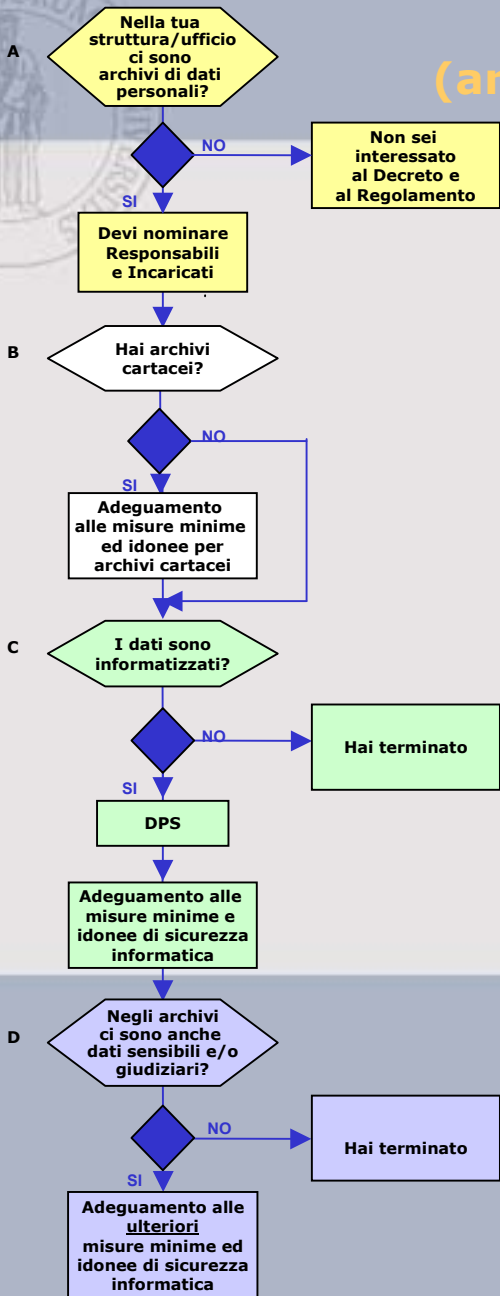


- **Incaricati del trattamento (obbligatori)** sono coloro che effettuano fisicamente i trattamenti (es. ricercatore, impiegato di segreteria,....)
- Le **nomine** degli incaricati sono effettuate **per iscritto dal titolare o dal responsabile** del trattamento, se designato, **all'interno della propria struttura** (un esempio sul [sito CSIAF](#))
- **CSIAF**, qualora non sia stato designato il responsabile del trattamento, **nomina gli incaricati del trattamento anche al di fuori della propria struttura, d'intesa con i dirigenti di area o i responsabili delle U.A. di riferimento**
- Si possono nominare **incaricati del trattamento per documentata preposizione** (es. impiegati dello stesso ufficio)

Nella nomina è necessario impartire le istruzioni

L'**elenco** dei responsabili e degli incaricati del trattamento devono essere pubblicati **sul sito web di Ateneo**

B. Adeguamento misure minime di sicurezza per archivi non informatizzati (artt. 35 del Codice e punti 27,28,29 dell'allegato B)



- **procedure scritte per una idonea custodia** degli atti e documenti **durante il trattamento** da parte degli incaricati

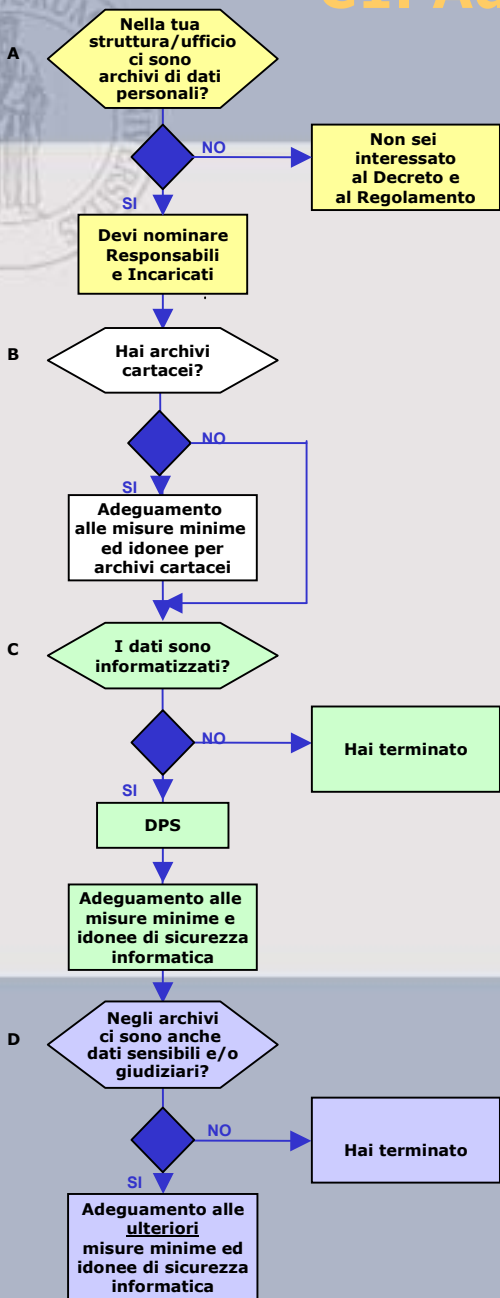
(es. vietato lasciare documenti incustoditi sulla scrivania o in cassetti aperti situati in stanze accessibili ai non incaricati)

- **controllo dell'accesso** agli archivi

(es. gli archivi devono essere chiusi a chiave in stanze chiuse a chiave; le chiavi sono disponibili solo agli autorizzati; gli accessi vengono registrati....)

- **aggiornamenti periodici** dell'individuazione **dell'ambito di trattamento** consentito agli incaricati

C1. Adeguamento misure minime di sicurezza per trattamento archivi informatizzati (art. 34 del Codice e punto 19 dell'allegato B)



Il Documento Programmatico sulla Sicurezza (**DPS**) **contiene:**

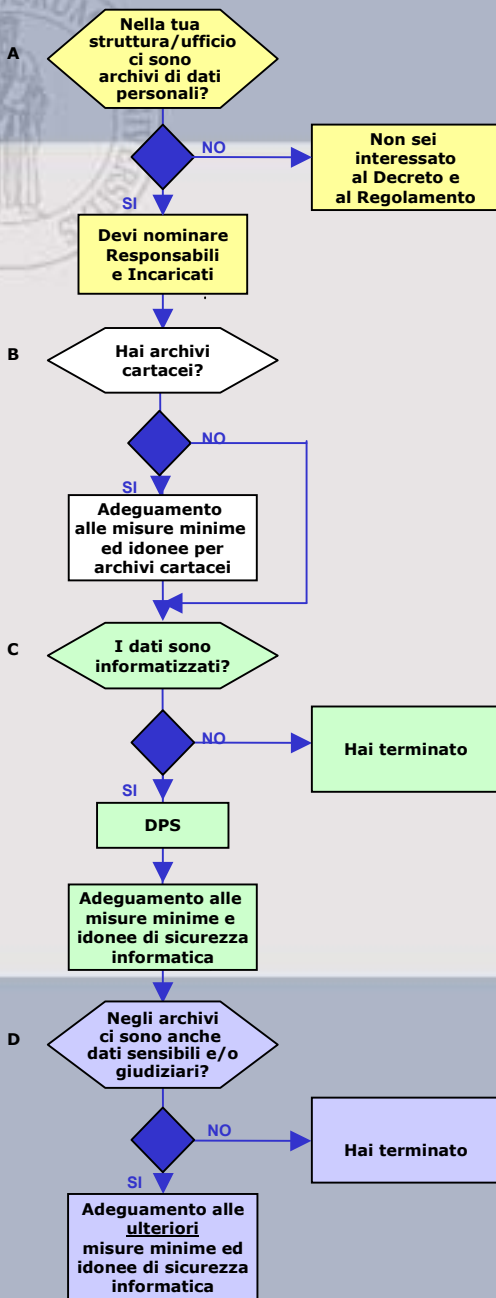
- l'elenco dei trattamenti
- la distribuzione dei compiti e delle responsabilità nelle strutture preposte ai trattamenti
- l'analisi dei rischi
- le misure da adottare per contrastare i rischi: integrità e disponibilità dei dati, riservatezza, protezione aree e locali, backup e ripristino dei dati, formazione
- la descrizione delle misure per garantire l'adozione delle misure minime da parte di terzi cui sono affidati i servizi
- l'individuazione dei criteri da adottare per la cifratura e la separazione dei dati sensibili (sanitari) da quelli personali .

Il DPS è un **documento a data certa** (un esempio sul [sito CSIAF](#) e sul [sito del Garante](#)).

Il DPS va **aggiornato entro il 31 marzo di ciascun anno.**

La **prima redazione** del DPS deve avvenire **entro il 31 dicembre 2004**

Adeguamento misure minime di sicurezza per trattamento archivi informatizzati (art. 34 del Codice e punti 1-18 dell'allegato B)



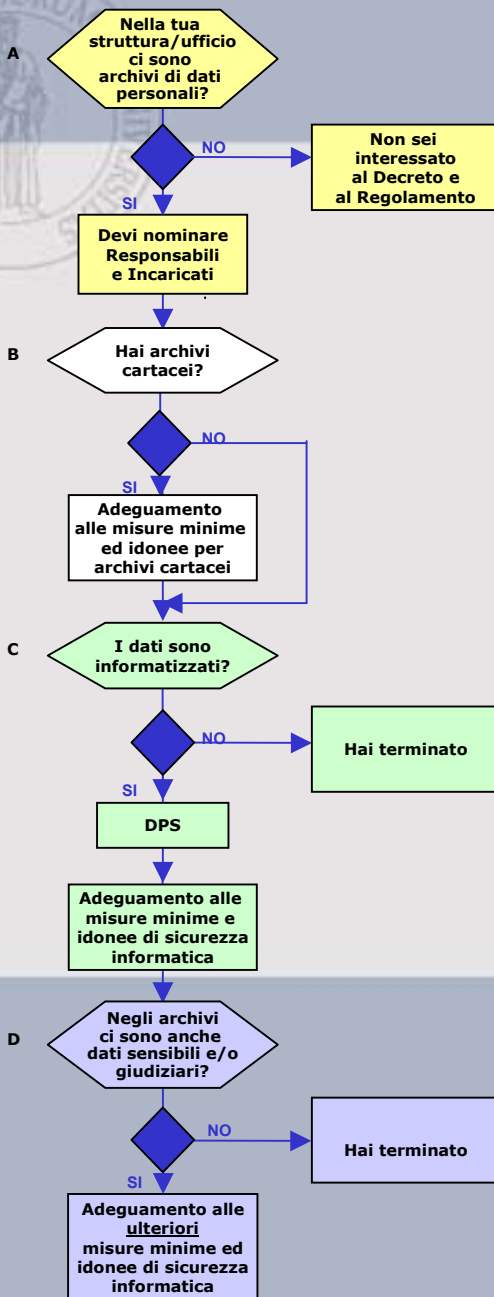
- **Autenticazione** (almeno user e password con lunghezza min. di 8 caratteri, obbligo di modifica al 1° utilizzo e poi ogni 3/6 mesi)
- **Procedure gestione credenziali di autenticazione** (disattivazione credenziali non utilizzate per 6 mesi o di qualità scadente, istruzioni sulla custodia e disposizioni scritte per assenza incaricato della custodia)
- **Sistema di autorizzazione** (profili utente)
- **Aggiornamento** periodico, almeno annuale, **ambito trattamento degli incaricati** e addetti alla gestione e manutenzione strumenti elettronici
- **Protezione strumenti elettronici** da accessi non consentiti (aggiornamento sw ogni 6 mesi x intrusione e ogni 12/6 mesi x vulnerabilità)
- **Procedure per custodia copie di sicurezza e ripristino** (eseguite almeno con frequenza settimanale)

Adeguamento alle misure minime entro il 31 dicembre 2004.

Le **misure minime non applicate nei termini** per problemi tecnici **devono essere attuate entro il 31 marzo 2005** e le **ragioni** della mancata attuazione devono essere **descritte** in un **documento a data certa entro il 31 dicembre 2004**

C3. Misure di tutela e garanzia

(punti 25 e 26 dell'allegato B)

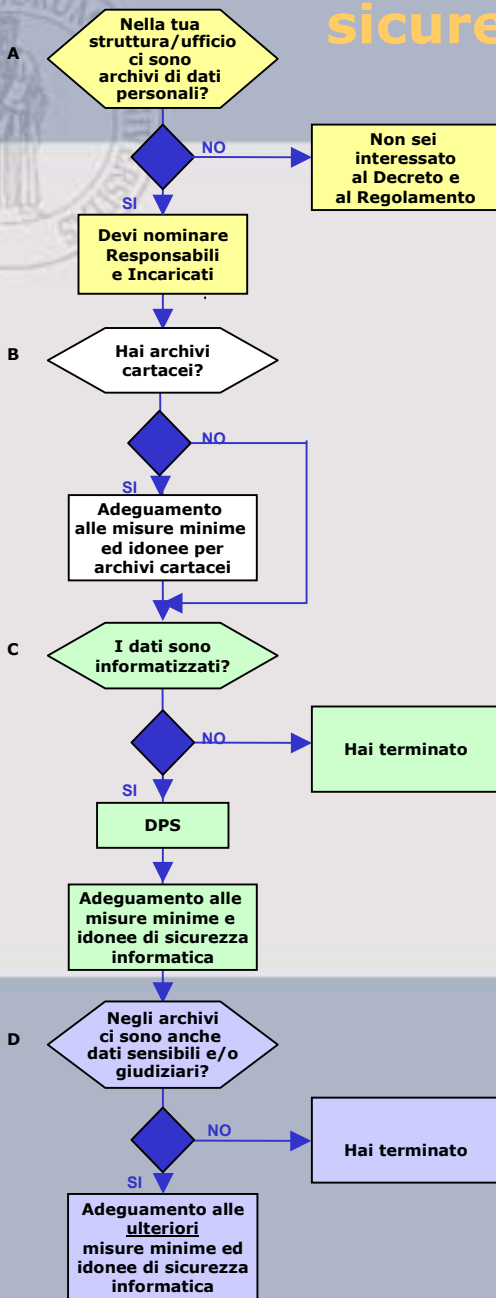


Il titolare deve riferire nella relazione al bilancio d'esercizio dell'avvenuta redazione o aggiornamento del DPS

Se adeguamento alle misure minime è realizzato avvalendosi di soggetti esterni ⇒ deve essere rilasciato attestato conformità alle disposizioni del Decreto

CSIAF offre un supporto con modulistica e documentazione messa a disposizione sul proprio sito <http://www.csiarf.unifi.it> e rispondendo a quesiti inviati alla casella: applicazione.privacy@unifi.it

D. Adeguamento ulteriori misure minime di sicurezza informatica (se dati sensibili o giudiziari) (art. 34 del Codice e punti 20-24 dell'allegato B)



- **Adozione** tecniche di **cifratura** ed altre **tecniche di protezione**
- **Separazione** dei **dati sensibili** dai **dati personali**
- **Istruzioni** tecniche ed organizzative per **custodia ed uso supporti rimovibili**
- **Distruzione supporti** rimovibili, se **non utilizzati**
- **Ripristino** dei dati in caso di distruzione o danneggiamento **entro 7gg**
- **Dati genetici** trattati da incaricati che operano **in locali non accessibili** ad altri soggetti non autorizzati



Altri obblighi del titolare: informativa (art. 13 del Decreto e 7 del Regolamento)

Non è obbligatoria se il trattamento avviene in base ad un obbligo di legge, ad un regolamento o alla normativa comunitaria

Può essere data all'interessato anche mediante affissione o depliant o moduli o volantini o su sito web



Altri obblighi del titolare (art. 37-41 del Decreto e 6, 8 del Regolamento)

I titolari devono provvedere agli adempimenti di notifica, comunicazione e richiesta di autorizzazione al Garante nei casi in cui questa sia necessaria

Per la Sanità il Decreto prevede disposizioni specifiche per il settore negli artt. 75 - 94



Diffusione incondizionata dei dati personali (art. 100 del Decreto e art. 10 del Regolamento)

Se l'interessato non si oppone (art. 7 c.4 del Decreto), si possono diffondere, anche a privati:

- i dati del personale anche cessato (nome e cognome, dati relativi alla carriera, produzione scientifica, attività di studio e ricerca, materie insegnate, sede di servizio con telefono o fax, struttura/organo collegiale di appartenenza.
- non si può diffondere lo stato matricolare, azioni di responsabilità davanti alla Corte dei Conti, ai procedimenti penali, disciplinari, inchieste ispettive, notizie relative al rendimento e all'efficienza.

Si possono diffondere dati statistici o comunque in forma anonima e aggregata (vedi anche Titolo V – capo III del Codice e Codice di Deontologia e buona Condotta del 16/4/2004)

Gli esiti degli esami possono essere diffusi mediante affissione di elenchi. La comunicazione via web è consentita solo all'interessato.



Diffusione condizionata dei dati personali (artt. 11 e 12 del Regolamento)

Se l'interessato non si oppone (art. 7 c.4 del Decreto), si possono diffondere, anche a privati:

- i dati degli studenti (compresi gli esiti finali ed intermedi), dei laureati e laureandi, borsisti, specializzandi, dottorandi, allievi corsi di formazione professionale per inviti ad incontri, manifestazioni, riunioni e congressi su tematiche connesse al mondo universitario e per inserimento professionale nel mondo del lavoro.

Le segreterie possono rilasciare certificati contenenti dati personali degli studenti o laureati, dietro presentazione (anche via fax) di delega con firma autenticata dell'interessato o senza firma autentica con documenti di identità in copia dell'interessato e del delegato (anche via fax).



Sanzioni (artt. 161 - 172 del Decreto)

Alcuni esempi:

- **Violazione informativa:**
 - da € 3000 a € 18.000 per dati personali
 - da €5.000 a € 30.000 per dati sensibili o giudiziari
- **mancata adozione misure minime:**
 - da € 10.000 a € 50.000 e arresto fino a 2 anni
- **trattamento illecito: reclusione da 6 a 36 mesi**