

DECRETO RETTORALE N. 271/2009 DEL 23.02.2009
TESTO UNICO SULLA PRIVACY E SULL'UTILIZZO DEI SISTEMI INFORMATICI

IL RETTORE

- Vista la legge 9 maggio 1989, n. 168;
- Vista la direttiva n. 95/46/CE del Parlamento Europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché della libera circolazione dei dati;
- Visto il decreto legislativo 30 giugno 2003, n. 196, recante il "Codice in materia di protezione dei dati personali", con particolare riferimento agli articoli 18, 20, 21, 22 e 181, comma 1, lett. a);
- Visto il decreto legge 27 luglio 2005, n. 144, convertito con modificazioni dalla legge 31 luglio 2005 n. 155 recante "Misure urgenti per il contrasto del terrorismo internazionale";
- Visto il decreto del 16 agosto 2005 recante "Misure di preventiva acquisizione di dati anagrafici dei soggetti che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso ad Internet utilizzando tecnologia senza fili, ai sensi dell'articolo 7, comma 4, del decreto-legge 27 luglio 2005, n. 144 convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155";
- Visto il provvedimento del Garante per la protezione dei dati personali del 30 giugno 2005 concernente il regolamento in materia di trattamento dei dati sensibili e giudiziari;
- Visto il provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007 concernente l'utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro (G.U. 10 marzo 2007 n. 58);
- Visto il provvedimento del Garante per la protezione dei dati personali del 14 giugno 2007 concernente le linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico (G.U. 13 luglio 2007 n. 161);
- Ravvisata la necessità, ai fini dell'attuazione degli articoli 20 e 21, del D.lgs. n. 196/2003, di identificare: i tipi di dati sensibili e giudiziari trattati nell'ambito delle attività dell'Università degli studi di Bologna; le finalità di rilevante interesse pubblico perseguite dal trattamento e le operazioni eseguite con gli stessi dati;
- Ritenuto di indicare sinteticamente le operazioni ordinarie che questa Università deve necessariamente svolgere per perseguire le finalità di rilevante interesse pubblico individuate per legge (operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione);
- Considerato che possono spiegare effetti maggiormente significativi per l'interessato le operazioni svolte, pressoché interamente mediante siti web, o volte a definire in forma completamente automatizzata profili o personalità di interessati, nonché le interconnessioni e i raffronti tra banche di dati gestite da diversi titolari, oppure i raffronti con altre informazioni, anche sensibili e giudiziarie, detenute dal medesimo titolare del trattamento, nonché infine la comunicazione dei dati a terzi;
- Ritenuto altresì di individuare analiticamente nelle schede allegate, con riferimento alle predette operazioni che possono spiegare effetti maggiormente significativi per l'interessato, quelle effettuate da questa Università: in particolare le operazioni di interconnessione, raffronto tra banche di dati gestite da diversi titolari, oppure con altre informazioni sensibili e giudiziarie detenute dal medesimo titolare del trattamento, nonché di comunicazione a terzi;
- Considerato che per quanto concerne tutti i trattamenti di cui sopra è stato verificato il rispetto dei principi e delle garanzie previste dall'art. 22 del Codice, con particolare riferimento alla pertinenza, non eccedenza e indispensabilità dei dati sensibili e giudiziari utilizzati rispetto alle finalità perseguite; all'indispensabilità delle predette operazioni per il perseguimento delle finalità di rilevante interesse pubblico individuate per legge, nonché all'esistenza di fonti normative idonee a rendere lecite le medesime operazioni o, ove richiesta, all'indicazione scritta dei motivi;
- Considerata l'attività specifica del Gruppo di lavoro CRUI-Università in materia di regolamento di dati sensibili e giudiziari;
- Visto lo schema tipo di regolamento sul trattamento dei dati sensibili e giudiziari predisposto dalla CRUI-Università in conformità al parere espresso dal Garante per la protezione dei dati personali, ai sensi dell'art. 154, comma 1, lett. g), del D.lgs. 30 giugno 2003, n. 196, in data 14 dicembre 2005;
- Verificata la rispondenza del presente Regolamento al predetto schema tipo e quindi la non necessità di

sottoporlo al preventivo parere del Garante;
Visto lo Statuto di Ateneo;
Visto le "Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione - verso una cultura della sicurezza" adottate sotto forma di Raccomandazione del Consiglio in occasione della 1037^a sessione del Consiglio dell'OCSE, il 25 luglio 2002;
Viste le "Linee Guida per la sicurezza ICT delle pubbliche amministrazioni" emanate dal CNIPA nel marzo 2006;
Visto il D.R. 21.05.1998 n. 182 Regolamento per l'utilizzo della rete scientifico-amministrativa di Ateneo (ALMAnet);
Visto il D.R. 5.11.2002 n. 435 con cui si sono recepiti i principi di legge in materia di trattamento dei dati personali;
Vista la deliberazione del Consiglio di Amministrazione assunta nella seduta del 20.12.2005 inerente all'approvazione del Regolamento sui dati sensibili e giudiziari (D.R. 26.04.2006 n. 3/111);
Quant'altro visto e considerato;

DECRETA

E' emanato il Testo Unico sulla Privacy e sull'Utilizzo dei Sistemi Informatici in allegato e facente parte integrante del presente decreto.

Bologna, 23.02.2009

Il Rettore
Pier Ugo Calzolari

Testo Unico sulla Privacy e sull'Utilizzo dei Sistemi Informatici

INDICE

Testo Unico sulla Privacy e sull'Utilizzo dei Sistemi Informatici	3
PARTE I. PRINCIPI E DISPOSIZIONI GENERALI	5
Art. 1. Oggetto	5
Art. 2. Ambito di applicazione	5
Art. 3. Finalità	5
Art. 4. Attività istituzionali	6
Art. 5. Definizioni	6
Art. 6. Politiche organizzative e responsabilità	7
PARTE II. DATI PERSONALI	7
TITOLO I. REQUISITI	7
Art. 7. Modalità del trattamento e requisiti dei dati	7
TITOLO II. ORGANIZZAZIONE E RESPONSABILITÀ	8
Art. 8. Titolare del trattamento	8
Art. 9. Responsabile del trattamento	8
Art. 10. Incaricati del trattamento	8
Art. 11. Trattamento di dati personali condivisi	8
Art. 12. Trattamenti di dati delegati a soggetti esterni	9
TITOLO III. ADEMPIMENTI	9
Art. 13. Notificazione delle banche dati	9
Art. 14. Obblighi di comunicazione	9
Art. 15. Sistemi di videosorveglianza e di controllo accessi	9
TITOLO IV. CIRCOLAZIONE, COMUNICAZIONE E DIFFUSIONE DEI DATI	10
Art. 16. Circolazione interna di dati	10
Art. 17. Richieste di comunicazione dei dati personali	10
Art. 18. Comunicazione e diffusione dei dati	10
Art. 19. Diffusione delle valutazioni d'esame	11
Art. 20. Diffusione dei risultati di concorsi e selezioni	11
Art. 21. Annuario	12
TITOLO V. DATI SENSIBILI, GIUDIZIARI E GENETICI	12
Art. 22. Trattamento di dati sensibili e giudiziari	12
Art. 23. Trattamento di dati sensibili e giudiziari per finalità di ricerca	13
Art. 24. Trattamento dei dati genetici	13
PARTE III. RETE, SERVIZI DI RETE E APPLICAZIONI INFORMATICHE	14
TITOLO I. PROFILI GENERALI	14
Art. 25. Principi generali	14
Art. 26. Autenticazione informatica e telematica	14
Art. 27. Obblighi dell'utente	14
Art. 28. Limiti d'uso	15
TITOLO II. RETE ALMANET	15
Art. 29. Rete ALMAnet	15
Art. 30. Misure tecniche di sicurezza	15
Art. 31. Gestione dell'infrastruttura della dorsale ALMAnet	16
TITOLO III. RESPONSABILITÀ	16
Art. 32. Organizzazione	16
Art. 33. Compiti del Responsabile di struttura	16
Art. 34. Compiti del Referente informatico	17

PARTE IV. CONTROLLI E SANZIONI	17
Art. 35. Controlli ammessi	17
Art. 36. Sanzioni	18
PARTE V. DISPOSIZIONI ABROGATIVE, INTEGRATIVE E NORME TRANSITORIE	18
Art. 37. Disposizioni abrogative	18
Art. 38. Disposizioni integrative	19
Art. 39. Norme transitorie	19
Art. 40. Entrata in vigore	19
Allegato A. DISCIPLINARE PER IL CORRETTO TRATTAMENTO DELLE CREDENZIALI ISTITUZIONALI	20
Art. 1. Utenti e convenzioni sui nomi	20
Art. 2. Obblighi inerenti alle password	20
Art. 3. Disattivazione delle credenziali istituzionali	20
Art. 4. Cancellazione delle credenziali	21
Art. 5. Autorizzazione a risorse informatiche	21
Allegato B. DISCIPLINARE IN MATERIA DI ACCESSO E UTILIZZO DELLA RETE E DEI SISTEMI INFORMATIVI D'ATENEO	23
PARTE I. IDENTIFICAZIONE DELL'UTENTE IN RETE	23
Art. 1. Validità dell'autorizzazione ad accedere alla rete ALMAnet	23
Art. 2. Accesso remoto alla Rete ALMAnet	23
PARTE II. MISURE TECNICHE E ORGANIZZATIVE	23
TITOLO I. RETI	23
Art. 3. Gestione degli indirizzi IP	23
Art. 4. Dynamic Host Configuration Protocol (DHCP) e NAT	24
TITOLO II. SERVIZI	24
Art. 5. Gestione e implementazione dei servizi di rete della propria struttura	24
Art. 6. Gestione dei domini internet locali	25
Art. 7. Utilizzo dei servizi wireless	25
Art. 8. Utilizzo di cartelle condivise e spazi di rete personali	25
Art. 9. Utilizzo postazioni di lavoro	26
Art. 10. Cancellazione di file e messaggi di un utente deceduto	26
TITOLO III. SICUREZZA E GESTIONE DEGLI INCIDENTI	27
Art. 11. Politiche di sicurezza sulla rete ALMAnet	27
Art. 12. Rilevazione delle intrusioni	27
Art. 13. Modalità di gestione degli incidenti	27
PARTE III. TRATTAMENTO DEI DATI DI TRAFFICO TELEMATICO	28
Art. 14. Ambito di trattamento	28
Art. 15. Modalità di conservazione	28
Allegato C. DISCIPLINARE PER L'UTILIZZO DELLA POSTA ELETTRONICA	29
PARTE I. PROFILI GENERALI SULL'UTILIZZO DELLA POSTA ELETTRONICA D'ATENEO	29
Art. 1. Oggetto e finalità	29
Art. 2. Soggetti utilizzatori del servizio di posta elettronica	29
Art. 3. Gestione tecnica del servizio	29
Art. 4. Interruzione servizio	30
Art. 5. Validità dei profili autorizzativi per l'uso del servizio di posta elettronica	30
PARTE II. UTILIZZO DELLE LISTE DI DISTRIBUZIONE	31
Art. 6. Principi generali	31

Art. 7. Autorizzazione all'uso delle liste	31
Art. 8. Controllo su liste di distribuzione	31

Allegato D. TRATTAMENTO DI DATI SENSIBILI E GIUDIZIARI	32
SCHEDA A	32
SCHEDA B	37
SCHEDA C	39
SCHEDA D	42

PARTE I. PRINCIPI E DISPOSIZIONI GENERALI

Art. 1. Oggetto

1. Il presente Testo Unico contiene i principi e le disposizioni in materia di trattamento dei dati personali e di sicurezza dell'informazione, utilizzo della rete ALMANET e dei servizi tramite essa erogati o usufruiti.

Art. 2. Ambito di applicazione

1. La persona fisica o giuridica che, nell'ambito delle attività istituzionali dell'Ateneo, tratta dei dati personali di titolarità dell'Università di Bologna, è soggetta alle prescrizioni contenute nel presente Testo Unico.

2. Chiunque, pur non trattando dati personali, accede alla rete informatica e telematica di Ateneo e/o utilizza i servizi tramite essa erogati o usufruiti è soggetto al rispetto dei principi e delle prescrizioni contenute nel presente Testo Unico.

3. Il presente Testo Unico, in attuazione del Codice in materia di protezione dei dati personali (art. 20, comma 2 e art. 21, comma 2, del D.lgs. 30 giugno 2003, n. 196), identifica, nell'art.22 e nell'Allegato D, le tipologie di dati sensibili e giudiziari, nonché le operazioni eseguibili per lo svolgimento delle finalità istituzionali dell'Università.

Art.3. Finalità

1. L'Ateneo svolge il trattamento dei dati personali per finalità istituzionali e nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

2. Nel rispetto dei predetti principi, l'Ateneo promuove l'utilizzo della rete e dei servizi tramite essa erogati o usufruiti.

3. Il trattamento dei dati, anche di quelli personali, mediante sistemi informatici e telematici risponde, in ottemperanza al principio di buon andamento dell'azione amministrativa, all'esigenza di dematerializzazione della documentazione cartacea attraverso la progressiva informatizzazione dei procedimenti dell'Ateneo. La rete ALMANet costituisce uno strumento tecnologico a supporto di tale azione di semplificazione e modernizzazione amministrativa.

4. L'Ateneo promuove un approccio metodologico alla tutela dei dati impegnandosi nella realizzazione di un proprio sistema di gestione della sicurezza delle informazioni al fine di assicurare il più elevato livello di protezione del patrimonio informativo dell'Ente. L'Ateneo si ispira agli standard internazionali e alle metodologie di analisi e gestione del rischio che considerano in modo integrato tutte le componenti della sicurezza dei dati – i dati stessi, le persone, le tecnologie e le procedure – e prevedono la definizione e il coordinamento delle politiche di sicurezza, l'analisi del rischio, l'implementazione di controlli e la verifica periodica dell'efficacia degli stessi.

Art. 4. Attività istituzionali

1. L'Università provvede al trattamento, alla diffusione e alla comunicazione dei dati nell'ambito del perseguimento dei propri fini istituzionali.
2. Ai fini del presente Regolamento, sono attività istituzionali tutte le attività di ricerca, di didattica, amministrative, di servizio e altre attività previste in convenzioni stipulate dall'Ateneo con soggetti pubblici o privati.
3. Rientrano tra le attività istituzionali anche le attività di informazione e di comunicazione istituzionale finalizzate a:
 - a. illustrare e favorire la conoscenza delle disposizioni normative e regolamentari d'Ateneo, al fine di facilitarne l'applicazione;
 - b. promuovere conoscenze allargate e approfondite su temi di rilevante interesse pubblico e sociale;
 - c. illustrare le attività dell'Ateneo e il loro funzionamento;
 - d. favorire l'accesso ai servizi d'Ateneo, promuovendone la conoscenza;
 - e. promuovere l'immagine delle strutture dell'Ateneo, conferendo conoscenza e visibilità ad eventi d'importanza locale, regionale, nazionale e internazionale.

Art.5. Definizioni

1. Ai fini del presente Regolamento si intende per:
 - a. "*rete ALMAnet*", l'insieme di tutte le infrastrutture e le apparecchiature che consentono il collegamento informatico e telematico all'interno dell'Ateneo;
 - b. "*Ateneo*" o "*l'Università*", l'Alma Mater Studiorum - Università di Bologna in tutte le sue articolazioni istituzionali e territoriali;
 - c. "*Ce.S.I.A.*", Centro per lo Sviluppo e Gestione dei Servizi Informatici di Ateneo, struttura dell'Università di Bologna dedicata alla gestione, manutenzione e sicurezza dei principali sistemi informativi d'Ateneo;
 - d. "*Responsabile di struttura*", Preside, Direttore, Dirigente o figura equivalente di ciascuna struttura di cui si compone l'Ateneo;
 - e. "*utente*", qualsiasi soggetto che acceda ai servizi informatici e/o alla Rete d'Ateneo;
 - f. "*Directory Service d'Ateneo (DSA)*", sistema di autenticazione e autorizzazione istituzionale dell'Alma Mater Studiorum - Università di Bologna;
 - g. "*file illegale*" o "*software illegale*", i file o i programmi che si pongono in contrasto a principi o prescrizioni sanciti dalla normativa vigente o dal presente regolamento;
 - h. "*dorsale ALMAnet*", l'insieme delle infrastrutture e delle apparecchiature che consentono il collegamento informatico e telematico tra le diverse sedi, nonché l'accesso alle reti telematiche esterne;
 - i. "*ccTLD*", country-code Top-Level Domains, domini DNS di primo livello costituiti da due lettere, designati per un determinato paese o territorio;
 - j. "*gTLD*", generic Top-Level Domains domini DNS di primo livello non riferiti a uno specifico territorio (Es: .edu, .int, .gov, .mil);
 - k. "*GARR*", il Consorzio di Gestione e Ampliamento delle Reti di Ricerca;
 - l. "*rete GARR*", la rete italiana della ricerca;
 - m. "*Referente informatico*", persona fisica con competenze tecniche preposta alla gestione e alla connessione in rete dei sistemi informatici appartenenti alla struttura;
 - n. "*NAT*", Network Address Translation, è una tecnica che consiste nel modificare gli indirizzi IP (di sorgente e/o di destinazione) dei pacchetti di una connessione in modo da presentare verso l'esterno uno o più indirizzi IP diversi da quelli originali;
 - o. "*C.S.S*", il Comitato Scientifico e di Sviluppo del Ce.S.I.A.;
 - p. "*CERT*", (Computer Emergency Response Team) Ce.S.I.A.: Servizio del Ce.S.I.A. che gestisce gli incidenti informatici;
 - q. "*APA*", Access Port Administrator, referente dell'Università di Bologna per l'interazione con la direzione del GARR;
 - r. "*liste opt-out*", liste di distribuzione basate sul principio secondo il quale l'utente che non vuole ricevere e-mail indesiderate ha la possibilità di far registrare questa sua preferenza tramite alcuni strumenti messi a disposizione dall'Ateneo;
 - s. "*liste opt-in*", liste di distribuzione basate sulla possibilità che l'utente decida se aderire o meno a una determinata lista.

Art.6. Politiche organizzative e responsabilità

1. Il Magnifico Rettore e gli Organi Accademici definiscono le politiche di sicurezza, da implementare a tutela dei dati personali e/o sancite dal presente Testo Unico, per gli specifici ambiti di competenza.
2. La scelta degli strumenti e delle soluzioni tecnologiche che consentono l'attuazione delle politiche di sicurezza di cui al comma 1 sono di competenza del Ce.S.I.A. quando l'attuazione di tali politiche dipende dall'infrastruttura della rete ALMAnet (wired e wireless) o dal servizio di connettività, dai sistemi di calcolo centrali di Ateneo (in merito alla gestione della server farm), dai servizi distribuiti fruibili da tutto il personale di Ateneo attraverso la rete ALMAnet (ne costituiscono un esempio la gestione dell'identità digitale e la posta elettronica). Le modalità di utilizzo delle suddette risorse, da parte di qualunque altro servizio informatico o da parte delle altre strutture dell'Ateneo, sono definite dal Ce.S.I.A.
3. Il Ce.S.I.A. effettua le scelte di cui al comma 2 in base a criteri di opportunità, convenienza economica, efficienza ed efficacia e ne dà la massima pubblicità fino a fornire un servizio di supporto a tutte le strutture organizzative di Ateneo che debbano conformarsi a tali scelte. Resta ferma, nel rispetto dei principi previsti dallo Statuto di Ateneo ed entro i limiti di cui all'art.25 comma 4, l'autonomia nella scelta degli strumenti e delle soluzioni tecnologiche più adeguate per i contenuti delle attività di ricerca e di formazione. Tale autonomia deve essere comunque temperata con le esigenze di corretto funzionamento dei sistemi informativi d'Ateneo.
4. Il Ce.S.I.A., tra i suoi compiti:
 - a. effettua attività di monitoraggio della sicurezza della rete e dei sistemi presenti sulla Rete ALMAnet, predisponendo annualmente una relazione sull'attività di monitoraggio svolta;
 - b. propone al Magnifico Rettore e agli Organi Accademici l'adozione di nuove politiche di sicurezza e l'attuazione di eventuali interventi correttivi a tutela di dati e sistemi informativi dell'Ateneo, anche sperimentando metodologie, modelli e sistemi nell'ambito delle finalità di cui all'3 comma 4;
 - c. rende note le scelte tecnologiche e organizzative adottate, anche mediante la pubblicazione sui siti d'Ateneo.
5. Nei casi in cui il Magnifico Rettore, anche a seguito delle attività di monitoraggio di cui al comma 4 lettera a) del presente articolo, rilevi una mancata aderenza a principi e prescrizioni del presente Regolamento da parte delle strutture dell'Ateneo, concorda con gli Organi Accademici, per gli ambiti di rispettiva competenza, l'adozione di eventuali interventi correttivi e ne dispone l'attuazione.

PARTE II. DATI PERSONALI

TITOLO I. REQUISITI

Art.7. Modalità del trattamento e requisiti dei dati

1. I sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in casi di necessità.
2. I dati personali oggetto di trattamento sono:
 - a. trattati in modo lecito e secondo correttezza;
 - b. raccolti e registrati per scopi determinati, espliciti e legittimi, e utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
 - c. esatti e, se necessario, aggiornati;
 - d. pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
 - e. conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

TITOLO II. ORGANIZZAZIONE E RESPONSABILITÀ

Art.8. Titolare del trattamento

1. L'Alma Mater Studiorum - Università di Bologna è Titolare dei dati personali, ivi compresi i dati contenuti nelle banche dati automatizzate o cartacee, detenuti dall'Università. L'Ateneo, in quanto Titolare, prende le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza.

Art.9. Responsabile del trattamento

1. Il Responsabile del trattamento è un soggetto, con adeguate competenze professionali, garante per la propria struttura del pieno rispetto delle disposizioni vigenti in materia di tutela dei dati personali e del presente Regolamento.

2. I Responsabili del trattamento dei dati personali sono individuati nei Responsabili delle strutture in cui si articola l'Ateneo.

3. Il Titolare, nella persona del Magnifico Rettore, può comunque designare, con proprio provvedimento e in deroga al comma 2, un Responsabile del trattamento dei dati diverso dai soggetti sopra indicati.

4. I compiti affidati al Responsabile del trattamento devono essere analiticamente specificati per iscritto.

5. Il Responsabile del trattamento predispone tutte le condizioni organizzative, logistiche e amministrative affinché i propri collaboratori operino conformemente a quanto disposto dalla normativa vigente e dal presente Regolamento.

6. Il Responsabile del trattamento ha l'obbligo di formare gli incaricati della propria struttura sia in relazione alle corrette modalità di trattamento dei dati che in relazione all'uso delle rete e dei servizi erogati coordinandosi con le Aree e i Servizi dell'Amministrazione Generale competenti.

Art.10. Incaricati del trattamento

1. Il Responsabile del trattamento nomina per iscritto gli incaricati che trattano i dati personali.

2. L'incaricato è tenuto ad attenersi alle istruzioni impartite dal Titolare o dal Responsabile.

3. Per i dati personali trattati nell'ambito delle attività di ricerca e di didattica, i docenti sono incaricati al trattamento dai Responsabili delle relative strutture di ricerca e di didattica per i dati di competenza.

Art.11. Trattamento di dati personali condivisi

1. Qualora due o più strutture dell'Ateneo operino utilizzando una stessa banca dati per finalità differenti, deve essere sottoscritto, dai rispettivi Responsabili di trattamento, in via preventiva, un documento in cui siano analiticamente esplicitate le proprie responsabilità sui dati rispetto alle operazioni di trattamento da loro effettuate.

2. Nel caso in cui queste responsabilità non siano state preventivamente individuate, ciascuna struttura si ritiene Responsabile della specifica operazione di trattamento di dati svolta coerentemente alle attività istituzionali che le sono state attribuite.

Art.12. Trattamenti di dati delegati a soggetti esterni

1. Nel caso di attività esternalizzate, il Titolare è tenuto a individuare le responsabilità connesse al trattamento dei dati personali affidate ai soggetti esterni, valutando l'opportunità di nominare tale soggetto quale incaricato o Responsabile esterno o, eventualmente, individuando una contitolarità nel trattamento.
2. Il Titolare esercita attività di vigilanza sull'attività di trattamento effettuata dal Responsabile esterno.
3. Il Responsabile esterno è tenuto a comunicare al Titolare la lista aggiornata dei propri incaricati al trattamento oggetto della nomina.

TITOLO III. ADEMPIMENTI

Art.13. Notificazione delle banche dati

1. Ciascuna struttura dell'Ateneo, nel rispetto delle misure minime previste dal D.Lgs. 196/03 e ai fini della compilazione del Documento Programmatico sulla Sicurezza, è tenuta a comunicare al Titolare, entro il 31 marzo di ogni anno:
 - a. la tipologia di dati personali trattati nell'ambito delle attività istituzionali della propria struttura, le finalità e le modalità del trattamento;
 - b. il luogo ove i dati sono custoditi e le categorie di interessati cui i dati si riferiscono;
 - c. le specifiche operazioni svolte sui dati, specificandone l'eventuale ambito di comunicazione o diffusione all'esterno;
 - d. gli eventuali trasferimenti di dati previsti verso Paesi non appartenenti all'Unione Europea o fuori dal territorio nazionale;
 - e. la descrizione delle misure di sicurezza adottate a tutela dei dati personali.

Art.14. Obblighi di comunicazione

1. Il Responsabile del trattamento, quando oggettivamente impossibilitato ad adottare in autonomia adeguate misure di protezione a tutela dei dati trattati, è tenuto a darne tempestiva comunicazione al Titolare che valuterà le possibili soluzioni tecnologiche e organizzative per adempiere alla normativa vigente.
2. Chiunque necessiti di trattare dei dati di titolarità dell'Ateneo per compiti o finalità che sono collaterali all'attività istituzionale o di dati che possono comportare rischi specifici per i diritti e le libertà dell'individuo, è tenuto a darne comunicazione preventiva al Titolare che decide in merito all'autorizzazione.

Art.15. Sistemi di videosorveglianza e di controllo accessi

1. Ciascuna struttura dell'Ateneo può adottare sistemi di videosorveglianza e di controllo accessi in particolari aree o attività soggette a concreti rischi e per le quali ricorra un'effettiva esigenza di deterrenza, al fine di migliorare la sicurezza all'interno degli edifici ove si svolgono le attività istituzionali proprie dell'Ente e allo scopo di tutelare il patrimonio universitario.
2. Non è consentito, nel pieno rispetto dello Statuto dei lavoratori, l'uso di impianti e apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.
3. È onere del Responsabile della struttura nella quale sono installati i sistemi di videosorveglianza e controllo accessi:
 - a. adottare le garanzie di cui all'Art. 4 della legge del 20 maggio 1970, n. 300;
 - b. garantire l'osservanza dei principi di necessità, finalità e proporzionalità del trattamento dei dati;
 - c. garantire il rispetto delle prescrizioni imposte dal Garante e, più in generale, dalla normativa vigente, anche in relazione all'utilizzo di particolari tecnologie e/o apparecchiature;
 - d. documentare adeguatamente le ragioni dell'installazione di tali sistemi in un atto autonomo ai fini dell'eventuale esibizione in occasione di visite ispettive, oppure dell'esercizio dei diritti dell'interessato o di contenzioso.

TITOLO IV. CIRCOLAZIONE, COMUNICAZIONE E DIFFUSIONE DEI DATI

Art. 16. Circolazione interna di dati

1. L'accesso ai dati personali da parte delle strutture e dei dipendenti dell'Università, comunque limitato ai casi in cui sia finalizzato al perseguimento dei fini istituzionali, è ispirato al principio della circolazione delle informazioni, secondo il quale l'Università provvede all'organizzazione delle informazioni e dei dati a sua disposizione mediante strumenti, anche di carattere informatico, atti a facilitarne l'accesso e la fruizione anche presso le strutture didattiche e di ricerca.
2. Ogni richiesta d'accesso ai dati personali da parte delle strutture e dei dipendenti dell'Università, debitamente motivata, può essere soddisfatta con riferimento ai soli dati essenziali per svolgere attività istituzionali.
3. Non si considera comunicazione la conoscenza dei dati personali da parte delle persone incaricate per iscritto di compiere le operazioni del trattamento dal Titolare o dal Responsabile e che operano sotto la diretta autorità di questi ultimi.

Art. 17. Richieste di comunicazione dei dati personali

1. Ogni richiesta, rivolta da soggetti privati all'Università, finalizzata a ottenere la comunicazione di dati personali deve essere scritta e motivata.
2. Al fine di ottenere la comunicazione dei dati, i soggetti privati presentano una richiesta scritta al Titolare indicando:
 - a. il nome, la denominazione o la ragione sociale del soggetto richiedente;
 - b. i dati ai quali la domanda si riferisce;
 - c. le finalità e le modalità di utilizzo dei dati richiesti;
 - d. l'eventuale ambito di comunicazione dei dati richiesti;
 - e. l'impegno a utilizzare i dati esclusivamente per le finalità per le quali sono stati richiesti e nell'ambito delle modalità indicate.
3. Le richieste provenienti da enti pubblici finalizzate alla comunicazione dei dati sono soddisfatte quando necessarie al perseguimento dei fini istituzionali dell'ente richiedente.

Art.18. Comunicazione e diffusione dei dati

1. Il Titolare del trattamento valuta eventuali richieste di comunicazione o diffusione di dati personali a soggetti terzi, sia pubblici che privati, e decide in ordine all'opportunità di concedere l'autorizzazione.
2. La comunicazione e la diffusione dei dati di natura non sensibile o giudiziaria da parte dell'Università sono permesse quando:
 - a. siano previste da norme di legge, di Regolamento o dalla normativa comunitaria;
 - b. siano necessarie per finalità di ricerca scientifica o di statistica e si tratti di dati anonimi o aggregati;
 - c. siano richieste per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati, con l'osservanza delle norme che regolano la materia;
 - d. siano necessarie per il soddisfacimento di richieste di accesso ai documenti amministrativi;
 - e. rientrino nelle attività di informazione e di comunicazione previste dalla legge 7 giugno 2000, n. 150.
3. L'Ateneo può comunicare ad altre pubbliche amministrazioni e diffondere, anche sui propri siti web, i dati costituiti dai nominativi del proprio personale, dei referenti e dei collaboratori, del ruolo ricoperto, dei recapiti telefonici e degli indirizzi telematici istituzionali, al fine di favorire la comunicazione istituzionale, consentendo la migliore rintracciabilità del personale e delle funzioni svolte.
4. L'Ateneo può comunicare al proprio personale, anche per via telematica mediante i propri siti web, per finalità di trasparenza, gli incentivi previsti per particolari responsabilità e ai ruoli ricoperti o collegati alla partecipazione a particolari progetti.
5. Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico nonché in relazione al principio di trasparenza cui si ispirano le pubbliche amministrazioni, l'Università può comunicare e diffondere, anche a privati e per via telematica, dati comuni relativi ad attività di studio e di ricerca, ivi compresi i dati delle valutazioni inerenti alle attività di ricerca dell'Ateneo.

6. L'Ateneo può comunicare e diffondere, anche per via telematica mediante i propri siti web, i dati relativi agli incarichi professionali e di collaborazione conferiti.

7. L'Ateneo può comunicare a enti pubblici e privati i dati necessari alla gestione del rapporto di lavoro, relativi al personale trasferito, comandato, distaccato o comunque assegnato in servizio a un ente diverso da quello di appartenenza.

8. L'Ateneo può comunicare a soggetti pubblici e privati i dati relativi al proprio personale, collaboratori e studenti, per consentire loro di fruire di agevolazioni e servizi. Al fine di favorirne l'integrazione nel territorio e nell'ambiente universitario, possono altresì essere comunicati i dati inerenti agli studenti di scambio a enti, istituti o associazioni.

9. L'Ateneo consente, su richiesta di soggetti privati e pubblici, la comunicazione e diffusione di dati ed elenchi riguardanti studenti, diplomati, laureandi e laureati, specializzati, borsisti, dottorandi, assegnisti, e altri profili formativi, al fine di favorirne le esperienze formative e professionali e l'eventuale collocazione nel mondo del lavoro; tale finalità deve essere dichiarata nella richiesta, affinché i dati siano utilizzati con le sole modalità per le quali sono stati comunicati e diffusi.

Art.19. Diffusione delle valutazioni d'esame

1. In ottemperanza ai principi contenuti nell'Art. 11 lettere d) ed e) del D.Lgs. 196/03 e ai principi di trasparenza cui l'Ateneo fa riferimento, è consentita all'Ateneo la pubblicazione dei dati inerenti alle valutazioni d'esame, anche sui propri siti web.

2. La pubblicazione di tali dati è consentita unicamente mediante la diffusione del numero di matricola dello studente e del voto conseguito.

3. Le valutazioni sono rese disponibili per un periodo di tempo non superiore a sei mesi.

Art.20. Diffusione dei risultati di concorsi e selezioni

1. In ottemperanza ai principi contenuti nell'Art. 11 lettere d) ed e) del D.Lgs. 196/03 e ai principi di trasparenza cui l'Ateneo fa riferimento, è consentito all'Ateneo la pubblicazione di esiti di prove concorsuali e selettive, anche sui propri siti web.

2. Per garantire la necessaria pubblicità di tali informazioni, la trasparenza delle procedure concorsuali e al contempo tutelare il diritto alla protezione dei dati personali dell'individuo, l'esito della selezione, quando pubblicato sui siti web d'Ateneo, deve essere accessibile ai soli partecipanti, salvo diverse disposizioni di legge.

3. Nel caso di diffusione delle valutazioni sui siti web d'Ateneo, tali informazioni sono pubblicate per un periodo di tempo non superiore a sei mesi.

Art.21. Annuario

1. L'Ateneo può procedere alla pubblicazione, anche su web, del proprio annuario. L'annuario, come previsto dal regio decreto 6 aprile 1924, n. 674, contiene:
 - a. l'elenco delle fondazioni, borse o assegni e le norme relative;
 - b. l'indicazione delle varie autorità accademiche;
 - c. l'elenco nominativo dei docenti e ricercatori con l'eventuale indicazione dei relativi insegnamenti e del settore scientifico-disciplinare;
 - d. il sommario dei corsi che durante l'anno accademico sono tenuti dai docenti;
 - e. il calendario scolastico e gli orari dei singoli corsi;
 - f. l'elenco nominativo del personale tecnico-amministrativo;
 - g. le statistiche, redatte in forma aggregata e anonima, dei laureati dell'anno accademico precedente e degli studenti iscritti in ciascuna facoltà, con indicazione dell'anno di corso;
 - h. tutti gli altri dati statistici relativi al funzionamento dell'Università;
 - i. l'elenco delle pubblicazioni fatte dai docenti, ricercatori, assegnisti, dottorandi, borsisti, laureati frequentatori e studenti nell'anno accademico precedente.

TITOLO V. DATI SENSIBILI, GIUDIZIARI E GENETICI

Art.22. Trattamento di dati sensibili e giudiziari

1. Il presente regolamento, in attuazione delle disposizioni di cui all'art. 20, comma 2, e 21, comma 2, del D.lgs. 30 giugno 2003, n. 196, riproduce nelle schede di cui all'allegato D, che formano parte integrante del Regolamento, i tipi di dati sensibili e giudiziari per i quali è consentito il relativo trattamento da parte degli Uffici e delle Strutture dell'Università, nonché le operazioni eseguibili in riferimento alle specifiche finalità di rilevante interesse pubblico perseguite nei singoli casi ed espressamente elencate nella Parte II del D.lgs. n. 196/2003 (artt. 62-73, 86, 95, 98 e 112).
2. Ai sensi dell'art. 22, del D.lgs. n. 196/2003, in relazione alla identificazione effettuata, è consentito il trattamento dei soli dati sensibili e giudiziari indispensabili per svolgere le attività istituzionali, previa verifica della loro pertinenza e completezza, ferma restando l'inutilizzabilità dei dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali secondo quanto disposto dall'art. 11 del D.lgs. n. 196/2003. Qualora l'Università, nell'espletamento della propria attività istituzionale, venga a conoscenza, ad opera dell'interessato o, comunque, non a richiesta dell'Ateneo, di dati sensibili o giudiziari non indispensabili allo svolgimento dei fini istituzionali sopra citati, tali dati, ai sensi degli artt. 11 e 22 del D.lgs. n. 196/2003, non potranno essere utilizzati in alcun modo, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.
3. Le operazioni di interconnessione, raffronto e comunicazione individuate nel presente regolamento sono ammesse soltanto se indispensabili allo svolgimento degli obblighi o compiti di volta in volta indicati, per il perseguimento delle rilevanti finalità di interesse pubblico specificate e nel rispetto delle disposizioni rilevanti in materia di protezione dei dati personali, nonché degli altri limiti stabiliti dalla legge e dai regolamenti. I raffronti e le interconnessioni con altre informazioni sensibili e giudiziarie detenute dall'Università sono consentite soltanto previa verifica della loro stretta indispensabilità nei singoli casi ed indicazione scritta dei motivi che ne giustificano l'effettuazione. Le predette operazioni, se effettuate utilizzando anche di dati di diversi titolari del trattamento, sono ammesse esclusivamente previa verifica della loro stretta indispensabilità nei singoli casi e nel rispetto dei limiti e con le modalità stabiliti dalle disposizioni legislative che le prevedono (art. 22 del D.lgs. n. 196/2003).
4. A tal fine, ed in relazione alle finalità di rilevante interesse pubblico previste dal D.lgs. 196/2003, sono identificate quattro macro categorie recanti le seguenti denominazioni dei trattamenti:
 - A - Gestione del rapporto di lavoro del personale docente, dirigente, tecnico-amministrativo, dei collaboratori esterni e dei soggetti che intrattengono altri rapporti di lavoro diversi da quello subordinato;
 - B - Attività di ricerca scientifica;
 - C - Attività didattica e gestione delle iscrizioni e delle carriere degli studenti;
 - D - Gestione del contenzioso giudiziale, stragiudiziale e attività di consulenza.

5. Per ciascuna di queste categorie di trattamento è redatta una scheda che specifica:

A - denominazione del trattamento;

B - indicazione del trattamento, descrizione riassuntiva del contesto;

C - principali fonti normative legittimanti il trattamento. In relazione a tali fonti ogni successiva modifica o integrazione legislativa sarà automaticamente da intendersi come recepita, sempre che non modifichi i tipi di dati trattati e le operazioni effettuate in relazione alle specifiche finalità perseguite;

D - rilevanti finalità di interesse pubblico perseguite dal trattamento;

E - tipi di dati trattati;

F - operazioni eseguibili, distinguendo fra il trattamento "ordinario" dei dati (raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione) e particolari forme di trattamento (interconnessione e raffronto di dati, comunicazione e diffusione).

Art.23. Trattamento di dati sensibili e giudiziari per finalità di ricerca

1. I coordinatori di un'attività di ricerca scientifica o statistica nella quale sono trattati dei dati sensibili è tenuto a fornire preventivamente al Titolare e al Responsabile di trattamento della propria struttura di appartenenza una comunicazione contenente:

a. il nome dei soggetti coinvolti nel progetto;

b. la tipologia di dati trattati;

c. le finalità e le modalità di utilizzo dei dati richiesti;

d. le misure di sicurezza adottate a tutela dei dati;

e. l'eventuale ambito di comunicazione dei dati richiesti;

f. l'impegno a utilizzare i dati esclusivamente per le finalità per le quali sono stati richiesti e nell'ambito delle modalità indicate.

Art.24. Trattamento dei dati genetici

1. Il trattamento di dati genetici per attività di ricerca scientifica e statistica è consentito quando conforme alle disposizioni del d.lgs. 196/03 e alle regole dettate dall'Autorità Garante per la protezione dei dati personali.

2. Il coordinatore di progetti di ricerca nei quali sono utilizzati anche dati genetici presenta, preventivamente all'inizio dell'attività, adeguata comunicazione, al Titolare e al Responsabile del trattamento dati, in merito a:

a. il nome dei ricercatori coinvolti nel progetto;

b. la tipologia di dati trattati;

c. le finalità e le modalità di utilizzo dei dati richiesti;

d. le misure di sicurezza adottate a tutela dei dati;

e. l'eventuale ambito di comunicazione dei dati richiesti;

f. l'impegno a utilizzare i dati esclusivamente per le finalità per le quali sono stati richiesti e nell'ambito delle modalità indicate.

3. Il Titolare è tenuto a chiedere l'autorizzazione al Garante per le attività che richiedono la disponibilità di dati genetici.

PARTE III. RETE, SERVIZI DI RETE E APPLICAZIONI INFORMATICHE

TITOLO I. PROFILI GENERALI

Art.25. Principi generali

1. Tutti i servizi informatici e telematici, la posta elettronica, nonché le applicazioni rese disponibili dall'Ateneo, sono da considerarsi strumento di lavoro per tutto il personale dell'Ateneo, nonché un mezzo per favorire la dematerializzazione dei procedimenti amministrativi e la comunicazione interna ed esterna all'Ateneo.
2. L'utilizzo della rete ALMANet, dei servizi e delle applicazioni informatiche d'Ateneo è consentito esclusivamente nell'ambito dei fini istituzionali dell'Ateneo.
3. Tutte le applicazioni e i sistemi di posta elettronica, ivi compresi quelli gestiti localmente dalle strutture d'Ateneo, devono essere conformi alle disposizioni di legge e a quelle contenute nel presente Testo Unico.
4. Ciascuna struttura può attivare nuovi servizi informatici locali nel rispetto di quanto definito all'Art. 5 dell'Allegato B e tenuto conto dei servizi informatici resi disponibili dal Ce.S.I.A. o da altre strutture d'Ateneo che sono istituzionalmente preposte a erogarli.
5. L'utente non può opporsi, se non per motivi legittimi, alla ricezione di comunicazioni per fini istituzionali. La legittimità di tali motivi è valutata dal Rettore o da un suo delegato.

Art.26. Autenticazione informatica e telematica

1. L'accesso alla rete, ai servizi di rete e alle applicazioni informatiche dell'Ateneo, da parte degli utenti, avviene mediante l'utilizzo delle credenziali di autenticazione appositamente attribuite mediante il Directory Service d'Ateneo o altri dispositivi di identificazione forniti dal Ce.S.I.A., definiti "credenziali istituzionali".
2. La struttura che renda disponibile agli utenti eventuali applicazioni, servizi o connettività alla rete ALMANet assicura che gli utenti si identifichino secondo quanto indicato al comma 1 del presente articolo e utilizzino, come sistema unitario di identificazione e autorizzazione informatica e telematica, le credenziali istituzionali.
3. Eventuali eccezioni al comma 2 sono valutate, anche per periodi limitati, in accordo con il Ce.S.I.A.
4. La struttura di cui al comma 3 garantisce, con mezzi propri, l'ottemperanza alle misure minime di sicurezza previste dal Codice Privacy (D.Lgs. 196/03) e, più in generale, alla normativa vigente.
5. Le credenziali istituzionali sono personali, non cedibili e utilizzabili esclusivamente dal proprietario.
6. Le credenziali istituzionali possono essere attribuite anche a utenti temporanei mediante gli strumenti individuati e messi a disposizione dal Ce.S.I.A.
7. Le credenziali istituzionali non possono essere assegnate ad altri incaricati, neppure in tempi diversi.

Art.27. Obblighi dell'utente

1. L'utente è pienamente responsabile delle proprie attività e dei dati trasmessi e/o resi pubblici mediante l'uso delle credenziali istituzionali a lui associate.
2. L'utente è tenuto a conservare segretamente la propria password, a non cederla a terzi e a non lasciare sessioni di lavoro aperte e incustodite.
3. È fatto obbligo all'utente, tra l'altro, di segnalare al Ce.S.I.A. l'abuso o un eventuale sospetto abuso di utilizzo delle proprie credenziali.

Art.28. Limiti d'uso

1. In relazione a quanto disposto in via generale dall'Art. 25 comma 2, è vietato, a titolo esemplificativo, usare la rete, i servizi e le applicazioni dell'Ateneo:

- a. per scopi che violino le leggi penali, civili e amministrative in materia di disciplina delle attività e dei servizi svolti sulla rete;
- b. per scopi che siano in contrasto con quanto previsto dalla AUP (Acceptable Use Policy del GARR) e dai regolamenti della rete GARR;
- c. per scopi e/o attraverso modalità contrastanti con il presente Testo Unico;
- d. per qualsiasi tipo di uso commerciale non inerente all'attività istituzionale compiuta;
- e. per attività che danneggiano l'immagine e il buon nome dell'Ateneo;
- f. per compiere atti che violino la riservatezza altrui;
- g. per attività che violino le leggi a tutela delle opere dell'ingegno e dei diritti di autore (tra cui trasferimenti illeciti di software, basi di dati, filmati, musica etc.);
- h. per attività non istituzionali che influenzino negativamente la regolare operatività della rete o ne limitino l'utilizzo e le prestazioni per gli altri utenti;
- i. per conseguire l'accesso non autorizzato a risorse di rete interne o esterne all'Ateneo;
- j. per attività che distruggano risorse (persone, capacità, elaboratori) dall'utilizzo cui sono state destinate;
- k. in modo anonimo o utilizzando risorse che consentano tale uso.

2. L'utente non può svolgere inoltre attività che possano recar danno o pregiudizio all'Università o a terzi. A titolo esemplificativo, non è consentito utilizzare le rete e i servizi tramite essa erogati o usufruiti per finalità inerenti alla comunicazione e/o diffusione di:

- a. pubblicità di prodotti e/o servizi manifesta o occulta;
- b. propaganda elettorale nazionale o internazionale, salvo quanto previsto all'Art. 7 comma 2 lettera d) dell'Allegato C;
- c. messaggi di carattere commerciale privato;
- d. altri contenuti contrari o non conformi alla legge e alle attività istituzionali dell'Ateneo.

3. Eventuali deroghe ai commi 1 e 2 del presente articolo possono essere autorizzate, per brevi periodi, dal Magnifico Rettore esclusivamente per finalità di ricerca o didattica, agendo nei limiti o nell'osservanza della legge.

TITOLO II. RETE ALMANET

Art.29. Rete ALMAnet

1. La rete ALMAnet rappresenta un servizio fornito all'utenza scientifica, didattica e amministrativa, le cui modalità di utilizzo sono regolate dal presente Testo Unico e dagli allegati A, B, C e D.

2. La rete ALMAnet è connessa alla rete GARR e, tramite quest'ultima, a Internet. Pertanto l'uso delle risorse e dei servizi di Internet tramite la rete d'Ateneo è subordinato al rispetto da parte degli utenti delle norme tecniche dettate dagli organi del GARR.

3. Ogni struttura collegata alla rete ALMAnet non può essere connessa a reti di altri provider o di organizzazioni esterne, salvo casi eccezionali espressamente autorizzati dal Ce.S.I.A., che ne verifica la congruenza con le politiche di routing e di sicurezza dell'Ateneo e compatibilmente con il parere espresso dagli Organi dell'Ateneo preposti.

Art.30. Misure tecniche di sicurezza

1. Conformemente a quanto stabilito nel presente Testo Unico e compatibilmente con le risorse finanziarie e di personale disponibili, il Ce.S.I.A. deve, a titolo esemplificativo:

- a. garantire la fornitura e la funzionalità dei servizi essenziali di rete;
- b. garantire lo sviluppo e la gestione di ALMAnet, conformemente alle delibere accademiche e alle indicazioni del C.S.S.;

- c. implementare le misure tecniche a protezione dei collegamenti verso l'esterno e della dorsale ALMAnet;
- d. disporre le misure tecniche che le strutture e/o gli utenti devono adottare al fine di garantire il miglior funzionamento della rete e dei servizi;
- e. assistere le strutture nell'adozione delle misure tecniche affinché siano applicate ed applicabili;
- f. promuovere accordi e/o convenzioni di collaborazione con centri, associazioni, istituti, enti scientifici e terze parti interessati allo sviluppo e all'utilizzo di ALMAnet.

Art.31. Gestione dell'infrastruttura della dorsale ALMAnet

1. La politica e la gestione del routing sono di competenza esclusiva del Ce.S.I.A., così come la gestione delle reti TCP/IP (Internet) dell'Ateneo e delle relative sottoreti, del dominio DNS di secondo livello "unibo.it" e dei relativi sottodomini, del monitoraggio della dorsale ALMAnet.

TITOLO III. RESPONSABILITÀ

Art. 32. Organizzazione

1. Fatto salvo quanto previsto al comma 3 per le Aree dell'Amministrazione Generale, ciascuna struttura dell'Ateneo è dotata di almeno un Referente informatico i cui compiti sono esplicitati nell'Art.34; se opportuno, un Referente può essere designato anche a servizio di più strutture.
2. Nei casi in cui una struttura non si possa avvalere di un Referente informatico verrà supportata in una prima fase dal Ce.S.I.A. che, in un'ottica di progetto, ne metterà in sicurezza i sistemi informativi. Terminata tale fase transitoria, verrà individuato dall'Ateneo un Referente informatico al quale sarà affidata completamente la gestione dell'infrastruttura dei servizi informatici della struttura in oggetto.
3. Le Aree dell'Amministrazione Generale sono supportate dal Ce.S.I.A. per gli aspetti tecnici e tecnologici.
4. Nel caso in cui più strutture siano coordinate per gli aspetti informatici da un'unica unità organizzativa, anche per esigenze di dislocazione territoriale, in coerenza con il modello Multicampus, il Responsabile di tale unità garantisce l'assolvimento dei compiti attribuiti al Referente Informatico, di cui all'Art.34, per tutte le strutture rappresentate. Ne costituiscono un esempio i Responsabili delle Aree dei Servizi Informatici dei Poli Scientifico-Didattici della Romagna.
5. L'unità di cui al comma 4 può essere coinvolta dal Ce.S.I.A. in progetti sulla sicurezza informatica di importanza strategica per l'Ateneo, al fine di collaborare nella definizione delle politiche e delle scelte tecnologiche che contribuiscano alla definizione di un sistema globale d'Ateneo per la gestione della Sicurezza dell'Informazione, anche partecipando attivamente allo studio ed alla realizzazione di nuovi servizi.
6. Il Referente informatico è individuato nel Responsabile dei servizi informatici della struttura ove questo ruolo sia formalmente previsto.

Art.33. Compiti del Responsabile di struttura

1. Il Responsabile di Struttura, compatibilmente con le risorse a sua disposizione, nell'ambito delle sue funzioni:
 - a. è garante, all'interno della propria struttura, dell'applicazione delle misure di sicurezza definite dalla normativa vigente e delle prescrizioni del presente Testo Unico;
 - b. appronta le misure derivanti dalle scelte politiche, tecnologiche e organizzative definite in Ateneo;
 - c. nomina uno o più referenti informatici per la propria struttura, salvo il caso in cui tale attività sia già stata esaurita implicitamente nelle circostanze di cui all'art. 32 comma 6;
 - d. predispone tutte le condizioni organizzative, logistiche e amministrative affinché i propri collaboratori possano svolgere efficacemente il proprio compito, ivi compresa la formazione e l'aggiornamento degli amministratori dei servizi informatici erogati dalla struttura;
 - e. rende noto il presente Testo Unico agli utenti della propria struttura e, se necessario, stabilisce ulteriori disposizioni per i servizi con validità interna alla struttura, conformemente ai regolamenti d'Ateneo e a quanto stabilito dalla normativa vigente;

f. nel caso di variazioni organizzative, comunica tempestivamente al Ce.S.I.A. il nominativo dei referenti informatici;

g. comunica al Ce.S.I.A., entro il 15 febbraio di ogni anno, tutte le informazioni relative all'organizzazione della gestione dei servizi informatici erogati dalla struttura, in particolare i riferimenti delle persone con funzioni di amministrazione dei servizi di rete.

2. Il Responsabile di struttura, previa valutazione dell'opportunità e della necessità e sentito il parere del Referente Informatico, può autorizzare un soggetto ad amministrare la propria postazione di lavoro e delegare a lui le responsabilità del corretto uso e funzionamento della postazione, dandone adeguata comunicazione al Referente Informatico e al Ce.S.I.A. L'utente a cui è stata delegata la gestione della propria postazione di lavoro, sottoscrive un modulo di presa di responsabilità e garantisce, a seguito di segnalazione del Referente Informatico, l'intervento per la risoluzione dei problemi e incidenti informatici nei tempi e nelle modalità di cui all'Art. 12 dell'Allegato B.

Art. 34. Compiti del Referente informatico

1. Il Referente informatico tra i suoi compiti:

a. riferisce al proprio Responsabile di Struttura eventuali attività, in essere o da adottare, per mettere in sicurezza la propria struttura, anche in riferimento a eventuali collaborazioni con il Ce.S.I.A.;

b. opera secondo le direttive e le procedure stabilite dal Ce.S.I.A. per quanto concerne il corretto uso e funzionamento dei sistemi informativi d'Ateneo, delle infrastrutture tecnologiche e l'implementazione di adeguate misure di sicurezza informatica;

c. controlla, sotto il profilo tecnico, ogni Sistema in Rete e i Servizi relativi alle strutture di sua competenza e si riferisce al Ce.S.I.A. per ogni violazione o sospetto di violazione della sicurezza informatica e/o al presente Testo Unico;

d. adotta compatibilmente con le risorse a sua disposizione, tutte le misure idonee per prevenire l'utilizzo illecito della rete e dei servizi di rete salvaguardando opportunamente le reti locali, i server e le postazioni di lavoro ed effettuando il monitoraggio delle proprie reti locali;

e. rappresenta l'interfaccia della struttura verso il Ce.S.I.A. regolando i flussi di comunicazione tra la struttura e il Ce.S.I.A.;

f. comunica al Ce.S.I.A. tutte le informazioni relative all'infrastruttura e all'architettura dei servizi informatici erogati dalla struttura;

g. risolve tempestivamente gli incidenti di sicurezza segnalati dal CERT del Ce.S.I.A. nei tempi previsti dai Regolamenti GARR e secondo le modalità indicate nel presente Testo Unico;

h. qualora nell'ambito delle ordinarie attività di gestione dei sistemi informativi di competenza, rilevi file illegali o dal contenuto palesemente non istituzionale provvede a darne segnalazione al proprio Responsabile di Struttura.

PARTE IV. CONTROLLI E SANZIONI

Art. 35. Controlli ammessi

1. Il Ce.S.I.A. o altri soggetti delegati dal Titolare hanno facoltà di effettuare controlli, anche preventivi, sul corretto uso e funzionamento degli strumenti informatici nel rispetto dei diritti e delle libertà fondamentali dei lavoratori o dei soggetti esterni che utilizzano strumenti informatici dell'Ateneo al fine di evitare usi impropri della rete o dei servizi di rete messi a disposizione dall'Ateneo.

2. Possono essere effettuati controlli automatizzati sul traffico di rete volti a inibire l'accesso a siti o categorie di siti di palese natura non istituzionale.

3. I controlli sulle attività svolte mediante utilizzo dei sistemi informatici sono ammessi nei seguenti casi:

a. quando previsti da fonte normativa o regolamentare;

b. nel caso in cui si verificano eventi dannosi o situazioni di pericolo non impediti da preventivi accorgimenti tecnici;

c. su segnalazione dell'Autorità Giudiziaria;

- d. quando, per ragioni di continuità del servizio, sia indispensabile reperire dei file o dei messaggi di un lavoratore, secondo le modalità di cui al comma 5 del presente articolo;
 - e. nel caso in cui, nell'ambito delle ordinarie attività di gestione dei sistemi informativi di competenza, siano rilevati file illegali o dal contenuto palesemente non istituzionale;
 - f. nell'ambito di controlli saltuari a campione per le finalità di cui al comma 1.
4. Nei casi in cui, a seguito di un controllo, si rilevino comportamenti illegali o non istituzionali, il Ce.S.I.A. o altri soggetti delegati dal Titolare potranno intervenire valutando se:
- a. inviare avvisi collettivi o individuali in cui verranno segnalati i comportamenti non corretti;
 - b. rimuovere i file, senza alcun preavviso all'utente, nei casi in cui i file possano limitare l'utilizzo di risorse o possano recar danno all'Ateneo;
 - c. inibire l'accesso a siti o categorie di siti di palese natura non istituzionale;
 - d. informare, nei casi in cui i comportamenti non corretti si ripetano nel tempo o risultino particolarmente gravi, il Magnifico Rettore o il Direttore Amministrativo, per i rispettivi ambiti di competenza, che adotteranno i provvedimenti più opportuni di cui all'Art. 36.
5. Il Responsabile di struttura, in caso di assenza prolungata di un lavoratore, anche quando dovuta al termine del periodo di collaborazione con l'Ateneo, e al fine di garantire la continuità lavorativa, chiede al Ce.S.I.A. di reperire i file di interesse per l'Ateneo giustificando adeguatamente i motivi della richiesta e informando per conoscenza il proprio lavoratore presso la propria residenza/domicilio eletto per le comunicazioni.

Art. 36. Sanzioni

1. I comportamenti in violazione della normativa vigente e del presente Testo Unico che hanno una rilevanza disciplinare, fermi restando i diversi profili di responsabilità civile e penale, saranno sanzionati secondo le forme e le modalità previste dai rispettivi ordinamenti del personale coinvolto.
2. Tali comportamenti sono segnalati al Rettore o al Direttore Amministrativo che valuteranno le modalità di intervento più idonee, anche a tutela di eventuali danni economici e/o di immagine subiti dall'Ateneo.
3. Salvo quanto previsto nell'Art. 12 dell'Allegato B, nel caso di necessità e di urgenza e al fine di evitare compromissioni al normale funzionamento della rete o porre termine ad attività contrarie alla normativa vigente o al presente Testo Unico, il Direttore del Ce.S.I.A. potrà disporre con proprio atto la sospensione temporanea dell'accesso alla Rete ALMAnet o ai servizi, a un utente o a un gruppo di utenti, fino alla rimozione delle cause che hanno originato il problema.

PARTE V. DISPOSIZIONI ABROGATIVE, INTEGRATIVE E NORME TRANSITORIE

Art. 37. Disposizioni abrogative

1. Dalla data di entrata in vigore del presente codice sono sostituiti integralmente i seguenti regolamenti:
 - a. Regolamento per la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, in attuazione dell'Art. 27 della legge 31/12/1996, n. 675 emanato con Decreto Rettorale n. 435 del 5 novembre 2002
 - b. Regolamento per l'utilizzo della rete scientifico-amministrativa di Ateneo (ALMAnet) emanato con Decreto Rettorale n. 182 del 21 maggio 1998;
 - c. Regolamento sui dati sensibili e giudiziari emanato con Decreto Rettorale n. 3/111 del 26 aprile 2006.

Art.38. Disposizioni integrative

1. Sono da considerarsi parte integrante al presente Testo Unico i seguenti documenti:
 - ALLEGATO A. Disciplinare per il corretto uso delle credenziali
 - ALLEGATO B. Disciplinare tecnico in materia di accesso e utilizzo della rete dell'Università
 - ALLEGATO C. Disciplinare per l'utilizzo della posta elettronica
 - ALLEGATO D. Trattamenti di dati sensibili e giudiziari ammessi in Ateneo.

Art. 39. Norme transitorie

1. Le strutture dell'Ateneo devono adeguarsi agli obblighi previsti dagli artt. 19 e 20 entro diciotto mesi dall'entrata in vigore del presente Testo Unico.
2. Le strutture dell'Ateneo devono adeguarsi agli obblighi previsti dall'art. 26 entro diciotto mesi dall'entrata in vigore del presente Testo Unico.
3. Le informazioni richieste all'Art. 33 comma g) devono essere comunicate al Ce.S.I.A., per la prima volta, entro due mesi dall'entrata in vigore del presente Testo Unico.
4. Le credenziali nella forma di cui all'Art. 1 comma 3 dell'Allegato A sono rese disponibili entro tre mesi dall'entrata in vigore del presente Testo Unico.
5. Le disposizioni previste dall'Art. 3 dell'Allegato A devono essere attuate entro tre mesi dalla data di entrata in vigore del presente Testo Unico.
6. Le disposizioni previste dall'Art. 4 dell'Allegato A devono essere attuate entro nove mesi dalla data di entrata in vigore del presente Testo Unico.
7. Le disposizioni di cui all'Art. 2 comma 2 Allegato B devono essere attuate entro sei mesi dalla data di entrata in vigore del presente Testo Unico.
8. Le strutture che utilizzano indirizzi IP delle classi di cui all'Art. 3 commi 3 e 4 Allegato B per indirizzamento privato facendo uso della tecnica di NAT devono passare all'indirizzamento di cui al comma 5 dello stesso articolo entro nove mesi dall'entrata in vigore dello stesso Testo Unico.
9. Le strutture di Ateneo che utilizzino, di fatto, indirizzi IP della classe di cui all'Art. 3 comma 3 Allegato B e che vogliano mantenerne l'uso, devono verificare con il Ce.S.I.A., entro tre mesi dall'entrata in vigore del presente Testo Unico, la possibilità di assegnazione. Non possono comunque essere in alcun modo utilizzate tecniche di NAT all'interno della rete ALMAnet per nascondere l'utilizzo di tali indirizzi IP. In ogni caso, il tempo per l'adeguamento alle prescrizioni di cui al presente Testo Unico è di nove mesi dalla sua entrata in vigore.
10. Le disposizioni previste dall'Art. 4 dell'Allegato B devono essere attuate entro nove mesi dalla data di entrata in vigore del presente Testo Unico.
11. Le disposizioni previste dall'Art. 5 dell'Allegato C devono essere attuate entro tre mesi dalla data di entrata in vigore del presente Testo Unico.

Art. 40. Entrata in vigore

1. Il presente Testo Unico entra in vigore dalla data di pubblicazione del Bollettino Ufficiale d'Ateneo.

Allegato A. DISCIPLINARE PER IL CORRETTO TRATTAMENTO DELLE CREDENZIALI ISTITUZIONALI

Art. 1. Utenti e convenzioni sui nomi

1. Le credenziali istituzionali, salvo casi di omonimia, possono essere fornite nella forma *nome.cognome@unibo.it* alle seguenti categorie di soggetti:
 - a. Personale docente, ricercatore e tecnico amministrativo;
 - b. Dottorandi, Borsisti, assegnisti, stagisti o altri soggetti titolari di contratti di ricerca o di didattica;
 - c. Collaboratori e consulenti titolari di un contratto con l'Ateneo;
 - d. Altre forme di collaborazione in cui l'attività lavorativa sia prevalentemente svolta presso l'Ateneo.
2. Le credenziali sono fornite, inoltre, nella forma *nome.cognome@studio.unibo.it* a:
 - a. Iscritti a corsi di studio dell'Ateneo ed ex-studenti dell'Ateneo;
 - b. Studenti stranieri di scambio;
 - c. Preimmatricolati;
3. Sono altresì fornite credenziali d'autenticazione nella forma *nome.cognome@esterni.unibo.it*, o in altra forma definita dal Ce.S.I.A., a:
 - a. Referenti di enti, associazioni o società esterne che collaborano a qualunque titolo con l'Ateneo e che abbiano necessità di accedere ad alcuni servizi offerti dai sistemi informativi dell'Ateneo;
 - b. Ospiti dell'Ateneo di Bologna per convegni, periodi di studio, etc. che abbiano necessità di accedere ad alcuni servizi offerti dai sistemi informativi dell'Ateneo.
4. Per scopi di mera gestione tecnica e accesso a servizi informatici da parte di altre applicazioni informatiche sono fornite credenziali, dette di servizio, nella forma *descrizionebreveutente.acronimoservizioacceduto-tipologiaservizioacceduto@unibo.it*.
5. Nelle credenziali indicate ai commi precedenti, il prefisso «nome.cognome» può subire aggiustamenti per motivi organizzativi (es.: casi di omonimia) o tecnici (es.: eccessiva lunghezza del nome o del cognome rispetto agli standard informatici), salvaguardando, in ogni caso, la piena riconoscibilità del soggetto.
6. Eventuali deroghe alle convenzioni sui nomi devono essere concordate con l'Ufficio Dirigenziale Direzione Cultura e Comunicazione Istituzionale dell'Ateneo, compatibilmente con eventuali vincoli tecnologici.
7. Il Ce.S.I.A. valuta l'opportunità di assegnazione di altre tipologie di account per particolari esigenze organizzative e/o tecniche.

Art. 2. Obblighi inerenti alle password

1. È fatto obbligo all'utente di:
 - a. utilizzare password composte da almeno otto caratteri alfanumerici e simboli speciali, non contenenti riferimenti agevolmente riconducibili all'incaricato;
 - b. modificare la propria password al primo utilizzo;
 - c. cambiare la propria password almeno ogni sei mesi;
 - d. cambiare la propria password, almeno ogni tre mesi, nel caso di trattamento di dati sensibili o di dati giudiziari.
2. Il Ce.S.I.A., mediante i sistemi di autenticazione forniti centralmente, può implementare meccanismi per il cambio password obbligatorio, anche con scadenze più restrittive di quelle previste al comma 1 lettere c) e d).

Art. 3. Disattivazione delle credenziali istituzionali

1. A eccezione dei docenti a contratto, dei dottorandi, degli assegnisti di ricerca e dei borsisti post-doc e degli studenti di cui all'Art. 1 comma 2 lettere a) e c) del presente allegato, le credenziali di

autenticazione sono disattivate dopo un mese dal termine del rapporto con l'Ateneo e, in ogni caso, per un tempo non eccedente rispetto alle finalità per le quali sono state fornite.

2. Le credenziali di autenticazione assegnate ai Docenti a contratto sono disattivate dopo sei mesi dal termine dell'anno accademico cui il contratto si riferisce.
3. Le credenziali di autenticazione assegnate ai dottorandi, agli assegnisti di ricerca e ai borsisti post-doc sono disattivate dopo sei mesi dal termine del rapporto formalmente stabilito con l'Ateneo.
4. Le credenziali di autenticazione assegnate a studenti preimmatricolati vengono disattivate dopo sette mesi dall'attivazione delle credenziali nel caso di mancata conferma d'iscrizione da parte dello stesso.
5. A eccezione dei casi previsti nel presente allegato all'Art. 1 comma 2 lettera a) e b) e all'Art. 1 comma 4 del presente allegato, le credenziali di autenticazione sono disattivate se non utilizzate da almeno sei mesi.
6. È onere del Ce.S.I.A. provvedere, entro un mese dalla segnalazione di morte del titolare di un account o dalla dichiarazione di morte presunta, alla disattivazione delle sue credenziali.
7. La riattivazione delle credenziali può essere eseguita dal Ce.S.I.A.:
 - a. su richiesta dell'interessato, nei casi in cui esse siano associate a un dipendente in servizio che non ne abbia fatto uso per un periodo maggiore di sei mesi;
 - b. su richiesta scritta del Responsabile dei dati trattati dall'incaricato, nei casi in cui esse siano associate a soggetti che, pur non in costanza di un rapporto formale con l'Ateneo, continuano a collaborare con l'Ente per attività di ricerca o didattica.
8. Le credenziali di autenticazione sono disattivate a ex-studenti dell'Ateneo solo su richiesta esplicita dell'interessato.
9. Le credenziali sono altresì disattivate nei casi e con le modalità di cui all'Art. 36 comma 3 del Regolamento.

Art. 4. Cancellazione delle credenziali

1. La cancellazione delle credenziali è prevista:
 - a. decorsi sei mesi dalla disattivazione delle credenziali nei casi in cui il soggetto titolare delle stesse sia deceduto o ne sia dichiarata la morte presunta;
 - b. decorsi ventiquattro mesi dalla disattivazione delle credenziali istituzionali per i soggetti indicati nell'Art. 1 comma 3 del presente allegato;
 - c. nei casi di credenziali istituzionali create dal Ce.S.I.A. e assegnate a persone fisiche per brevissimi periodi o per gestione tecnica, entro un termine non eccedente rispetto alle finalità per le quali si è fornito l'account.

Art. 5. Autorizzazione a risorse informatiche

1. La concessione del diritto di un soggetto incaricato al trattamento ad accedere a una o a più risorse informatiche dell'Ateneo, in cui la profilazione dei diritti d'accesso per l'utente non sia gestita automaticamente dal sistema d'identificazione centrale (DSA) bensì localmente alla risorsa in oggetto, deve essere valutata dal relativo Responsabile di trattamento (o persona da lui delegata per tale attività).
2. L'accesso alle risorse informatiche dell'Ateneo è consentito agli utenti abilitati in relazione al ruolo ricoperto, per il solo periodo di durata del rapporto con l'Ente e, nei casi di cui al comma 3, non oltre i termini di disattivazione delle credenziali.
3. Costituiscono eccezione al comma di cui sopra:
 - a. l'utilizzo della posta elettronica, come regolato nell'Allegato C;
 - b. l'abilitazione a connettersi a internet, come regolato nell'Allegato B;
 - c. l'accesso o l'utilizzo di specifici servizi o applicazioni, espressamente individuati dal Ce.S.I.A. e inerenti al rapporto di lavoro o di studio con l'Ateneo (Es: Cedolini, Stipendi Web, Presenze Web, Autocertificazioni).
4. Nel caso di cessazione del diritto di un incaricato ad accedere a una o a più risorse informatiche dell'Ateneo, in cui la profilazione dei diritti d'accesso per l'utente non sia gestita in maniera automatica dal sistema d'identificazione centrale (DSA) bensì localmente alla risorsa in oggetto, è onere del rispettivo Responsabile di trattamento (o persona da lui delegata per tale attività) assicurarsi, presso gli

amministratori dei servizi informatici corrispondenti, dell'avvenuta disattivazione delle autorizzazioni associate a tale incaricato.

Allegato B. DISCIPLINARE IN MATERIA DI ACCESSO E UTILIZZO DELLA RETE E DEI SISTEMI INFORMATIVI D'ATENEO

PARTE I. IDENTIFICAZIONE DELL'UTENTE IN RETE

Art. 1. Validità dell'autorizzazione ad accedere alla rete ALMAnet

1. L'autorizzazione a connettersi sulla Rete ALMAnet mediante i punti di accesso wired e wireless resi disponibili dall'Ateneo è concessa agli utenti per un tempo non eccedente rispetto alle finalità per le quali tale autorizzazione è stata concessa.
2. Gli utenti possono utilizzare il servizio di connettività entro il mese successivo al termine del rapporto formalmente stabilito con l'Ateneo, salvo quanto previsto nei casi di cui ai commi 3 e 4 del presente articolo.
3. Gli studenti preimmatricolati e i soggetti di cui all'Allegato A articolo 1 comma 3 lettera a) non sono abilitati a usufruire del servizio di connettività.
4. L'abilitazione a connettersi alla Rete mediante gli strumenti messi a disposizione dell'Ateneo è revocata:
 - a. ai docenti a contratto, agli assegnisti, ai borsisti post-doc al momento della disattivazione delle credenziali istituzionali attribuitegli;
 - b. agli studenti stranieri di scambio, al termine del periodo di permanenza nel nostro Ateneo;
 - c. ai soggetti di cui all'Allegato A articolo 1 comma 3 lettera b), al termine del periodo di permanenza nell'Ateneo.
5. L'abilitazione o il prolungamento, alla scadenza, dell'autorizzazione al servizio di connettività tramite la rete ALMAnet può essere effettuata solo per motivi legittimi e su richiesta motivata del proprio Responsabile di Struttura.

Art. 2. Accesso remoto alla Rete ALMAnet

1. L'utente che, nell'ambito delle proprie attività lavorative e/o di collaborazione con l'Ateneo, abbia effettiva necessità di usufruire o gestire, non occasionalmente, servizi telematici interni raggiungibili soltanto dalla Rete ALMAnet, può essere autorizzato dal Ce.S.I.A. ad accedervi mediante l'utilizzo di un servizio di VPN (Virtual Private Network) su richiesta del Responsabile di struttura.
2. E' consentito l'accesso remoto alla Rete ALMAnet via modem esclusivamente per finalità legate all'amministrazione di sistemi informatici e su linee che non consentono l'uscita verso l'esterno.

PARTE II. MISURE TECNICHE E ORGANIZZATIVE

TITOLO I. RETI

Art. 3. Gestione degli indirizzi IP

1. Il Ce.S.I.A. sovrintende all'indirizzamento IPv4 sia pubblico che privato (RFC1918) all'interno della rete ALMAnet, nonché all'indirizzamento globale IPv6 (RFC3513).
2. Le reti IPv4 pubbliche assegnate alla rete ALMAnet sono gestite dal Ce.S.I.A. che può delegare la gestione di sottoreti a strutture dell'Ateneo che ne abbiano comprovata necessità e che ne facciano richiesta.
3. La rete privata di classe A 10.0.0.0/8 (RFC 1918) è gestita dal Ce.S.I.A. che ne può assegnare sottoreti a strutture dell'Ateneo che ne abbiano necessità e che ne facciano richiesta.
4. Le reti private di classe B 172.16.0.0/12 (RFC 1918) sono gestite dal Ce.S.I.A. e riservate alla gestione e monitoraggio della rete dati e voce dell'Università di Bologna.

5. Le reti private di classe C (RFC 1918) 192.168.0.0/16 sono utilizzabili dalle strutture dell'Ateneo di Bologna per la gestione dell'indirizzamento privato.
6. Ogni struttura che necessita di un range di indirizzi IP deve presentare apposita domanda al Ce.S.I.A. sottoscritta dal proprio Responsabile, dalla quale risulti il nominativo del referente tecnico e la presa visione del presente Testo Unico. In relazione a tali indirizzi, la struttura ha l'obbligo di tenere aggiornato un registro in cui si tenga traccia della corrispondenza tra l'indirizzo IP e l'utente interno. La tenuta del registro deve avvenire secondo le modalità stabilite dal Ce.S.I.A., con la possibilità di utilizzare gli strumenti informatici messi a disposizione centralmente. È espressamente vietata all'utente l'autoassegnazione dell'indirizzo IP.
7. Relativamente all'indirizzamento IPv4, il Ce.S.I.A. privilegia l'uso di indirizzi privati. Per ottimizzare l'uso di indirizzi IP pubblici il Ce.S.I.A. valuta la reale necessità di strutture che ne facciano richiesta, eventualmente assegnando range di indirizzi IPv4 privati della rete 10.0.0.0/8 qualora lo si ritenesse sufficiente a soddisfare le esigenze di connettività della struttura richiedente.
8. La struttura che non utilizza un range di indirizzi IP assegnatole è tenuta a darne opportuna comunicazione al Ce.S.I.A. che ne assumerà la completa disponibilità e gestione.

Art. 4. Dynamic Host Configuration Protocol (DHCP) e NAT

1. Per un monitoraggio più efficace della rete e per una più granulare risoluzione degli incidenti di sicurezza da parte del CERT, il Ce.S.I.A. promuove l'uso di tecniche di NAT solo sul bordo della rete ALMANet, mediante l'assegnazione di range della classe A privata 10.0.0.0/8 alle strutture dell'Ateneo che ne facciano richiesta e sconsigliando l'uso di tali tecniche sulle reti locali delle stesse strutture.
2. Le strutture che comunque facciano uso di tecniche di NAT, utilizzando le reti private di cui all'Art. 3 comma 5 del presente allegato, devono darne tempestiva comunicazione al Ce.S.I.A.
3. Le strutture che facciano uso di server DHCP per la configurazione dinamica di rete degli host e/o di tecniche di NAT devono tenere traccia degli IP assegnati conservando i dati di traffico nel rispetto di quanto previsto nel presente allegato.

TITOLO II. SERVIZI

Art. 5. Gestione e implementazione dei servizi di rete della propria struttura

1. Il Responsabile di Struttura che ritiene necessaria l'attivazione di un servizio informatico non fornito dal Ce.S.I.A. o di un servizio che, sebbene sia disponibile attraverso il Ce.S.I.A., abbia funzionalità non coincidenti con quelle fornite, comunica tale esigenza al Ce.S.I.A. evidenziando gli obiettivi che intende raggiungere mediante tale attivazione.
2. Il Ce.S.I.A., a seguito di tale comunicazione, può provvedere a:
 - a. programmare l'implementazione dei nuovi servizi richiesti, laddove si rilevi un interesse concreto e diffuso;
 - b. estendere le funzionalità di servizi già esistenti;
 - c. consigliare alle strutture l'utilizzo di servizi già implementati o in fase di implementazione anche in altre strutture;
 - d. declinare, fornendo adeguate giustificazioni, la richiesta di attivazione del nuovo servizio, lasciando alla struttura la decisione sulla possibilità di implementarlo autonomamente secondo quanto definito al comma 3.
3. La singola struttura può erogare servizi informatici, nel rispetto di quanto definito nei comma precedenti, compatibilmente con le proprie risorse e in osservanza del presente Testo Unico.
4. Ogni struttura è tenuta a dare notifica al Ce.S.I.A. dell'elenco dei propri servizi erogati mediante la rete ALMANet (es. posta elettronica, Web, DNS, FTP, DHCP, NAT, ecc.), attraverso le modalità che saranno comunicate dal Ce.S.I.A. stesso.

Art. 6. Gestione dei domini internet locali

1. La semplice registrazione di nomi o la richiesta di delega di una zona DNS può essere effettuata secondo le modalità e le tempistiche indicate dal Ce.S.I.A. e rese pubbliche sui siti istituzionali.
2. I nomi di host che fanno parte della rete dell'Università di Bologna devono essere, in via prioritaria, registrati sotto il dominio "unibo.it".
3. Eventuali richieste di registrazione di nomi, sotto un dominio diverso da "unibo.it", debitamente motivate, sono inviate all'APA che provvede a verificarne la rispondenza agli scopi del GARR, concedendo o negando l'autorizzazione alla registrazione. Tali richieste sono autorizzate solo in via eccezionale e concesse sotto i ccTLD ".it" o ".eu".
4. Nel caso in cui si rilevino particolari necessità di registrazione di domini tramite "Registrar" privati, per servizi che risiedono fisicamente sulla rete ALMANet (ad esempio sotto i gTLD .net, .org, .info), la registrazione sarà consentita previa autorizzazione dell'APA che ne verificherà debitamente l'effettiva necessità. Per tali richieste, sarà comunque cura e onere delle strutture richiedenti provvedere alla registrazione.
5. Non è in ogni caso consentito registrare:
 - a. domini sotto il gTLD ".com" (che per definizione caratterizza attività di tipo commerciale);
 - b. domini intestati a singole persone fisiche.
6. La persona che richiede il servizio DNS, solidalmente al proprio Referente informatico di struttura, tra l'altro:
 - a. si fa carico della raggiungibilità di tutti i nodi del dominio che ne facciano richiesta e che ne abbiano il diritto;
 - b. garantisce la compilazione e la manutenzione delle tabelle DNS attenendosi alle disposizioni del Ce.S.I.A.;
 - c. garantisce la presenza di adeguate competenze tecniche per offrire un supporto di primo livello sulle problematiche di rete agli utenti della struttura di appartenenza.

Art. 7. Utilizzo dei servizi wireless

1. Oltre a quanto stabilito per le reti cablate, la rete wireless deve essere usata secondo le modalità del presente Testo Unico, nonché in osservanza di quanto stabilito dall'ordinamento italiano e dalla normativa del GARR.
2. La struttura che intende implementare autonomamente il servizio wireless è tenuta a darne comunicazione al Ce.S.I.A. che, a seguito di tale comunicazione, assume il compito di verificarne la conformità alla normativa e al presente Testo Unico e di fornire indicazioni sulle caratteristiche minime degli apparati da usare. Il Ce.S.I.A. ha altresì il compito di autorizzare preventivamente il posizionamento degli apparati nelle diverse sedi dell'Ateneo affinché non si generino interferenze che possano compromettere il buon funzionamento di impianti preesistenti.
3. La struttura deve garantire la confidenzialità nel trasferimento delle credenziali di autenticazione (utilizzo di un protocollo criptato per le fasi di autenticazione).

Art. 8. Utilizzo di cartelle condivise e spazi di rete personali

1. L'Ateneo, tramite il Ce.S.I.A. o mediante i servizi informatici implementati localmente dalle strutture, può mettere a disposizione dei propri utenti, cartelle di rete a uso esclusivo o condiviso ovvero unità di memoria accedibili dall'interno della Rete ALMANet, mediante le quali è possibile condividere e/o conservare file inerenti alla propria attività lavorativa che vengono memorizzate su di un file server.
2. Tali spazi possono essere utilizzati esclusivamente per finalità istituzionali. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.
3. Sulle cartelle in oggetto vengono svolte regolari attività di controllo, amministrazione e backup da parte dell'amministratore del servizio. L'amministratore ha visibilità delle cartelle ed è autorizzato a cancellare i file solo nei casi di evidente natura non istituzionale.

4. L'amministratore del servizio è tenuto al backup delle sole informazioni di natura istituzionale presenti sul file server mentre altre unità di memorizzazione a uso personale, come ad esempio il disco rigido della propria postazione di lavoro o dischi rigidi esterni, non sono soggetti a backup e, pertanto, la responsabilità del salvataggio dei dati ivi contenuti è a carico del singolo utente.
5. Per i servizi di cui al comma 1, entro sei mesi dalla conclusione del rapporto di collaborazione dell'utente con l'Ateneo, saranno cancellati tutti i file contenuti nelle cartelle a uso esclusivo.

Art. 9. Utilizzo postazioni di lavoro

1. Per garantire una maggiore sicurezza dei sistemi, non è consentito agli utenti di installare e utilizzare, nelle postazioni di lavoro, software illegale o software espressamente vietato dal proprio amministratore di sistema.
2. Nell'eventualità si rilevi, anche mediante sistemi inventariali di software, l'esistenza di programmi che violino il diritto d'autore, il Ce.S.I.A. agisce nel rispetto degli artt. 35 e 36 del Testo Unico; l'amministratore di sistema locale della struttura, invece, previa autorizzazione del proprio Responsabile, può provvedere:
 - a. a inviare avvisi collettivi, all'interno della struttura di riferimento, mediante i quali l'utenza sarà richiamata all'osservanza di corrette norme di comportamento;
 - b. a rimuovere il software, senza alcun preavviso all'utente, nei casi in cui software e file possano limitare l'utilizzo di risorse o possano recar danno all'Ateneo;
 - c. a effettuare, nei casi in cui i comportamenti non corretti si ripetano nel tempo o risultino particolarmente gravi, una segnalazione al Magnifico Rettore o al Direttore Amministrativo, per i rispettivi ambiti di competenza, che adotteranno i provvedimenti più opportuni di cui all'Art. 36.
3. Le postazioni sono sostituite dal proprio amministratore di sistema nei casi in cui, per motivi di sicurezza o affidabilità, si renda necessaria la sostituzione del computer. In tali casi saranno correttamente trasferiti sulla nuova postazione i soli dati di rilevanza istituzionale.

Art.10. Cancellazione di file e messaggi di un utente deceduto

1. I messaggi contenuti nella casella di posta elettronica di un utente deceduto o del quale è stata dichiarata la morte presunta o eventuali file contenuti nella sua postazione di lavoro saranno resi accessibili dalla struttura che la gestisce solo per ragioni di continuità del servizio, secondo le finalità di cui all'Art. 35 comma 5 e, comunque, entro i termini di cui all'Art. 4 comma 1 dell'allegato A.
2. Eventuali file o messaggi contenuti nella posta elettronica di un utente deceduto o del quale è stata dichiarata la morte presunta, nella sua postazione di lavoro o negli spazi di rete personali saranno eliminati dalla struttura che ne cura la gestione tecnica contestualmente alla cancellazione delle credenziali.
3. Eventuali file riconducibili a un utente deceduto o del quale è stata dichiarata la morte presunta potranno essere conservati dall'Ateneo per un periodo superiore a quello previsto al comma 2 e al comma 3 del presente articolo, su richiesta dell'Autorità Giudiziaria, di chi ha un interesse proprio, di chi agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione. Tale richiesta dovrà essere inviata per iscritto all'Ateneo entro sei mesi dalla morte dell'utente.

TITOLO III. SICUREZZA E GESTIONE DEGLI INCIDENTI

Art. 10. Politiche di sicurezza sulla rete ALMAnet

1. Il Ce.S.I.A. implementa le politiche di sicurezza sul bordo e sulla dorsale della rete ALMAnet, fornendo linee guida e supporto per l'implementazione di tali politiche nelle reti locali di ciascuna struttura.
2. L'accesso alla rete ALMAnet è protetto mediante l'uso di firewall e/o di altri apparati di rete che implementano regole di controllo del traffico finalizzate a migliorare e garantire la continuità del servizio di connettività alla rete ALMAnet.
3. Il Ce.S.I.A. configura gli apparati di rete posti sul bordo della rete ALMAnet bloccando l'accesso a qualunque connessione proveniente dall'esterno, ad eccezione delle connessioni verso gli host e i servizi che gli verranno espressamente comunicati dal Referente Informatico o dal Responsabile di struttura.
4. Il Ce.S.I.A. concede l'accesso agli host e servizi di cui al comma 3 dopo avere effettuato un vulnerability assessment sui sistemi in oggetto e aver verificato l'assenza di vulnerabilità manifeste. La connessione è fornita solo a seguito della risoluzione di eventuali vulnerabilità da parte del Referente Informatico.
5. Il Ce.S.I.A., che durante l'attività di monitoraggio (costituita anche da vulnerability assessment periodici) rilevi delle vulnerabilità di un sistema, comunica al Referente Informatico la necessità di attuare degli interventi correttivi definendo il tempo massimo entro il quale intervenire. Nel caso in cui il Referente Informatico non provveda a eliminare le vulnerabilità nei tempi stabiliti, il Ce.S.I.A. può intervenire interrompendo la connettività del sistema in oggetto.

Art. 11. Rilevazione delle intrusioni

1. Il CERT utilizza sistemi di rilevamento delle intrusioni, software e hardware, localizzati sulla rete ALMAnet. Tali sistemi sono adottati dal Ce.S.I.A. al solo fine di identificare eventuali accessi non autorizzati ai computer e alle reti locali dell'Ateneo e di intervenire nel caso di compromissioni.
2. I sistemi di rilevamento delle intrusioni possono essere utilizzati dal CERT per reagire in tempo reale agli attacchi in corso.
3. Durante tali attività, pur potendo acquisire informazioni personali e non, anche riservate, che transitano sulla rete ALMAnet, i componenti del CERT non possono raccogliere, copiare, registrare, organizzare, conservare, estrarre, comunicare, diffondere alcun dato personale ad eccezione di quelli strettamente necessari al perseguimento delle finalità indicate al comma 1 e salvo i casi espressamente previsti dalla legge o dai regolamenti.

Art. 12. Modalità di gestione degli incidenti

1. Le attività di monitoraggio della dorsale ALMAnet e di rilevazione di anomalie si svolgono sotto la responsabilità del CERT del Ce.S.I.A., cui compete di norma la notifica di apertura dell'incidente. Questa avviene attraverso la segnalazione al Referente informatico di struttura e, per conoscenza, al Responsabile di Struttura con l'indicazione di intervenire sulle macchine compromesse. Di tale intervento è responsabile il Referente informatico, che ha l'obbligo di provvedere al distacco dalla rete di singoli utenti o di porzioni della rete, sino alla rimozione delle cause che hanno originato il problema. A seguito di tali adempimenti, il Referente informatico notifica l'intervento risolutore al CERT che, dopo gli opportuni controlli, potrà dichiarare la chiusura dell'incidente. In casi di necessità e urgenza, al fine di evitare compromissioni al normale funzionamento della rete o porre termine ad attività contrarie alla normativa vigente o al presente Regolamento, il distacco di un utente o di una porzione di rete può essere effettuato dal CERT che ne darà comunicazione al Referente informatico della struttura.
2. La gestione degli incidenti deve avvenire nei tempi previsti dal Regolamento GARR.
3. Il Referente informatico di struttura, qualora rilevi delle anomalie, ha l'obbligo di darne comunicazione tempestiva al Ce.S.I.A., secondo le indicazioni che saranno comunicate dal Ce.S.I.A. stesso. La chiusura dell'incidente si svolge nelle modalità indicate nel comma 1 del presente articolo.

PARTE III. TRATTAMENTO DEI DATI DI TRAFFICO TELEMATICO

Art. 14. Ambito di trattamento

1. Qualunque struttura dell'Ateneo che, per obblighi di legge o di regolamenti, è tenuta al mantenimento dei log file (registri informatizzati che tengono traccia delle connessioni degli utenti e dei servizi da essi acceduti), deve trattare tali dati conformemente alla normativa vigente e alle disposizioni fornite centralmente dal Ce.S.I.A.
2. Per sole finalità di ordinaria gestione tecnica, le strutture d'Ateneo che gestiscono localmente dei servizi informatici hanno facoltà di conservare e accedere ai file di traffico telematico inerenti alla propria struttura, per un periodo non eccedente a tre mesi, salvo diverse disposizioni previste dalla normativa vigente.
3. La struttura di cui ai commi 1 e 2 del presente articolo, ha l'obbligo di presentare all'interessato l'informativa relativa alla gestione dei dati di traffico. Ai sensi dell'Art. 13 del decreto legislativo n. 196 del 30 giugno 2003, tale comunicazione contiene, fra le altre informazioni:
 - a. le finalità e le modalità della conservazione dei dati di traffico telematico;
 - b. le categorie di soggetti che detengono i log file;
 - c. l'identificazione del Titolare e dei Responsabili;
 - d. i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o i soggetti esterni che possono venirne a conoscenza.

Art. 15. Modalità di conservazione

1. Per una corretta registrazione dei log file, la struttura è obbligata a sincronizzare i propri server mediante NTP con i time server individuati e resi noti dal Ce.S.I.A.
2. Le modalità di conservazione dei file di log, le specifiche sulle informazioni da conservare nonché l'individuazione delle misure di sicurezza a tutela dei dati sono definite dal Garante per la Protezione dei Dati Personali e dalla normativa vigente.

Allegato C. DISCIPLINARE PER L'UTILIZZO DELLA POSTA ELETTRONICA

PARTE I. PROFILI GENERALI SULL'UTILIZZO DELLA POSTA ELETTRONICA D'ATENEO

Art. 1. Oggetto e finalità

1. L'Università di Bologna, tramite il Ce.S.I.A., rende disponibile agli studenti, ai docenti, al personale tecnico-amministrativo dell'Università e ad altri soggetti autorizzati un indirizzo di posta elettronica appartenente al dominio "unibo.it" e suoi eventuali sottodomini, secondo le convenzioni sui nomi definite all'Art. 1 dell'Allegato A e all'articolo 2 del presente Allegato.
2. Le comunicazioni ufficiali e istituzionali da parte dell'Ateneo sono inviate esclusivamente all'indirizzo di posta istituzionale assegnato; è fatto obbligo a ogni utente di utilizzare tale casella di posta.
3. L'utilizzo degli indirizzi di cui al comma 1 del presente articolo costituisce "trattamento dei dati personali" e, pertanto, da conformarsi alle disposizioni del D.lgs. 196/2003.
4. L'Ateneo ha facoltà di fornire ai propri utenti altri servizi di posta elettronica, a esclusivo uso personale, ove utilizzabili a supporto dell'attività di collaborazione con l'Ateneo.

Art. 2. Soggetti utilizzatori del servizio di posta elettronica

1. Tutti gli utenti definiti all'Art. 1 comma 1 e 2 dell'Allegato A possono accedere al servizio di posta elettronica utilizzando le proprie credenziali istituzionali.
2. Nel caso di assenza programmata, il dipendente è tenuto ad attivare sistemi di risposta automatica ai messaggi di posta elettronica ricevuti, nei quali indicherà eventuali indirizzi istituzionali alternativi ai quali fare riferimento per l'invio di comunicazioni.
3. Al fine di agevolare la comunicazione istituzionale e favorire la circolazione delle informazioni, sono altresì forniti indirizzi per unità/strutture organizzative o indirizzi legati alla carica, utilizzati prevalentemente per liste di distribuzione o caselle di posta elettronica, il cui accesso è consentito a uno o più lavoratori. A titolo esemplificativo, l'account di posta elettronica può essere fornito a:
 - a. Cariche, nella forma acronimostruttura.carica@unibo.it;
 - b. Organi, nella forma acronimostruttura.organo.carica@unibo.it;
 - c. Soggetti dell'Ateneo che nell'ambito di progetti, ricerche o altre forme di attività di collaborazione necessitano di tale strumento di lavoro nella forma acronimostruttura.testodastabilire@unibo.it.

Art. 3. Gestione tecnica del servizio

1. Il Ce.S.I.A. implementa misure di protezione automatizzate antivirus e antispam per il servizio di posta istituzionale, decidendone le tecnologie e le modalità operative, per contrastare la ricezione di messaggi di posta elettronica non desiderati contenenti virus, comunicazioni e/o materiali pubblicitari o altro materiale dal contenuto potenzialmente dannoso.
2. Il Ce.S.I.A. decide le politiche di backup dei messaggi esplicitandone le modalità di attuazione sul suo sito web.
3. Il Ce.S.I.A., pur adottando tutte le misure tecniche ritenute necessarie e sufficienti a minimizzare il rischio di perdita di informazioni di interesse dell'utente, non può essere ritenuto responsabile dell'eventuale cancellazione, danneggiamento, mancato invio, mancata ricezione o ritardo nella consegna di messaggi, se dovuti a malfunzionamenti o a guasti dei sistemi di posta, dei sistemi di protezione e di backup.
4. Il Ce.S.I.A. si impegna ad adottare delle soluzioni tecniche che limitino la cancellazione immediata dei messaggi di posta identificati come spam, entro i limiti consentiti dall'infrastruttura adottata e salvaguardando, per quanto possibile, l'operatività degli utenti.

Art. 4. Interruzione servizio

1. Per garantire un'adeguata protezione del servizio di posta, in ragione degli aggiornamenti rilasciati dai produttori software e hardware del servizio e salvaguardando il più possibile l'operatività dell'utente, il Ce.S.I.A. procede alla manutenzione e aggiornamento del sistema di posta al minimo una volta al mese.
2. Il Ce.S.I.A. ha l'obbligo di comunicare con adeguato anticipo operazioni di manutenzione straordinaria che possano causare interruzioni del servizio di posta elettronica.
3. Il Ce.S.I.A. può procedere a interruzioni straordinarie del servizio di posta elettronica, nei casi di effettiva necessità e urgenza.
4. Il Ce.S.I.A. si riserva la facoltà di dismettere alcuni dei suoi servizi di posta elettronica favorendo la migrazione al sistema di posta istituzionale, ad esempio, nei casi in cui i sistemi utilizzati risultino obsoleti e non conformi alle prescrizioni tecniche imposte dalla normativa vigente e dal presente Regolamento.
5. La dismissione del servizio di cui al comma 4 avviene previa comunicazione all'utente, da parte del Ce.S.I.A., all'indirizzo di posta elettronica che si intende dismettere. Decorso tre mesi dalla data di tale comunicazione, l'utente non potrà più accedere alla casella di posta dismessa ma potrà continuare a ricevere, nel caso in cui sia stato impostato un inoltra ad altra casella istituzionale, per i successivi tre mesi, eventuali messaggi indirizzati al vecchio sistema. Decorso sei mesi dalla data della prima comunicazione inviata dal Ce.S.I.A. per notificare la dismissione del servizio di posta, l'utente non potrà più utilizzare in alcun modo il servizio, né reperire i messaggi di posta elettronica ivi contenuti.

Art. 5. Validità dei profili autorizzativi per l'uso del servizio di posta elettronica

1. Il servizio di posta elettronica istituzionale sarà disattivato un mese dopo il termine del rapporto con l'Ateneo.
2. Costituiscono eccezione al predetto termine i seguenti casi:
 - a. per gli studenti, il servizio sarà disattivato su richiesta esplicita dell'interessato a seguito dell'interruzione della carriera universitaria o, comunque, nei tempi e con le modalità definite dal Ce.S.I.A., funzionali alla sostenibilità della gestione del servizio, e opportunamente rese note all'utente;
 - b. per studenti stranieri di scambio, il servizio sarà disattivato decorso un mese dal termine del periodo di permanenza nell'Ateneo;
 - c. per i docenti a contratto, gli assegnisti e i borsisti post-doc il servizio sarà disattivato al momento della disattivazione delle credenziali;
 - d. nel caso di soggetti deceduti, il servizio verrà disattivato entro un mese dalla notifica al Ce.S.I.A. dell'avvenuto decesso.
3. La cancellazione di tutti i messaggi contenuti nella casella disabilitata avverrà dopo sei mesi dalla disattivazione del servizio di posta elettronica.
4. Per i casi non contemplati nel presente Regolamento, il Ce.S.I.A. individua e diffonde le politiche di disattivazione del servizio di posta elettronica e di cancellazione dei messaggi.

PARTE II. UTILIZZO DELLE LISTE DI DISTRIBUZIONE

Art. 6. Principi generali

1. L'utilizzo delle liste di distribuzione costituisce "trattamento dei dati personali" e deve, dunque, svolgersi nell'ambito delle attività istituzionali dell'ente e nel rispetto delle disposizioni previste dal d.lgs. 196/2003.
2. Le liste di distribuzione di Ateneo costituiscono uno strumento volto ad agevolare lo scambio di informazioni tra gli utenti dell'Ateneo nello svolgimento delle proprie attività istituzionali.
3. La pubblicità di liste di distribuzione sui sistemi informativi d'Ateneo non ne legittima l'utilizzo per finalità contrastanti con il presente Regolamento o con la normativa vigente in materia di tutela dei dati personali.
4. Le liste per la distribuzione di comunicazioni mediante posta elettronica, aventi come destinatari studenti, dipendenti e/o collaboratori dell'Università di Bologna, sono predisposte e concesse in uso secondo i criteri tassativamente individuati all'Art. 7 del presente allegato.

Art. 7. Autorizzazione all'uso delle liste

1. È competenza del Ce.S.I.A. la creazione e la gestione informatizzata delle liste di distribuzione istituzionali generate dal sistema di Directory Service d'Ateneo.
2. L'abilitazione all'utilizzo di liste di distribuzione deve essere autorizzata dal Titolare del trattamento dei dati personali, previa istruttoria a cura dell'Ufficio Dirigenziale Direzione Cultura e Comunicazione Istituzionale, nei casi in cui le liste di distribuzione siano finalizzate all'invio:
 - a. di informazioni inerenti alla promozione di convegni, eventi e attività formative analoghe;
 - b. di messaggi da parte di soggetti privati;
 - c. di materiale informativo da parte di altri soggetti pubblici;
 - d. di messaggi di propaganda elettorale svolta dai candidati durante il periodo di elezione degli Organi Accademici;
 - e. di comunicazioni che potrebbero presentare profili di non evidente carattere istituzionale.
3. In sede di autorizzazione (comma 2 del presente articolo), sono valutati a titolo esemplificativo:
 - a. le modalità e i tempi di autorizzazione all'uso delle liste;
 - b. i tempi di validità delle stesse;
 - c. le tipologie di liste (ad esempio la concessione di liste opt-in o di liste opt-out) che, in relazione a specifici casi, possono essere più idonee a evitare un trattamento di dati difforme dai principi e dalle prescrizioni del d.lgs. 196/03.
4. L'abilitazione all'utilizzo di liste di distribuzione a uso interno non rientranti nei casi esplicitati al comma 2 del presente articolo è autorizzata dal Ce.S.I.A.

Art. 8. Controllo su liste di distribuzione

1. L'Ateneo può effettuare controlli a campione sulla legittimità del contenuto delle e-mail inviate mediante liste di distribuzione, al fine di verificarne l'aderenza alle disposizioni normative e alle prescrizioni contenute nel presente Regolamento.
2. Constatata la violazione delle norme del presente Regolamento, l'autorizzazione all'uso delle liste di distribuzione di Ateneo è revocata dal Titolare del trattamento dei dati.

Allegato D. TRATTAMENTO DI DATI SENSIBILI E GIUDIZIARI

SCHEDA A

Denominazione del trattamento
Gestione del rapporto di lavoro del personale dipendente (docente, dirigente, tecnico–amministrativo), dei collaboratori esterni e dei soggetti che intrattengono altri rapporti di lavoro diversi da quello subordinato.
Indicazione del trattamento e descrizione riassuntiva del contesto
<p>Sono di seguito descritte le principali caratteristiche:</p> <p>dati inerenti lo stato di salute per esigenze di: gestione del personale, verifica dell'attitudine a determinati lavori, idoneità al servizio, assunzioni del personale appartenente alle c.d. categorie protette, avviamento al lavoro degli inabili, maternità, igiene e sicurezza sul luogo di lavoro, equo indennizzo, causa di servizio, svolgimento di pratiche assicurative e previdenziali obbligatori e contrattuali, trattamenti assistenziali, riscatti e ricongiunzioni previdenziali, denunce di infortunio e/o sinistro, fruizione di particolari esenzioni o permessi lavorativi per il personale dipendente, collegati a particolari condizioni di salute dei dipendenti o dei loro familiari;</p> <p>dati inerenti lo stato di salute dei dipendenti e dei loro familiari acquisiti ai fini dell'assistenza fiscale e dell'erogazione dei benefici socio assistenziali contrattualmente previsti;</p> <p>dati idonei a rilevare l'adesione a sindacati o ad organizzazioni di carattere sindacale per gli adempimenti connessi al versamento delle quote di iscrizione o all'esercizio dei diritti sindacali;</p> <p>dati idonei a rilevare le opinioni politiche o le convinzioni religiose o l'adesione a partiti politici, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale per esigenze connesse alle elezioni ed al riconoscimento di permessi (anche per particolari festività e bandi di concorso), aspettative;</p> <p>dati inerenti l'obiezione di coscienza e le convinzioni inerenti la sperimentazione animale;</p> <p>dati idonei a rivelare l'origine razziale ed etnica ai fini dell'instaurazione e della gestione di rapporti di lavoro con lavoratori stranieri;</p> <p>dati sensibili e giudiziari che rilevano nell'ambito di procedimenti disciplinari a carico del personale e, in generale, nei giudizi pendenti di fronte a tutte le giurisdizioni che coinvolgono docenti, dipendenti, collaboratori esterni.</p> <p>E' di seguito descritto sinteticamente il flusso informativo dei dati.</p>

I dati sensibili e giudiziari sopra descritti inerenti il rapporto di lavoro, raccolti sia presso gli interessati che presso i terzi, vengono trattati dagli Uffici e/o dalle Strutture competenti dell'Ateneo, sia su base cartacea che su base informatica.

Principali fonti normative

Codice Civile (artt. 2094-2134); Codice di procedura civile (artt. 409 e ss.); R.D. 1038/1933 (*Approvazione del Regolamento di procedura per i giudizi innanzi alla Corte dei Conti*); L. 96/1955 (*Provvidenze a favore dei perseguitati politici antifascisti o razziali e dei loro familiari superstiti*); D.P.R. 3/1957 (*Testo unico delle disposizioni concernenti lo statuto degli impiegati civili dello Stato*); D.P.R. 361/1957 (*Approvazione del testo unico delle leggi recanti norme per la elezione della Camera dei deputati*); L. 69/1992 (*Interpretazione autentica del comma 2 dell'articolo 119 del testo unico delle leggi recanti norme per la elezione della Camera dei deputati, approvato con D.P.R. 361/1957, in materia di trattamento dei lavoratori investiti di funzioni presso i seggi elettorali*); D.P.R. 1124/1965 (*Testo unico delle disposizioni per l'assicurazione obbligatoria contro gli infortuni sul lavoro e le malattie professionali*); L. 300/1970 (*Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento*); L. 336/1970 (*Norme a favore dei dipendenti civili dello Stato ed Enti pubblici ex combattenti ed assimilati*); L. 6 Dicembre 1971 n. 1034 (*Istituzione dei Tribunali amministrativi regionali*); D.P.R. 1092/1973 (*Approvazione del testo unico delle norme sul trattamento di quiescenza dei dipendenti civili e militari dello Stato*); L. 200/1974 (*Disposizioni concernenti il personale non medico degli istituti clinici universitari*); D.P.R. 833/1978 (*Istituzione del servizio sanitario nazionale*); D.P.R. 761/1979 (*Stato giuridico del personale delle unità sanitarie locali*); D.P.R. 382/1980 (*Riordinamento della docenza universitaria, relativa fascia di formazione nonché sperimentazione organizzativa e didattica*); L. 14 aprile 1982, n. 164 e successive modifiche (*Norme in materia di rettificazione di attribuzione di sesso*); L. 8 marzo 1989, n. 101 (*Norme per la regolazione dei rapporti tra lo Stato e l'Unione delle Comunità Ebraiche Italiane*); L. 205/1990 (*Disposizioni in materia di giustizia amministrativa*); L. 104/1992 (*Legge quadro per l'assistenza, l'integrazione sociale ed i diritti delle persone handicappate*); D.Lgs. 502/1992 (*Riordino della disciplina in materia sanitaria, a norma dell'art. 1 della L. 23 Ottobre 1992 n. 421*); L. 537/1993 (*Interventi correttivi di finanza pubblica*); D.P.R. 487/1994 (*Regolamento recante norme sull'accesso agli impieghi nelle pubbliche amministrazioni*); D.Lgs. 626/1994 (*Igiene e sicurezza sul lavoro*); L. 335/1995 (*Riforma del sistema pensionistico obbligatorio e complementare*); D.Lgs. 564/1996 (*Attuazione della delega conferita dall'art. 1, comma 39, della L. 8 Agosto 1995 n. 335, in materia di contribuzione figurativa e di copertura assicurativa*

per periodi non coperti da contribuzione); L. 59/1997 (*Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa*); D.M. 187/1997 (*Regolamento recante modalità applicative delle disposizioni contenute all'articolo 2, comma 12, della L. 8 Agosto 1995 n. 335, concernenti l'attribuzione della pensione di inabilità ai dipendenti delle amministrazioni pubbliche iscritti a forme di previdenza esclusive dell'assicurazione generale obbligatoria*); D.P.R. 260/1998 (*Regolamento recante norme per la semplificazione dei procedimenti di esecuzione delle decisioni di condanna e risarcimento di danno erariale, a norma dell'art. 20, comma 8, della L. 15.03.1997 n. 59*); L. 230/1998 (*Nuove norme in materia di obiezione di coscienza*); L. 210/1998 (*Norme per il reclutamento dei ricercatori e dei professori universitari di ruolo*); L. 488/1999 (*Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato. Legge Finanziaria 2000*); L. 68/1999 (*Norme per il diritto al lavoro dei disabili*); D.Lgs. 517/1999 (*Disciplina dei rapporti fra Servizio sanitario nazionale ed università, a norma dell'articolo 6 della L. 30 novembre 1998 n. 419*); D.Lgs. 267/2000 (*Testo unico delle leggi sull'ordinamento degli enti locali*); D.lgs. 445/2000 (*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*); D.Lgs. 165/2001 (*Norme generali sull'ordinamento del lavoro alle dipendenze delle Pubbliche Amministrazioni*); D.P.R. 461/2001 (*Regolamento recante semplificazione dei procedimenti per il riconoscimento della dipendenza delle infermità da causa di servizio, per la concessione della pensione privilegiata ordinaria e dell'equo indennizzo, nonché per il funzionamento e la composizione del comitato per le pensioni privilegiate ordinarie*); D.Lgs. 151/2001 (*Testo unico delle disposizioni legislative in materia di tutela e sostegno della maternità e della paternità, a norma dell'art. 15 della L. 8 Marzo 2000, n. 53*); D.M. 31 gennaio 2001 (*Procedimento di riscossione dei crediti conseguenti a decisioni di condanna della Corte dei Conti a carico dei responsabili per danno erariale in attuazione dell'art. 4 del D.P.R. 24 giugno 1998 n. 260*); D.P.R. 334/2004 (*Regolamento recante norme di attuazione del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulle condizioni dello straniero*); C.C.N.L e gli altri contratti vigenti del comparto università; Statuto di Ateneo; Regolamento per la Finanza e la Contabilità ed altri Regolamenti di Ateneo vigenti.

Finalità di rilevante interesse pubblico perseguite

Sono contenute nei seguenti articoli del Codice:

- ART. 112: "*instaurazione e gestione da parte dei soggetti pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato*";
- ART. 65: "*applicazione della disciplina in materia di a) elettorato attivo e passivo (...)*";

- ART 66: “*applicazione (...) delle disposizioni in materia di tributi, in relazione ai contribuenti, ai sostituti ed ai responsabili d’imposta, nonché in materia di deduzioni e detrazioni*”;
- ART 68: "*applicazione della disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni*";
- ART. 70: " *applicazione della legge 8 luglio 1998 n. 230, e delle altre disposizioni di legge in materia di obiezione di coscienza*".

Caratteristiche del trattamento

cartaceo

informatico

Tipi di dati SENSIBILI e/o GIUDIZIARI trattati

origine razziale etnica

convinzioni religiose, filosofiche, d’altro genere

convinzioni politiche, sindacali

stato di salute: patologie attuali, patologie pregresse, dati sulla salute relativi anche ai familiari, terapie in corso a fini assicurativi

vita sessuale soltanto in relazione ad un eventuale rettificazione di attribuzione di sesso

dati di carattere giudiziario

Operazioni eseguibili

Trattamento “ordinario” dei dati

Raccolta: presso gli interessati presso terzi

Elaborazione Registrazione Organizzazione Consultazione Modifica

Cancellazione Estrazione Blocco Selezione Utilizzo

Conservazione Distruzione

Particolari forme di elaborazione

Interconnessioni e raffronti di dati:

con altri trattamenti o banche dati appartenenti a Uffici e Strutture dell'Università che si occupano: della gestione del personale, della gestione del contenzioso, della gestione delle risorse finanziarie.

con altri soggetti pubblici o privati:

Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000;

Comunicazione ai seguenti soggetti per le seguenti finalità:

INPDAP – INPS (per erogazione e liquidazione trattamento di pensione, L. 335/1995; L. 152/1968);

Comitato di verifica per le cause di servizio e Commissione medica territorialmente competente (nell’ambito della procedura per il riconoscimento della causa di servizio/equo indennizzo, ai sensi del DPR 461/2001);

INAIL, Autorità di P.S., Sportello unico per l'immigrazione (DPR n. 334/2004) e/o altre Autorità previste dalla legge (per denuncia infortunio, DPR 1124/1965);

Strutture sanitarie competenti (per visite fiscali, art. 21 CCNL del 06/07/1995, CCNL di comparto);

Soggetti pubblici e privati ai quali, ai sensi delle leggi regionali/provinciali, viene affidato il servizio di formazione del personale (le comunicazioni contengono dati sensibili soltanto nel caso in cui tali servizi siano rivolti a particolari categorie di lavoratori, ad es. disabili);

Centro per l'impiego o organismo territorialmente competente per le assunzioni ai sensi della legge 68/1999;

Amministrazioni provinciali e Centro regionale per l'impiego in ordine al prospetto informativo delle assunzioni, cessazioni e modifiche al rapporto di lavoro, redatto ai sensi della L. 68/1999;

Autorità giudiziaria (C.P. e C.P.P.);

Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali;

Ministero delle Finanze, nell'ambito dello svolgimento da parte delle Università del ruolo di Centro di assistenza fiscale (CAF), relativamente alla dichiarazione dei redditi dei dipendenti (art.17 D.M. 164/1999 e art. 2-bis D.P.R. 600/1973);

Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, nell'ambito della mobilità dei lavoratori.

SCHEDA B

Denominazione del trattamento
Attività di ricerca scientifica
Indicazione del trattamento e descrizione riassuntiva del contesto
<p>Sono di seguito descritte le principali caratteristiche:</p> <ol style="list-style-type: none">1. dati sensibili e giudiziari trattati nell'ambito delle attività di ricerca inerenti <i>in toto</i> le scienze tecniche (agraria, architettura, chimica, biologia, ingegneria), scienze mediche e scienze umanistiche (economiche e sociali, giuridiche, politiche, sociologiche e letterarie), scienze della formazione;2. dati sensibili trattati nell'ambito delle attività didattiche e assistenziali connesse alla ricerca;3. dati inerenti lo stato di salute acquisiti nell'ambito delle strutture sanitarie convenzionate. <p>E' di seguito descritto sinteticamente il flusso informativo dei dati.</p> <p>I dati sensibili e giudiziari inerenti l'attività di ricerca scientifica, contenuti in documenti cartacei, informatici e/o in audio e video-registrazioni, raccolti sia presso gli interessati che presso terzi, possono essere trattati dalle strutture di ricerca e dai ricercatori, di volta in volta designati incaricati o responsabili, sia su base cartacea che su base informatica, mediante le operazioni nel prosieguo meglio descritte.</p> <p>Potranno essere desunti dati sensibili anche dal trattamento delle immagini e/o dalle dichiarazioni raccolte nel corso di eventuali video-conferenze, tele-consulti, video-registrazioni o interviste che rappresentano possibili modalità di raccolta dei dati a scopo di ricerca, previa informativa all'interessato sugli scopi dell'iniziativa e sulla volontarietà della partecipazione alla ricerca, avendo cura di specificare nel progetto di ricerca i tipi di dati trattati e le operazioni eseguite in concreto.</p>
Principali fonti normative
<p>L. 398/1989 (<i>Norme in materia di borse di studio universitarie</i>); L. 390/1991 (<i>Norme sul diritto agli studi universitari</i>); L. 449/1997 (<i>Misure per la stabilizzazione della finanza pubblica</i>); D.M. 11.2.1998 (<i>Determinazione dell'importo e dei criteri per il conferimento di assegni per la collaborazione ad attività di ricerca</i>); D.M. 21.5.1998 n. 242; D.M. 30.4.1999 n. 224 (<i>Norme in materia di dottorato di ricerca</i>); D.P.C.M. 9.4.2001 (<i>Disposizioni per l'uniformità di trattamento sul diritto agli studi universitari</i>); D.lgs. 517/1999 (<i>Disciplina dei rapporti fra servizio sanitario nazionale ed università, a norma dell'art. 6 della L. 30 novembre 1998 n. 419</i>); D.P.R. 382/1980 (<i>Riordino della docenza universitaria, relativa fascia di formazione nonché sperimentazione organizzativa e didattica</i>); Codice di deontologia e buona condotta per i trattamenti di dati personali per scopi storici del 14.3.2001; Codice di deontologia e buona condotta per i trattamenti di dati personali a scopi statistici e scientifici del 16.6.2004; Accordo finanziario n. 2004/67/TS; Normativa previdenziale; Normativa fiscale di riferimento; Statuto di Ateneo; Regolamento per la Finanza e la</p>

Contabilità ed altri Regolamenti di Ateneo vigenti.
<i>Finalità di rilevante interesse pubblico perseguite</i>
<p>Sono contenute nei seguenti articoli del Codice:</p> <ul style="list-style-type: none"> - ART. 95: "istruzione e formazione in ambito scolastico, professionale, superiore o universitario"; - ART. 98: "trattamenti effettuati da pubblici: per scopi storici (...), per scopi scientifici".
Caratteristiche del trattamento
cartaceo X informatico X
Tipi di dati SENSIBILI e/o GIUDIZIARI trattati
<p>origine razziale X etnica X </p> <p>convinzioni religiose, filosofiche, d'altro genere X </p> <p>convinzioni politiche, sindacali X </p> <p>stato di salute: patologie attuali, patologie pregresse, dati sulla salute relativi anche ai familiari, terapie X </p> <p>vita sessuale nell'ambito delle attività di ricerca inerenti le scienze umane e biomediche X </p> <p>dati di carattere giudiziario X </p>

Operazioni eseguibili
Trattamento "ordinario" dei dati
<p>Raccolta: presso gli interessati X presso terzi X </p> <p>Registrazione X Organizzazione X Conservazione X Consultazione X Elaborazione* X </p> <p>Modificazione X Selezione X Estrazione X Utilizzo X Blocco X Cancellazione X </p> <p>Distruzione X </p> <p>* L'operazione di elaborazione comprende le cautele destinate a rendere anonimo successivamente alla raccolta il dato sensibile e/o giudiziario oggetto di trattamento ai fini della ricerca, a meno che l'abbinamento al materiale di ricerca dei dati identificativi dell'interessato sia temporaneo ed essenziale per il risultato della ricerca, e sia motivato, altresì, per iscritto nel progetto di ricerca. I risultati della ricerca non possono essere diffusi se non in forma anonima.</p>
Particolari forme di elaborazione
<p>Interconnessioni e raffronti di dati: X </p> <p>con altri trattamenti o banche dati delle Strutture di Ricerca e/o di altri Uffici e Strutture dell'Università.</p> <p>Comunicazione ai seguenti soggetti: X </p> <p>Altre università, istituzioni e organismi pubblici e privati aventi finalità di ricerca, esclusivamente nell'ambito di progetti congiunti.</p>

Altre università, istituzioni e organismi pubblici e privati, aventi finalità di ricerca e non partecipanti a progetti congiunti, limitatamente ad informazioni prive di dati identificativi e per scopi storici o scientifici chiaramente determinati per iscritto nella richiesta dei dati.

In tali casi, si applicano le ulteriori garanzie previste dagli artt. 8 e 9 del Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e scientifici.

SCHEDA C

Denominazione del trattamento
Attività didattica e gestione delle iscrizioni e delle carriere degli studenti.
Indicazione del trattamento e descrizione riassuntiva del contesto
<p>Sono di seguito descritte le principali caratteristiche:</p> <ol style="list-style-type: none">1. dati relativi agli studenti e/o a familiari diversamente abili o ad elementi reddituali ai fini di un eventuale controllo sulle autocertificazioni relative alle tasse universitarie e di eventuali esoneri dal versamento delle tasse universitarie e/o fruizione di eventuali agevolazioni previste dalla legge, nonché dati relativi alla gestione dei contributi straordinari per iniziative degli studenti;2. dati relativi allo status di rifugiato per la fruizione di esoneri e borse di studio;3. dati relativi allo stato di gravidanza al fine di attuare tutte le cautele necessarie per la tutela della donna in stato di gravidanza, sia per motivi didattici, quali la frequenza di laboratori, sia al fine della fruizione di eventuali agevolazioni e benefici di legge;4. dati idonei a rivelare le opinioni politiche o l'adesione a partiti, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale per esigenze connesse allo svolgimento delle procedure elettorali interne all'Ateneo;5. dati sensibili e giudiziari che rilevano nell'ambito di procedimenti disciplinari a carico degli studenti;6. dati relativi alla condizione di disabile per attività di interpretariato, tutorato, trasporto e servizi analoghi per tutti gli studenti portatori di handicap. <p>E' di seguito descritto sinteticamente il flusso informativo dei dati.</p> <p>I dati sensibili e giudiziari sopra descritti inerenti l'attività didattica e la gestione delle iscrizioni e delle carriere degli studenti, raccolti sia presso gli interessati che presso i terzi, vengono trattati dagli Uffici e/o dalle</p>

Strutture competenti, sia su base cartacea che su base informatica.

Principali fonti normative

R.D. 1592/1933 e successive modificazioni e integrazioni. (*Testo unico delle leggi sull'istruzione superiore*);
R.D. 1269/1938 e successive modificazioni e integrazioni. (*Approvazione del regolamento sugli studenti*);
D.P.R. 382/1980 (*Riordinamento della docenza universitaria, relativa fascia di formazione nonché sperimentazione organizzativa e didattica*); L. 168/1989 (*Istituzione del Ministero dell'Università e della Ricerca scientifica e Tecnologica*); L. 398/1989 (*Norme in materia di borse di studio universitarie*);
L. 341/1990 (*Riforma degli ordinamenti didattici universitari*); L. 390/1991 (*Norme sul diritto agli studi universitari*); L. 104/1992 (*Legge-quadro per l'assistenza, l'integrazione sociale ed i diritti delle persone handicappate*); D.M. 224/1999 (*Norme in materia di dottorato di ricerca*); D.lgs. 445/2000 (*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*); L. 148/2002 (*Ratifica ed esecuzione della Convenzione di Lisbona dell'11 aprile 1997*); D.M. 270/2004 (*Modifiche al Regolamento recante norme concernenti l'autonomia didattica degli Atenei, approvato con decreto MURST 3 novembre 1999, n. 509*); D.P.R. 334/2004 (*Regolamento recante norme di attuazione del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulle condizioni dello straniero*); D.M. 25/3/1998, n. 142 e L. 24 giugno 1997, n. 196 (*Normativa relativa agli stage*); DPCM 9 aprile 2001; L. 14 febbraio 2003, n. 30 (*c.d. Legge Biagi, di riforma del mercato del lavoro*); Contratto Istituzionale Socrates Erasmus vigente; Statuto di Ateneo, Regolamento Didattico di Ateneo, Regolamento per la Finanza e la Contabilità, Regolamento didattico d'Ateneo ed altri Regolamenti di Ateneo vigenti; Leggi Regionali vigenti in materia di diritto allo studio universitario.

Finalità di rilevante interesse pubblico perseguite

Sono contenute nei seguenti articoli del Codice:

- ART. 64: “*cittadinanza,immigrazione e condizione dello straniero*”;
- ART. 65: “*applicazione della disciplina in materia di a) elettorato attivo e passivo (...)*”;
- ART. 68: “*concessione, liquidazione, modifica e revoca di benefici economici, abilitazioni (...)*”;
- ART. 86: “*...assistenza, integrazione sociale e diritti delle persone handicappate (...)*”;
- ART. 95: “*istruzione e formazione in ambito scolastico, professionale, superiore o universitario (...)*”.

Caratteristiche del trattamento

cartaceo |X|

informatico |X|

Tipi di dati SENSIBILI e/o GIUDIZIARI trattati

origine razziale |X| etnica |X|

convinzioni religiose, filosofiche, d'altro genere |X|

convinzioni politiche, sindacali |X|

stato di salute: patologie attuali, patologie pregresse, dati sulla salute relativi anche ai familiari, terapie in corso a fini assicurativi |X|

vita sessuale soltanto in relazione ad un eventuale rettificazione di attribuzione di sesso |X|

dati di carattere giudiziario |X|

Operazioni eseguibili

Trattamento "ordinario" dei dati

Raccolta: presso gli interessati |X| presso terzi |X|

Elaborazione |X| Registrazione |X| Organizzazione |X| Consultazione |X| Modifica |X|

Cancellazione |X| Estrazione |X| Blocco |X| Selezione |X| Utilizzo |X|

Conservazione |X| Distruzione |X|

Interconnessioni e raffronti di dati: |X|

con altri trattamenti o banche dati appartenenti a Uffici e Strutture dell'Università che si occupano della gestione delle risorse finanziarie, della gestione del contenzioso e della gestione dei servizi informatici;

con altri soggetti pubblici o privati: |X|

Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000;

Comunicazione ai seguenti soggetti per le seguenti finalità: |X|

Enti locali ai fini di eventuali sussidi a favore di particolari categorie di studenti, Avvocatura dello Stato, Ministero degli Affari esteri, Questure, Ambasciate, Procura della Repubblica relativamente a permessi di soggiorno, al riconoscimento di particolari status, Regione, altri operatori pubblici e privati accreditati o autorizzati e potenziali datori di lavoro ai fini dell'orientamento e inserimento nel mondo del lavoro (ai sensi della legge 30/2003, sulla riforma del mercato del lavoro, e successive attuazioni), enti di assicurazione per pratiche infortuni.

Organismi Regionali di Gestione (Enti dotati di autonomia amministrativo-gestionale istituiti ai sensi della L. 390/91 in materia di diritto agli studi universitari) ed altri istituti per favorire la mobilità internazionale degli studenti, ai fini della valutazione dei benefici economici e dell'assegnazione degli alloggi (Legge 390/1991 e Leggi regionali in materia).

SCHEDA D

Denominazione del trattamento
Gestione del contenzioso giudiziale, stragiudiziale e attività di consulenza
Indicazione del trattamento e descrizione riassuntiva del contesto
<p>Sono di seguito descritte le principali caratteristiche: dati sensibili e giudiziari inerenti i soggetti coinvolti.</p> <p>E' di seguito descritto sinteticamente il flusso informativo dei dati.</p> <p>I dati sensibili e giudiziari sopra descritti inerenti la gestione del contenzioso e l'attività di consulenza, raccolti sia presso gli interessati che presso i terzi, vengono acquisiti dagli Uffici preposti e inviati agli Uffici e/o alle Strutture competenti, che operano il trattamento di tali dati sia su base cartacea che su base informatica.</p>
<i>Principali fonti normative</i>
<p>Codice Civile; Codice di Procedura Civile; Codice Penale; Codice di Procedura Penale; R.D. 642/1907 (<i>Regolamento per la procedura innanzi alle sezioni giurisdizionali del Consiglio di Stato</i>); R.D. 1054/1924 (<i>Approvazione del testo unico delle leggi sul Consiglio di Stato</i>); R.D. 1038/1933 (<i>Approvazione del Regolamento di procedura per i giudizi innanzi alla Corte dei Conti</i>); D.P.R. 3/1957 (<i>Testo unico delle disposizioni concernenti lo statuto degli impiegati civili dello Stato</i>); L. 300/1970 (<i>Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento</i>); L. 336/1970 (<i>Norme a favore dei dipendenti civili dello Stato ed Enti pubblici ex combattenti ed assimilati</i>); L. 1034/1971 (<i>Istituzione dei Tribunali Amministrativi Regionali</i>); L. 689/81 (<i>Modifiche al sistema penale</i>); D.lgs. 285/1992 (<i>Codice della Strada</i>); D.lgs. 546/1992 (<i>Disposizioni sul Processo Tributario</i>); D.P.R. 487/1994 (<i>Regolamento recante norme sull'accesso agli impieghi nelle pubbliche amministrazioni</i>); L. 335/1995 (<i>Riforma del sistema pensionistico obbligatorio e complementare</i>); D.M. 187/1997 (<i>Regolamento recante modalità applicative delle disposizioni contenute all'articolo 2, comma 12, della L. 8 Agosto 1995 n. 335, concernenti l'attribuzione della pensione di inabilità ai dipendenti delle amministrazioni pubbliche iscritti a forme di previdenza esclusive dell'assicurazione generale obbligatoria</i>); D.P.R. 260/1998 (<i>Regolamento recante norme per la semplificazione dei procedimenti di esecuzione delle decisioni di condanna e risarcimento di danno erariale, a norma dell'art. 20, comma 8, della L. 15.03.1997 n. 59</i>); L. 205/2000 (<i>Disposizioni in materia di giustizia amministrativa</i>); D.lgs. 445/2000 (<i>Testo unico delle disposizioni legislative e</i></p>

regolamentari in materia di documentazione amministrativa); L. 241/1990 (Nuove norme sul procedimento amministrativo); D.lgs. 165/2001 (Norme generali sull'ordinamento del lavoro alle dipendenze delle Pubbliche Amministrazioni); D.P.R. 461/2001 (Regolamento recante semplificazione dei procedimenti per il riconoscimento della dipendenza delle infermità da causa di servizio, per la concessione della pensione privilegiata ordinaria e dell'equo indennizzo, nonché per il funzionamento e la composizione del comitato per le pensioni privilegiate ordinarie); D.M. 31 gennaio 2001 (Procedimento di riscossione dei crediti conseguenti a decisioni di condanna della Corte dei Conti a carico dei responsabili per danno erariale in attuazione dell'art. 4 del D.P.R. 24 giugno 1998 n. 260); C.C.N.L. e gli altri contratti vigenti del Comparto Università; Statuto di Ateneo; Regolamento per la Finanza e la Contabilità ed altri Regolamenti di Ateneo vigenti.

Finalità di rilevante interesse pubblico perseguite

Sono contenute nei seguenti articoli del Codice:

- ART. 71, comma 1, lett. A): " *applicazione delle norme in materia di sanzioni amministrative e ricorsi*";
- ART. 71, comma 1, lett. B): " *far valere il diritto di difesa in sede amministrativa o giudiziaria (...)*";
- ART. 67, comma 1, lett. A): " *verifica della legittimità, del buon andamento, dell'imparzialità dell'attività amministrativa, nonché della rispondenza di detta attività a requisiti di razionalità, economicità, efficienza ed efficacia per le quali sono comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti*".

Caratteristiche del trattamento

cartaceo |X|

informatico |X|

Tipi di dati SENSIBILI e/o GIUDIZIARI trattati

origine razziale |X| etnica |X|

convinzioni religiose, filosofiche, d'altro genere |X|

convinzioni politiche, sindacali |X|

stato di salute: patologie attuali, patologie pregresse, dati sulla salute relativi anche ai familiari, terapie in corso |X|

vita sessuale |X|

dati di carattere giudiziario |X|

Operazioni eseguibili
Trattamento “ordinario” dei dati
<p>Raccolta: presso gli interessati X presso terzi X </p> <p>Elaborazione X Registrazione X Organizzazione X Consultazione X Modifica X </p> <p style="padding-left: 40px;">Cancellazione X Estrazione X Blocco X Selezione X Utilizzo X </p> <p>Conservazione X Distruzione X </p>

Particolari forme di elaborazione
<p>Interconnessioni e raffronti di dati: X </p> <p>con altri trattamenti o banche dati appartenenti a Uffici e Strutture dell’Università che si occupano: della gestione del personale, della gestione delle risorse finanziarie, della gestione dell’attività didattica e di ricerca, della stipula-esecuzione dei contratti e della gestione delle procedure formali ed informali di scelta del contraente.</p> <p>Comunicazione ai seguenti soggetti per le seguenti finalità: X </p> <p>Avvocatura distrettuale e generale dello Stato, ai fini della gestione del contenzioso penale, civile ed amministrativo;</p> <p>Autorità Giudiziaria di qualsiasi ordine e grado, arbitri, Amministrazioni interessate ai fini della gestione dei ricorsi straordinari al Presidente della Repubblica, Organi di Polizia giudiziaria, Commissioni Tributarie, Uffici Provinciali del Lavoro ai fini del tentativo obbligatorio di conciliazione;</p> <p>Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte quando dovuto;</p> <p>Compagnie di assicurazione, in caso di polizze assicurative che prevedano tali comunicazioni.</p>