Manuale Operativo per la Protezione dei Dati Personali

Versione 1.0 ***14/12/2014***

Per la politica generale di Ateneo sul trattamento dei dati personali si rinvia all'Area InfoServizi "Protezione dei dati personali" del Portale di Ateneo
https://intranet.unitn.it/infoservizi/protezione-dei-dati-personali
(accesso riservato al solo personale di Ateneo)

Per le problematiche generali di sicurezza ICT e la documentazione tecnica dei servizi ICT gestiti dalla Direzione SISTI si rinvia al portale ICTS@unitn della Direzione medesima
http://icts.unitn.it/

SOMMARIO

1 INTRODUZIONE

Alla luce degli obblighi imposti dal D. Lgs. 196 30 giugno 2003 "Codice in materia di protezione dei dati personali", l'Università degli studi di Trento, nel contesto della propria organizzazione, adotta le misure minime e idonee di protezione e sicurezza dei dati personali al fine di assicurare un livello di protezione e sicurezza dei dati personali conforme a quanto disposto dagli artt.31, 33, 34, 35 e dal "Disciplinare tecnico in materia di misure minime di sicurezza" del Codice medesimo.

In linea con la legislazione nazionale in tema di sicurezza ICT nella Pubblica Amministrazione e ai provvedimenti, indicazioni e linee guida emanati dal Garante per la protezione dei dati personali, il presente Manuale Operativo per la protezione dei dati personali si propone di fornire alle strutture e ai soggetti dell'Ateneo coinvolti a vario titolo nell'adempimento agli obblighi imposti dal Codice un valido strumento per l'adozione delle misure di sicurezza e protezione dei dati personali.

In accordo alle buone pratiche internazionali in materia di sicurezza ICT, la sicurezza delle informazioni può essere definita come la salvaguardia della Riservatezza(*), dell'Integrità(**) e della Disponibilità(***) delle informazioni medesime.

I requisiti di sicurezza delle informazioni sono soddisfatti implementando misure di sicurezza di varia natura quali politiche, procedure, strutture organizzative e funzioni o meccanismi tecnici, raggruppabili in alcune aree omogenee: Politica di Sicurezza dei Dati Personali, Organizzazione e Personale, Inventario delle Risorse e dei Trattamenti, Sicurezza Fisica, Sicurezza degli Strumenti Elettronici, Controllo degli Accessi, Verifiche di Conformità.

L'adozione dei principi generali e delle buone pratiche nell'ambito della sicurezza ICT, nel quadro degli obiettivi di conformità al Codice e dell'attuale organizzazione dell'Ateneo, permette di:

- disporre di un valido strumento per adempiere agli obblighi di sicurezza e protezione dei dati personali imposti dal Codice nell'ottica di un miglioramento continuo;
- affrontare le problematiche di sicurezza ICT attraverso un approccio coerente e completo;
- accrescere la consapevolezza e diffondere la cultura della sicurezza ICT tra il personale dell'Ateneo.

Si segnala che il D.L. 9 febbraio 2012, n. 5 - convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35 (pubblicata sulla Gazzetta Ufficiale del 6 aprile 2012, n. 82) - ha, tra l'altro, modificato alcune disposizione del Codice in materia di protezione di dati personali, abrogando, in particolare, la redazione e l'aggiornamento annuale da parte del Titolare del Documento Programmatico per la Sicurezza (DPS).

(*) Assicurare che le informazioni siano accessibili ai soli soggetti autorizzati.
(**) Assicurare l'accuratezza e la completezza delle informazioni e del loro trattamento.
(***) Assicurare che i soggetti autorizzati abbiano accesso alle informazioni quando richiesto.

2 FONTI NORMATIVE

Vengono elencate di seguito le principali fonti normative concernenti l'ambito di applicazione del presente Manuale Operativo:

- Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e ss.mm.ii (nel seguito Codice);
- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" e ss.mm.ii.. (nel seguito CAD);
- Decreto del Presidente del Consiglio dei Ministri Dipartimento per l'Innovazione e le Tecnologie 16 gennaio 2002 "Sicurezza informatica e delle telecomunicazioni nelle Pubbliche Amministrazioni Statali";
- Decreto Rettorale 14 gennaio 2002, n. 27 "Regolamento di Attuazione delle Norme sulla Tutela delle Persone e di Altri Soggetti rispetto al Trattamento di Dati Personali e per l'Adozione di Misure Minime di Sicurezza" (nel seguito Regolamento);
- Decreto Rettorale 22 dicembre 2005, n. 1192 "Regolamento per il Trattamento dei Dati Sensibili e Giudiziari in attuazione del D.Lgs. 196/2003";
- Decreto Rettorale 4 agosto 1997, n. 729, Decreto Rettorale 29 dicembre 2000, n.1635 "Norme relative all'Accesso ed all'Uso della Rete Informatica e Telematica d'Ateneo";
- GARR-AUP-00 24 novembre 2000 "GARR Acceptable Use Policy";
- "Guida Operativa per Redigere il Documento Programmatico sulla Sicurezza (DPS)", Garante per la Protezione dei Dati Personali 11 giugno 2004;
- Provvedimento del Garante 31 luglio 2002, n. 13 "Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (Sistan);
- Provvedimento del Garante 29 aprile 2004 " Videosorveglianza - provvedimento generale" e ss.mm.ii.;
- Provvedimento del Garante 16 giugno 2004, n. 2 "Codice di Deontologia e di Buona Condotta per i Trattamenti di Dati Personali per Scopi Statistici e Scientifici";
- APSS PAT, dicembre 2004 "Disciplinare per lo scambio informativo tra Azienda Provinciale per i Servizi Sanitari e soggetti "Contitolari" o "Responsabili esterni" di trattamenti di dati personali";
- Provvedimento del Garante 1 marzo 2007 "Lavoro: Le linee Guida del garante per Posta Elettronica e Internet" e ss.mm.ii.;
- Provvedimento del Garante 14 giugno 2007 "Linee Guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" e ss.mm.ii.;
- Provvedimento del Garante 24 luglio 2008 "Recepimento normativo in tema di dati di traffico telefonico e telematico" e ss.mm.ii.;
- Provvedimento del Garante 13 ottobre 2008 "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali";
- Provvedimento del Garante 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e ss.mm.ii. (nel seguito Provvedimento);
- Autorizzazione n. 1/2009 al trattamento dei dati sensibili nei rapporti di lavoro del 16 dicembre 2009;
- Autorizzazione n. 2/2009 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale del 16 dicembre2009;
- Decreto del Direttore Generale 25 gennaio 2008, n. 5 "Organizzazione della Struttura Tecnico-Amministrativa" e ss.mm.ii..

3 TERMINI E DEFINIZIONI

La tabella seguente elenca le definizioni dei principali termini utilizzati nel presente Manuale Operativo(*).

Termine	Definizione
Trattamento	Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.
Dato personale	Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
Dati identificativi	I dati personali che permettono l'identificazione diretta dell'interessato.
Dati sensibili	I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
Dati giudiziari	I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
Dato anonimo	Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.
Titolare	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Responsabile	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
Incaricato	La persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile.
Interessato	La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.
Banca di dati	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.
Misure minime	Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.
Strumenti elettronici	Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.
Autenticazione informatica	L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.
Credenziali di autenticazione	I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica (es. UserID e Password).
Parola chiave (Password)	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

(*) Vedasi l'art. 4 del Codice.

Profilo di autorizzazione	L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.
Sistema di autorizzazione	L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

4 AMBITO DI APPLICAZIONE E SCOPO

4.1 Ambito di Applicazione

Il presente Manuale Operativo si applica ai dati personali, censiti e comunicati dai Responsabili del trattamento nelle modalità specificate dal D.R. n.27 del 14 gennaio 2002 "Regolamento di attuazione delle norme sulla tutela delle persone e di altri soggetti rispetto al trattamento di dati personali e per l'adozione di misure minime di sicurezza" trattati con e senza l'ausilio di strumenti elettronici da parte dell'Università degli studi di Trento.

4.2 Scopo

Il presente Manuale Operativo è redatto con l'obiettivo di garantire la conformità agli obblighi di sicurezza e di protezione dei dati personali imposti dagli artt.31, 33, 34, 35 e dall'Allegato B del Codice.

Nell'ambito dei generali obblighi di sicurezza imposti dall'art.31 del Codice, o previsti da speciali disposizioni, il presente Manuale Operativo si propone:

- di assicurare l'adozione di misure minime di sicurezza tali da garantire un livello minimo di protezione dei dati personali, come disposto dagli artt. 33, 34, 35 del Codice;
- di rappresentare un valido strumento per l'adozione di idonee misure di sicurezza, in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, tali da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta dei dati medesimi.

La protezione e la sicurezza dei dati è realizzata attraverso misure di sicurezza di natura fisica (protezione delle aree e dei locali dove sono ubicati gli archivi cartacei di dati e gli strumenti elettronici), logica (protezione dell'accesso ai sistemi e ai dati) e organizzativa (procedure, norme e istruzioni per la gestione delle attività, individuazione dei ruoli, compiti e responsabilità del personale in materia di sicurezza e protezione dei dati) adottate dal Titolare, dai Responsabili del trattamento, dalla Direzione SISTI, dalle altre strutture interne o esterne all'Ateneo addette alla gestione e manutenzione degli strumenti elettronici, dagli Amministratori di Sistema e dagli Incaricati del trattamento.

5 POLITICA DI SICUREZZA E PROTEZIONE DEI DATI PERSONALI

La politica di sicurezza dei dati personali specifica i requisiti generali di sicurezza e protezione dei dati personali adottati dell'Ateneo.

5.1 Politica di Sicurezza e Protezione dei Dati Personali

La conformità alle normative applicabili in materia di sicurezza e protezione dei dati personali con particolare riferimento alle misure di sicurezza imposte dagli artt.31, 33, 34, 35 e dall'Allegato B del D.Lgs. n.196 30 giugno 2003 "Codice in materia di protezione dei dati personali" rappresentano i requisiti di sicurezza e di protezione dei dati personali oggetto di trattamento da parte dell'Ateneo.

Il presente Manuale Operativo elenca le misure di sicurezza da adottare nel trattamento di dati personali da parte del Titolare, dei Responsabili del trattamento, della Direzione SISTI, delle altre strutture interne o esterne all'Ateneo addette alla gestione e manutenzione degli strumenti elettronici, degli Amministratori di Sistema e degli Incaricati del trattamento, secondo quanto disposto dagli artt.31, 33, 34, 35 e dall'Allegato B del D. Lgs. 30 giugno 2003, n.196 "Codice in Materia di Protezione dei Dati Personali".

Le normative applicabili in materia di sicurezza e protezione dei dati personali, il Regolamento e le eventuali Direttive del Titolare e dei Responsabili del trattamento in merito alle finalità, alle modalità e al profilo della sicurezza dei trattamenti e degli strumenti utilizzati sono parte integrante del presente Manuale Operativo.

6 ORGANIZZAZIONE E PERSONALE

L'organizzazione della sicurezza dei dati personali specifica, nel contesto organizzativo dell'Ateneo, i ruoli, le responsabilità, i compiti del personale in materia di sicurezza e protezione dei dati e specifica i criteri per garantire la sicurezza e la protezione dei dati quando le responsabilità delle attività di trattamento sono affidate, in tutto o in parte, all'esterno dell'Ateneo.

6.1 Individuazione delle Figure previste dalle Normative

6.1.1 Titolare del trattamento

L'Università degli studi di Trento è Titolare dei dati personali detenuti dall'Università stessa. Al Titolare spettano le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza. Il Titolare vigila, anche tramite verifiche periodiche, sulla puntuale osservanza delle proprie istruzioni e direttive da parte dei Responsabili del trattamento.

6.1.2 Responsabili del trattamento

I Responsabili del trattamento di dati personali nell'ambito delle strutture dell'Ateneo sono così individuati (art.3 co.2 del Regolamento):

- per le strutture amministrative e di servizio dell'Ateneo, i Dirigenti responsabili delle strutture stesse;
- per le strutture didattiche e di ricerca, i Responsabili delle strutture stesse.

Il Responsabile del trattamento è la persona fisica, la persona giuridica, la Pubblica Amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento di dati personali (art.4 lett.g), art.29 del Codice).

I Responsabili sono individuati tra i soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, compreso il profilo relativo alla sicurezza.

Il Titolare, nella persona del Rettore, può designare, con proprio provvedimento, Responsabili del trattamento altri soggetti, rispetto a quelli individuati dall'art.3 co.2 del Regolamento, anche esterni all'Ateneo, cui affidare l'espletamento di attività strumentali (art.29 del Codice, art.3 del Regolamento).

6.1.2.1 Nomina

I Responsabili del trattamento dei dati personali in Ateneo sono individuati e nominati, , come disposto dall'art.3 co.2, co.3 del Regolamento (art.4 lett.g), art.29 del Codice).

L'elenco aggiornato delle strutture organizzative di primo livello dell'Ateneo e dei nominativi dei Responsabili del trattamento dei dati personali è disponibile nell'area InfoServizi Protezione dei dati personali del portale di Ateneo https://intranet.unitn.it/infoservizi/protezione-dei-dati-personali (accesso riservato al solo personale di Ateneo).

6.1.2.2 Principali Compiti

I Responsabili del trattamento assolvono ai principali compiti seguenti:

- effettuano il trattamento attenendosi alle istruzioni e alle direttive impartite dal Titolare;
- censiscono i trattamenti effettuati presso le strutture di propria responsabilità comunicando ogni variazione alla Direzione Generale, alla Direzione Risorse Umane e, per i trattamenti effettuati con l'ausilio di strumenti elettronici, alla Direzione SISTI;
- individuano e nominano gli Incaricati del trattamento e gli Amministratori di Sistema degli strumenti elettronici che operano sotto la propria diretta autorità;

- aggiornano periodicamente, con cadenza almeno annuale, la lista degli Incaricati e degli Amministratori di Sistema, l'ambito di trattamento loro consentito e i profili di autorizzazione loro assegnati;
- impartiscono istruzioni e direttive agli Incaricati e agli Amministratori di Sistema per lo svolgimento delle attività;
- validano le misure di sicurezza previste dal presente Manuale Operativo, in merito alla loro congruenza e completezza, adottate dalla Direzione SISTI per i trattamenti effettuati con l'ausilio di strumenti elettronici gestiti dalla Direzione medesima;
- adottano le misure di sicurezza previste dal presente Manuale Operativo, con l'eventuale supporto della Direzione SISTI, per i trattamenti effettuati con l'ausilio di strumenti elettronici gestiti autonomamente dalle strutture di propria responsabilità;
- adottano le misure di sicurezza previste dal presente Manuale Operativo per i trattamenti effettuati senza l'ausilio di strumenti elettronici;
- vigilano sul rispetto della politica di sicurezza e protezione dei dati personali adottata dall'Ateneo e sull'adozione delle misure di sicurezza previste dal presente Manuale Operativo.

Con riferimento agli specifici compiti attribuiti ai Responsabili del trattamento di dati personali per i progetti di ricerca per scopi statistici e scientifici in relazione all'adozione delle misure di sicurezza e agli altri obblighi imposti dalla normativa si rimanda al Provvedimento Generale del Garante 16 giugno 2004, n. 2 "Codice di Deontologia e di Buona Condotta per i Trattamenti di Dati Personali per Scopi Statistici e Scientifici".

Accanto al ruolo del Responsabile del trattamento si è ritenuto opportuno altresì individuare una figura di supporto al Responsabile medesimo nello svolgimento delle attività e dei compiti attribuiti nell'ambito della normativa in materia di protezione dei dati personali.

Nel contesto organizzativo dell'Ateneo tale figura è stata individuata nella figura dell'Assistente di Dipartimento/Centro, Assistente di Direzione(*). Nel caso in cui tale figura non sia prevista la funzione di supporto è svolta all'interno della segreteria della struttura responsabile, salvo indicazioni differenti esplicitamente indicate dal Responsabile del trattamento.

Coerentemente ai compiti assegnati ai Responsabili del trattamento, i principali compiti assegnati a tale figura di supporto sono i seguenti:

- compilazione e gestione della documentazione amministrativa richiesta dalla normativa in materia di protezione dei dati personali (es. redazione informativa, ecc.);
- supporto all'aggiornamento dell'elenco dei trattamenti di dati personali effettuati all'interno della struttura;
- supporto alle attività di coordinamento nell'applicazione della normativa all'interno della struttura;
- aggiornamento in merito agli adempimenti previsti dalla normativa;
- coordinamento con le altre strutture di Ateneo per le problematiche in materia di protezione dei dati personali;
- supporto al Responsabile per le attività di controllo e vigilanza sul rispetto della normativa.

6.1.3 Direzione Generale

Alla Direzione Generale è affidato il coordinamento dell'applicazione in Ateneo del D.Lgs.196/2003 "Codice in materia di protezione dei dati personali" e successive modifiche, nel quadro delle direttive date dal Rettore e dagli Organi di Governo dell'Ateneo (art.13 del Regolamento).

Nell'ambito di tale funzione, la Direzione Generale assolve in particolare ai principali compiti seguenti:

- cura l'attuazione della normativa in materia di protezione dei dati personali;

(*) Vedasi gli aggiornamenti degli Allegati A, B al D.D.G. del 25/01/2008, n. 5 "Organizzazione della Struttura Tecnico-Amministrativa".

- svolge compiti di consulenza e di supporto per il Titolare e funzioni di raccordo tra i Responsabili, anche al fine di garantire uniformità e certezza nell'applicazione della normativa;
- può proporre modifiche al Regolamento;
- tiene le relazioni con l'Ufficio del Garante per la protezione dei dati personali.

6.1.4 Direzione Sistemi Informativi, Servizi e Tecnologie Informatiche

La Direzione SISTI adotta le misure di sicurezza imposte dal Codice ed elencate nel presente Manuale Operativo per i trattamenti di dati personali effettuati con l'ausilio di strumenti elettronici gestiti dalla Direzione medesima. La Direzione SISTI supporta inoltre i Responsabili del trattamento nell'adozione delle misure di sicurezza di cui sopra per i trattamenti di dati personali effettuati con l'ausilio di strumenti elettronici gestiti autonomamente dai Responsabili medesimi.

La Direzione SISTI assolve ai principali compiti seguenti (art.9 del Regolamento):

- redige e aggiorna periodicamente il presente Manuale Operativo;
- adotta le misure minime e idonee di sicurezza imposte dal Codice nelle modalità specificate dal presente Manuale Operativo per i trattamenti di dati personali effettuati con l'ausilio di strumenti elettronici gestiti dalla Direzione medesima;
- individua e nomina gli Amministratori di Sistema afferenti alla Direzione medesima e aggiorna periodicamente, con cadenza almeno annuale, l'ambito del trattamento loro consentito;
- comunica periodicamente, anche tramite l'invio di copia del presente Manuale Operativo, ai Responsabili del trattamento, le misure di sicurezza e protezione adottate.

6.1.5 Incaricati del trattamento

Gli Incaricati del trattamento di dati personali sono le persone fisiche autorizzate a compiere le operazioni di trattamento dal Titolare o dal Responsabile (art..4 lett.h), art.30 del Codice).

6.1.5.1 Nomina

All'interno delle strutture di diretta responsabilità, i Responsabili del trattamento individuano e nominano per iscritto gli Incaricati del trattamento dei dati personali, nonché l'ambito del trattamento loro consentito (art.30 del Codice, art..3 co.4 del Regolamento).

Gli Incaricati del trattamento possono essere nominati individuando per iscritto l'ambito di trattamento individualmente consentito ovvero tramite preposizione degli stessi all'unità organizzativa di afferenza per la quale è individuato per iscritto l'ambito di trattamento consentito agli addetti all'unità medesima.

Salvo indicazioni differenti esplicitamente indicate dal Responsabile del trattamento, la nomina degli Incaricati del trattamento si suppone implicita nell'individuazione della struttura di afferenza degli Incaricati medesimi sulla base delle principali attività assegnate alla struttura di afferenza e dei trattamenti di dati personali effettuati dalla struttura stessa e comunicati dal Responsabile del trattamento.

L'organizzazione della struttura tecnico-amministrativa dell'Ateneo, le principali attività svolte dalle varie strutture e l'afferenza del personale tecnico-amministrativo alle strutture stesse sono individuati dal D.D.G. del 25/01/2008, n. 5 "Organizzazione della Struttura Tecnico-Amministrativa, Allegato A 'Organizzazione della Struttura Tecnico-Amministrativa' e Allegato B 'Dislocazione del Personale Tecnico-Amministrativo' e successivi aggiornamenti.

6.1.5.2 Principali Compiti

Gli Incaricati del trattamento, nello svolgimento delle attività di trattamento loro affidate, si attengono alle seguenti indicazioni:

- svolgono le attività loro affidate nel rispetto della normativa vigente in materia di sicurezza e protezione dei dati personali, delle istruzioni e direttive impartite dal Titolare o dal Responsabile e delle misure di sicurezza previste dal presente Manuale Operativo;

- accedono esclusivamente ai dati ai quali sono stati autorizzati ad accedere e richiedono e utilizzano soltanto i dati necessari allo svolgimento delle attività loro affidate;
- controllano e custodiscono con cura e diligenza gli atti e i documenti contenenti dati personali in modo che ad essi non accedano persone prive di autorizzazione, conservandoli negli appositi archivi al termine delle attività (regola della 'Scrivania Sicura');
- conservano gli atti e i documenti contenenti dati sensibili o giudiziari in contenitori o armadi dotati di serratura;
- collaborano con i referenti informatici nell'attuare le misure di sicurezza previste per gli strumenti elettronici;
- custodiscono e non divulgano il codice di identificazione personale (UserID) e la parola chiave (Password) di accesso agli strumenti elettronici e ai dati loro assegnati, modificando quest'ultima al primo utilizzo e successivamente almeno ogni 6 mesi per il trattamento di dati personali e ogni 3 mesi per il trattamento di dati sensibili o giudiziari (regole d'uso della parola chiave);
- non lasciano incustodita la propria stazione di lavoro e gli strumenti elettronici utilizzati durante una sessione di trattamento o attivano permanentemente la funzione di blocco automatico con parola chiave della stazione di lavoro e degli strumenti stessi (regola dello 'Schermo Sicuro');
- segnalano ai referenti informatici qualunque problema o anomalia della propria stazione di lavoro e degli strumenti elettronici utilizzati;
- informano il proprio Responsabile sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti o situazioni critiche.

6.1.6 Amministratori di sistema

Gli Amministratori di sistema sono le persone fisiche che, sulla base degli incarichi loro assegnati presso le strutture di afferenza, svolgono attività di gestione e manutenzione di impianti di elaborazione corrispondenti o assimilabili a quelle dell'amministratore di sistema (*System Administrator*), di basi di dati (*Database Administrator*), di sistemi software complessi quali i sistemi ERP (*Entreprise Resource Planning*), di reti locali e apparati di sicurezza (*Network Administrator*) in tutti i casi in cui tali attività rendano tecnicamente possibile l'accesso, anche fortuito, a dati personali (par.1, punto 1 del Provvedimento).

Gli estremi identificativi delle persone fisiche designate Amministratori di sistema sono riportati, con l'elenco delle funzioni ad esse attribuiti, in un documento interno all'Ateneo mantenuto aggiornato e disponibile da parte del Titolare e dei Responsabili del trattamento.

6.1.6.1 Individuazione

All'interno delle strutture di diretta responsabilità, i Responsabili del trattamento individuano per iscritto gli Amministratori di sistema, nonché gli ambiti di operatività loro consentiti in base al profilo di autorizzazione assegnato. Gli ambiti di operatività possono essere definiti per settori o aree applicative anche con riferimento alle attività assegnate alle strutture di afferenza. La designazione quale Amministratore di sistema deve essere in ogni caso individuale e deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve offrire anche sulla base delle ordinarie attività svolte e dei compiti assegnati all'interno della struttura di afferenza, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza. In ogni caso le funzioni di Amministratore di sistema sono attribuite nel quadro della designazione ad Incaricato del trattamento in conformità all'art.30 del Codice.

La Direzione SISTI provvede all'aggiornamento periodico dell'elenco degli Amministratori di sistema afferenti alle proprie strutture.

6.1.6.2 Principali Compiti

Gli Amministratori di Sistema, nello svolgimento delle attività loro affidate, si attengono alle seguenti indicazioni (art.30 del Codice):

- svolgono le attività loro affidate nel rispetto della normativa vigente in materia di sicurezza e protezione dei dati personali, delle istruzioni e direttive impartite dal Titolare o dal Responsabile e delle misure di sicurezza previste dal presente Manuale Operativo;
- accedono esclusivamente ai dati ai quali sono stati autorizzati ad accedere e richiedono e utilizzano soltanto i dati necessari allo svolgimento delle attività loro affidate;
- svolgono le attività loro affidate osservando le disposizioni tecniche, organizzative e operative previste dal presente Manuale Operativo per la gestione e manutenzione e l'attuazione delle misure di sicurezza per gli strumenti elettronici;
- supportano gli utenti nell'attuare le misure di sicurezza previste per gli strumenti elettronici;
- custodiscono e non divulgano il codice di identificazione personale (UserID) e la parola chiave (Password) di accesso agli strumenti elettronici e ai dati loro assegnati, modificando quest'ultima al primo utilizzo e successivamente almeno ogni 6 mesi per il trattamento di dati personali e ogni 3 mesi per il trattamento di dati sensibili o giudiziari (regole d'uso della parola chiave);
- non lasciano incustodita la propria stazione di lavoro e gli strumenti elettronici utilizzati durante una sessione di lavoro o attivano permanentemente la funzione di blocco automatico con parola chiave della stazione di lavoro e degli strumenti stessi (regola dello 'Schermo Sicuro');
- supportano gli utenti nella risoluzione di qualunque problema o anomalia della stazione di lavoro e degli strumenti elettronici utilizzati;
- informano il proprio Responsabile sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti o situazioni critiche.

6.1.6.3 Incaricati della Custodia delle Copie delle Credenziali di Autenticazione

La Direzione SISTI non conserva copie delle credenziali di autenticazione degli Incaricati e quindi non è prevista l'individuazione dei soggetti incaricati della loro custodia (punto 10 dell'Allegato B del Codice).

La disponibilità dei dati o degli strumenti elettronici, in caso di prolungata assenza o impedimento degli Incaricati che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, è assicurata attraverso l'uso di una parola chiave (Password) temporanea o di credenziali di autenticazione temporanee (UserID e Password), attivate e utilizzate per lo svolgimento dei soli interventi necessari e quindi disattivate.

Il Responsabile del trattamento conserva traccia degli interventi effettuati e ne informa tempestivamente gli eventuali Incaricati interessati.

6.2 Sicurezza dei Dati Personali nei Rapporti con Soggetti Terzi

6.2.1 Protezione dei dati personali per le attività affidate all'esterno dell'Ateneo

Nel caso in cui l'Ateneo affidi all'esterno attività continuative connesse al trattamento di dati personali, il Rettore nomina per iscritto Responsabile esterno del trattamento il soggetto a cui le attività sono affidate, specificando i trattamenti interessati e l'ambito di trattamento consentito, i compiti affidati e le eventuali istruzioni per il loro svolgimento nonché i criteri adottati, comprese eventuali verifiche periodiche, per garantire l'adozione delle misure minime di sicurezza imposte dal Codice per i trattamenti oggetto dell'affidamento.

Nel caso in cui si adottino misure minime di sicurezza avvalendosi di soggetti esterni, questi ultimi rilasciano una attestazione di conformità degli interventi effettuati alle disposizioni dell'Allegato B del Codice (punto 25 dell'Allegato B del Codice).

Nel caso in cui l'Ateneo affidi all'esterno servizi di amministrazione di sistema, il Titolare o il Responsabile esterno conservano direttamente e specificamente gli estremi identificativi delle persone fisiche preposte quali Amministratori di sistema (punto 2 lett.d) del Provvedimento).

6.3 Gestione degli Incidenti di Sicurezza informatica

Presso la Direzione SISTI è attivo un presidio organizzativo denominato CERT@unitn (Computer Emergency Response Team) per la gestione e il coordinamento delle attività di risposta agli incidenti di sicurezza informatica che presentano una rilevanza e una criticità a livello di Ateneo.

Il personale segnala tempestivamente eventuali incidenti di sicurezza informatica o malfunzionamenti degli strumenti elettronici, dei servizi, delle applicazioni (es. infezione da virus informatico) alla struttura informatica di riferimento al fine di ridurre i rischi di ulteriori danni ai dati e agli strumenti elettronici, riportando tutte le informazioni utili alla risoluzione del problema (lo strumento elettronico e il servizio coinvolti, i sintomi del problema, ogni messaggio che appare sullo schermo, ecc.).

Si rinvia alla pagina CERT@unitn http://icts.unitn.it/certunitn del portale ICTS@unitn della Direzione SISTI per la documentazione tecnica del servizio.

7 REGISTRO DEI TRATTAMENTI DI DATI PERSONALI

Il registro dei trattamenti di dati personali specifica l'elenco dei trattamenti di dati personali effettuati presso le strutture dell'Ateneo e le modalità per il suo aggiornamento periodico.

7.1 Registro dei Trattamenti di Dati Personali

I Responsabili del trattamento aggiornano periodicamente l'elenco dei trattamenti di dati personali effettuati presso le strutture di loro responsabilità, sulla base dei processi e delle attività svolte dalle strutture stesse che comportano un trattamento di dati personali, comunicandolo alla Direzione Generale, alla Direzione Risorse Umane e, per i trattamenti effettuati con l'ausilio di strumenti elettronici, alla Direzione SISTI (art.4 del Regolamento).

Il registro aggiornato dei trattamenti di dati personali è disponibile nell'area InfoServizi Protezione dei dati personali del portale di Ateneo https://intranet.unitn.it/infoservizi/protezione-dei-dati-personali (accesso riservato al solo personale di Ateneo).

Il registro è redatto sulla base delle comunicazioni periodiche effettuate dai Responsabili del trattamento e dell'articolazione organizzativa tecnico-amministrativa dell'Ateneo come individuata dal D.D.G. del 25/01/2008, n. 5 "Organizzazione della Struttura Tecnico-Amministrativa, Allegato A 'Organizzazione della Struttura Tecnico-Amministrativa' e successivi aggiornamenti che elenca le strutture tecnico-amministrative di Ateneo e le principali attività loro assegnate.

8 SICUREZZA FISICA DEI DATI PERSONALI

La sicurezza fisica dei dati personali comprende le misure per la protezione fisica delle aree e dei locali, degli strumenti elettronici utilizzati per il trattamento e degli archivi cartacei, degli atti e dei documenti contenenti dati personali al fine di prevenire accessi fisici non autorizzati, danneggiamento o perdita dei dati medesimi.

8.1 Trattamenti Effettuati con l'Ausilio di Strumenti Elettronici

8.1.1 Protezione delle aree e dei locali

Gli strumenti elettronici contenenti dati personali compresi i supporti rimovibili di memorizzazione e le copie di sicurezza utilizzate per le attività di salvataggio e ripristino sono protetti collocandoli in aree o locali dotati di misure di sicurezza fisica adeguate alla loro criticità e ai dati memorizzati al fine di prevenire accessi non autorizzati, trattamenti non consentiti o loro danneggiamento. I supporti rimovibili di memorizzazione e le copie di sicurezza utilizzate per le attività di salvataggio e ripristino contenenti dati sensibili o giudiziari sono conservati in contenitori o armadi dotati di serratura o in aree o locali ad accesso controllato (art.34 co.1 lett.f), punto 21 dell'Allegato B del Codice).

Le principali misure di sicurezza per la protezione delle aree e dei locali comprendono sistemi attivi e passivi di controllo dell'accesso (portierato, ingressi dotati di serratura, sistemi a bagde magnetico, sistemi di allarme antintrusione e antifurto, sistemi di videosorveglianza), sistemi antincendio, sistemi di climatizzazione, gruppi di continuità per l'alimentazione elettrica, armadi e/o casseforti blindati e/o ignifughi per la conservazione delle copie di sicurezza nonché altre misure necessarie sulla base della specifica situazione fisico/ambientale (es. sistema antiallagamento).

Si rinvia alla pagina Servizi di Datacenter http://icts.unitn.it/servizi-di-datacenter del portale ICTS@unitn della Direzione SISTI per la documentazione tecnica del servizio.

8.1.2 Regola dello 'schermo sicuro'

Gli Incaricati non lasciano incustodito e accessibile lo strumento elettronico utilizzato durante una sessione di trattamento. Anche nel caso di assenza temporanea, terminano la sessione di trattamento o attivano il blocco con parola chiave dello strumento o, in alternativa, attivano permanentemente la funzione di blocco automatico con parola chiave dello strumento stesso (Screen Saver protetto con Password) (punto 9 dell'Allegato B del Codice).

8.2 Trattamenti Effettuati senza l'Ausilio di Strumenti Elettronici

8.2.1 Regola della 'scrivania sicura'

Gli Incaricati, nello svolgimento delle operazioni di trattamento, controllano e custodiscono con cura e diligenza gli atti e i documenti contenenti dati personali in modo che ad essi non accedano persone prive di autorizzazione, conservandoli negli appositi archivi al termine delle operazioni (art.35 co.1 lett.b), punti 27, 28 dell'Allegato B del Codice).

8.2.2 Protezioni ulteriori degli archivi cartacei contenenti dati sensibili o giudiziari

Gli archivi cartacei contenenti dati sensibili o giudiziari sono conservati in contenitori o armadi dotati di serratura o in aree o locali ad accesso controllato (portierato, ingressi dotati di serratura, sistemi di controllo dell'accesso tramite bagde magnetico, sistemi di allarme antintrusione e antifurto, sistemi di videosorveglianza). Nel caso in cui le aree o i locali non siano dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura degli uffici, sono identificate e registrate (art.35 co.1 lett.c), punto 29 dell'Allegato B del Codice).

9 SICUREZZA DEGLI STRUMENTI ELETTRONICI

La sicurezza degli strumenti elettronici comprende le misure per la gestione e la manutenzione degli strumenti elettronici, l'integrità del software e dei dati personali, la protezione della rete e dei servizi di rete, la disponibilità e il ripristino dei dati e dei sistemi in caso di incidenti, guasti o malfunzionamenti.

9.1 Protezione degli Strumenti Elettronici e dei Dati Personali

9.1.1 Aggiornamento del software

Gli aggiornamenti periodici dei software di base e applicativi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne difetti (*Software Patches*) sono effettuati con frequenza almeno annuale per i trattamenti di dati personali e semestrale per i trattamenti di dati sensibili o giudiziari (punto 17 dell'Allegato B del Codice).

Si rinvia alla pagina Servizi di Datacenter http://icts.unitn.it/servizi-di-datacenter del portale ICTS@unitn della Direzione SISTI per la documentazione tecnica del servizio.

9.1.2 Protezione da codice malevolo

Gli strumenti elettronici e i dati personali sono protetti contro il rischio di intrusione e dall'azione di programmi di cui all'art.615-*quinquies*(*) del Codice Penale tramite *Sistema Antivirus* aggiornato con frequenza almeno semestrale (art.34 co.1 lett.e), punto 16 dell'Allegato B del Codice).

Si rinvia alla pagina AVAS - Antivirus e Antispam http://icts.unitn.it/avas-antivirus-e-antispam del portale ICTS@unitn della Direzione SISTI per la documentazione tecnica del servizio.

9.1.3 Integrità e disponibilità dei dati personali

La Direzione SISTI e le strutture addette alla gestione e manutenzione degli strumenti elettronici adottano misure tecniche, organizzative e procedurali per il salvataggio periodico dei dati personali con frequenza almeno settimanale e il loro eventuale ripristino nel caso di danneggiamento degli stessi o degli strumenti elettronici. Il ripristino dell'accesso ai dati sensibili o giudiziari, in caso di danneggiamento degli stessi o degli strumenti elettronici, è garantito entro 7 giorni (*Backup&Restore*) (art.34 co.1 lett.f), punti 18, 23 dell'Allegato B del Codice).

Si rinvia alla pagine Servizi di Datacenter http://icts.unitn.it/servizi-di-datacenter, Risorse di rete, cartelle condivise, backup http://icts.unitn.it/risorse-di-rete-cartelle-condivise-backup del portale ICTS@unitn della Direzione SISTI per la documentazione tecnica dei servizi.

9.1.4 Isolamento degli strumenti elettronici contenenti dati sensibili o giudiziari

Gli strumenti elettronici contenenti dati sensibili o giudiziari sono protetti contro l'accesso abusivo di cui all'art.615-*ter*(**) del Codice Penale mediante *Firewall* di sistema o di rete ovvero altro idoneo strumento elettronico (punto 20 dell'Allegato B del Codice).

Si rinvia alla pagina Rete dati http://icts.unitn.it/rete-dati del portale ICTS@unitn della Direzione SISTI per la documentazione tecnica del servizio.

9.1.5 Cifratura dei dati sensibili

Le strutture di Ateneo che trattano nell'esercizio delle professioni sanitarie dati sensibili idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche dati con le modalità di cui all'art.22

(*) Art. 615-*quinquies* Codice Penale "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico".
(**) Art. 615-*ter* Codice Penale "Accesso abusivo ad un sistema informatico o telematico".

co.6[*] del Codice adottano misure tecniche e/o organizzative per la cifratura dei dati sensibili o la loro separazione al fine di consentire il trattamento disgiunto dei medesimi dagli altri dati personali che permettono di identificare direttamente gli Interessati (punto 24 dell'Allegato B del Codice).

9.1.6 Gestione dei data log

Le registrazioni (*Data Log*) generati dagli strumenti elettronici (sistemi e applicativi) che contengono dati personali sono trattati dalle strutture addette alla loro gestione e manutenzione nel rispetto delle normative vigenti in relazione alle misure tecniche, organizzative e procedurali imposte per la loro gestione, compreso il profilo di autorizzazione all'accesso, e alle finalità per la loro conservazione e il loro utilizzo.

I *Data Log* che contengono dati personali sono trattati dalla Direzione SISTI e dalle strutture addette alla gestione e manutenzione degli strumenti elettronici per le seguenti finalità:

- monitoraggio dei sistemi e applicativi gestiti, dei servizi erogati e della sicurezza informatica;
- documentazione per eventuali contestazioni o controversie;
- adempimento a obblighi di legge.

9.1.7 Dismissione e riuso degli strumenti elettronici e dei supporti di memorizzazione

I supporti di memorizzazione (compresi i supporti di memorizzazione contenuti negli strumenti elettronici e le copie di sicurezza utilizzate per le attività di salvataggio e ripristino) contenenti dati personali, se non più utilizzati, sono distrutti o resi inutilizzabili. Possono essere riutilizzati soltanto se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili (punto 22 dell'Allegato B del Codice).

Si rinvia alla pagina Dismissioni attrezzature informatiche http://icts.unitn.it/dismissioni-attrezzature-informatiche del portale ICTS@unitn della Direzione SISTI per la documentazione tecnica del servizio.

[*] Art. 22 co. 6 del Codice "I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità".

10 CONTROLLO DELL' ACCESSO AI DATI PERSONALI

Il controllo dell'accesso ai dati personali specifica le misure per limitare l'accesso agli strumenti elettronici e ai dati personali, l'accesso agli archivi cartacei, agli atti e ai documenti contenenti dati personali da parte dei soli soggetti autorizzati al loro trattamento.

10.1 Trattamenti Effettuati con l'Ausilio di Strumenti Elettronici

10.1.1 Controllo dell'accesso agli strumenti elettronici e ai dati personali

Il trattamento di dati personali effettuato con l'ausilio di strumenti elettronici è consentito agli Incaricati del trattamento dotati di:

- credenziali di autenticazione (UserID e Password) atte al superamento di una procedura di autenticazione (sistema di autenticazione informatica);
- profilo di autorizzazione atto al superamento di una procedura di autorizzazione nel caso siano previsti profili di autorizzazione di ambito diverso per gli Incaricati del trattamento (sistema di autorizzazione informatica).

La Direzione SISTI o la struttura addetta alla gestione e manutenzione degli strumenti elettronici gestiscono il rilascio, l'aggiornamento e la disattivazione delle credenziali di autenticazione (sistema di autenticazione informatica) e l'assegnazione e l'aggiornamento dei profili di autorizzazione agli Incaricati (sistema di autorizzazione informatica), sulla base delle richieste inviate dei Responsabili del trattamento (art.34 co.1 lett.a) c) d), art. 30 co.2, punti 1, 2, 3, 12, 13, 15 dell'Allegato B del Codice).

Si rinvia alla pagina Autenticazione & Account http://icts.unitn.it/autenticazione-account del portale ICTS@unitn della Direzione SISTI per la documentazione tecnica del servizio.

10.1.1.1 Sistema di Autenticazione Informatica

L'accesso agli strumenti elettronici e ai dati è controllato tramite una sistema di autenticazione informatica degli Incaricati basato sull'utilizzo di credenziali di autenticazione (art.34 co.1 lett.a) b), punti 1, 2, 3, 4, 5, 6, 7, 8 dell'Allegato B del Codice):

- le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato (UserID) associato a una parola chiave (Password) conosciuta solamente dall'Incaricato;
- la parola chiave rispetta le regole d'uso adottate(*);
- le credenziali di autenticazione sono relative a uno specifico trattamento o a un insieme di trattamenti;
- ad ogni Incaricato sono assegnate individualmente una o più credenziali di autenticazione;
- il codice per l'identificazione assegnato ad un Incaricato non può essere riassegnato ad altri Incaricati.
- le credenziali di autenticazione sono disattivate in caso di perdita della qualità che consente all'Incaricato l'accesso ai dati ovvero se non utilizzate per più di 6 mesi(**);

Attualmente il principale meccanismo adottato in Ateneo per l'autenticazione degli utenti è rappresentato dall'uso di UserID e Password.

A partire dall'anno 2015 il sistema di autenticazione centralizzata di Ateneo affiancherà al meccanismo di autenticazione basato su UserID e Password, l'utilizzo della Tessera Sanitaria-Carta Nazionale dei Servizi (TS-CNS) (art.64 del CAD, punto 2 dell'Allegato B del Codice).

Si rinvia alla pagine Anagrafica di Ateneo - Identity Management (ADA) http://icts.unitn.it/ada e Carta Nazionale dei Servizi http://icts.unitn.it/carta-nazionale-dei-servizi del portale ICTS@unitn della Direzione SISTI per la documentazione tecnica del servizio.

(*) Vedasi par. 10.1.3 'Regole d'uso della parola chiave';
(**) Con l'eventuale esclusione delle credenziali di autenticazione preventivamente autorizzate per le sole attività di gestione tecnica degli strumenti elettronici.

10.1.1.2 Sistema di Autorizzazione Informatica

L'accesso ai dati e alle funzionalità degli strumenti elettronici è controllato tramite un sistema di autorizzazione basato su profili di autorizzazione assegnati agli Incaricati (art.34 co.1 lett.c) d), punti 12, 13, 14, 15 dell'Allegato B del Codice):

- i profili di autorizzazione, in relazione alle caratteristiche degli strumenti elettronici, specificano i dati accessibili dall'Incaricato e le operazioni eseguibili sugli stessi.
- i profili di autorizzazione sono assegnati per singolo Incaricato, per unità organizzativa di afferenza o per classe omogenea di incarico.
- Gli Incaricati accedono ai soli dati necessari per lo svolgimento delle operazioni di trattamento loro affidate;
- i profili di autorizzazione sono individuati dal Responsabile del trattamento che verifica, con cadenza almeno annuale, la sussistenza delle condizioni per la loro conservazione da parte degli Incaricati.

Si rinvia alla pagina Anagrafica di Ateneo - Identity Management (ADA) http://icts.unitn.it/ada del portale ICTS@unitn della Direzione SISTI per la documentazione tecnica del servizio.

10.1.2 Aggiornamento della lista degli incaricati e degli amministratori di sistema

I Responsabili del trattamento aggiornano periodicamente, con cadenza almeno annuale, la lista degli Incaricati e i profili di autorizzazione loro assegnati (art.34 co.1 lett.d), art. 30 co.2, punti 14, 15 dell'Allegato B del Codice).
I Responsabili del trattamento verificano periodicamente, con cadenza almeno annuale, l'adeguatezza dell'operato degli Amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalle norme vigenti rispetto ai trattamenti di dati personali (punto 2 lett.e) del Provvedimento).

10.1.3 Regole d'uso della parola chiave

La parola chiave (Password), prevista dal sistema di autenticazione informatica e utilizzata degli Incaricati deve (punti 4, 5 dell'Allegato B del Codice):

- essere composta da almeno 8 caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- non contenere riferimenti agevolmente riconducibili all'Incaricato;
- essere modificata dall'Incaricato al primo utilizzo;
- essere modificata dall'Incaricato almeno ogni 6 mesi per il trattamento di dati personali e ogni 3 mesi per il trattamento di dati sensibili o giudiziari;
- essere mantenuta segreta da parte dell'Incaricato.

Le regole d'uso della parola chiave (Password) sono implementate tramite requisiti tecnico- funzionali degli strumenti elettronici e regole di comportamento rispettate dagli utenti. I servizi di autenticazione centralizzati gestiti dalla Direzione SISTI richiedono il cambio della Password da parte degli utenti almeno ogni 6 mesi.

10.2 Trattamenti Effettuati senza l'Ausilio di Strumenti Elettronici

10.2.1 Controllo dell'accesso agli archivi cartacei di dati personali

Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito agli Incaricati del trattamento, individuati e nominati dal Responsabile del trattamento, per i quali è individuato l'ambito del trattamento loro consentito. L'ambito di trattamento può essere assegnato per singolo Incaricato, per unità organizzativa di afferenza o per classe omogenea di incarico (art.35 co.1 lett.a), art.30 co.2 e punto 27 dell'Allegato B del Codice).

10.2.2 Aggiornamento della lista degli incaricati

I Responsabili del trattamento aggiornano periodicamente, con cadenza almeno annuale, la lista degli Incaricati del trattamento e l'ambito del trattamento loro consentito (art.35 co.1 lett.a), art. 30 co.2 e punto 27 dell'Allegato B del Codice).

11 VERIFICHE DI CONFORMITÀ NORMATIVA E TECNICA

Le verifiche di conformità normativa e tecnica dei trattamenti di dati personali comprendono i controlli, effettuati dal Titolare e dai Responsabili del trattamento, del rispetto della politica di sicurezza dei dati personali adottata dall'Ateneo e le verifiche, effettuate dalla Direzione SISTI e dalle altre strutture addette alla gestione e manutenzione degli strumenti elettronici, della conformità tecnica degli strumenti elettronici alle misure di sicurezza previste dal presente Manuale Operativo.

11.1 Verifiche della Conformità ai Requisiti di Sicurezza e Protezione dei Dati Personali

11.1.1 Conformità alla politica di sicurezza dei dati personali

Il Titolare e i Responsabili del trattamento, nell'ambito delle loro competenze e responsabilità indicate dal Regolamento e dal presente Manuale Operativo, vigilano sul rispetto della politica di sicurezza dei dati personali adottata dall'Ateneo e sull'adozione delle misure di sicurezza previste dal presente Manuale Operativo (art.29 del Codice).

11.1.2 Conformità tecnica degli strumenti elettronici

La Direzione SISTI, e le altre strutture addette alla gestione e manutenzione degli strumenti elettronici, verificano periodicamente la conformità tecnica degli strumenti elettronici alle misure di sicurezza previste dal presente Manuale Operativo (art.9 del Regolamento).

La Direzione SISTI verifica periodicamente l'adozione delle misure di sicurezza per i trattamenti effettuati con l'ausilio di strumenti elettronici gestiti dalla medesima. Per i trattamenti effettuati con strumenti elettronici non gestiti dalla Direzione SISTI, la verifica di conformità tecnica degli strumenti elettronici è svolta dal Responsabile del trattamento e dalla struttura addetta alla loro gestione e manutenzione, con l'eventuale supporto, della Direzione SISTI.

ALLEGATO RIEPILOGO DELLE MISURE DI SICUREZZA

Riepilogo delle Misure di Sicurezza	Applicabilità		
	Tutti i Trattamenti	**Trattamenti effettuati senza l'ausilio di strumenti elettronici**	**Trattamenti effettuati con l'ausilio di strumenti elettronici**
Politica di Sicurezza e Protezione dei Dati Personali			
5.1 Politica di Sicurezza e Protezione dei Dati Personali	X		
Organizzazione e Personale			
6.1 Individuazione delle Figure Previste dalle Normative			
6.1.1 Titolare del Trattamento	X		
6.1.2 Responsabili del Trattamento	X		
6.1.3 Direzione Generale	X		
6.1.4 Direzione Sistemi Informativi, Servizi e Tecnologie Informatiche			X
6.1.5 Incaricati del Trattamento	X		
6.1.6 Amministratori di Sistema			X
6.2 Sicurezza dei Dati Personali nei Rapporti con Soggetti Terzi			
6.2.1 Protezione dei Dati Personali per le Attività Affidate all'Esterno dell'Ateneo	X		
6.4 Gestione degli Incidenti di Sicurezza Informatica			X
Registro dei Trattamenti di Dati Personali			
7.1 Registro dei Trattamenti di Dati Personali	X		
Sicurezza Fisica dei Dati Personali			
8.1 Trattamenti Effettuati con l'Ausilio di Strumenti Elettronici			
8.1.1 Protezione delle Aree e dei Locali			X
8.1.2 Regola dello 'schermo sicuro'			X
8.2 Trattamenti Effettuati senza l'Ausilio di Strumenti Elettronici			
8.2.1 Regola della 'scrivania sicura'		X	
8.2.2 Protezioni Ulteriori degli Archivi Cartacei contenenti Dati Sensibili o Giudiziari		X	
Sicurezza degli Strumenti Elettronici			
9.1 Protezione degli Strumenti Elettronici e dei Dati			

9.1.2 Aggiornamento del Software			X
9.1.3 Protezione da Codice Malevolo			X
9.1.4 Integrità e Disponibilità dei Dati Personali			X
9.1.5 Isolamento degli Strumenti Elettronici contenenti Dati Sensibili o Giudiziari			X
9.1.6 Cifratura dei Dati Sensibili			X
9.1.7 Gestione dei Data Log			X
9.1.8 Dismissione e Riuso degli Strumenti Elettronici e dei Supporti di Memorizzazione			X
Controllo dell'Accesso ai Dati Personali			
10.1 Trattamenti Effettuati con l'Ausilio di Strumenti Elettronici			
10.1.1 Controllo dell'Accesso agli Strumenti Elettronici e ai Dati Personali			X
10.1.1.1 Sistema di Autenticazione Informatica			X
10.1.1.2 Sistema di Autorizzazione Informatica			X
10.1.2 Aggiornamento della Lista degli Incaricati, degli Amministratori di Sistema e dei Profili di Autorizzazione			X
10.1.3 Regole d'Uso della Parola Chiave			X
10.2 Trattamenti Effettuati senza l'Ausilio di Strumenti Elettronici			
10.2.1 Controllo dell'Accesso agli Archivi Cartacei di Dati Personali		X	
10.2.2 Aggiornamento della Lista degli Incaricati e dell'Ambito del Trattamento		X	
Verifiche di Conformità Normativa e Tecnica			
11.1 Verifiche della Conformità ai Requisiti di Sicurezza e Protezione dei Dati Personali			
11.1.1 Conformità alla Politica di Sicurezza e Protezione dei Dati Personali	X		
11.1.2 Conformità Tecnica degli Strumenti Elettronici			X