UNIVERSITÀ DEGLI STUDI FIRENZE

Decreto n. 580 prot. 85920

Il Rettore e Il Direttore Generale

Oggetto: Soggetti del trattamento dei dati personali. Referenti per la protezione dei dati personali e Incaricati del trattamento.

Visto il *Regolamento generale sulla protezione dei dati personale* (di seguito Regolamento UE o GDPR) di cui al Regolamento UE 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;

Considerato che il suddetto Regolamento UE è obbligatorio e direttamente operante in ciascuno degli Stati membri dell'Unione Europea, fatta eccezione per alcuni ambiti sui quali esso stesso richiede l'integrazione regolatoria degli Stati membri;

Preso atto che a norma dell'art.99 del GDPR, quest'ultimo dovrà trovare applicazione negli Stati membri a partire dal 25 maggio 2018, prevalendo sulla normativa nazionale in materia ove incompatibile;

Visto che non sono ancora state adottate disposizioni nazionali di adeguamento della normativa interna a quella europaa, in particolare del D.Lgs 196/2003 recante " *Codice in materia di protezione dei dati personali*" adottato in attuazione alla Direttiva 95/46/CE, ormai abrogata;

Precisato che con il GDPR si passa dal concetto di Privacy come diritto individuale alla riservatezza, ovvero, diritto di escludere gli altri dalla propria sfera privata, a quello di **diritto alla protezione dei dati personali** come diritto fondamentale autonomo, che si estende oltre la sfera della vita privata dell'interessato, anche ai rapporti di quest'ultimo con la persona fisica, giuridica o l'autorità pubblica che tratta i suoi dati, garantendo all'interessato il potere di controllare e di pretendere che i propri dati personali siano raccolti e trattati nel rispetto della legge (diritto alla autodeterminazione informativa);

Considerato che il GDPR prevede:
- il rafforzamento delle garanzie e dei diritti azionabili da parte dell'interessato dal trattamento per il controllo delle proprie informazioni;
- un'accresciuta responsabilità del Titolare del trattamento dei dati attraverso l'introduzione del principio di *responsabilizzazione* (*accountability)* secondo il quale è rimesso al Titolare del trattamento il compito di individuare, in base alla natura dei dati personali trattati, all'ambito di

applicazione, alle finalità perseguite ed ai rischi che i trattamenti effettuati comportano per i diritti e le libertà degli interessati, quali siano le misure di sicurezza tecniche ed organizzative adeguate da adottare nonché il compito di dimostrare, in qualsiasi momento, che il trattamento dei dati avviene in piena conformità a quanto previsto dal GDPR, secondo un approccio non più squisitamente formale, ma fortemente sostanziale, in cui la protezione dei dati personali divenga valore che permea l'intero agire del soggetto Titolare;

Ritenuto che nelle more dell'adeguamento della normativa nazionale alle disposizioni del GDPR, sia necessario proseguire nel percorso attuativo già descritto ed avviato con il Decreto del Direttore Generale n.2003 (prot. n.176730), del 27 novembre 2017, procedendo, in questa sede, all'individuazione dei soggetti interni ai quali si ritiene opportuno assegnare incarichi e responsabilità in merito alle attività di trattamento dei dati personali di cui l'Ateneo è Titolare;

Rilevato che, come precisato dal Garante per la protezione dei dati personali nella propria *Guida all'applicazione del Regolamento Europeo in materia di protezione dei dati personali*, e confermato dal Codau, nelle *Linee guida in materia di privacy e protezione dei dati personali in ambito universitario*, l'individuazione di un'organizzazione funzionale alla protezione dei dati, nella quale siano delineati i trattamenti che competono ad ogni struttura ed indicati, secondo afferenze, mansioni e responsabilità i **soggetti coinvolti nella protezione dei dati personali** costituisce misura di sicurezza di tipo organizzativo necessaria;

Ritenuto che sia necessario creare, a livello istituzionale, una sinergia tra i processi e le direttive relative alla gestione del trattamento dei dati personali e l'adozione di misure di sicurezza dei sistemi informatici;

Considerato che, in base all'art. 4, n.7), del GDPR il **Titolare del trattamento dei dati** (*Controller*)**,** con riguardo a tutti i dati trattati per lo svolgimento dei propri compiti di pubblico interesse ed il perseguimento delle proprie finalità istituzionali, è l'Università degli Studi di Firenze;

Considerato altresì che a norma del combinato disposto degli artt. 4, n.8) e 28 del GDPR il Responsabile del trattamento dei dati (*Processor*) è <u>solo</u> il soggetto esterno a cui sono affidati trattamenti per finalità proprie del titolare del trattamento, con conseguente formale superamento della definizione di responsabile interno del trattamento prevista nel "*Regolamento di attuazione del Codice di protezione dei dati personali in possesso dell'Università degli Studi di Firenze"* approvato con D.R. 29 dicembre 2005, n.1177 (prot. n.79382).

Ritenuto necessario precisare che i soggetti designati come responsabili interni del trattamento, ai sensi dell'art.3 del suddetto "*Regolamento di attuazione del Codice di protezione dei dati personali in possesso dell'Università degli Studi di Firenze"* di cui al D.R. 29 dicembre 2005, n.1177 (prot. n.79382), nelle more del suo aggiornamento, sono da intendersi oggi denominati **Referenti per la protezione dei dati;**

UNIVERSITÀ
DEGLI STUDI
FIRENZE

Preso atto che tutti i soggetti, dipendenti e collaboratori, che materialmente compiono operazioni di trattamento sui dati personali in possesso dell'Ateneo, devono essere **istruiti** a norma dell'art.29 del GDPR secondo il quale "… *chiunque agisca sotto la … autorità …del titolare, che abbia accesso a dati personali, non può trattare dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli stati membri*";

Precisato che per **trattamento di dati personali**, a norma dell'art.4, n.2) del GDPR, si intende qualsiasi operazione o insieme di operazioni riguardante una persona fisica identificata o identificabile, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Precisato altresì che per **dato personale**, a norma dell'art. 4, n.1), del GDPR si intende " *qualsiasi informazione riguardante una* ***persona fisica*** *identificata o identificabile (<<interessato>>)"* e che si considera *"identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica culturale o sociale*";

Preso atto che l'Università degli Studi di Firenze si è dotata del **Registro delle attività di trattamento**, in attuazione dell'art. 30 del GDPR, nel quale sono analiticamente individuati i trattamenti e le finalità dei trattamenti perseguite da ogni unità organizzativa/struttura/dipartimento, che si allega, per estratto, al presente atto sotto la lettera " **A**" e che sarà pubblicato per esteso nell'apposita sezione del sito istituzionale;

Ritenuto necessario designare come **Incaricati del trattamento** dei dati personali di cui l'Ateneo è Titolare, e quindi di autorizzare al trattamento, tutti i soggetti, dipendenti e collaboratori, che materialmente compiono operazioni di trattamento dei dati detenuti, in virtù della loro documentata preposizione alle strutture per le quali, il suddetto Registro delle attività di trattamento, stabilisce l'ambito e le finalità dei trattamenti consentiti al personale afferente alla struttura medesima;

Precisato che la designazione quale Incaricato del trattamento dei dati personali non implica l'attribuzione di nessuna ulteriore funzione rispetto a quelle già proprie del dipendente o del collaboratore, costituendo una misura di sicurezza di tipo organizzativo necessaria, che deve essere accompagnata dall'adeguata informazione e formazione, di tali soggetti, da parte del Titolare sulle modalità cui attenersi nel trattamento dei dati;

Tutto ciò premesso e considerato

DECRETANO

1. di designare quali **Referenti per la protezione dei dati** (ex Responsabili dei dati):

- i Dirigenti delle Aree dell'amministrazione centrale;
- i Direttori dei Centri di Servizio;
- i Responsabili amministrativi dei Dipartimenti relativamente ai dati personali trattati nella gestione amministrativa delle rispettive strutture;
- i Direttori dei Dipartimenti relativamente ai dati personali raccolti **e** trattati nell'ambito delle attività di ricerca condotte dal Dipartimento e dai Centri di ricerca a questo afferenti.

2. i Referenti per la protezione dei dati, come sopra individuati, sono tenuti a:

- conoscere e rispettare le disposizioni di legge, di regolamento nonché le istruzioni impartite dal Titolare in materia di protezione dei dati personali ed i loro successivi aggiornamenti, nonché a vigilare sul loro rispetto da parte dei dipendenti e collaboratori afferenti alla rispettiva struttura;
- adottare le opportune misure di sicurezza per garantire la protezione dei dati personali trattati qualora, tali dati, dovessero essere raccolti in autonomia dalle strutture di propria competenza al di fuori degli archivi cartacei ed informatizzati o dei server gestiti in maniera centralizzata dall'Ateneo, inviando, in tali casi, al RPD una dettagliata comunicazione scritta che indichi:
  - finalità e modalità del trattamento;
  - natura dei dati, luogo dove sono custoditi, categorie di interessati cui i dati si riferiscono;
  - ambito di comunicazione e diffusione dei dati;
  - una descrizione delle misure di sicurezza adottate;
  - eventuale connessione con altri trattamenti o banche dati.
- adottare le opportune misure di sicurezza dei sistemi informatici, qualora tali sistemi dovessero essere gestiti, in autonomia, dalle strutture di cui sono responsabili, in accordo con le disposizioni di legge nonché con le indicazioni impartite dal Responsabile per la Transizione Digitale (RTD)
- comunicare, entro il 30 settembre di ogni anno, al Responsabile per la Protezione dei Dati (RPD) ed al Responsabile per la Transizione Digitale (RTD) l'elenco degli archivi di dati personali, cartacei ed informatizzati, e dei server attivi, gestiti in maniera autonoma dalle strutture di cui sono responsabili, accompagnato da una dichiarazione dell'avvenuta adozione delle misure di sicurezza adottate per la protezione dei dati personali;
- tenere ed aggiornare l'inventario degli archivi di dati personali cartacei ed informatizzati e dei server attivi gestiti in maniera autonoma dalla struttura di cui sono responsabili;
- far compilare ai responsabili scientifici dei progetti di ricerca, prima dell'avvio di ogni progetto di ricerca, la "**Scheda di analisi dei progetti di ricerca**" che si allega al presente atto sotto la lettera "**B**" ed inviarla senza indugio al RPD;
- assicurarsi che tutti i dipendenti e collaboratori afferenti alla struttura di propria competenza, prendano visione del presente decreto e dei relativi allegati nonché dei futuri aggiornamenti;
- vigilare affinché tutti i dipendenti e collaboratori afferenti alla struttura di propria competenza, operino nel rispetto delle istruzioni impartite;
- garantire che, al momento della raccolta dei dati, sia resa all'interessato, ai sensi degli artt. 13 e 14 del GDPR, la dovuta informativa;

- prendere visione della procedura da attivare in caso di violazione di dati personali (c.d. **procedura segnalazione *data breach***) allegata al presente decreto sotto la lettera "**C**";
- raccogliere ogni segnalazione di violazione, anche solo presunta, di dati personali da parte di dipendenti, collaboratori e/o interessati e riferirla, senza indugio, al Responsabile della Protezione dei Dati (*RPD*) come previsto nella sopra indicata procedura di segnalazione del *data breach;*
- raccogliere ogni segnalazione di violazione, anche solo presunta, dei sistemi informatici, compresi quelli eventualmente gestiti in autonomia dalle strutture di cui sono responsabili, e riferirla, senza indugio, al Responsabile per la Transizione Digitale (RTD).

3. i Referenti per la protezione dei dati, ove ciò si a reso necessario dalla dimensione della struttura e/o dalla complessità dei trattamenti di competenza, possono nominare, nell'ambito del personale strutturato afferente alla struttura medesima, **sub-referenti per la protezione dei dati** cui delegare compiti e responsabilità loro proprie, con riguardo a singole categorie di procedimenti o a singole attività di ricerca. Ai sub-referenti è fatto divieto di delegare ulteriormente. L'atto di delega, da redigersi per iscritto, dovrà essere comunicato al Responsabile per la protezione dati (RPD);

4. di designare come **Incaricati del trattamento** dei dati personali, per i trattamenti e le finalità di pertinenza di ciascuna unità organizzativa/ struttura/ dipartimento, individuate nel Registro delle attività di trattamento, tutto il personale strutturato e non (personale tecnico amministrativo, personale docente e ricercatore) documentalmente assegnato a quella unità organizzativa/ struttura/ dipartimento deputata a compiere operazioni di trattamento sui dati personali in possesso dell'Ateneo;

5. di designare altresì come **Incaricati del trattamento** dei dati personali, per i trattamenti e le finalità di pertinenza di ciascuna unità organizzativa/ struttura/ dipartimento, individuate nel Registro delle attività di trattamento, qualunque persona fisica che, a seguito di atto di assegnazione anche temporaneo (collaborazioni coordinate e continuative, contratti a progetto, 150 ore per studenti, stage, volontari del servizio civile, dottorandi, borsisti, tutor, assegnisti di ricerca, ecc.) si trovi ad afferire a quella unità organizzativa/ struttura/ dipartimento deputata a compiere operazioni di trattamento sui dati personali trattati dall'Ateneo;

6. di impartire a tutti i soggetti sopra individuati, **Referenti per la protezione dei dati** ed **Incaricati** dei trattamenti, le **Istruzioni per la protezione dei dati,** sintetizzate nell'allegato "**D**" al presente decreto, che saranno dettagliate e meglio specificate nell'apposita sezione del sito istituzionale;

7. di stabilire che all'atto della sottoscrizione di ogni nuovo contratto di lavoro o di costituzione di un qualsiasi rapporto di collaborazione (collaborazioni coordinate e continuative, contratti a progetto, 150 ore per studenti, stage, volontari del servizio civile, dottorandi, borsisti, tutor, assegnisti di ricerca, ecc.) sia comunicata al dipendente/collaboratore la designazione dello stesso quale **Incaricato del trattamento** dei dati personali trattati dalla struttura di assegnazione, come

individuati nel Registro delle attività di trattamento, e siano consegnate le Istruzioni per la protezione dei dati sopra indicate;

8. di dare mandato a ciascun **Referente per la protezione dei dati** di portare il presente decreto a conoscenza di tutto il personale accademico, tecnico-amministrativo, strutturato e non, già in servizio, nonché dei vari collaboratori esterni documentalmente assegnati alle strutture di loro afferenza, per le quali sia individuato, nel Registro delle attività di trattamento, l'ambito dei trattamenti consentito agli addetti alla struttura medesima;

9. di incaricare il **Responsabile della Protezione dei Dati** (**RPD**), Dott. Massimo Benedetti, e il **Responsabile per la Transizione Digitale** (**RTD**) Ing. Marius Bogdan Spinu, di predisporre, in collaborazione con il competente Ufficio Formazione, adeguati percorsi di informazione, formazione e aggiornamento del personale, sulle procedure e sui sistemi di sicurezza atti a tutelare il trattamento, la conservazione e l'integrità dei dati personali;

10. di dare mandato all'Ufficio funzionale di supporto al Responsabile della protezione dei dati, istituito con il D.D 2003/2017, di predisporre, per tutti i trattamenti effettuati dall'Ateneo, i *form* delle informative di cui i **Referenti per la protezione dei dati** e gli **Incaricati del trattamento** dovranno avvalersi prima di procedere alla raccolta dei dati personali;

11. per quanto non espressamente disposto con il presente atto, restano in vigore, nelle more del loro adeguamento, le disposizioni del "*Regolamento di attuazione del Codice di protezione dei dati personali in possesso dell'Università degli Studi di Firenze*" approvato con D.R. 29 dicembre 2005, n.1177 (prot. n.79382) e del " *Regolamento per il trattamento dei dati sensibili e giudiziari in attuazione del decreto legislativo 196/2003*" approvato con D.R. 4 ottobre 2006, n.906 (prot.51471).

Firenze 24 maggio 2018

Si allegano al presente atto:

Allegato A: Estratto del **Registro delle attività di trattamento**

Allegato B: **Scheda di analisi per progetti di ricerca**

Allegato C: **Procedura segnalazione *data breach***

Allegato D: **Istruzioni per la protezione dei dati personali**

F.to Digitalmente Il Rettore
Prof. Luigi Dei

F.to Digitalmente Il Direttore Generale
Dr.ssa Beatrice Sassi

Allegato A

Registro delle attività di trattamento*

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Titolare	**Università degli Studi di Firenze** **P.zza S.Marco, 4 - 50121 Firenze** **P.IVA/Cod.Fis. 01279680480** **Posta certificata: ateneo@pec.unifi.it**
Rappresentante legale	**Rettore Prof. Luigi Dei** **Piazza S. Marco, 4 - 50121 Firenze** **Tel. 055 2757211** **rettore@unifi.it -** **Posta certificata: rettore@pec.unifi.it**
Responsabile Protezione Dati	**Dott. Massimo Benedetti** **Piazza S. Marco, 4 - 50121 Firenze** **Tel. 055 2757667** **privacy@adm.unifi.it** **Posta certificata: ateneo@pec.unifi.it**

* Per quanto riguarda le parti in grigio attualmente l'Ateneo sta provvedendo ad individuare l0'ubicazione degli archivi cartacei sia quella dei server. Inoltre sta provvedendo all'individuazione e regolamentazione dei trattamenti di cui è contitolare o responsabile di trattamento dei dati

TRATTAMENTO	UFFICIO	FINALITA'	TIPI DI DATI PERSONALI	DATI PERSONALI STRETTAMENTE NECESSARI PER PERSEGUIRE LA FINALITÀ DESCRITTA	TIPOLOGIA TRATTAMENTO I = informatici C = Cartacei
Orientamento	Orientamento e Job Placement	Favorire azioni di accompagnamento e monitoraggio atte a prevenire la dispersione scolastica e ad agevolare la scelta del percorso universitario	Dati identificativi, categorie particolari di dati personali (disabilità), giudiziari	Dati anagrafici, dati di contatto, scuola frequentata/ente di riferimento, aree di interesse	I e C
Erogazione dei test di ingresso o alla verifica dei requisiti di accesso	Numero programmato	Consentire lo svolgimento delle prove di ammissione ai Corsi di Laurea a numero rogrammato e le prove per la valutazione della preparazione iniziale, ove previsto. I dati personali dell'interessato e i risultati ottenuti nelle prove potranno essere oggetto di trattamento anche per finalità di ricerca statistica o scientifica o per individuare delle azioni volte al miglioramento dei servizi didattici	Dati identificativi,categorie particolari di dati personali (dati inerenti lo stato di salute), dati personali relativi a condanne penali e reati (nel caso di studenti detenuti). Nel caso di disabilità o in presenza di disturbi specifici dell'apprendimento l'utente dovrà fornire anche eventuali certificazioni della diagnosi	Dati anagrafici, di contatto, estremi documenti identificativi, dati per la verifica dei requisiti (es. titoli) sono dati necessari per l'erogazione del servizio e per il perseguimento di attività di ricerca scientifica e/o statistica	I e C
Erogazione del percorso formativo e gestione della carriera (dall'immatricolazione alla laurea)	Area Servizi alla Didattica, Unità di Processo "Offerta Formativa", Unità Funzionale "Didattica integrata con Servizio Sanitario Regionale e con la Scuola di Scienze della Salute Umana, Unità Funzionale "Interventi a favore degli Studenti", Unità Funzionale "Sportello Unico Capponi", Unità Funzionale "Sportello Unico Morgagni", Unità Funzionale "Sportello Unico Novoli"	Permettere la gestione degli eventi inerenti la carriera dello studente, quali la gestione del piano di studio, la registrazione degli esami e la domanda di laurea	Dati identificativi, categorie particolari di dati personali (stato di salute), dati personali relativi a condanne penali e reati	Dati anagrafici, di contatto, dati per la verifica dei requisiti e inerenti la carriera (es: titoli, valutazione di prove intermedie, prova finale), dati sulla provenienza dello studente, ulteriori dati necessari (esempio: informazioni sul permesso di soggiorno). Altre informazioni non obbligatorie in termini generali ma richieste in situazioni specifiche: dati bancari, ISEE, fotografia, contatti telefonici, contatti email personale/i). Sono di seguito descritte atre tipologie di dati sensibili e/o dati personali relativi a condanne penali e reat trattatii: a. dati relativi agli studenti e/o a familiari diversamente abili o ad elementi reddituali per 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; b. dati relativi allo status di rifugiato per la fruizione di esoneri e borse di studio; c. 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; d. 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; e. dati sensibili e dati personali relativi a condanne penali e reati	I e C

TRATTAMENTO	UFFICIO	FINALITA'	TIPI DI DATI PERSONALI	DATI PERSONALI STRETTAMENTE NECESSARI PER PERSEGUIRE LA FINALITÀ DESCRITTA	TIPOLOGIA TRATTAMENTO I = informatici C = Cartacei
Attività di tirocinio	Orientamento e Job Placement, Unità Funzionale "Didattica integrata con Servizio Sanitario Regionale e con la Scuola di Scienze della Salute Umana"	I dati sono trattati per la gestione dei tirocini curriculari, ovvero avviati per studenti ancora iscritti ad un CdS, che extracurriculari, dedicati a soggetti che hanno già concluso il percorso di studi. I dati sono trattati, ad esempio, nell'ambito della stipula della convenzione tra l'Università e l'ente/azienda o nell'ambito delle attività svolte con il supporto del tuto	Dati identificativi, categorie particolari di dati personali (in caso di disabilità o nel caso di disturbi specifici dell'apprendimento, dati del transgender nel caso in cui non sia intervenuta una sentenza di cambio di genere)	Dati anagrafici, di contatto e di carriera degli studenti. Dati dei referenti aziendali o rappresentati legali delle aziende, informazioni necessarie per la stipula della convenzione	I e C
Attività di job placement	Orientamento e Job Placement	Fornire a studenti/laureati ed aziende/enti l'assistenza necessaria per l'inserimento nel mondo del lavoro, attraverso canali dedicati. Inoltre, al fine del miglior orientamento in uscita, i dati sono trattati per l'organizzazione di seminari, career day, ecc.	Dati identificativi, categorie particolari di dati personali (disabilità, transgender)	Dati anagrafici, di contatto e di carriera degli studenti, CV Dati dei referenti aziendali e/o rappresentati legali, informazioni necessarie per la stipula della convenzione	I e C
Attività di fundraising, di comunicazione e informazione istituzionale e sviluppo di community	UF - Progetti di Ricerca Internazionale, Dipartimenti, Funzione Trasversale Comunicazione e Public Engagement, Unità di Processo "Servizi di Comunicazione ", UP - Iniziative di Public Engagement ed Eventi, UF - Prodotti e strumenti per la comunicazione istituzionale e per gli studenti	I dati sono trattati: - per finalità di reperimento fondi; - sviluppo di community (anche relativi a ex studenti o ex dipendenti dell'Ateneo); - promozione dell'immagine dell'Ateneo e delle sue attività, conferendo conoscenza e visibilità ad eventi organizzati dallo stesso e nei quali è coinvolto	Dati identificativi	Dati anagrafici, di contatto, eventuali video e immagini di studenti e dipendenti, soggetti terzi (ex studenti, sostenitori, ecc.)	I e C
Rilevazioni statistiche e valutazione della didattica	Area Servizi alla Didattica, Coordinamento Programmazione, Organizzazione e Controllo	Il dato è trattato a fini di rilevazioni statistiche volte a perseguire fini istituzionali dell'Ateneo (es: attività di ricerca o attività di quality assurance o attività volte a migliorare l'immagine complessiva dell'Ateneo)	Dati identificativi	Dipende dalla rilevazione richiesta e dall'ambito. Esempio: potrebbero essere trattati dati anagrafici (e/o di contatto) e dati di carriera per verificare l'adeguatezza della formazione acquisita in università, la coerenza delle competenze apprese rispetto alla futura attività lavorativa dello studente, l'utilità del titolo ottenuto rispetto all'attività lavorativa svolta o da svolgere	I e C
Diffusione dell'elaborato finale o di elementi ad esso connessi	Sistema Bibliotecario Di Ateneo, Orientamento e job placement, Area Servizi Alla Didattica	Garantire la divulgazione dell'elaborato finale (tesi di laurea, tesi di dottorato, ecc.) e/o di elementi ad esso connessi (autore, titolo e, in genere, metadati associati), nel rispetto delle leggi sul diritto di autore	Dati identificativi	Dati anagrafici, di carriera, dati di contatto e dati inerenti l'elaborato finale	I e C

TRATTAMENTO	UFFICIO	FINALITA'	TIPI DI DATI PERSONALI	DATI PERSONALI STRETTAMENTE NECESSARI PER PERSEGUIRE LA FINALITÀ DESCRITTA	TIPOLOGIA TRATTAMENTO I = informatici C = Cartacei
Servizi di tutorato, assistenza, inclusione sociale	Orientamento e job placement, Area Servizi Alla Didattica, Scuole, Dipartimenti	Trattamento finalizzato a servizi di tutorato, assistenza, inclusione sociale, supporto a persone con disabilità o disturbi specifici dell'apprendimento (DSA). È escluso il trattamento di dati personali per fini strettamente connessi alla gestione della carriera universitaria. Il trattamento di questi dati attiene ad esempio: - Servizi che possono essere messi a disposizione per supportare gli studenti con disabilità negli spostamenti da e verso le strutture universitarie; - La diffusione di informazioni o iniziative utili a favorire l'inclusione sociale; - L'erogazione di servizi di supporto durante tutto il percorso di studi, con l'obiettivo di individuare e progettare i tipi di sostegno necessari ad ogni studente per svolgere con profitto il proprio corso di studi	Dati Identificativi, categorie particolari di dati personali (inerenti lo stato di salute)	Dati anagrafici, di carriera, sensibili (legati, ad esempio, alla specifica disabilità o DSA)	I e C
Erogazione di servizi e attività per il diritto allo studio	Area Servizi Alla Didattica, Unità Funzionale "Interventi a favore degli Studenti"	Il trattamento è finalizzato a garantire il diritto allo studio attraverso il quale lo studente ha la possibilità di fruire di agevolazioni, sussidi, borse di studio e servizi: - per il miglioramento delle condizioni di studio e di vita degli studenti; per la realizzazione di attività culturali, sportive e ricreative a favore della popolazione studentesca	Dati Identificativi, categorie particolari di dati personali (disabilità, DSA o, nel caso di organizzazioni studentesche che hanno una connotazione politica o religiosa, potrebbero essere trattati dati idonei a rivelare convinzioni politiche, religiose, filosofiche, ecc..)	Dati anagrafici, di carriera, sensibili, economici per procedure di esonero o di rimborso, borse di studio	I e C
Procedimenti di natura disciplinare a carico di studenti	Area Servizi alla Didattica, Unità di Processo "Affari Legali (patrocinio, consulenze, contenzioso, redazione)", Unità Funzionali "Sportelli Unici", Unità Funzionale "Segreteria e Cerimoniale"	Il trattamento è finalizzato allo svolgimento di procedimenti disciplinari a carico di studenti	Dati identificativi, categorie particolari di dati personali e dati personali relativi a condanne penali e reati	Dati anagrafici, di carriera e dati inerenti lo specifico procedimento	I e C

TRATTAMENTO	UFFICIO	FINALITA'	TIPI DI DATI PERSONALI	DATI PERSONALI STRETTAMENTE NECESSARI PER PERSEGUIRE LA FINALITÀ DESCRITTA	TIPOLOGIA TRATTAMENTO I = informatici C = Cartacei
Gestione degli spazi	Unità di Processo "Gestione Aule e Strutture" Dipartimenti	Il dato è trattato al fine di permettere l'utilizzo degli spazi dell'Ateneo, per attività quali: - assegnazione degli spazi alle strutture, allocazione delle persone negli spazi; - controllo accessi ai varchi da parte di: dipendenti, collaboratori e studenti; - la gestione centralizzata e coordinata delle aule e deglispazi per la didattica; - la gestione delle procedure amministrative per richieste di spazi per eventi istituzionali; - la gestione delle procedure amministrative per richieste di spazi da parte di soggetti terzi	Dati identificativi, categorie particolari di dati personali (dati inerenti lo stato di salute).	Con riferimento al richiedente lo spazio, verranno trattati dati di anagrafica personale e di carriera. In relazione all'utilizzo degli spazi da parte di soggetti terzi, verranno trattati anche ulteriori dati personali, riconducibili ad esigenze di carattere amministrativo (es. per verificare la validità delle autorizzazioni ad accedere a spazi d'Ateneo). Per l'accesso agli spazi da parte di soggetti disabili, potranno esser trattati dati inerenti lo stato di salute. L'eventuale decisione di effettuare il controllo degli accessi potrebbe comportare la raccolta di dati di ingresso/uscita/identificativo utente (ad es. il badge)	I e C
Gestione delle postazioni	SIAF - Sistema Informatico dell'Ateneo Fiorentino	Il dato è trattato per garantire il corretto funzionamento di postazioni di lavoro fisse / mobili assegnate agli utenti, la sicurezza delle stesse e per fornire il necessario supporto nell'utilizzo. Per questo tipo di trattamento è necessario effettuare la DPIA	Qualsiasi tipologia di dato utilizzato dall'utente (in alcuni casi perfino di natura genetica se l'utente dovesse svolgere ricerca nel campo della genetica medica)	Dati relativi all'utente, struttura di afferenza, dati di contatto. Associazione utenti/postazioni assegnate. Nella gestione delle postazioni, in dipendenza del tipo di intervento, potrebbero verificarsi da parte degli amministratori di sistema accessi, anche fortuiti, a categorie particolari di dati personali memorizzati sulle postazioni, in ragione dell'effettiva capacità di azione sulle informazioni e della rilevanza e specificità del ruolo	I e C
Gestione degli organi e delle cariche istituzionali Gestione degli elenchi per l'elettorato attivo e passivo	Unità di Processo "Affari Generali"	Il dato è trattato, nell'ambito del rinnovo degli organi istituzionali, per la gestione degli elenchi dell'elettorato attivo e passivo, per le sostituzioni dei componenti e per verificare i requisiti di eleggibilità. In dato considerato è inerente alle elezioni in senso stretto e a eventuali valutazioni di incompatibilità	Dati identificativi, categorie particolari di dati personali (es: per l'appartenenza a organizzazioni sindacali, associazioni politiche, religiose, ecc), dati personali relativi a condanne penali e reati. I verbali potrebbero riportare dati relativi allo stato di salute nel caso in cui un elettore abbia fatto ricorso al voto assistito	Oltre ai nominativi, al ruolo e a eventuali informazioni connesse alla presentazione delle liste elettorali, in alcuni Atenei e/o per alcune elezioni specifiche, potrebbero rendersi necessaria la: - Consultazione del Casellario Giudiziale (dato acquisito e conservato tipicamente in forma cartacea dall'ufficio preposto). - Consultazione carriera studente per verifica dello stato di attività e di regolarità dei pagamenti.	I e C
Gestione degli organi e delle cariche istituzionali Nomina degli eletti e delle cariche accademiche	Unità di Processo "Affari Generali"	Il dato è trattato ai fini della gestione della nomina degli eletti e dalle cariche accademiche, nonché per la verifica della presenza di eventuali cause di incompatibilità con la carica da assumere	Dati identificativi, categorie particolari di dati personali, dati personali relativi a condanne penali e reati	Dati di anagrafica e di carriera, dati di contatto e dati personali relativi a condanne penali e reati per l'eventuale consultazione del casellario giudiziale	I e C

TRATTAMENTO	UFFICIO	FINALITA'	TIPI DI DATI PERSONALI	DATI PERSONALI STRETTAMENTE NECESSARI PER PERSEGUIRE LA FINALITÀ DESCRITTA	TIPOLOGIA TRATTAMENTO I = informatici C = Cartacei
Pubblicizzazione di atti ai fini di trasparenza	Responsabile Prevenzione Corruzione e Trasparenza Unità di Processo "Servizi di Comunicazione"	Il dato è trattato per finalità di trasparenza come da normativa vigente sul sito istituzionale per la parte di “Amministrazione Trasparente”. Si precisa che i dati potrebbero essere originariamente raccolti per finalità differente (ad es. espletamento di un incarico istituzionale), ma che, per vincoli normativi, vengono trattati anche a tal fine	Dati identificativi	Dati di carriera, dati di reddito, curriculum vitae, cariche, sovvenzioni, contributi, sussidi, vantaggi economici, spese sostenute. Tale trattamento riguarda, ad es., la pubblicazione del C.V. e della situazione reddituale delle cariche del Consiglio di Amministrazione e del Senato Accademico, nonché del C.V. e dei dati retributivi del Direttore Generale e dei Dirigenti	I e C
Gestione degli infortuni	Unità di Processo "Amministrazione Personale Tecnico-Amministrativo e Collaboratori ed Esperti Linguistici" Unità di Processo "Affari Generali" Unità di Processo "Servizi Generali" Area Servizi Economali, Patrimoniali e Logistici	Il trattamento viene effettuato in relazione agli infortuni occorsi al personale docente, tecnico amministrativo, agli studenti ed ai soggetti terzi in visita. In particolare nell’ambito della gestione di tali eventi da parte degli uffici dell’Ateneo preposti, dalla presa in carico della segnalazione di infortunio fino alla chiusura della relativa pratica, includendo: l’interazione con enti esterni - la gestione di eventuali prescrizioni da parte dell’INAIL l’apertura e gestione della segnalazione di sinistro nell’ambito di copertura delle polizze assicurative dell’Ateneo la valutazione delle proposte di liquidazione del danno gli eventuali prolungamenti del periodo di infortunio	Dati identificativi, categorie particolari di dati personali (dati inerenti lo stato di salute)	Dati anagrafici, di carriera e dati inerenti lo stato di salute. Dati specifici relativi all’infortunio occorso (es referti, certificati)	I e C

TRATTAMENTO	UFFICIO	FINALITA'	TIPI DI DATI PERSONALI	DATI PERSONALI STRETTAMENTE NECESSARI PER PERSEGUIRE LA FINALITÀ DESCRITTA	TIPOLOGIA TRATTAMENTO I = informatici C = Cartacei
Trattamento in ambito bibliotecario	SBA	Il dato è trattato al fine di consentire al personale docente, tecnico amministrativo, popolazione studentesca e ai cittadini, di accedere ai servizi centralizzati offerti dal sistema bibliotecario e ai locali e servizi offerti dalle singole Biblioteche di Ateneo (consultazione e prestito patrimonio bibliografico e documentale su supporto cartaceo e elettronico, prestito interbibliotecario e document delivery, reference, ecc.) e per informazione sulle attività e servizi offerti. I dati possono essere oggetto di trattamento in forma anonima per lo svolgimento di attività statistiche e rilevazioni del grado di soddisfazione finalizzate al miglioramento dei servizi offerti. Differente è il caso che la biblioteca tratti dati relativi alle condizioni di salute nel caso eroghi servizi specificamente o esclusivamente rivolti a utenti con disabilità (es.	Identificativi (Dati anagrafici, di contatto, estremi documenti identificativi nel caso di utenti esterni), categorie particolari di dati personali (esempio nel caso di utenti in stato di transizione) È altresì possibile che la biblioteca tratti dati relativi alle condizioni di salute nel caso eroghi servizi specificamente o esclusivamente rivolti a utenti con disabilità (es. postazioni o dispositivi con tecnologie assistive, ecc.)	Dati anagrafici, di contatto e di carriera (personale o studenti), materiali bibliografici e documentali in prestito o consultati	I e C
Servizi di protocollo e conservazione documentale *** Gestione del protocollo in entrata/uscita	Unità di Processo "Archivio e trattamento degli atti" Dipartimenti Aree Strutture	Gestione del protocollo informatico nelle fasi di entrata/uscita al fine di fornire data e ora certa agli atti acquisiti o trasmessi da una Pubblica Amministrazione. Le registrazioni di protocollo ed i file a esso associati, prodotti e raccolti nell'ambito delle funzioni dell'Ente ed entro le Aree Organizzative Omogenee dello stesso per l'espletamento di procedimenti, affari ed attività, sono: accessibili ai responsabili ed agli operatori preposti, con diritti di registrazione e consultazione definiti da specifiche policy indicate nel manuale di gestione del protocollo; ottemperano quando previsto dal DPCM 3.13.2013 – regole tecniche per il protocollo informatico e in particolare dagli articoli 6, 7, 8, 18, 20, 21; sottoposte alla gestione dei pacchetti di distribuzione e di versamento sulla base degli accordi presi con il conservatore accreditato prescelto	In funzione del procedimento/affare/attività i documenti possono contenere dati personali, anche appartenenti a particolari categorie (es sensibili o giudiziari). Ogni dato e documento inserito nel sistema di protocollo potrebbe contenere tali dati nella: - descrizione del documento e sua rappresentazione, oggetto, allegati, classificazione, file associati (nativi digitali o loro conversione in formato digitale) - indicazione dei corrispondenti/contraenti e dei responsabili e assegnatari del documento	Dati anagrafici dei mittenti e destinatari. Il campo oggetto, incluso nel nucleo minimo delle informazioni necessarie per la registrazione a protocollo, potrebbe per sua natura riportare dati personali, anche appartenenti a particolari categorie (es sensibili o giudiziari). I dati trattati dipendono dallo specifico procedimento/affare/attività e sempre nell'osservanza del DPCM 3.12.2013, tanto in materia di protocollo informatico (ai sensi degli articoli 40bis, 41, 47, 57bis e 71 del CAD) tanto in materia di conservazione (ai sensi degli articoli 20, commi 3 e 5bis, 23ter, comma 3, 43, commi 1 e 3, 44, 44bis e 71 comma 1 del CAD) Potrebbe rendersi necessaria anche la registrazione di ulteriori dati personali per supportare e motivare (a titolo di esempio): la creazione del pacchetto di distribuzione per motivi legali o accessi agli atti concorsuali l'accesso al sistema di conservazione per la verifica dell'operato del conservatore o per verifiche di carattere tecnico	I e C

TRATTAMENTO	UFFICIO	FINALITA'	TIPI DI DATI PERSONALI	DATI PERSONALI STRETTAMENTE NECESSARI PER PERSEGUIRE LA FINALITÀ DESCRITTA	TIPOLOGIA TRATTAMENTO I = informatici C = Cartacei
Servizi di protocollo e conservazione documentale *** Conservazione Documentale	Unità di Processo "Archivio e trattamento degli atti" Dipartiment Aree Strutture	Gestione delle attività di conservazione documentale ai sensi della normativa vigente	Ogni dato e documento inserito nel sistema di protocollo informatico e potenziale oggetto di invio in conservazione, ovvero: descrizione del documento e sua rappresentazione, ovvero numero di protocollo ed eventuale repertorio, data, oggetto, allegati, classificazione, file associati (nativi digitali o loro conversione in formato digitale) indicazione dei corrispondenti/contraenti e dei responsabili e assegnatari del documento In funzione del procedimento/affare/attività i documenti possono contenere dati personali, anche appartenenti a particolari categorie (es. sensibili o giudiziari)	Dati anagrafici dei mittenti e destinatari. Il campo oggetto, incluso nel nucleo minimo delle informazioni necessarie per la registrazione a protocollo, potrebbe per sua natura riportare dati personali, anche appartenenti a particolari categorie (es sensibili o giudiziari). I dati trattati dipendono dallo specifico procedimento/affare/attività e sempre nell'osservanza del DPCM 3.12.2013, tanto in materia di protocollo informatico (ai sensi degli articoli 40bis, 41, 47, 57bis e 71 del CAD) tanto in materia di conservazione (ai sensi degli articoli 20, commi 3 e 5bis, 23ter, comma 3, 43, commi 1 e 3, 44, 44bis e 71 comma 1 del CAD) Potrebbe rendersi necessaria anche la registrazione di ulteriori dati personali per supportare e motivare (a titolo di esempio): la creazione del pacchetto di distribuzione per motivi legali o accessi agli atti concorsuali l'accesso al sistema di conservazione per la verifica dell'operato del conservatore o per verifiche di carattere tecnico.	I e C
Acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso *** Acquisizione di beni e servizi	Centrale d'acquisto Dipartimenti	Il dato è trattato per consentire la verifica di posizioni giudiziarie, fiscali e di condotta di fornitori ed operatori economici che sono in rapporto con l'Ateneo al fine di: svolgere le attività preliminari connesse alle procedure di acquisizione di beni e servizi; coordinare e analizzare la redazione della documentazione tecnica, amministrativa e contrattuale; gestire il procedimento e le attività connesse (stipula del contratto, monitoraggio dei tempi del procedimento in affidamento)	Identificativi, dati personali relativi a condanne penali e reati	Potrebbe rendersi necessaria la registrazione di dati personali presenti nella documentazione inerente: - DURC (acquisendo parte dei dati da Inps e altri da Inail) - Visure camerali (acquisiti da Infocamere) - Certificato di Casellario Giudiziale (Tribunale) accertamenti sulla situazione societaria e personale delle controparti (Anac) - Verifica regolarità fiscale (Agenzia delle entrate ed Equitalia per il pregresso) Nel caso di acquisti sopra soglia è necessario altresì acquisire i dati inerenti. - Offerta economica, in sede di apertura del fascicolo di gara (svolto dalla Commissione per la valutazione dell'offerta); - Certificazioni antimafia (acquisita presso la Prefettura/Questura). Tali verifiche potrebbero essere svolte anche per i casi di avvalimento	I e C
Acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso *** Verifiche sull'espletamento di lavori, in cantiere o presso installazioni in Ateneo	Area Edilizia	Il dato è trattato per la valutazione amministrativa ed economica di terzi, fornitori dell'Ateneo per l'espletamento di lavori in appalto, verifiche sui cantieri o presso installazioni in Ateneo	Identificativi, dati personali relativi a condanne penali e reati	Potrebbe rendersi necessaria la registrazione di dati personali per consentire, ad esempio la consultazione del contratto dei lavoratori delle ditte appaltatrici e di quelle sub-appaltate. La verifica di atti relativi ai dipendenti delle società	I e C

TRATTAMENTO	UFFICIO	FINALITA'	TIPI DI DATI PERSONALI	DATI PERSONALI STRETTAMENTE NECESSARI PER PERSEGUIRE LA FINALITÀ DESCRITTA	TIPOLOGIA TRATTAMENTO I = informatici C = Cartacei
Acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso *** Gestione del contenzioso e del recupero crediti	Ufficio Funzionale per la Gestione dei Procedimenti Disciplinari del Personale Tecnico	Il dato è trattato per: la gestione dei contenziosi instaurati avanti le diverse autorità giudiziarie in cui sia coinvolta l'Università; l'attività di recupero dei crediti dell'Università nei confronti di personale docente/ricercatore e tecnico-amministrativo, degli studenti e di soggetti terzi inadempienti	Identificativi, dati personali relativi a condanne penali e reati	I dati trattati possono essere differenti a seconda del tipo di contenzioso; includerà in ogni caso i dati anagrafici e il tipo di rapporto con l'Ateneo; potrebbe includere dati sanitari. Per il recupero crediti, la tipologia di dati trattati sarà in correlazione alla categoria di interessati coinvolta	I e C
Servizi di posta elettronica e strumenti di collaboration *** Accesso agli strumenti di collaboration	SIAF - Sistema Informatico dell'Ateneo Fiorentino *** Comunicazione in Rete	Al fine di favorire la collaborazione, l'Ateneo potrebbe fornire strumenti informatici (es: web conference, spazi virtuali di collaborazione, ecc) tramite i quali possono essere trattati dati personali funzionali: all'erogazione del servizio stesso a connesse attività di risoluzione dei guasti (troubleshooting) alla valutazione dell'uso del servizio e della qualità (es: mediante rilevazioni statistiche basate sull'uso di tali strumenti) a garantire la sicurezza informativa dei dati trattati mediante tali strumenti di collaboration	Identificativi, categorie particolari di dati personali	A seconda del tipo di attività o strumento di collaborazione potrebbero essere utilizzati dati quali, l'indirizzo di posta elettronica, l'indirizzo IP del sistema utilizzato, dati relativi alla carriera, dati anagrafici, ecc..	I e C
Servizi di posta elettronica e strumenti di collaboration *** Erogazione di servizi di posta elettronica	SIAF - Sistema Informatico dell'Ateneo Fiorentino *** Comunicazione in Rete	Al fine di favorire la comunicazione istituzionale tramite i servizi di posta elettronica, l'Ateneo potrebbe trattare dati personali funzionali a: l'erogazione del servizio stesso lo svolgimento attività connesse alla risoluzione dei guasti (troubleshooting) la valutazione dell'uso del servizio e della qualità dei servizio (es: mediante rilevazioni statistiche basate sull'uso di tali strumenti) garantire la sicurezza informativa dei dati trattati (tramite ad esempio la gestione di incidenti di sicurezza e tramite azioni preventive sulla diffusione di messaggi contenenti malware)	Identificativi	Indirizzi e-mail. All'atto della creazione dell'account o in caso di cambio di status dell'utente all'interno dell'Ateneo (se sono previste differenze di gestione delle caselle a seconda del ruolo), anche anagrafica dell'utente (codice fiscale, matricola, ruolo ricoperto). Nella gestione legata al troubleshooting, incidenti di sicurezza e azioni preventive sulla diffusione di messaggi malevoli, potrebbe rendersi necessario il trattamento dei seguenti dati connessi ai messaggi di posta: casella di posta sorgente, casella destinataria, server in entrata e uscita, server di transito, oggetto mail, timestamp	I e C

TRATTAMENTO	UFFICIO	FINALITA'	TIPI DI DATI PERSONALI	DATI PERSONALI STRETTAMENTE NECESSARI PER PERSEGUIRE LA FINALITÀ DESCRITTA	TIPOLOGIA TRATTAMENTO I = informatici C = Cartacei
Erogazione del servizio Eduroam	SIAF - Sistema Informatico dell'Ateneo Fiorentino *** Comunicazione in Rete	Il trattamento è volto a garantire l'accesso in mobilità degli utenti alla rete Eduroam. Nel caso l'ente sia IdP e nel caso accetti di avere informazioni relative ai propri utenti, l'ente potrà ricevere i log di connessione degli utenti appartenenti alla propria organizzazione anche quando tali utenti sono in altre università. Se l'ente è un SP, allora tratterà dati personali di utenti appartenenti ad altra organizzazione solo nel caso in cui l'IdP di appartenenza dell'utente non supporti il passaggio anonimo delle identità degli utenti	Identificativi	Username, MAC, IP, timestamp	I e C
Svolgimento di prove concorsuali/selezioni	Area Risorse Umane Ufficio Reclutamento e Selezioni	Consentire agli interessati di accedere ai ruoli previsti dai bandi di Ateneo, accertandone la sussistenza dei requisiti richiesti per l'espletamento delle attività di selezione	Dati identificativi, categorie particolari di dati personali, dati personali relativi a disabilità o a condanne penali e reati	Dati anagrafici (nome, cognome, la data ed il luogo di nascita, CF residenza, cittadinanza italiana), documento identità, contatti, curriculum vitae, eventuali disabilità, eventuali condanne penali, cariche politiche (solo ai commissari di concorso), titoli, ecc., esiti concorso	I e C
Gestione del rapporto di lavoro o di collaborazione, anche per personale in convenzione	Area Risorse Umane	Gestione dell'offerta formativa e dell'assegnazione degli incarichi(quadro didattico). Gestione della struttura organizzativa, dell'anagrafica del personale e registrazione degli eventi di carriera (giuridico). Gestione delle pratiche assicurative e previdenziali; trattamenti assistenziali; denunce e pratiche di infortunio, trattamenti assistenziali trattamento dei dati inerenti i procedimenti disciplinari a carico del personale e nei giudizi pendenti di fronte a tutte le giurisdizioni che coinvolgono docenti, dipendenti, collaboratori gestione delle risorse umane (posizioni organizzative, profili di competenza, repertorio aziendale delle conoscenze, processo di selezione, politiche retributive). Gestione della formazione. Rilevazione e gestione delle presenze, gestione retributiva, gestione dei provvedimenti per il	Dati identificativi, categorie particolari di dati personali, dati personali relativi a disabilità o a condanne penali e reati.	Dati anagrafici (nome, cognome, la data ed il luogo di nascita, CF residenza, cittadinanza italiana), dati bancari , fiscali e previdenziali. Per la gestione dei dati anagrafici e amministrativo contabili dei collaboratori esterni possono essere trattati dati inerenti l'anagrafica, dati bancari, fiscali e previdenziali. Per la gestione del personale docente possono essere trattati dati relativi alla costituzione/cessazione del rapporto di lavoro, alle procedure di valutazione comparativa, al reclutamento, agli affidamenti, agli incarichi esterni. Per la gestione personale T.A. possono essere trattati dati relativi alla costituzione/cessazione del rapporto di lavoro, a concorsi e selezioni, a incarichi esterni, alla mobilità. Per la gestione degli istituti contrattuali possono essere trattati dati relativi a congedi, permessi, aspettative, malattie, infortuni, partecipazioni a scioperi e assemblee, ecc.	I e C

TRATTAMENTO	UFFICIO	FINALITA'	TIPI DI DATI PERSONALI	DATI PERSONALI STRETTAMENTE NECESSARI PER PERSEGUIRE LA FINALITÀ DESCRITTA	TIPOLOGIA TRATTAMENTO I = informatici C = Cartacei
Formazione e aggiornamento professionale	Area Formazione	Erogazione di attività didattiche e di formazione/aggiornamento (frontale, multimediale e a distanza). Rientrano in questo tipo di trattamento anche i trattamenti per: - Iscrizione a corsi di formazione - Gestione dei registri delle attività didattiche: consuntivazione attività didattiche e non, a preventivo e consuntivo; - Valutazioni qualità, nell'ipotesi in cui i questionari possano essere indirettamente riconducibili a un interessato; - Eventuali attestati di frequenza ai corsi	Personali, categorie particolari di dati personali (solo per i casi in cui debbano essere predisposte misure particolari per l'organizzazione dei corsi)	In relazione allo specifico corso/servizio erogato, potrebbero essere trattati: dati presenti in anagrafica, dati di carriera, curriculum vitae, ore di rendicontazione della docenza, iscrizioni e partecipazioni a corsi di formazione	I e C
Gestione di progetti di ricerca	Area Servizi alla Ricerca e al Trasferimento Tecnologico - CsaVRI	Curare le attività legate ai finanziamenti per la ricerca e la formazione scientifica; garantire il coordinamento delle attività di ricerca, in particolare a livello comunitario ed internazionale; favorire lo sviluppo dell'attività di ricerca e valorizzarne i risultati	Dati identificativi	Dati di anagrafica e di carriera, dati di contatto, codici identificativi univoci internazionali (es.: ORCID) riferiti a uno specifico ricercatore. Per quanto riguarda l'anagrafica della gestione dei progetti: dati descrittivi ricerca, finanziamenti e cofinanziamenti erogati, gruppo ricerca (anagrafica interni), enti partner e ente finanziatore. Per quanto attiene gli strumenti di rendicontazione e di consuntivazione (ad es. tramite TimeSheet UGOV) sono trattati: Anagrafica, Carriera, Attribuzione Ore a ricerca e didattica	I e C
Monitoraggio e Valutazione della Ricerca	Area Servizi alla Ricerca e al Trasferimento Tecnologico - CsaVRI- Servizio di supporto al Nucleo di Valutazione e Struttura Tecnica Permanente	Il trattamento è finalizzato al monitoraggio e valutazione della ricerca: classificazione e catalogazione dei prodotti della ricerca (IRIS Sistema di Gestione dei dati della Ricerca) e valutazione della ricerca	Dati identificativi	Dati di anagrafica e di carriera, dati di contatto, codici identificativi univoci internazionali (es.: ORCID) riferiti a uno specifico ricercatore. Per quanto riguarda l'anagrafica della gestione dei progetti: dati descrittivi ricerca, finanziamenti e cofinanziamenti erogati, gruppo ricerca (anagrafica interni), enti partner e ente finanziatore. Per quanto attiene gli strumenti di rendicontazione e di consuntivazione (ad es. tramite TimeSheet UGOV) sono trattati: Anagrafica, Carriera, Attribuzione Ore a ricerca e didattica	I e C
Trasferimento Tecnologico	Area Servizi alla Ricerca e al Trasferimento Tecnologico - CsaVRI	Il trattamento è finalizzato alla valorizzazione commerciale dei risultati della ricerca scientifica e tecnologica conseguiti nell'ambito dell'organizzazione universitaria, nonché alla tutela dell'opera dell'ingegno. In particolare i dati sono trattati per la valorizzazione delle invenzioni, per il deposito delle domande di brevetto e per la ricerca di partner interessati alla commercializzazione dei brevetti	Dati identificativi	Dati di anagrafica e di carriera, dati di contatto	I e C

TRATTAMENTO	UFFICIO	FINALITA'	TIPI DI DATI PERSONALI	DATI PERSONALI STRETTAMENTE NECESSARI PER PERSEGUIRE LA FINALITÀ DESCRITTA	TIPOLOGIA TRATTAMENTO I = informatici C = Cartacei
Politiche Welfare	Area Risorse Umane	Il dato è trattato al fine di consentire la promozione di politiche volte a consentire al personale dell'Ateneo di fruire di agevolazioni, servizi e/o sussidi.	Dati identificativi, categorie particolari di dati personali (disabilità, DSA)	Anagrafica (eventualmente anche dati familiari), carriera e dati, ISEE. Potrebbero rendersi necessari altri dati connessi al tipo di servizio.	I e C
Salute e sicurezza delle persone nei luoghi di lavoro	Area Risorse umane Unità di Processo "Servizio Prevenzione e Protezione"	Il dato è trattato dal **Medico Competente** al fine di svolgere l'attività di sorveglianza sanitaria obbligatoria del personale, ottemperando agli obblighi di legge come definiti dal D. Lgs. 81/08 - Testo Unico in materia di salute e sicurezza del lavoro e dal D.Lgs. 230/95 Il dato è trattato dall'**Ufficio Prevenzione, Protezione e Sicurezza** al fine di supportare il Medico Competente nell'attività di sorveglianza sanitaria obbligatoria del personale, ottemperando agli obblighi di legge come definiti dal D. Lgs. 81/08 - Testo Unico in materia di salute e sicurezza del lavoro	Personali, categorie particolari di dati personali (dati inerenti lo stato di salute, referti medici)	Dati anagrafici, dati di contatto, dati inerenti lo stato di salute, dati inerenti l'attività lavorativa svolta e di carriera	I e C
Erogazione del servizio di telefonia fissa e mobile		Il dato è trattato al fine di gestire tutte le attività inerenti la gestione delle linee telefoniche fisse e/o mobili e dei dispositivi, la relativa rendicontazione, nonché il servizio di assistenza all'utenza	Dati identificativi	Anagrafica del personale, carriera, struttura di afferenza, prefissi (livelli di autorizzazione per l'effettuazione di chiamate), chiamate da/all'esterno, spese, abilitazioni alla doppia fatturazione, altre informazioni sul traffico dati, quali: a. il numero o l'identificazione dell'utente e del soggetto cui la chiamata è trasmessa; b. il numero totale degli scatti o il tempo di durata del traffico da considerare per il periodo di rendicontazione; c. il tipo, l'ora di inizio e la durata delle chiamate effettuate e il volume dei dati trasmessi; d. la data della chiamata o dell'utilizzazione del servizio; e. informazioni concernenti i pagamenti. Con riguardo alla telefonia mobile, verranno trattati anche ulteriori dati personali con finalità di rendicontazione ed addebito	I e C

TRATTAMENTO	CATEGORIE DI INTERESSATI	NOTE SUI DIRITTI DELL'INTERESSATO	CONSENSO	INFORMATIVA	CONSERVAZIONE
Orientamento	Studenti delle Scuole Superiori Studenti Persone che decidono volontariamente di aderire ad attività di orientamento e che in casi particolari possono essere anche minorenni Referenti presenti nelle Scuole	Non è consentita la rettifica dei risultati previsti nelle prove di orientamento	Non necessario perché connesso allo svolgimento di attività di interesse pubblico	Link Informativa	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Erogazione dei test di ingresso o alla verifica dei requisiti di accesso	Soggetti che intendono iscriversi a un corso di laurea. In particolare nella maggior parte dei casi si tratta di studenti delle superiori (superiori ai 16 anni)	Per quanto attiene la cancellazione, potrebbe essere concessa la cancellazione dei dati di contatto (es: indirizzo e-mail o numero di telefono), a meno che il dato non sia conservato per altre finalità (es: l'interessato è anche un dipendente dell'Ateneo). Coloro che risultano iscritti a una prova o selezione e non si siano presentati possono chiedere la cancellazione anche dei dati anagrafici. Nel caso in cui l'interessato si opponga al trattamento della diffusione del suo nominativo tramite la graduatoria, potrebbe essere consentita la sostituzione del nominativo con le iniziali, ferma restando la necessaria valutazione che ciascun Ateneo dovrà fare in merito ai tempi di pubblicazione delle graduatorie	Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	Link Informativa	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Erogazione del percorso formativo e gestione della carriera (dall'immatricolazione alla laurea)	Studenti Familiari (solo a fini dell'esercizio al diritto allo studio)	In merito alla cancellazione dei dati – non può essere concessa la cancellazione di dati personali che, per la normativa vigente o in ragione di regole d'Ateneo previste nei massimari o nei regolamenti interni: a) possono essere cancellati solo successivamente alla data di richiesta dell'interessato; b) devono essere conservati illimitatamente nel tempo. In merito alla rettifica dei dati, deve essere concessa la rettifica del sesso, soprattutto a fronte di una sentenza che stabilisca l'avvenuto cambio di genere	Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente tranne nei casi di mobilità studentesca extra UE	Link Informativa	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Attività di tirocinio	Studenti, specializzandi, referenti e rappresentanti legali dell'azienda		Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	Link Informativa	Illimitata in attesa in attesa di approvazione del Massimario di scarto

TRATTAMENTO	CATEGORIE DI INTERESSATI	NOTE SUI DIRITTI DELL'INTERESSATO	CONSENSO	INFORMATIVA	CONSERVAZIONE
Attività di job placement	Laureati, studenti, referenti aziendali e rappresentanti legali		Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	Link Informativa	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Attività di fundraising, di comunicazione e informazione istituzionale e sviluppo di community	Studenti, Laureati, Terzi donanti, Personale, collaboratori ricerca, docenti esterni		Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente. In qualche caso potrebbe essere necessario qualora il trattamento riguardi dati identificativi di soggetti particolari	Link Informativa	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Rilevazioni statistiche e valutazione della didattica	Studenti, Docenti	Cancellazione non possibile per questionari anonimizzati	Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente e finalità di interesse pubblico	Link Informativa	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Diffusione dell'elaborato finale o di elementi ad esso connessi	Studenti di corsi di Laurea e post Laurea (specializzazione, dottorato, master)	L'interessato può opporsi in qualsiasi momento alla diffusione del dato	Acquisire il consenso per permettere allo studente di individuare i dati che possono essere oggetto di diffusione, salvo il caso in cui la diffusione dei dati sia prevista da norma di legge o da un regolamento d'Ateneo	Link Informativa	Illimitata in attesa in attesa di approvazione del Massimario di scarto

TRATTAMENTO	CATEGORIE DI INTERESSATI	NOTE SUI DIRITTI DELL'INTERESSATO	CONSENSO	INFORMATIVA	CONSERVAZIONE
Servizi di tutorato, assistenza, inclusione sociale	Studenti di corsi di laurea e post laurea, specializzandi, dottorandi, familiari/accompagnatori/curatori		Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	Link Informativa	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Erogazione di servizi e attività per il diritto allo studio	Studenti, specializzandi, dottorandi, familiari		Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	Link Informativa	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Procedimenti di natura disciplinare a carico di studenti	Studenti, specializzandi, dottorandi, eventuali ulteriori soggetti coinvolti nel procedimento		Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	Link Informativa	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Gestione degli spazi	Tutti i dipendenti, collaboratori, studenti e soggetti terzi			Con riferimento a soggetti interni all'ente, le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'attivazione del rapporto con l'Ateneo (assunzione, immatricolazione, attivazione del contratto di collaborazione). Nel caso di soggetti terzi, dovrà essere rilasciata apposita informativa all'atto del conferimento dei dati	Illimitata in attesa in attesa di approvazione del Massimario di scarto

TRATTAMENTO	CATEGORIE DI INTERESSATI	NOTE SUI DIRITTI DELL'INTERESSATO	CONSENSO	INFORMATIVA	CONSERVAZIONE
Gestione delle postazioni	Tutti gli utilizzatori di postazioni soggette ad autenticazione	Anche in relazione alla tipologia di monitoraggio effettuato e ai software utilizzati, nell'eventualità in cui possa derivarne un controllo a distanza del lavoratore, occorrerà verificare la necessità di stipulare un accordo con le rappresentanze sindacali o con la sede territoriale competente dell'Ispettorato nazionale del lavoro. Al contrario, l'installazione e utilizzo di software per garantire il monitoraggio, la sicurezza e la gestione delle postazioni saranno possibili se strettamente connessi al rapporto di lavoro	Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente. In qualche caso potrebbe essere necessario qualora il trattamento riguardi dati identificativi di soggetti o attività particolari	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'attivazione del rapporto con l'Ateneo (assunzione, attivazione del contratto di collaborazione) o al momento dell'iscrizione a un corso (per gli studenti)	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Gestione degli organi e delle cariche istituzionali Gestione degli elenchi per l'elettorato attivo e passivo	Tutti i potenziali eletti ed elettori	Eventuale cancellazione solo dopo espletamento degli obblighi di legge o regolamento interno	Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	Con riferimento a soggetti interni all'ente, le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'attivazione del rapporto con l'Ateneo (assunzione, immatricolazione, attivazione del contratto di collaborazione). Nel caso di soggetti terzi, dovrà essere rilasciata apposita informativa all'atto del conferimento	Illimitata in attesa in attesa di approvazione del Massimario di scarto

TRATTAMENTO	CATEGORIE DI INTERESSATI	NOTE SUI DIRITTI DELL'INTERESSATO	CONSENSO	INFORMATIVA	CONSERVAZIONE
Gestione degli organi e delle cariche istituzionali Nomina degli eletti e delle cariche accademiche	Tutto il personale dell'organizzazione, studenti, eventuali terzi	Eventuale cancellazione solo dopo decadenza carica, espletamento degli obblighi di legge o regolamento interno	Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa: al momento dell'assunzione, per il personale Docente/Ricercatore e Tecnico Amministrativo; al momento dell'immatricolazione, per la popolazione studentesca	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Pubblicizzazione di atti ai fini di trasparenza	Personale dell'organizzazione, studenti, soggetti terzi	L'eventuale cessazione di carica, incarico o rapporto di lavoro o collaborazione dell'interessato non implicano la corrispondente rimozione delle relative informazioni dalle pagine web di pubblicazione ai fini della trasparenza, comunque subordinata a suddetti obblighi di legge. Non possono pertanto essere accolte eventuali richieste di rimozione di informazioni da tali pagine che risultino in contrasto con gli obblighi di pubblicazione	Non necessario perché connesso allo svolgimento di adempimenti normativi	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa: - al momento dell'assunzione, per il personale Docente/Ricercatore e Tecnico Amministrativo; - al momento dell'immatricolazione, per la popolazione studentesca; - all'atto dell'inizio del rapporto di collaborazione per soggetti esterni	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Gestione degli infortuni	Tutto il personale dell'organizzazione e soggetti terzi		Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti all'atto dell'apertura del sinistro	Illimitata in attesa in attesa di approvazione del Massimario di scarto

TRATTAMENTO	CATEGORIE DI INTERESSATI	NOTE SUI DIRITTI DELL'INTERESSATO	CONSENSO	INFORMATIVA	CONSERVAZIONE
Trattamento in ambito bibliotecario	Tutto il personale dell'organizzazione e soggetti terzi	Cancellazione solo dopo espletamento degli obblighi di legge o regolamento interno (es. completata restituzione di materiale bibliografici e documentali in prestito, ecc.) e in assenza di vincoli archivistici	Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere rese nel momento in cui l'utente accede ad un servizio bibliotecario	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Servizi di protocollo e conservazione documentale *** Gestione del protocollo in entrata/uscita	Studenti, personale, terzi		Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa: al momento dell'assunzione, per il personale Docente/Ricercatore e Tecnico Amministrativo; - al momento dell'immatricolazione, per la popolazione studentesca all'inizio di un rapporto di collaborazione con un soggetto esterno	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Servizi di protocollo e conservazione documentale *** Conservazione Documentale	Studenti, personale, terzi		Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa: a momento dell'assunzione, per il personale Docente/Ricercatore e Tecnico Amministrativo; al momento dell'immatricolazione, per la popolazione studentesca	Illimitata in attesa in attesa di approvazione del Massimario di scarto

TRATTAMENTO	CATEGORIE DI INTERESSATI	NOTE SUI DIRITTI DELL'INTERESSATO	CONSENSO	INFORMATIVA	CONSERVAZIONE
Acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso *** Acquisizione di beni e servizi	Fornitori di beni e servizi, operatori economici		Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	L'informativa può essere resa al momento della pubblicazione del bando per la fornitura di beni o servizi. Al momento della stipula del contratto si può consegnare un'ulteriore informativa più specifica in funzione del servizio reso o del bene acquisito	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso *** Verifiche sull'espletamento di lavori, in cantiere o presso installazioni in Ateneo	Fornitori		Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	L'informativa è predisposta al momento della gara e allegata al bando	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso *** Gestione del contenzioso e del recupero crediti	Sono interessati potenzialmente tutti i soggetti che abbiano un rapporto con l'Ateneo: personale docente-ricercatore, personale tecnico-amministrativo, studenti dell'Ateneo o di altri Atenei, candidati, soggetti terzi (fornitori). Può interessare anche persone che non hanno rapporti di alcun tipo con l'Ateneo (es. studente di scuola superiore che accede ai locali per informazioni). Con riguardo ad alcuni contenziosi e procedimenti di recupero crediti potrebbero essere interessati anche i familiari dei soggetti direttamente coinvolti (ad es. richiesta di restituzione borse di studio a seguito di verifica autocertificazione situazione reddituale/patrimoniale)		Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	Le informazioni inerenti il trattamento di dati personali per questa finalità potrebbero essere inserite in un'apposita informativa o nell'informativa generale resa: al personale docente/ricercatore e tecnico-amministrativo; agli studenti; a soggetti terzi e aziende fornitrici di beni e servizi	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Servizi di posta elettronica e strumenti di collaboration *** Accesso agli strumenti di collaboration	Personale dipendente, collaboratori esterni, studenti interni, studenti di altro ateneo, altri soggetti utilizzatori del servizio		Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	L'informativa dovrebbe essere resa prima dell'accesso al sistema, qualora non specificato in informative specifiche	Illimitata in attesa in attesa di approvazione del Massimario di scarto

TRATTAMENTO	CATEGORIE DI INTERESSATI	NOTE SUI DIRITTI DELL'INTERESSATO	CONSENSO	INFORMATIVA	CONSERVAZIONE
Servizi di posta elettronica e strumenti di collaboration *** Erogazione di servizi di posta elettronica	Personale dipendente e non (inclusi docenti a contratto), studenti, associazioni ufficiali, ospiti frequentatori	Cancellazione solo dopo un determinato periodo dalla cessazione del rapporto	Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa: all'assunzione, per il personale docente/ricercatore e tecnico-amministrativo; all'immatricolazione, per gli studenti; alla richiesta di creazione dell'account per soggetti terzi	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Erogazione del servizio Eduroam	Personale docente e tecnico amministrativo, studenti, ospiti di università federate	Cancellazione log di autenticazione	Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	Le informazioni registrate vengono mantenute per un periodo di 6 (sei) mesi, o maggiore se prescritto dalla legislazione in vigore. https://www.servizi.garr.it/eduroam/aderire/documenti-template/1-regolamento-della-federazione-italiana-eduroam	Illimitata in attesa in attesa di approvazione del Massimario di scarto
Svolgimento di prove concorsuali/selezioni	Partecipanti alla selezione/concorso		Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	L'informativa deve essere resa specificatamente per la selezione	Illimitata in attesa in attesa di approvazione del Massimario di scarto

TRATTAMENTO	CATEGORIE DI INTERESSATI	NOTE SUI DIRITTI DELL'INTERESSATO	CONSENSO	INFORMATIVA	CONSERVAZIONE
Gestione del rapporto di lavoro o di collaborazione, anche per personale in convenzione	Tutti i dipendenti dell'organizzazione e collaboratori	In merito alla cancellazione dei dati – non può essere concessa la cancellazione di dati personali che, per la normativa vigente o in ragione di regole d'Ateneo previste nei massimari o nei regolamenti interni devono essere conservati illimitatamente nel tempo	Non necessario perché connesso allo svolgimento di attività di istituzionali dell'ente	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'assunzione e dell'avvio del rapporto di collaborazione	L'anagrafica e i dati di carriera sono conservati dall'Ateneo illimitatamente nel tempo. I dati inerenti graduatorie o verbali sono conservati illimitatamente nel tempo. La conservazione dei restanti dati è sotteso ai tempi di conservazione degli atti amministrativi che li contengono (per maggiori info si veda il "Massimario di selezione dei documenti inerenti al fascicolo di personale universitario")
Formazione e aggiornamento professionale	Personale (personale docente, T.A., assegnisti, collaboratori, studenti 150 ore, laureati frequentatori)	Potrebbe essere garantita l'opposizione a specifiche operazioni di trattamento delle riprese audio-video (es: nel caso di diffusione del video su internet)		L'informativa potrebbe essere inclusa tra le informazioni rese al momento della gestione del rapporto di dipendenza o collaborazione. Nel caso in cui, durante la sessione di formazione, siano registrate le immagini e/o le voci di docenti e/o partecipanti, si rende opportuno informare gli interessati di tale trattamento mediante, ad esempio, affissione dei cartelli informativi	Gli atti connessi alle attività di formazione svolte dai partecipanti potrebbero avere un tempo di conservazione simile a quello previsto per gli atti di carriera. La conservazione delle registrazioni audio/video dovrà essere stabilita nell'informativa in relazione alle specifiche finalità perseguite dall'ente

TRATTAMENTO	CATEGORIE DI INTERESSATI	NOTE SUI DIRITTI DELL'INTERESSATO	CONSENSO	INFORMATIVA	CONSERVAZIONE
Gestione di progetti di ricerca	Personale Docente/Ricercatori/Assegnisti/Dottorandi e Tecnico Amministrativo			Le informazioni inerenti questo trattamento potrebbero essere integrate nell'informativa generale inerente la gestione del rapporto di lavoro	I tempi di conservazione dei dati sono strettamente dipendenti dagli ambiti di gestione (es: carriera, rendicontazione, ecc..) e dalle norme vigenti in tali ambiti
Monitoraggio e Valutazione della Ricerca	Personale Docente/Ricercatori/Assegnisti/Dottorandi e Tecnico Amministrativo			Le informazioni inerenti questo trattamento potrebbero essere integrate nell'informativa generale inerente la gestione del rapporto di lavoro	I tempi di conservazione dei dati sono strettamente dipendenti dagli ambiti di gestione (es: carriera, rendicontazione, ecc..) e dalle norme vigenti in tali ambiti
Trasferimento Tecnologico	Personale Docente/Ricercatori/Assegnisti/Dottorandi e Tecnico Amministrativo, soggetti partner e finanziatori			L'informativa è da prendersi al primo contatto	I tempi di conservazione dei dati sono strettamente dipendenti dagli ambiti di gestione (es: carriera, rendicontazione, ecc..) e dalle norme vigenti in tali ambiti
Politiche Welfare	Dipendenti e familiari			Le informazioni inerenti questo trattamento dovrebbero essere integrate nell'informativa generale inerente la gestione del rapporto di lavoro	Basato prevalentemente su obblighi di legge e regolamenti

TRATTAMENTO	CATEGORIE DI INTERESSATI	NOTE SUI DIRITTI DELL'INTERESSATO	CONSENSO	INFORMATIVA	CONSERVAZIONE
Salute e sicurezza delle persone nei luoghi di lavoro	Tutti i dipendenti dell'organizzazione ed eventualmente studenti (es. Cdl di area medica) e collaboratori sulla base dei protocolli di rischio in rapporto alle attività svolte			Le informazioni inerenti questo trattamento dovrebbero essere integrate nell'informativa generale inerente la gestione del rapporto di lavoro. Inoltre, informativa specifica per il servizio da rendere all'interessato all'atto della visita medica	I tempi di conservazione dei dati sono strettamente dipendenti dagli ambiti di gestione (es: fascicolo sanitario/referti/gestione amministrativa) e dalle norme vigenti in tali ambiti
Erogazione del servizio di telefonia fissa e mobile	Tutti gli intestatari di un'utenza fissa e/o mobile; soggetti che ricevono o effettuano delle chiamate su utenze d'Ateneo			Con riferimento alla telefonia fissa, le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'assunzione. In relazione alla telefonia mobile, è opportuno rilasciare apposita informativa all'atto della consegna del telefono di servizio	6 mesi per i dati di traffico telefonico (nel caso di dati non tracciati dall'operatore telefonico) I tempi di conservazione dei dati di traffico telefonico tracciati dall'operatore sono quelli stabiliti dalla normativa vigente

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Orientamento	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi utilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi "profili di autorizzazione", a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati ai trattamenti. Tipicamente le credenziali sono composte da: • un identificativo dell'utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E' stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle "Misure Minime di sicurezza informatica per le pubbliche amministrazioni" di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell'amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l'inventario dei dispositivi autorizzati e non autorizzati, l'inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	
Erogazione dei test di ingresso o alla verifica dei requisiti di accesso	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi utilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi "profili di autorizzazione", a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati ai trattamenti. Tipicamente le credenziali sono composte da: • un identificativo dell'utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E' stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle "Misure Minime di sicurezza informatica per le pubbliche amministrazioni" di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell'amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l'inventario dei dispositivi autorizzati e non autorizzati, l'inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Erogazione del percorso formativo e gestione della carriera (dall'immatricolazione alla laurea)	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	
Attività di tirocinio	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Attività di job placement	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	
Attività di fundraising, di comunicazione e informazione istituzionale e sviluppo di community	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Rilevazioni statistiche e valutazione della didattica	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	
Diffusione dell’elaborato finale o di elementi ad esso connessi	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Servizi di tutorato, assistenza, inclusione sociale	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	
Erogazione di servizi e attività per il diritto allo studio	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Procedimenti di natura disciplinare a carico di studenti	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	
Gestione degli spazi	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Gestione delle postazioni	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	
Gestione degli organi e delle cariche istituzionali Gestione degli elenchi per l’elettorato attivo e passivo	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Gestione degli organi e delle cariche istituzionali Nomina degli eletti e delle cariche accademiche	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	
Pubblicizzazione di atti ai fini di trasparenza	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Gestione degli infortuni	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	
Trattamento in ambito bibliotecario	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Servizi di protocollo e conservazione documentale *** Gestione del protocollo in entrata/uscita	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	
Servizi di protocollo e conservazione documentale *** Conservazione Documentale	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso *** Acquisizione di beni e servizi	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	
Acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso *** Verifiche sull’espletamento di lavori, in cantiere o presso installazioni in Ateneo	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso *** Gestione del contenzioso e del recupero crediti	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	
Servizi di posta elettronica e strumenti di collaboration *** Accesso agli strumenti di collaboration	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Servizi di posta elettronica e strumenti di collaboration *** Erogazione di servizi di posta elettronica	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	
Erogazione del servizio Eduroam	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Svolgimento di prove concorsuali/selezioni	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	
Gestione del rapporto di lavoro o di collaborazione, anche per personale in convenzione	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Formazione e aggiornamento professionale	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	
Gestione di progetti di ricerca	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Monitoraggio e Valutazione della Ricerca	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali nell'ottica di una riassegnazione in quelle che presentano criticità circa l'attribuzione delle attività al personale ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. Formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	
Trasferimento Tecnologico	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali nell'ottica di una riassegnazione in quelle che presentano criticità circa l'attribuzione delle attività al personale ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. Formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Politiche Welfare	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	
Salute e sicurezza delle persone nei luoghi di lavoro	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione.	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	MISURE DI SICUREZZA ORGANIZZATIVE	MISURE DI SICUREZZA LOGICHE	MISURE DI SICUREZZA TECNOLOGICHE	UBICAZIONE SERVER/ARCHIVI CARTACEI
Erogazione del servizio di telefonia fissa e mobile	Sono stati individuati all'interno dell'organizzazione le figure dei Referenti per la protezione dati (Dirigenti, Direttori dei Centri di servizio, RAD, Direttori dei Dipartimento) e degli autorizzati al trattamento (personale strutturato e non e chiunque a qualunque titolo venga assegnato anche temporaneamnte ad una struttura). Si sta provvedendo ad una ricognizione del personale all'interno delle singole Aree Dirigenziali, nell'ottica di una riassegnazione in quelle aree che presentano criticità circa l'attribuzione delle attività al personale, ai fini della corretta individuazione di chi effettua il trattamento. Sono state predisposte istruzioni operative, riviste le informative e predisposti i facsimili di atti con specifico riferimento ai casi di contitolarità e di responsabile del trattamento esterno. E' prevista una formazione mirata anche attraverso l'implementazione di un modulo e-learning	Gli applicativi tutilizzati prevedono l'accesso tramite credenziali di autorizzazione; possono anche essere definiti a livello applicativo diversi “profili di autorizzazione”, a seconda delle operazioni consentite a ciascuno dei Referenti per la Protezione Dati e degli autorizzati all trattamentoi. Tipicamente le credenziali sono composte da: • un identificativo dell’utente (User ID), che è la parte pubblica delle credenziali; • una parola chiave di autenticazione (password), che è la parte riservata delle credenziali. Per l'accesso a molti applicativi è previsto un sistema di autenticazione unico basato su User ID e password. E' in corso una ricognizione degli applicativi presenti all'interno dell'Ateneo e dei relativi sistemi di autenticazione	E’ stata effettuata un analisi del rischio in base ad una segregazione stratificata della rete e dei sistemi diversificati in base al tipo utente e/o servizio fornito nel rispetto delle “Misure Minime di sicurezza informatica per le pubbliche amministrazioni” di cui alla Circolare Agid 2/2017. Quali domini sicurezza sono stati individuati i seguenti domini di sicurezza divisi per tipologia di area e/o di utenza; - Data Center - Postazioni stabili dell’amministrazione (PC) e apparati collegati in rete - Postazioni Thin Client Sono invece riportati qui in modo sintetico gli elementi relativi ad i seguenti sotto-ambiti: Wi-fii Ambito dei dipartimenti/ricerca Sistemi gestiti da fornitori esterni – le misure minime sono oggetto dei contratti di fornitura. In tali domini sono stati presi in considerazione quali settori di intervento: l’inventario dei dispositivi autorizzati e non autorizzati, l’inventario dei software autorizzati e non autorizzati, proteggere le configurazioni di hardware e software sui dispositivi, mobili, laptop, workstation e server, valutazioni e correzione delle vulnerabilità, uso appropriato dei privilegi di amministrazione, difese contro i malware, copie di sicurezza, protezione dati. Le risultanze di dettaglio sono contenute nel documento prot. n. 357 del 02/01/2018	

TRATTAMENTO	CONTITOLARE	RAPPRESENTANTE DEL CONTITOLARE	RESPONSABILE DEL TRATTAMENTO	DESTINATARI DELLE COMUNICAZIONI DI DATI PERSONALI	PAESE TERZO/ORGANIZZAZIONE INTERNAZIONALE	SE APPLICABILE LE GARANZIE ADEGUATE PER IL TRASFERIMENTO
Orientamento				Tutor e borsisti; Uffici competenti in materia di orientamento ad es. Servizio Assistenza Disabili, Enti quali Almalaurea, Strutture addette a Counseling Psicologico	I dati non sono comunicati all'estero	
Erogazione dei test di ingresso o alla verifica dei requisiti di accesso				Uffici di Ateneo preposti alla gestione dell'iscrizione e delle carriere degli studenti, Scuole, ricercatori, servizi che si occupano di definire azioni volte al miglioramento della qualità della didattica. Cineca (per corsi a numero programmato nazionale), società esterne alle quali è affidata la gestione di test (soprattutto nei casi di corsi a numero programmato locale), CISIA (quale Titolare autonomo), Ambasciate (in relazione all'eventuale visto rilasciato) Personale coinvolto nella gestione delle procedure	I dati non sono comunicati all'estero	
Erogazione del percorso formativo e gestione della carriera (dall'immatricolazione alla laurea)				Strutture interne dell'Ateneo preposte quali,ad esempio, Segreterie Studenti, , Scuole, Dipartimenti, strutture preposte alla Comunicazione. Responsabili di trattamento: eventuali fornitori di servizi per uso di canali social (es. gruppo ex-alumni); società che stampano le pergamene di laurea; ecc. Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000; 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; Enti di assicurazione per pratiche infortuni; Organismi Regionali di Gestione (Enti dotati di autonomia amministrativo-gestionale istituiti ai sensi delle norme vigenti 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; Agenzia Entrate per 730 nel caso di dottorandi o specializzandi; MIUR; Soggetti pubblici e privati per consentire agli studenti di fruire di agevolazioni, sussidi 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; Finanziatori di premi, borse di dottorato e assegni, anche stranieri, nel caso di studenti e/o dottorandi che abbiano usufruito di finanziamenti Atenei stranieri, impegnati in percorsi formativi con rilascio di titoli congiunti; Servizi penitenziari	I dati inerenti agli studenti di scambio possono essere traferiti, su richiesta a: 1) Autorità all'estero (nel caso in cui sia necessario verificare il titolo di studi per ragioni professionali o per prosecuzione degli studi); 2) Ambasciate all'estero (anche per esoneri dal servizio militare); 3) Università extra UE (nell'ambito di scambi internazionali per studenti in-going e out-going)	
Attività di tirocinio				Medico del lavoro o strutture sanitarie convenzionate per verifiche o cure (nei casi in cui si renda necessario verificare di aver contratto malattie infettive o nel caso di infortuni) Regione e Direzione territoriale del lavoro. 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	Solo per tirocini attivati con Enti/aziende con sede all'estero	
Attività di job placement				Strutture di Ateneo preposte al Passaggio dati a Enti/aziende coinvolti nel placement. Potenziali datori di lavoro: Enti/Aziende Privati quali ad es. Banche, Comunità, Case di Cura, Fondazioni, Consorzi, congregazioni, Diocesi e Associazioni, Studi professionali gli Enti e le Aziende diventano titolari autonomi nel trattamento effettuato, comunque connesso ai fii di selezione del personale. Categorie particolari di dati personali o dati personali relativi a condanne penali e reati potranno essere comunicati ove previsto per legge o regolamento Almalaurea, nel caso in cui l'attività sia gestita in convenzione con tale soggetto	Solo nei casi di placement presso Enti/aziende con sede all'estero	

TRATTAMENTO	CONTITOLARE	RAPPRESENTANTE DEL CONTITOLARE	RESPONSABILE DEL TRATTAMENTO	DESTINATARI DELLE COMUNICAZIONI DI DATI PERSONALI	PAESE TERZO/ORGANIZZAZIONE INTERNAZIONALE	SE APPLICABILE LE GARANZIE ADEGUATE PER IL TRASFERIMENTO
Attività di fundraising, di comunicazione e informazione istituzionale e sviluppo di community				Strutture di Ateneo preposte al servizio, servizi esterni di gestione community e/o fundraising, società di spedizione, società organizzatrici di eventi.	Sono nel caso in cui i destinatari sopra riportati (es: società americana che organizza un evento di ricerca presso l'Ateneo italiano) operino/trattino i dati in aree extra U	
Rilevazioni statistiche e valutazione della didattica				Strutture di Ateneo preposte al servizio (ad es. strutture dell'Area Servizi alla Didattica, Dipartimenti, Consigli di Dipartimento, Commissioni, Nucleo di Valutazione), ANVUR, MIUR		
Diffusione dell'elaborato finale o di elementi ad esso connessi				Gli sportelli unici, biblioteche, i relatori/correlatori/contro-relatori della tesi trattano i dati personali nell'ambito della finalità descritta nella presente scheda. Nel caso di tesi di dottorato i dati (metadati e Full Text - dopo periodo embargo se presente) sono inviati alla Biblioteca Nazionale. Trattandosi di diffusione, i destinatari sono indeterminabili.		
Servizi di tutorato, assistenza, inclusione sociale				Strutture di Ateneo preposte, società di trasporti, helping services, meeting services, tutor, associazioni o organizzazioni con le quali sono avviate attività di collaborazione per la realizzazione delle finalità suddette (esempio: fondazioni che si occupano di DSA, associazioni specifiche).		
Erogazione di servizi e attività per il diritto allo studio				Strutture di Ateneo preposte (es segreterie studenti), enti esterni per realizzare servizi integrati a favore degli studenti universitari e preposti per favorire l'esercizio del diritto allo studio		
Procedimenti di natura disciplinare a carico di studenti				Strutture di Ateneo preposte, Autorità Giudiziaria, Docenti	Per studenti internazionali, Università di provenienza	
Gestione degli spazi				Strutture di Ateneo preposte alla gestione logistica, responsabili di struttura ed eventuali soggetti delegati alla gestione della logistica. Alcune informazioni potrebbero essere disponibili con accesso pubblico (es: consultazione da rubrica della collocazione delle persone negli spazi).		
Gestione delle postazioni				Gestore delle postazioni e dell'assistenza	Eventuale produttore di soluzioni SW installate (S.O., applicativi, endpoint security)	
Gestione degli organi e delle cariche istituzionali Gestione degli elenchi per l'elettorato attivo e passivo				Strutture di Ateneo preposte alla gestione logistica, responsabili di struttura ed eventuali soggetti delegati alla gestione della logistica. Alcune informazioni potrebbero essere disponibili con accesso pubblico (es: consultazione da rubrica della collocazione delle persone negli spazi)		
Gestione degli organi e delle cariche istituzionali Nomina degli eletti e delle cariche accademiche				Ufficio di Ateneo preposto, tutta la popolazione dell'organizzazione		
Pubblicizzazione di atti ai fini di trasparenza				Ufficio di Ateneo preposto, tutta la popolazione dell'organizzazione. Si precisa che tali dati sono soggetti a diffusione		
Gestione degli infortuni				Uffici dell'Ateneo coinvolti nella gestione degli infortuni, broker, compagnia assicuratrice, Inail, eventuali ulteriori enti coinvolti (Aziende ospedaliere)	I dati saranno comunicati e/o trasferiti all'estero in presenza di una compagnia assicuratrice estera o nel caso di soggetti coinvolti in infortuni all'estero	
Trattamento in ambito bibliotecario				Strutture Bibliotecarie dell'ente, altre strutture dell'Ateneo (es. Segreterie Studenti per nulla osta per iter conseguimento titolo). Eventuali aziende/cooperative che prestano servizio per le biblioteche dell'ente. Nel caso in cui i servizi bibliotecari siano integrati con quelli di altri enti sottoscrittori di una convenzione ad hoc. Biblioteche di altre istituzioni e università (prestito interbibliotecario/document delivery)	Nel caso di utilizzo in cloud di soluzioni Integrated Library Systems (ILS) ed altri applicativi per servizi di biblioteca quali Discovery tool, link resolver, Ask a librarian, ecc	
Servizi di protocollo e conservazione documentale *** Gestione del protocollo in entrata/uscita				Strutture di Ateneo e loro operatori e delegati preposte al processo di gestione documentale attraverso l'utilizzo dei sistemi di protocollo informatico o applicativi verticali che concorrono al popolamento del registro di protocollo informatico. Mittenti o destinatari delle registrazioni a protocollo		

TRATTAMENTO	CONTITOLARE	RAPPRESENTANTE DEL CONTITOLARE	RESPONSABILE DEL TRATTAMENTO	DESTINATARI DELLE COMUNICAZIONI DI DATI PERSONALI	PAESE TERZO/ORGANIZZAZIONE INTERNAZIONALE	SE APPLICABILE LE GARANZIE ADEGUATE PER IL TRASFERIMENTO
Servizi di protocollo e conservazione documentale *** Conservazione Documentale				Strutture di Ateneo – e loro operatori e delegati - preposte al processo di gestione documentale e alla conservazione. -Conservatore digitale accreditato AgID Destinatari del pacchetto di distribuzione per motivi legali o accesso agli atti (interni Ateneo o esterni) previa autorizzazione della struttura organizzativa coinvolta.		
Acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso *** Acquisizione di beni e servizi				Strutture preposte all'acquisto di beni e servizi, alla liquidazione o alla gestione del contenzioso; struttura preposta al rispetto delle norme su trasparenza e anticorruzione		
Acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso *** Verifiche sull'espletamento di lavori, in cantiere o presso installazioni in Ateneo				Strutture di Ateneo preposte al processo (area edilizia e sicurezza sul lavoro)	Normalmente non ci sono comunicazioni all'esterno	
Acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso *** Gestione del contenzioso e del recupero crediti				Ufficio d'Ateneo preposto, Avvocatura dello Stato (quando rappresenta l'Ateneo in giudizio), Autorità Giudiziarie, MIUR (nei casi di coinvolgimento anche del Ministero nel contenzioso), Presidenza del Consiglio dei Ministri (ad es. per i casi di contenzioso riguardanti l'adeguamento retributivo dei medici specializzandi) e Agenzia delle Entrate (nel caso di iscrizione a ruolo dei crediti)	Potrebbe esser necessaria la comunicazione e/o il trasferimento di dati all'estero nei casi di contenzioso con soggetti esteri e nel caso di recupero crediti da debitori esteri, con affidamento della pratica a professionisti stabiliti nei paesi dei soggetti con i quali si sia instaurata la lite	
Servizi di posta elettronica e strumenti di collaboration *** Accesso agli strumenti di collaboration				Ufficio di Ateneo preposto alla gestione e/o utilizzo dello strumento di collaboration	Solo in caso di servizio erogato outsourcer estero e nel caso in cui sia lecita la comunicazione di tali dati personali	
Servizi di posta elettronica e strumenti di collaboration *** Erogazione di servizi di posta elettronica				Struttura di Ateneo preposta al servizio di posta elettronica (in genere area IT) e aziende fornitrici	Solo in caso di servizio erogato outsourcer estero e nel caso in cui sia lecita la comunicazione di tali dati personali	
Erogazione del servizio Eduroam				Università federate, Polizia in caso di incidente	Università federate se estere	
Svolgimento di prove concorsuali/selezioni				Area del personale e strutture di Ateneo per finalità istituzionali o per osservanza obblighi legislativi (nome, cognome ed esito pubblico). Membri delle Commissioni esaminatrici MIUR nell'ambito delle comunicazioni obbligatorie previste per il presonale docente e ricercatore che risulti vincitore. Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000	I dati non sono comunicati all'estero	

TRATTAMENTO	CONTITOLARE	RAPPRESENTANTE DEL CONTITOLARE	RESPONSABILE DEL TRATTAMENTO	DESTINATARI DELLE COMUNICAZIONI DI DATI PERSONALI	PAESE TERZO/ORGANIZZAZIONE INTERNAZIONALE	SE APPLICABILE LE GARANZIE ADEGUATE PER IL TRASFERIMENTO
Gestione del rapporto di lavoro o di collaborazione, anche per personale in convenzione				Strutture di Ateneo (ad es. Strutture del Personale e Stipendi) Altri soggetti pubblici o privati, tra cui: - Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000; - 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; - Direzione Territoriale del lavoro (per le aspettative e per i casi di contenzioso) - 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);	I dati personali potrebbero essere trasferiti all'estero nel caso di periodi di formazione del personale all'estero.	
Formazione e aggiornamento professionale				Strutture di Ateneo deputate alla formazione e all'aggiornamento professionale di dipendenti e collaboratori altre Università (ad esempio nell'ambito di corsi di formazione erogati tra più università partner) Enti/Aziende esterne eroganti il servizio di formazione e aggiornamento professionale Enti pubblici convenzionati, con lo scopo di migliorarne la fruibilità e di garantire la qualità e l'efficacia della formazione sul territorio nazionale.	Eventuali Università/Enti esteri, ad esempio per favorire la formazione all'estero dei dipendenti dell'Ateneo	
Gestione di progetti di ricerca				Strutture di Ateneo deputate (Contabilità, Servizi per Ricerca) CINECA (Responsabili esterni) ANVUR Soggetti finanziatori (MIUR, Regioni, UE, ecc.)	Enti/Aziende estere quali partecipanti alla ricerca o finanziatori	
Monitoraggio e Valutazione della Ricerca				Strutture di Ateneo deputate (Contabilità, Servizi per Ricerca) CINECA (Responsabili esterni) ANVUR Soggetti finanziatori (MIUR, Regioni, UE, ecc.)	Enti/Aziende estere quali partecipanti alla ricerca o finanziatori	
Trasferimento Tecnologico				Strutture di Ateneo deputate (Area della Ricerca), Istituzioni, Consulenti, altri Atenei, Uffici brevetti, Partners	In occasione del deposito di domande di brevetto internazionali e della stipula di accordi con soggetti extra UE.	
Politiche Welfare				Strutture di Ateneo preposte Fornitori/Enti/Cooperative ad es. per attività dopo Lavoro, Aziende per erogazione polizze assicurative per il personale Enti esterni per realizzare servizi integrati a favore dei dipendenti e/o preposti a favorire l'attuazione di politiche Welfare	I dati non sono comunicati all'estero	
Salute e sicurezza delle persone nei luoghi di lavoro				Ufficio Prevenzione, Protezione e Sicurezza; Ufficio Personale; ASST, Responsabili di struttura, Medico competente	I dati non vengono comunicati all'estero, salvo casi specifici che lo richiedano (es. emergenze sanitarie, ricerche svolte all'estero o svolte sul territorio italiano con necessità di trasmissione all'estero)	
Erogazione del servizio di telefonia fissa e mobile				I responsabili delle strutture per le utenze di competenza; i soggetti che gestiscono la fatturazione nelle singole strutture; la struttura che si occupa della gestionedei servizi di telefonia.	I dati non sono comunicati all'estero	

Allegato B

SCHEDA DI ANALISI PER PROGETTI DI RICERCA

Descrizione del Progetto	
1. Data di inizio prevista	
2. Data di fine prevista	
3. Ipotesi/Breve stato dell'arte/giustificazione teorica	
4. Obiettivi/Risultati attesi	
5. Metodologia	
6. Descrizione della procedura	

Modalità e procedure	
7. Modalità di raccolta dei dati	☐ utilizzo di questionari ☐ interviste strutturate o semi-strutturate ☐ interviste in profondità ☐ focus group ☐ raccolta di diari (diary keeping) ☐ osservazione del comportamento dei soggetti a loro insaputa ☐ osservazione del comportamento dei soggetti ☐ registrazioni audio o video dei soggetti ☐ somministrazione di stimoli, compiti o procedure e registrazione di risposte comportamentali, opinioni o giudizi ☐ somministrazione di stimoli, compiti o procedure che il soggetto potrebbe trovare fastidiosi, stressanti, fisicamente o psicologicamente dolorosi, sia durante sia successivamente la conduzione dello studio ☐ registrazione di movimenti ☐ immersione in ambienti di realtà virtuale ☐ registrazione di potenziali evocati ☐ somministrazione di test, questionari o protocolli sperimentali attraverso internet (web, posta elettronica) ☐ utilizzo di test neuropsicologici e di tecniche di neuroimmagine ☐ somministrazione di sostanze o agenti (ad es., farmaci, alcol) ☐ partecipazione ad un trial clinico

	☐ altro *(specificare)* _____ _____ *Allegare copia delle domande che verranno poste (se previsto dalla procedura utilizzata); ove questo non sia possibile, indicare gli argomenti che verranno trattati* _____ _____ _____ _____
8. Descrizione del flusso dei dati	

	Partecipanti al progetto
9. Tipologia	☐ Maggiori d'età ☐ Minori d'età ☐ Studenti ☐ Lavoratori ☐ Soggetti con disabilità fisica e psichica o con limitata capacità d'intendere o volere ☐ Soci, associati, aderenti o iscritti a organizzazioni a carattere religioso, politico, filosofico o sindacale ☐ Condannati, detenuti, imputati, indagati o sottoposti a misure di sicurezza o prevenzione ☐ Volontari sani ☐ Pazienti ☐ altro _____ _____ _____
10. Numero indicativo di partecipanti	
11. Caratteristiche del gruppo di partecipanti alla ricerca	☐ Gruppi omogenei per abitudini sessuali ☐ Gruppi omogenei per appartenenza razziale o etnica ☐ Gruppi omogenei per area geografica ☐ Gruppi omogenei per caratteristiche fisiche

	☐ Gruppi omogenei per consanguineità ☐ Gruppi omogenei per fattori di rischio ☐ Gruppi omogenei per convinzioni religiose, filosofiche, politiche o sindacali *Specificare eventuali e ulteriori criteri di inclusione/esclusione* _____ _____ _____
12. È possibile che alcuni dei soggetti si trovino in una posizione di dipendenza nei confronti del ricercatore o dei suoi collaboratori, tale per cui si possa supporre che l'espressione del consenso a partecipare allo studio non sia del tutto libera e priva da ogni tipo di pressione?	☐ Sì ☐ No *Se sì, indicare come si intende provvedere per minimizzare la possibilità che il soggetto si senta obbligato a prendere parte alla ricerca (ad es. nel rapporto studente/professore, paziente/medico, dipendente/datore di lavoro)* *Esempio: Il soggetto valuta senza alcuna fretta o pressione psicologica le informazioni ricevute tramite i moduli e decide di aderire alla ricerca, fornendo il consenso al trattamento dei dati, solo in un momento successivo alla cura/incontro informativo* _____ _____ _____
13. Come verranno diffuse le informazioni/l'invito a partecipare alla ricerca?	
14. È prevista qualche forma di incentivo per i partecipanti allo studio?	☐ Sì ☐ No *Se sì, indicare quali* _____ _____ _____

Modalità e procedure	
15. Rischi per i partecipanti	☐ Nessuno ☐ Rischi sociali, legali o economici ☐ Disagi o rischi per il benessere fisico e psicologico ☐ altro *(specificare)* _____ _____ _____
16. Benefici per i partecipanti	☐ Nessuno ☐ Benefici di natura sociale ottenuti attraverso un miglioramento delle conoscenze scientifiche ☐ Compenso o altri vantaggi materiali ☐ altro *(specificare)* _____ _____ _____
17. È prevista una specifica polizza di assicurazione per responsabilità civile aggiuntiva a quella di Ateneo? *[Da compilare soprattutto nel caso di sperimentazioni mediche]*	☐ Sì, è stata stipulata una polizza assicurativa che copre tutti i danni strettamente connessi alla partecipazione allo studio. La copertura assicurativa è stata stipulata con la seguente compagnia assicurativa: *Nome* | *telefono* | *fax* | *Numero polizza assicurativa* | | | | | ☐ Lo studio è no-profit e osservazionale e viene utilizzata l'assicurazione d'Ateneo ☐ Lo studio è no-profit, interventistico e viene aggiunto un premio assicurativo ☐ Non è prevista alcuna forma di assicurazione
18. Come si prevede di affrontare il caso in cui l'interessato intenda non aderire alla ricerca (anche in un momento successivo)?	☐ L'interessato potrà ritirare il consenso in qualsiasi momento e senza fornire spiegazioni alcune, con la conseguente distruzione dei dati ☐ L'interessato potrà richiedere che tutti i dati precedentemente raccolti siano distrutti o resi anonimi in modo definitivo solo nelle fasi antecedenti alla irreversibile anonimizzazione o aggregazione ☐ altro *(specificare)* _____ _____ _____

	Comunicazione e diffusione dei dati
19. I dati <u>personali</u> (non anonimi o aggregati) vengono diffusi?	☐ No ☐ Sì Se sì, selezionare una o più modalità: ☐ Stampa quotidiana e periodica anche elettronica ☐ Stampati in genere ☐ TV ☐ Posta ☐ Fax ☐ Posta elettronica ☐ Internet ☐ A mezzo confezione del prodotto ☐ Affissione dei dati in luoghi pubblici ☐ Radio ☐ Telefono ☐ Televideo ☐ Agenzie di stampa ☐ Strumenti multimediali (cd, dvd...) ☐ Altro, specificare in dettaglio _____ _____
20. I dati <u>personali</u> (pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono comunicati?	☐ No ☐ Sì Se sì, selezionare uno o più ambiti di comunicazione: ☐ Soggetti privati ☐ Soggetti pubblici ☐ Persone giuridiche, società di persone o di capitali, imprese individuali ☐ Organi costituzionali o di rilevanza costituzionale ☐ Amministrazioni dello Stato ☐ Amministrazioni regionali ☐ Enti locali (comuni e province) ☐ Associazioni di enti locali ☐ Altre amministrazioni ed enti pubblici ☐ Organismi del servizio sanitario nazionale ☐ Enti pubblici non economici

	☐ Enti pubblici economici ☐ Autorità giudiziaria ☐ Uffici giudiziari ☐ Società di vigilanza private ☐ Società controllanti, controllate e/o collegate ☐ Associazioni di imprenditori o di imprese ☐ Organismi sindacali o patronali ☐ Organismi paritetici in materia di lavoro ☐ Consulenti e liberi professionisti anche in forma associata ☐ Banche ☐ Intermediari finanziari ☐ Gestori di sistemi informatici centralizzati (centrali rischi, antifrode, ecc.) ☐ Assicurazioni ☐ Soci associati e iscritti ☐ Clienti e/o utenti ☐ Altro, specificare in dettaglio _____ _____

	Trasferimento di dati all'estero (extra UE)
21. I dati <u>personali</u> (pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono trasferiti all'estero?	☐ No ☐ Sì Se sì, in che area geografica sono trasferiti i dati? ☐ Paesi dell'America del centro-nord ☐ Paesi dell'America del sud ☐ Paesi dell'area asiatica ☐ Paesi dell'area africana ☐ Paesi dell'Oceania ☐ Paesi dell'Europa extra UE In quale/i Paese/i all'interno dell'area _____ _____

<table>
<tr><th colspan="2">Soggetti coinvolti nel Progetto</th></tr>
<tr><td>22. Titolare</td><td></td></tr>
<tr><td>23. Responsabile scientifico</td><td></td></tr>
<tr><td>24. Personale coinvolto</td><td></td></tr>
<tr><td>25. È necessaria l’autorizzazione di altri Enti/soggetti terzi per l’accesso ai dati o per il coinvolgimento di partecipanti?</td><td>☐ Sì
☐ No

Se sì, allegare copia della lettera di autorizzazione e/o la lettera di richiesta di eventuali dati provenienti da soggetti terzi)</td></tr>
<tr><td>26. Sono previsti, ai sensi della normativa vigente, interventi che richiedono specifiche professionalità (ad es. medico, psicologo, infermiere, ecc.)?</td><td>☐ No
☐ Sì

Se sì, specificare quali istruzioni sono fornite in merito al trattamento dei dati personali

_____

_____</td></tr>
<tr><td>27. Ci sono eventuali partner, enti, sponsor o finanziatori che potrebbero venire a conoscenza dei dati personali?</td><td>☐ No
☐ Sì

Se sì, indicare tali soggetti e il ruolo che hanno del progetto

<table><tr><td>Nominativo</td><td>Ruolo</td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table></td></tr>
</table>

Allegato C

Procedura segnalazione VIOLAZIONE DATI PERSONALI (*DATA BREACH*)

Titolare del trattamento dati: Università degli Studi di Firenze

Responsabile della Protezione dei dati (RPD): dott. Massimo Benedetti – privacy@unifi.it – tel.: +39 055 2757667

Attività di segnalazione, raccolta informazioni, valutazione notifica della violazione

STEP	ATTIVITA'	CHI	A CHI	QUANDO	COME
1	**Rilevazione e segnalazione di data breach**	Tutto il personale, collaboratori, fornitori, responsabili	Al Responsabile amministrativo della struttura di riferimento (Dirigente, RAD, Direttore Tecnico) o al suo sostituto o al referente privacy se nominato	Appena se ne viene a conoscenza	Utilizzando le vie più brevi (telefono, di persona, e-mail)
2	**Raccolta informazioni sulla violazione**	Il responsabile della struttura o il sostituto o il referente privacy insieme ai soggetti coinvolti nella violazione (il responsabile della struttura nel caso non possa essere immediatamente disponibile, deve dare		Appena ricevuta la comunicazione	Utilizzando il modello fornito e raccogliendo informazioni dai soggetti coinvolti nella segnalazione e nel trattamento dei dati violati

		istruzioni precise alla persona che l'ha contattato per iniziare subito la raccolta delle informazioni, indicando dove reperire il modello predisposto a tale scopo)			
3	**Comunicazione del data breach**	Il responsabile amministrativo della struttura (RAD, Direttore Tecnico, Dirigente) o il sostituto o il referente privacy (in mancanza di tali figure la stessa persona che ha rilevato la violazione)	Al Titolare (da specificare quale organo di UNIFI è incaricato della notifica della violazione al Garante), RPD, esperti ICT	Appena ottenute informazioni di base sulla violazione	Utilizzando le vie più brevi
4	**Valutazione d'impatto**	Titolare, RPD, esperti ICT, soggetti coinvolti		Appena ricevuta la comunicazione	Utilizzando la metodologia indicata
5	**Individuazione delle azioni correttive**	RPD, esperti ICT, soggetti coinvolti		Appena terminata la valutazione d'impatto	Analizzando i risultati della valutazione d'impatto
6	**Comunicazione delle valutazioni effettuate e delle azioni da intraprendere**	RPD, responsabile della struttura o sostituto o referente privacy	Al Titolare		Tramite una breve relazione anche orale
7	**Notifica della violazione (se è necessaria)**	Titolare	Al Garante	Entro 72 ore dalla rilevazione	Mediante la modulistica predisposta dal Garante
8	**Comunicazione agli interessati coinvolti (se è necessaria)**	Titolare	Alle persone fisiche i cui dati sono stati violati	Nei termini indicati nella valutazione d'impatto	Comunicazione diretta alle singole persone o mediante pubblicazione in sito a loro accessibile delle eventuali conseguenze della violazione sulle categorie di persone fisiche interessate

9	**Disposizioni per l'attuazione delle misure correttive (se individuate)**	Responsabili delle strutture coinvolte	Ai soggetti incaricati di svolgere le attività	Nei termini indicati nella valutazione d'impatto	Devono essere indicate in dettaglio le operazioni da svolgere, chi è l'incaricato, i tempi di attuazione; prevedere eventuali operazioni di verifica dell'efficacia delle misure correttive
10	**Recepimento della risposta del Garante alla notifica (se effettuata)**	Titolare, RPD, responsabili delle strutture coinvolte, esperti ICT			Disposizioni per l'attuazione delle eventuali misure correttive indicate dal Garante; effettuazione di ulteriori indagini per approfondire le informazioni raccolte

Attività relative alla registrazione dell'incidente

STEP	ATTIVITA'	CHI	A CHI	QUANDO	COME
1	**Registrazione della violazione/aggiornamenti**	Ufficio RPD		Appena ricevuta la comunicazione	Compilando l'apposito registro con la descrizione della violazione, delle azioni intraprese e annotando i successivi aggiornamenti
2	**Registrazione della risposta del Garante**	Ufficio RPD		Al momento della ricezione	Annotando sul registro gli estremi della risposta del Garante e le eventuali prescrizioni in essa contenute
3	**Registrazione della prosecuzione/chiusura dell'incidente**	Ufficio RPD		In seguito alle indicazioni del RPD	Registra la chiusura dell'incidente se non necessita di ulteriori indagini o riporta le istruzioni per le ulteriori indagini

Attività inerenti la prosecuzione delle indagini

Da eseguire nel caso sia necessario acquisire ulteriori informazioni

STEP	ATTIVITA'	CHI	A CHI	QUANDO	COME
1	**Prosecuzione delle indagini**	RPD, responsabile della struttura o sostituto o referente privacy, soggetti coinvolti nella violazione e nei trattamenti di dati violati, esperti ICT		A seguito di indicazione da parte del Garante o del titolare; se previsto nella prima valutazione d'impatto; nel caso che le informazioni raccolte risultino incomplete o mancanti	Raccogliendo le informazioni mancanti, o approfondendo quelle note per rilevare eventuali impatti non riscontrati nella prima indagine
2	**Esecuzione di una nuova valutazione d'impatto**	Titolare, RPD, esperti ICT, soggetti coinvolti		Al momento che si ritiene di aver raccolto tutte le informazioni possibili sulla violazione	
3	**Comunicazione dei risultati del proseguimento delle indagini**	RPD, responsabile della struttura o sostituto o referente privacy	Al Titolare	appena terminato il lavoro	Tramite relazione sintetica sui risultati della valutazione d'impatto e sulle azioni necessarie, allegando il materiale informativo raccolto
4	**Aggiornamento della notifica al Garante (se necessario)**	Titolare	Al Garante	Appena sono disponibili i nuovi dati o secondo i termini stabiliti dal Garante	Mediante la modulistica predisposta o come indicato dal Garante
5	**Comunicazioni agli interessati (se necessario)**	Titolare		Nei tempi stabiliti nella valutazione	Contattando direttamente gli interessati oppure rendendo nota la violazione e le

				d'impatto	possibili conseguenze mediante pubblicazione accessibile alle categorie di interessati

Descrizione dei soggetti richiamati nelle procedure

Titolare - è il titolare del trattamento dei dati personali, cioè l'Università degli Studi di Firenze

RPD – è il Responsabile della protezione dati dell'Ateneo (detto anche DPO - Data Protection Officer). L'incarico è stato assegnato al dott. Massimo Benedetti

Responsabile della struttura – a seconda della struttura può essere il dirigente, il direttore tecnico, il presidente, il direttore, il responsabile amministrativo, il RAD. In sua assenza segue la procedura il sostituto o il referente privacy.

Referente privacy – è colui che ha avuto specifico incarico per gestire gli adempimenti in materia di protezione dei dati personali all'interno della propria struttura.

Garante – è l'autorità garante in Italia (http://www.garanteprivacy.it/) alla quale i titolari si rivolgono per gli adempimenti previsti dal GDPR (Regolamento UE 2016/679 del Parlamento Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Interessato – è la persona fisica alla quale si riferiscono i dati personali. Gli interessati possono essere raggruppati in categorie, quali ad esempio studenti, personale dipendente, collaboratori, ecc.

Ufficio RPD – Ufficio Funzionale di supporto al Responsabile della Protezione dei dati (https://www.unifi.it/cercachi-str-101495.html)

FORM PER RACCOLTA INFORMAZIONI

1. luogo e data dell'evento (anche approssimativi se non sono noti): _____
2. breve descrizione dell'evento:

   _____
3. indicazione dei trattamenti di dati coinvolti *(riportare elenco dei trattamenti?)*

   _____
4. banche dati o archivi anche cartacei che sono stati violati:

   _____
5. tipo di violazione
   - ☐ lettura (presumibilmente i dati non sono stati copiati)
   - ☐ copia (i dati sono ancora presenti sul sistema del titolare)
   - ☐ alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
   - ☐ cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
   - ☐ furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
   - ☐ altro: _____
6. Dispositivo oggetto della violazione
   - ☐ Computer
   - ☐ Rete
   - ☐ Dispositivo mobile
   - ☐ File o parte di un file
   - ☐ Strumento di backup
   - ☐ Documento cartaceo
   - ☐ Altro: _____

7. Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione: _____
8. Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?
   - ☐ N. _____persone
   - ☐ Circa _____persone
   - ☐ Un numero (ancora) sconosciuto di persone
9. Che tipo di dati sono oggetto di violazione?
   - ☐ Dati anagrafici/codice fiscale
   - ☐ Dati di accesso e di identificazione (user name,password, customer ID, altro)
   - ☐ Dati relativi a minori
   - ☐ 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

INFORMAZIONI PER LA COMPILAZIONE

DEFINIZIONI

<violazione di dati personali (data breach)>

la violazione di sicurezza che comporta accidentalmente o in modo illecito:

- la distruzione,
- la perdita,
- la modifica,
- la divulgazione o l'accesso non autorizzati

ai dati personali trasmessi, conservati o comunque trattati.

<distruzione (destruction)>

Non esistono più i dati

Non esistono più in forma che possa essere utilizzata dal titolare

<modifica (alteration, damage)>

Alterazione del dato

Corruzione del dato

Incompletezza del dato

<Perdita (loss)>

Il titolare non ha più il controllo sui dati

Il titolare non ha più i dati

<divulgazione (unauthorized or unlawful processing)>

Divulgazione di dati

Accesso ai dati da parte di destinatari non autorizzati

Trattamenti in violazione del GDPR

Elenco principali trattamenti di dati personali svolti in Ateneo

Trattamenti inerenti gli studenti :

- finalizzato all'orientamento
- finalizzato all'erogazione dei test di ingresso o alla verifica dei requisiti di accesso
- finalizzato per il percorso formativo e gestione della carriera
- finalizzato all'attività di tirocinio
- finalizzato all'attività di job placement
- finalizzato all'attività di foundraising, di comunicazione e informazione istituzionale e sviluppo di comunity
- finalizzato a rilevazioni statistiche e valutazione della didattica
- finalizzato al caso di diffusione dell'elaborato finale o di elementi ad esso connessi
- finalizzato a servizi di tutorato, assistenza, inclusione sociale
- finalizzato all'erogazione di servizi e attività per il diritto allo studio
- procedimenti di natura disciplinare a carico di studenti

Trattamenti inerenti a dipendenti e/o collaboratori:

- finalizzato allo svolgimento delle prove concorsuali
- finalizzato alla gestione del rapporto di lavoro
- finalizzato alla formazione e aggiornamento professionale

- finalizzato alla gestione di progetti di ricerca
- finalizzato al monitoraggio e alla valutazione della ricerca
- trattamenti nell'ambito di attività di trasferimento tecnologico
- trattamenti per politiche di welfare e per la fruizione di agevolazioni
- finalizzato alla salute e sicurezza delle persone nei luoghi di lavoro
    - trattamenti dell'ufficio Prevenzione, Protezione e Sicurezza
- finalizzato all'erogazione del servizio di telefonia fissa e mobile

Trattamenti trasversali o connessi ad attività trasversali:

- gestione degli spazi
- gestione delle postazioni di lavoro
- gestione degli organi e delle cariche istituzionali
    - finalizzato alla gestione degli elenchi per l'elettorato attivo e passivo
    - finalizzato alla nomina degli eletti e delle cariche accademiche
    - finalizzato alla pubblicizzazione di atti ai fini di trasparenza

Trattamento per la gestione degli infortuni

Trattamento in ambito bibliotecario

Trattamenti nell'ambito dei servizi di protocollo e conservazione documentale:

- finalizzato alla gestione del protocollo in entrata/uscita
- finalizzato alla conservazione documentale

Trattamenti per l'acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso:

- finalizzato all'acquisizione di beni e servizi
- finalizzato alle verifiche sull'espletamento di lavori, in cantiere o presso installazioni in Ateneo
- finalizzato alla gestione del contenzioso e del recupero crediti

Trattamenti nell'ambito dei servizi di posta elettronica e strumenti di collaboration:

- finalizzato all'accesso agli strumenti di collaboration
- finalizzato all'erogazione di servizi di posta elettronica

Trattamenti nell'ambito dell'erogazione federata di servizi:

- finalizzato all'erogazione del servizio Eduroam
- finalizzato all'accesso a servizi federati (es. IDEM)
- finalizzato all'accesso ai servizi con autenticazione SPID

Trattamenti relativi al tracciamento di informazioni non primarie:

- tracciamento sistemistico e di rete
- tracciamento applicativo

FAQ

1) Ho perduto lo smartphone su cui erano memorizzati messaggi di posta elettronica della mia casella UNIFI, devo effettuare la segnalazione?
   La segnalazione è necessaria se esiste il dubbio che eventuali dati personali contenuti nei messaggi di posta possano essere acceduti da terzi o se sono andati perduti. Non è necessaria se esiste una copia dei dati e se siamo certi che lo smartphone non può essere utilizzato da altri.
2) Il computer dell'ufficio è stato formattato in seguito ad un guasto. Devo fare la segnalazione?
   Se esiste un backup dei dati personali contenuti nel computer, non è necessaria la segnalazione.
3) Ho trovato che è stata forzata la serratura di un armadio contente archivi cartacei relativi alle carriere del personale tecnico amministrativo, ma sembra che non manchi nulla. Devo fare la segnalazione?
   La segnalazione è necessaria.
4) È stato rubato un notebook da un ufficio, nel quale erano contenuti dati personali. Devo fare la segnalazione?
   La segnalazione è necessaria.
5) Per errore ho inviato un messaggio di posta elettronica contenete una lista di studenti iscritti ad un corso con indicazione di matricola ed indirizzo e-mail a più destinatari sbagliati. Devo fare la segnalazione?
   La segnalazione è necessaria.
6) Ho lasciato, per sbaglio, alcune domande per usufruire della 104 su un bancone dell'ufficio a cui accedono più persone anche esterne. Devo fare la segnalazione?
   Deve essere fatta la segnalazione.
7) Non so chi devo informare di una violazione di dati personali che ho trovato su una pagina del sito web di Ateneo.

La segnalazione deve essere effettuata al responsabile della propria struttura di afferenza, il quale avvierà la procedura per la comunicazione al Titolare a al RPD. Se il responsabile non fosse reperibile rivolgersi al sostituto o al referente privacy se è stato nominato. In mancanza anche di questi contattare direttamente il Responsabile della protezione dati di Ateneo o il suo ufficio.

8) Mi sono accorto che un vecchio computer è stato hackerato. Apparentemente non sono stati rubati dati. Devo fare la segnalazione?
   È necessario effettuare la segnalazione.

UNIVERSITÀ DEGLI STUDI FIRENZE

Allegato D

ISTRUZIONI PER LA PROTEZIONE DEI DATI PERSONALI

Formazione

Tutti i soggetti, designati come Incaricati del trattamento dei dati personali di cui l'Università degli Studi di Firenze è titolare, sono tenuti a frequentare i corsi di formazione e aggiornamento organizzati dall'Ateneo sulle procedure e sui sistemi di sicurezza organizzativi, logici e fisici atti a tutelare il trattamento, la conservazione e l'integrità dei dati personali affidatigli per il trattamento e ad attenersi alle seguenti istruzioni.

Istruzioni per il trattamento dei dati personali

Ciascuno ha la responsabilità dei dati detenuti sulla propria stazione di lavoro e della loro protezione.

I soggetti Incaricati del trattamento dei dati detenuti dall'Ateneo, per il corretto e puntuale svolgimento del trattamento, dovranno:

1) visionare, nel **Registro delle attività di trattamento**, il contenuto dei trattamenti assegnati alla struttura di propria afferenza;

2) prendere visione, dal sito istituzionale dell'Università, delle **Istruzioni per la protezione dei dati personali** e delle **Istruzioni per i trattamenti con strumenti elettronici** e rispettare le prescrizioni in esse contenute;

3) prendere visione, dal sito istituzionale dell'Università, della **procedura per la segnalazione del *data breach*** e rispettare le prescrizioni in essa contenute.

Nel caso di trasferimento, anche temporaneo, ad altra struttura/ufficio, o nell'ipotesi di cessazione del rapporto di lavoro, l'Incaricato perde i privilegi di accesso ai dati personali riconosciuti all'ufficio di provenienza.

L'autorizzazione al trattamento dei dati si intenderà revocata con la cancellazione del soggetto dall'elenco dei dipendenti e collaboratori afferenti alla struttura interessata dal trattamento come risultante dal **Registro delle attività di trattamento.**

Regole generali per tutti i trattamenti

Nello svolgimento del trattamento devono essere osservate le norme di legge e di regolamento in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali.

In particolare:

- il trattamento dei dati personali, ai sensi dell'art. 5 del GDPR, deve rispettare i principi di **liceità**, **correttezza** e **trasparenza** nei confronti dell'interessato, e di **limitazione delle finalità** che devono essere determinate, esplicite e legittime

- i dati trattati devono essere pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattate (**minimizzazione dei dati**) e devono essere **esatti**, se necessario **aggiornati**.

I soggetti Incaricati del trattamento, nello svolgimento di qualunque operazione di trattamento (raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento, modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto, interconnessione, limitazione, cancellazione, distruzione compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali) sono tenuti a:

- prima di procedere alla raccolta dei dati, consegnare agli interessati la relativa informativa, reperibile sul sito istituzionale;

- consentire l'esercizio dei diritti e delle facoltà previste dagli artt.15, 16, 17, 18, 20, 21 del GDPR (diritto di accesso, di cancellazione, di limitazione del trattamento, diritto alla portabilità dei dati, diritto di opposizione) nel rispetto delle indicazioni fornite dal Titolare e dai Referenti per la protezione dei dati;

- collaborare, con gli altri soggetti Incaricati del medesimo trattamento, esclusivamente per i fini dello stesso e nel rispetto delle indicazioni fornite dal Titolare e dai Referenti per la protezione dei dati;

- non trasmettere all'esterno ed a soggetti terzi, informazioni circa i dati personali conosciuti in ragione del proprio ufficio, salvo che si tratti di comunicazione funzionale allo svolgimento dei compiti affidati, previa autorizzazione del Referente per la protezione dei dati.

- rispettare il suddetto obbligo di riservatezza anche nel periodo successivo all'eventuale cessazione del rapporto di lavoro o al trasferimento ad altra unità organizzativa, fino a quando le suddette informazioni non vengano divulgate da parte del Titolare, oppure divengano di dominio pubblico;

- accertarsi dell'identità del diretto interessato, prima di fornire informazioni circa i dati personali o il trattamento effettuato.

- segnalare qualsiasi anomalia e stranezza da cui si possa desumere una anche solo presunta violazione di dati personali al Referente per la protezione dei dati

- Nel caso di presenza in ufficio di un ospite o altro personale di servizio:
  - farlo attendere in luoghi in cui non sono presenti informazioni riservate o dati personali;
  - evitare di allontanarsi dalla scrivania in loro presenza, riporre i documenti e attivare il salvaschermo del PC prima di allontanarsi;

UNIVERSITÀ DEGLI STUDI FIRENZE

Trattamenti senza strumenti elettronici

Per quanto riguarda la eventuale documentazione cartacea, compresi i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali, gli Incaricati del trattamento sono tenuti a :

- conservare gli atti e i documenti contenenti dati personali per la durata del trattamento e successivamente riporli in archivi ad accesso controllato al fine di escludere l'accesso, agli stessi, da parte di persone non autorizzate al trattamento. A questo proposito sono tenuti a segnalare le eventuali necessità di dotazioni e arredi, in modo da poter adempiere a quanto prescritto;

- non lasciare gli atti e i documenti contenenti dati personali incustoditi su scrivanie o tavoli di lavoro e riporli nei relativi archivi a fine giornata;

- utilizzare gli appositi apparecchi "distruggi documenti" qualora si renda necessario distruggere i documenti contenenti dati personali; in assenza di tali strumenti, i documenti dovranno essere sminuzzati in modo da non essere più ricomponibili;

- adottate misure organizzative idonee per salvaguardare la riservatezza dei dati personali nei flussi di documenti cartacei all'interno degli uffici (es. trasmettere documenti in buste chiuse);

- se si è in attesa di un documento contenente informazioni riservate via fax, non lasciare incustodito l'apparecchio del fax ma rimuovere immediatamente il documento.

Trattamenti concernenti particolari categorie di dati personali (origine razziale, etnica, opinioni politiche, convinzioni religiose, convinzioni filosofiche, appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco la persona fisica, dati relativi allo stato di salute, alla vita sessuale, all'orientamento sessuale della persona) o dati relativi a condanne penali e reati.

Nel caso di trattamento delle suddette categorie di dati agli Incaricati del trattamento è richiesto il rispetto di norme di sicurezza aggiuntive quali:

- non fornire dati o informazioni di carattere sensibile per telefono, qualora non si abbia certezza assoluta sull'identità del destinatario;
- evitare di inviare, per fax o e-mail, documenti in chiaro contenenti dati sensibili: si suggerisce, in tal caso, di inviare la documentazione, senza alcun esplicito riferimento all'interessato (ad esempio, contrassegnando i documenti semplicemente con un codice);

- conservare, anche in corso di trattamento, i documenti, ancorché non definitivi, ed i supporti contenenti tali categorie di dati, in elementi di arredo muniti di serratura e non lasciarli incustoditi in assenza del soggetto autorizzato al trattamento;
- conservare i supporti ed i documenti recanti dati relativi alla salute e alla vita sessuale nei predetti contenitori muniti di serratura, separatamente da ogni altro documento;
- non memorizzare mai tali particolari categorie di dati su supporti removibili (pennette *usb*, *hard disk* esterni, *pc* portatili).

Trattamenti con strumenti elettronici.

Per quanto riguarda, in particolare, le elaborazioni e le altre fasi dei trattamenti effettuate attraverso strumenti informatici, agli Incaricati al trattamento dei dati è richiesto il rispetto delle c.d. buone pratiche per la sicurezza informatica come da normativa vigente.

In particolare, si dovranno seguire le precise indicazioni contenute nelle **Istruzioni per i trattamenti con strumenti elettronici,** disponibili sul sito istituzionale di Ateneo, in relazione alla:

- Gestione delle credenziali (utente e password)
- Scelta della password
- Difesa da attacchi informatici (virus, phishing, malware, ecc)
- Gestione delle postazioni di lavoro (pc, telefoni, tablet, stampanti, ecc.)
- Utilizzo degli applicativi e degli strumenti informatici
- Gestione delle apparecchiature dismesse

Gestione del materiale

Gestione del materiale di output

- se non utilizzati e quando ci si assenta dall'ufficio, provvedere a custodire in armadio o cassetto muniti di serratura i supporti removibili (es. chiavette USB, cd) contenenti informazioni riservate o strategiche;

- controllare attentamente lo stato delle stampe di documenti riservati e rimuovere immediatamente tali copie dalla stampante, onde evitare che personale non autorizzato abbia accesso alle informazioni;

- provvedere a rendere inintelligibili eventuali stampe non andate a buon fine.

Gestione del materiale cartaceo

- conservare i supporti cartacei contenenti dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati stessi (stanze, armadi, cassetti chiusi a chiave);