UNIVERSITÀ DI SIENA 1240

Regolamento sul trattamento dei dati personali

in attuazione del Regolamento UE 2016/679 e del D.Lgs. 196/2003

Emanato con D.R. n. 56/2022 del 13-01-2022 e pubblicato all'Albo on line di Ateneo il 13-01-2022

UNIVERSITÀ DI SIENA 1240

Sommario

Articolo 1. Oggetto, ambito e scopo

1. Il presente Regolamento è adottato in attuazione del Regolamento generale sulla protezione dei dati - Regolamento UE 2016/679 del parlamento europeo e del Consiglio del 27 aprile 2016 - (di seguito Regolamento UE o GDPR) e del Codice in materia di protezione dei dati personali emanato con il Decreto legislativo 30 giugno 2003, n. 196 e ss.mm. (di seguito Codice privacy).
2. Scopo del Regolamento è garantire che le procedure per il trattamento dei dati personali da parte dell'Università degli Studi di Siena (di seguito Università) avvengano nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale degli utenti, sia interni che esterni e di tutti coloro che hanno rapporti con l'Ateneo stesso.
3. L'Università in qualità di Titolare effettua i trattamenti di dati personali con o senza ausilio di processi automatizzati.
4. L'Università considera il trattamento lecito, corretto e trasparente dei dati personali un'azione prioritaria al fine di instaurare e mantenere un rapporto di fiducia con gli studenti, il personale e i terzi interessati.
5. Tutti coloro che, espressamente autorizzati, trattano dati personali all'interno dell'Università per l'espletamento di compiti propri della struttura cui funzionalmente afferiscono, dovranno effettuare il trattamento secondo la politica di protezione dei dati personali stabilita dal presente Regolamento.

Articolo 2. Contesto normativo

1. L'attuale normativa in materia di protezione dei dati personali si compone di disposizioni di fonti sovranazionali e nazionali.
2. Le disposizioni generali attualmente vigenti e non derogabili sono rappresentate da:
   a. Regolamento UE 2016/679: normativa direttamente efficace e vincolante per gli Stati Membri e per tutti i cittadini. In caso di conflitto tra il Regolamento UE e una legge nazionale va disapplicata la legge nazionale contrastante e applicato il Regolamento dell'UE;
   b. D.Lgs. 196/03 Codice in materia di protezione dei dati personali, entrato in vigore nel 2003 e tuttora vigente, come integrato dalle modifiche introdotte dal D.Lgs. 101/2018, che lo ha adeguato al regolamento UE

3. Integrano la disciplina cogente in materia di protezione dei dati, comprensiva dei Provvedimenti generali di carattere vincolante del Garante per la protezione dei dati personali, i cosiddetti atti di "soft law". Essi consistono nel complesso di strumenti e documenti operativi che, sebbene privi di forza vincolante, nondimeno hanno efficacia giuridica pratica. Tra questi atti rientrano:
   a. Le linee guida, le raccomandazioni e le migliori prassi pubblicate dal Comitato europeo per la protezione dei dati (EDPB) e i pareri pubblicati dal Gruppo di lavoro per la tutela dei dati personali (c.d. Gruppo art. P29);
   b. Le linee guida pubblicate dal Garante per la protezione dei dati personali.

Articolo 3. Definizioni

Si intende per:
   a. **dato personale**: qualunque informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
   b. **categorie particolari di dati**: i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, dati biometrici atti a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale;

c. **dati genetici**: i dati personali relative alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
d. **dati biometrici**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
e. **dati relativi alla salute**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
f. **dati giudiziari**: i dati relativi a condanne penali e a reati di una persona direttamente o indirettamente identificabile;
g. **dato anonimo:** qualsiasi informazione non riguardante una persona fisica identificata o identificabile;
h. **trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, la Strutturazione, 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;
i. **trattamento transfrontaliero**: trattamento di dati personali che ha luogo nell'ambito dell'attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
j. **comunicazione**: dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-*quaterdecies* del Codice privacy, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
k. **diffusione**: dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
l. **confidenzialità**: indica la protezione dei dati e delle informazioni scambiate tra un mittente e uno o più destinatari nei confronti di terze parti;
m. **anonimizzazione**: misura di sicurezza tecnica volta a impedire irreversibilmente l'identificazione dell'interessato a cui i dati si riferiscono;
n. **pseudonimizzazione**: il trattamento dei dati personali finalizzato ad ottenere che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative volte a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile. Proprio perché tale attribuzione resta possibile, i dati pseudonimizzati devono essere trattati come informazioni relative a una persona fisica identificabile, seppure in via indiretta, diversamente dai dati anonimi;
o. **profilazione**: qualsiasi forma di trattamento automatizzato di dati personali che utilizzi tali dati personali per valutare determinati aspetti personali relativi ad una persona fisica, in particolare per analizzare o prevedere aspetti inerenti il rendimento professionale, la situazione economica, la

salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

p. **cifratura**: misura tecnica di sicurezza informatica applicabile ai dati personali da parte del Titolare, destinata a rendere tali dati incomprensibili a chiunque non sia autorizzato ad accedervi;
q. **area dedicata nel Portale di Ateneo (o nel sito web istituzionale):** sezione del Portale a cui si accede esclusivamente previa autenticazione attraverso le credenziali di Ateneo. La sezione deve prevedere almeno due sottosezioni: una dedicata alle attività prettamente amministrative in cui pubblicare anche i fac-simile della modulistica utile alle usuali attività amministrative; l'altra dedicata alle attività di ricerca in cui pubblicare le indicazioni di base utili a chi gestisce attività e progetti di ricerca;
r. **Interessato**: la persona fisica cui si riferiscono i dati personali;
s. **Titolare**: la persona fisica o giuridica, l'autorità pubblica o altro organismo che assume le decisioni in ordine alle finalità e ai mezzi del trattamento dei dati personali, ivi compreso il profilo della sicurezza dei trattamenti;
t. **Contitolare**: la persona fisica o giuridica, l'autorità pubblica o altro organismo che determina le finalità e i mezzi del trattamento congiuntamente con un altro Titolare o con altri Titolari;
u. **Responsabile del trattamento** (o responsabile esterno): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, al di fuori dell'organizzazione presieduta dal Titolare, tratta dati personali per conto del Titolare (art. 28 del Regolamento UE);
v. **Responsabile della protezione dei dati (RPD) o Data protection officer (DPO)**: figura professionale esperta nella protezione dei dati che, tra le altre attività previste all'art. 39 del Regolamento UE, fornisce consulenza al Titolare e al personale, vigila sull'osservanza del Regolamento UE e funge da punto di contatto con il Garante per la protezione dei dati personali e con gli Interessati;
w. Security specialist: figura professionale esperta nella cyber security che collabora con il RPD;
x. **Designati del trattamento**: i responsabili delle strutture nell'ambito delle quali i dati personali sono gestiti per le finalità del Titolare; essi sono individuati sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono;
y. **Autorizzati (o incaricati) al trattamento:** le persone fisiche autorizzate a trattare i dati personali sotto l'autorità diretta del Titolare e/o del Designato del trattamento;
z. **referenti del trattamento dati per la ricerca:** la funzione di "referente del trattamento dei dati per la ricerca" è assegnata a personale che ricopre funzioni di particolare rilievo nelle attività di ricerca quali per esempio i responsabili scientifici dei progetti di ricerca;
aa. **Interlocutori per la privacy:** figure di supporto al Titolare del trattamento e al Responsabile della protezione dei dati (membri dei Gruppi di lavoro interdisciplinari a supporto del Titolare del trattamento e del Responsabile della protezione dei dati);
bb. **Amministratore di sistema (AdS)**: figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti nonché altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi;
cc. **destinatario**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazioni di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerati destinatari. Il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
dd. **terzo**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'Interessato, il Titolare del trattamento, il Responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;

ee. **informativa**: informazioni che, ai sensi degli artt. 13 e 14 GDPR, il Titolare del trattamento deve fornire all'Interessato per comunicargli da chi i suoi dati verranno trattati, per quale finalità, con quali mezzi, per quanto tempo e come potrà far valere i suoi diritti;

ff. **consenso**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

gg. **violazione dei dati personali (data breach)**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

hh. **misure tecniche e organizzative**: misure che il Titolare del trattamento deve porre in essere al fine di garantire, ed essere in grado di dimostrare, che il trattamento è effettuato in conformità alla normativa sul trattamento dei dati personali, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche;

ii. **registro delle attività di trattamento**: registro, in forma cartacea e/o digitale, delle attività di trattamento dei dati personali effettuate sotto la responsabilità dal Titolare (art. 30 del Regolamento UE);

jj. **valutazione d'impatto sulla protezione dei dati (DPIA)**: procedura atta a descrivere l'attività di trattamento, valutarne la particolare probabilità e gravità del rischio tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio. La valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio assicurando la protezione dei dati personali e dimostrando la conformità dell'attività di trattamento alla normativa in materia di protezione dei dati personali;

kk. **privacy by design**: principio introdotto dall'art. 25, par. 1 del Regolamento UE per cui il Titolare, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, mette in atto misure tecniche ed organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in maniera efficace i principi di protezione dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati;

ll. **privacy by default**: principio introdotto dall'art. 25, par. 2 del Regolamento UE per cui il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica;

mm. **autorità di controllo:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE. Per l'Italia l'autorità di controllo è il Garante per la protezione dei dati personali;

nn. **autorità di controllo interessata**: un'autorità di controllo interessata al trattamento di dati personali in quanto: a) il Titolare o il Responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;

oo. **rifiuti di apparecchiature elettriche ed elettroniche (RAEE)**: si intendono sia le apparecchiature telefoniche, elettriche, elettroniche o informatiche guaste oppure obsolete - o comunque

con loro parti guaste oppure obsolete - e quindi destinate ad essere eliminate mediante adeguato smaltimento. A titolo di esempio rientrano in questa tipologia di rifiuti: personal computer, tablet, CD, apparati elettromedicali, pennette USB, telefonini, … ;

pp. **reimpiego di AEE** operazioni che consentono l´utilizzo delle apparecchiature elettriche ed elettroniche guaste od obsolete - o di loro componenti guasti od obsoleti - per lo stesso scopo per il quale le apparecchiature erano state originariamente concepite, compreso il riutilizzo di dette apparecchiature o di loro componenti successivamente alla loro consegna presso i centri di raccolta, ai distributori, ai riciclatori o ai fabbricanti o ad altri cessionari a tal fine autorizzati;

qq. **riciclaggio di RAEE**: il ritrattamento in un processo produttivo dei materiali di rifiuto per un recupero differenziato di materie prime seconde**.**

Articolo 4. Principi Generali

1. Il trattamento dei dati personali viene effettuato dall'Università in applicazione dei principi previsti dall'art. 5 del Regolamento (UE).
2. In particolare, i dati personali sono:
   a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
   b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità ("limitazione della finalità"). Un ulteriore trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali;
   c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
   d. esatti e, se necessario, aggiornati. A tal fine sono adottate le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per i quali sono trattati ("esattezza");
   e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
   f. in alcuni casi, conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, e a condizione dell'attuazione di misure tecniche e organizzative adeguate richieste dal Regolamento UE ("limitazione della conservazione");
   g. trattati in maniera da garantire un'adeguata sicurezza mediante misure tecniche ed organizzative adeguate ("integrità e riservatezza") in modo da scongiurare trattamenti non autorizzati o illeciti o che comportino perdita, distruzione o danno accidentale.
3. L'Università adotta misure tecniche e organizzative adeguate in grado di comprovare il rispetto dei principi di cui al precedente comma ("principio di responsabilizzazione del Titolare").

Articolo 5. Base giuridica del trattamento

1. L'Università degli Studi di Siena è un'istituzione pubblica di alta cultura, che opera in conformità ai principi della Costituzione. I fini primari dell'Università sono la didattica, la ricerca scientifica e il trasferimento dei suoi risultati.
2. Il trattamento di dati personali effettuato dall'Università nell'esercizio dei suoi compiti istituzionali trova fondamento principalmente nella condizione di leicità prevista dall'art. 6, par. 1 lett. e) del Regolamento UE.
3. La base giuridica del trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è costituita esclusivamente da una norma di legge o, nei casi

previsti dalla legge, da fonti secondarie, secondo quanto previsto dall'art. 2-ter, comma 1 del Codice privacy.
4. Le finalità di interesse pubblico rilevante relativo a trattamenti effettuati nell'esercizio di pubblici poteri o nello svolgimento di compiti di interesse pubblico sono quelle riportate all'art. 2-sexies comma 2 del Codice privacy.
5. Gli ulteriori trattamenti di dati personali effettuati dall'Università sono leciti solo se sussiste una base giuridica alternativa tra quelle indicate dall'art. 6, par. 1 del Regolamento UE: il consenso dell'interessato (lett. a); l'esecuzione di un contratto di cui l'interessato è parte o l'esecuzione di misure precontrattuali adottate su richiesta dello stesso (lett. b); l'adempimento di un obbligo legale al quale è soggetto il Titolare (lett. c); la salvaguardia di interessi vitali dell'interessato o di un terzo (lett. d); il perseguimento di un legittimo interesse del Titolare o di terzi (lett. e).
6. L'eventuale consenso al trattamento deve essere libero, specifico, informato e inequivocabile; non è ammesso il consenso tacito o presunto e deve poter essere revocabile in qualsiasi momento con la stessa facilità con cui è stato prestato. In caso di minore età il consenso deve essere prestato dagli esercenti la responsabilità genitoriale.
7. Il perseguimento di un legittimo interesse del Titolare o di terzi non può valere come base giuridica del trattamento se, rispetto a tale interesse, prevalgono gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. Il trattamento deve sempre essere necessario al perseguimento dei fini per i quali viene lecitamente effettuato ("principio di necessità").
8. Per le ulteriori condizioni di liceità richieste per il trattamento dei dati particolari si rinvia ai successivi articoli (artt. 20 - 32) del presente Regolamento.

Articolo 6. Misure tecniche e organizzative per la protezione dei dati personali

1. L'Università dà attuazione alla normativa in materia di trattamento dei dati personali attraverso l'adozione di misure tecniche e organizzative adeguate a garantire la conformità del trattamento al Regolamento UE e al Codice privacy, tenendo conto della natura, dell'ambito di applicazione, del contesto, della base giuridica e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
Le suddette misure sono periodicamente riesaminate e aggiornate, tenuto conto dello stato dell'arte e dell'evoluzione tecnologica.
2. La valutazione di adeguatezza del livello di sicurezza, che le misure tecniche e organizzative possono garantire, presuppone l'effettuazione dell'analisi dei rischi che il trattamento presenta e che possono derivare, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai dati personali trasmessi, conservati o comunque trattati.
3. Le misure tecniche possono comprendere appositi Regolamenti, guide tematiche o schede tecniche, tra cui la Procedura per l'effettuazione della Data Protection Impact Assessment (DPIA) e aggiornate periodicamente.
4. Le misure organizzative, inclusa la formazione continua del personale, sono volte ad attuare in maniera efficace i principi di protezione dei dati personali.
5. I documenti che integrano le misure tecniche e organizzative per la protezione dei dati personali o che forniscono istruzioni per il trattamento dei dati personali, ai sensi dell'art. 29 GDPR, sono pubblicati sul sito istituzionale dell'Ateneo, all'interno delle aree riservate a cui si accede autenticandosi con le credenziali d'Ateneo o, se di portata generale, nel portale d'Ateneo www.unisi.it nella sezione dedicata alla privacy.
6. L'Università, ai sensi dell'art. 2-*quaterdecies* D.Lgs. 196/2003, attribuisce funzioni e compiti in materia di trattamenti di dati personali attraverso la nomina dei soggetti di cui agli articoli successivi, promuove la collaborazione tra questi, il Responsabile della prevenzione della corruzione e della trasparenza, il Responsabile della protezione dati personali e il Responsabile per la transizione al digitale per 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.

Articolo 7. Tipologie di dati trattati dall'Università

1. L'Università, in qualità di Titolare, effettua trattamenti di dati personali per lo svolgimento delle proprie finalità istituzionali, come individuate da disposizioni di legge, statutarie e regolamentari, e nei limiti imposti dal Regolamento UE, dal Codice privacy e dalle Linee guida e dai provvedimenti del Garante per la protezione dei dati personali.
2. L'Università tratta a titolo esemplificativo e non esaustivo:
   A. dati personali comuni;
   B. dati personali, anche di natura particolare, con riferimento a determinati servizi relativi al personale subordinato, parasubordinato o con rapporto di lavoro autonomo, ivi compresi i soggetti il cui rapporto di lavoro è cessato o altro personale operante a vario titolo nell'Università:
      - prove concorsuali/selezioni,
      - gestione del rapporto di lavoro,
      - formazione e aggiornamento professionale,
      - gestione di progetti di ricerca,
      - monitoraggio e valutazione della ricerca,
      - attività di trasferimento tecnologico,
      - politiche di welfare e per la fruizione di agevolazioni,
      - salute e la sicurezza delle persone nei luoghi di lavoro,
      - erogazione del servizio di telefonia fissa e mobile,
      - procedimenti di natura disciplinare a carico del personale;
   C. dati personali, anche di natura particolare, con riferimento a determinati servizi relativi a studenti intesi nell'accezione più ampia, per tutte le attività connesse allo status di studente:
      - attività di orientamento,
      - erogazione dei test di ingresso o alla verifica dei requisiti di accesso,
      - erogazione del percorso formativo e gestione della carriera (dall'immatricolazione al conseguimento del titolo),
      - attività di tirocinio,
      - attività di job placement,
      - attività di fundraising, di comunicazione e informazione istituzionale e sviluppo di community,
      - rilevazioni statistiche e valutazione della didattica,
      - diffusione dell'elaborato finale o di elementi ad esso connessi,
      - servizi di tutorato, assistenza, inclusione sociale,
      - servizi e attività per il diritto allo studio,
      - procedimenti di natura disciplinare a carico di studenti,
      - servizi di mobilità studenti in ingresso ed in uscita;
   D. dati personali, anche di natura particolare, con riferimento a determinati servizi relativi alla didattica e alla ricerca (compresa la ricerca scientifica in ambito medico - sanitario);
   E. dati personali, anche di natura particolare, per servizi relativi alle attività gestionali interne all'Ateneo e a quelle svolte per conto terzi, dati connessi ad attività trasversali:
      - gestione degli spazi,
      - gestione delle postazioni,
      - gestione degli organi e delle cariche istituzionali,
      - gestione degli infortuni,

- servizi bibliotecari,
- servizi di protocollo e conservazione documentale,
- acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso,
- servizi di posta elettronica e strumenti di collaboration,
- servizi di didattica a distanza,
- servizi di proctoring e di svolgimento degli esami online,
- erogazione federata di servizi,
- tracciamento di informazioni non primarie e gestione della sicurezza cibernetica,
- svolgimento di concorsi e riunioni on line.

3. Le suddette categorie di dati personali e le attività di trattamento che li hanno ad oggetto sono documentate e costantemente aggiornate dall'Università, ai sensi dell'art. 30 GDPR nel:

a. Registro del Titolare, con riferimento alle attività di trattamento di cui l'Università definisce i mezzi e le finalità (art. 30, par. 1 GDPR; e successivo art. 8, commi 1, 2 e 3 del presente Regolamento),
b. Registro del Responsabile del trattamento, con riferimento alle attività di trattamento che l'Università effettua per conto di un soggetto terzo (art 30, par. 2 GDPR; e successivo art. 8, comma 4 del presente Regolamento).

4. È compito dei Designati del trattamento, con il supporto e la collaborazione degli Interlocutori per la privacy, aggiornare e documentare il censimento periodico dei trattamenti in atto e segnalare eventuali nuovi trattamenti, contribuendo a mantenere costantemente aggiornato il Registro delle attività di trattamento dei dati personali dell'Università di cui al successivo articolo 8, commi 1, 2, e 3.

Articolo 8. Registri delle attività di trattamento dei dati personali

1. Il Titolare istituisce e aggiorna il "Registro delle attività di trattamento dei dati personali" (cd. Registro dei trattamenti) svolte sotto la propria responsabilità in cui sono censiti i trattamenti svolti dagli uffici e dalle strutture dell'Università.
2. Il Registro dei trattamenti contiene tutte le seguenti informazioni:

a. il nome e i dati di contatto del titolare del trattamento e del responsabile della protezione dei dati;
b. le finalità del trattamento;
c. una descrizione delle categorie di interessati e delle categorie di dati personali;
d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;
f. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati o le modalità per definirli;
g. ove possibile, il richiamo alle misure di sicurezza tecniche e organizzative adottate per la sicurezza del trattamento.

3. Il registro è costantemente aggiornato, pubblicato nell'area riservata del Portale di Ateneo e, su richiesta, messo a disposizione del Garante per la protezione dei dati personali.
4. Il Titolare, qualora l'Università tratti dati per conto di altri Titolari, istituisce e aggiorna il Registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento.

Il Registro dei trattamenti svolti dall'Università per conto di altri Titolari e per i quali l'Università si configura come "Responsabile del trattamento" contiene le seguenti informazioni:

a. il nome ed i dati di contatto dell'Università e del RPD;
b. le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c. i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;

d. il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Articolo 9. Circolazione dei dati all'interno dell'Università

1. L'accesso e l'utilizzo dei dati all'interno delle strutture e da parte del personale dell'Università è ispirato al principio della libera circolazione delle informazioni in funzione del raggiungimento delle finalità perseguite dall'Università.
2. L'Università provvede alla gestione delle informazioni e dei dati a sua disposizione mediante strumenti, anche di carattere informatico, atti a facilitarne l'accesso e la fruizione.
3. L'accesso ai dati personali all'interno delle strutture e da parte del personale dell'Università, connesso con lo svolgimento dell'attività inerente la loro specifica funzione, è consentito in via diretta e tracciato senza ulteriori formalità in misura necessaria per il perseguimento dell'interesse istituzionale. Resta ferma la responsabilità del richiedente derivante dall'utilizzo improprio dei dati e nell'ottica del bilanciamento tra i diritti e le libertà dell'interessato e l'interesse pubblico all'espletamento delle attività istituzionali.

Articolo 10. Titolare del trattamento dei dati

1. Il Titolare del trattamento dei dati è l'Università rappresentata legalmente dal Magnifico Rettore.
2. Tenuto conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Titolare adotta misure tecniche e organizzative atte a comprovare la conformità del trattamento al Regolamento UE e al Codice in materia di protezione dei dati personali ("principio di responsabilizzazione del Titolare").
3. Il Titolare promuove ogni opportuno strumento di informazione e sensibilizzazione per consolidare la consapevolezza del valore della protezione dei dati personali e predispone ogni anno, sentito il Responsabile della protezione dati, un piano formativo in materia di trattamento dei dati personali e di prevenzione dei rischi di violazione, al fine di garantire una gestione delle attività di trattamento informata, responsabile ed aggiornata. Tale formazione è integrata e coordinata con le attività pianificate in materia di prevenzione della corruzione nonché in tema di trasparenza e di accesso agli atti, ai documenti, ai dati ed alle informazioni. La frequenza è obbligatoria per tutti coloro che trattano dati personali.
4. Nel caso di trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, l'Università assicura che non sia pregiudicato il livello di protezione delle persone fisiche provvedendo all'adozione delle garanzie adeguate che permettano all'interessato diritti azionabili e mezzi di ricorso effettivi, previste al Capo V del GDPR.
5. Il Titolare coopera con il Garante per la protezione dei dati personali, con il supporto del Responsabile della protezione dati.

Articolo 11. Contitolare del trattamento dei dati

1. Quando uno o più titolari del trattamento determinano congiuntamente con l'Università le finalità e i mezzi del trattamento, essi sono Contitolari del trattamento.
2. I Contitolari del trattamento stabiliscono in modo trasparente, mediante un accordo interno, le rispettive responsabilità e i rispettivi obblighi derivanti dal Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, nonché le rispettive funzioni di comunicazione delle informazioni richieste dall'Informativa privacy, salvo quanto previsto dall'art. 26 del Regolamento UE.
3. L'accordo definisce adeguatamente i rispettivi ruoli e i rapporti dei Contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione da ciascun Contitolare nei confronti degli interessati.
4. L'interessato può esercitare i propri diritti nei confronti di ciascun Contitolare del trattamento.

Articolo 12. Responsabile della protezione dei dati personali (RPD)

1. L'Università in qualità di ente pubblico ha l'obbligo di nominare ai sensi dell'art. 37 del Regolamento UE

un Responsabile della protezione dei dati (RPD) o Data Protection Officer (DPO). La posizione del RPD è normata dall'art. 38 del Regolamento UE.

2. Il RPD, individuato in funzione delle qualità professionali, può essere un soggetto interno (dipendente dell'Università) o esterno, assolvendo in tal caso i suoi compiti in base a un contratto di servizi.

3. Il RPD è nominato, nel caso di soggetto interno, con decreto del Rettore.

4. Il RPD ha nello specifico i seguenti compiti:

a. informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente Regolamento nonché dalla normativa sovranazionale e nazionale relativa alla protezione dei dati;
b. sorvegliare sulle politiche del Titolare del trattamento, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c. sorvegliare sull'osservanza delle disposizioni derivanti dal regolamento UE, dalla normativa comunitaria e nazionale relativa alla protezione dei dati personali e dai Regolamenti di Ateneo in materia;
d. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati personali e sorvegliarne l'effettivo svolgimento e completamento;
e. segnalare al Titolare ed al Direttore Generale:
   le priorità di intervento in relazione alle novità normative e tecniche,
   eventuali inadempienze emerse in occasione dell'espletamento delle funzioni istituzionali;
f. cooperare con il Garante per la protezione dei dati personali;
g. fungere da punto di contatto per il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento UE, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
h. cooperare in ottica di *"accountability"* con il Titolare per la definizione delle istruzioni da impartire ai fini dell'adempimento degli obblighi in materia di trattamento dei dati personali e per le attività di informazione e formazione, rivolte alle strutture competenti, in merito alla tenuta del Registro delle attività di trattamento (c.d. Registro dei Trattamenti).

6. Nell'eseguire i propri compiti il RPD considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

7. L'Università mette a disposizione del RPD le risorse necessarie e adeguate a garantire lo svolgimento ottimale dei propri compiti, avvalendosi delle competenze e della collaborazione delle strutture universitarie.

8. Il RPD ha ampio accesso ai dati e alle informazioni ed è interpellato per ogni problematica inerente la protezione dei dati.

9. Il RPD, al fine di adempiere ai compiti a lui assegnati, ha diritto all'accesso al sistema di protocollo informatico (Titulus) come responsabile del procedimento (RPA) per tutti i procedimenti e le attività legate al suo ruolo.

10. L'Università garantisce che il RPD eserciti le proprie funzioni in modo autonomo e indipendente e in particolare, non assegna allo stesso attività o compiti che risultino in contrasto o in conflitto di interesse con la sua posizione.

11. Il RPD non riceve alcuna istruzione per quanto riguarda l'esecuzione dei compiti a lui affidati ai sensi dell'art. 39 del Regolamento UE.

12. L'Università non rimuove o penalizza il RPD in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni.

13. Il nominativo e i dati di contatto del RPD sono comunicati al Garante per la protezione dei dati personali. I dati di contatto del RPD sono indicati nelle informative privacy e pubblicati sul sito internet istituzionale.

14. L'Università costituisce a supporto del RPD una rete di Interlocutori per la privacy che dovranno collaborare funzionalmente con il RPD, nell'ambito delle strutture di appartenenza. La rete degli Interlocutori per la privacy può essere organizzata anche sotto forma di gruppo di lavoro interdisciplinare.
15. Il RPD, almeno una volta all'anno, redige una relazione in merito all'attività svolta, tenuto conto delle questioni che impattano con priorità ed urgenza sul trattamento dei dati. La relazione è inviata al Rettore.

Articolo 13. Responsabile del trattamento

1. È Responsabile del trattamento qualunque soggetto esterno che esegua, in base a un contratto/convenzione o altro atto giuridico, trattamenti di dati personali per conto dell'Università.
2. Il Responsabile del trattamento è nominato con atto giuridico conforme al diritto nazionale e fornisce garanzie ai sensi del paragrafo 3 dell'art. 28 del Regolamento UE, in particolare per quel che riguarda le misure tecniche e organizzative adeguate a consentire il rispetto delle disposizioni previste dallo stesso Regolamento UE.
3. Il Responsabile del trattamento può nominare mediante contratto o altro atto giuridico sub-responsabili del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che lo legano all'Università.
4. Qualora un sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile del trattamento conserva nei confronti dell'Università l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile.
5. Il Responsabile del trattamento risponde dinanzi all'Università dell'inadempimento del sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento.
6. Nell'informativa all'interessato sono indicati i responsabili del trattamento nominati ai sensi dell'art. 28 del Regolamento UE.

Articolo 14. Designati del trattamento

1. Il Titolare, considerata l'alta complessità dell'organizzazione universitaria, si avvale della possibilità riconosciuta dall'art. 2-quaterdecies d.lgs. 196/03, di affidare, a soggetti adeguatamente formati, funzioni e compiti in materia di trattamenti di dati personali a persone fisiche che operano nell'ambito del suo assetto organizzativo.
2. Nell'Università di Siena assumono il ruolo di Designati del trattamento, sulla base delle competenze attribuite alla rispettiva funzione organizzativa o carica istituzionale che ricoprono**,** i responsabili delle strutture nell'ambito delle quali i dati personali sono trattati per le finalità perseguite dall'Università.
3. All'interno dell'Università i Designati del trattamento sono così individuati:
Per le strutture amministrative:

- il direttore generale, per le attività di competenza della direzione generale,
- i dirigenti delle aree amministrative, per le attività di competenza della direzione e per gli uffici che non afferiscono ad una divisione,
- i responsabili di divisione,
- i direttori dei centri di servizio,
- i responsabili delle segreterie amministrative dei dipartimenti - relativamente ai dati personali trattati nella gestione amministrativa delle rispettive strutture.

Per le attività di didattica e di ricerca:

- i direttori dei dipartimenti - relativamente ai dati personali trattati nello svolgimento delle attività didattiche (ad esempio lezioni, esami, compilazioni dei registri, diari e syllabus) e nell'ambito delle attività di ricerca condotte dal dipartimento e dai centri di ricerca a questo afferenti.

3. Il Designato al trattamento, opportunamente formato riguardo alle competenze anche decisionali in materia di trattamento dei dati, opera con autonomia gestionale nell'ambito delle competenze affidategli,

collabora funzionalmente con il RPD per l'espletamento dei seguenti compiti all'interno della propria Struttura di afferenza e per gli ambiti espressamente definiti:

Con riferimento al personale assegnato o operante sotto la propria responsabilità dovranno:

a. fornire agli autorizzati (vedi successivo art. 15) specifiche istruzioni operative riguardanti le operazioni di raccolta, trattamento e archiviazione dei dati personali su supporto informatico e cartaceo e individuare l'ambito di trattamento consentito;
b. vigilare e verificare che gli autorizzati rispettino le istruzioni impartite e garantire che il trattamento dei dati avvenga in modo lecito e corretto, nel rispetto dei principi di cui all'art. 5 del Regolamento UE;
c. vigilare sul rispetto delle misure di sicurezza da parte del personale autorizzato, al fine di evitare rischi, anche accidentali, di distruzione o perdita di dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità del trattamento;
d. garantire la formazione del personale autorizzato e l'aggiornamento periodico autorizzando gli stessi a partecipare a corsi ed eventi formativi organizzati dall'Università in materia di protezione dei dati;
e. il direttore generale e i dirigenti di area amministrativa, devono individuare, in base alla complessità della Struttura ed all'eterogeneità dei dati trattati, le persone di riferimento (interlocutori per la privacy) che avranno il compito di supporto e raccordo nei rapporti con il Responsabile della protezione dei dati personali (RPD) per gli adempimenti previsti dalla normativa.

Con riferimento ai dati trattati dovranno:

f. attenersi scrupolosamente alle disposizioni previste dal Regolamento UE e alle procedure, istruzioni, fac-simili predisposte in materia di protezione dei dati personali dal Titolare del trattamento e consultabili all'interno dell'area dedicata nel Portale di Ateneo;
g. redigere ed aggiornare l'elenco delle tipologie dei dati trattati nell'ambito della Struttura di competenza e trasmetterlo al Titolare e al Responsabile della protezione dei dati;
h. comunicare al Titolare e al RPD con adeguato preavviso, anche nel caso di passaggio dalla modalità cartacea a quella elettronica, eventuali nuovi trattamenti, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, anche nel caso di passaggio dalla modalità cartacea a quella elettronica;
i. comunicare al Titolare e al RPD le modifiche relative alle attività di trattamento dei dati, nonché gli eventuali mutamenti organizzativi o tecnici (acquisizione di nuove banche dati e/o applicativi hardware, etc.) che possano avere impatto rispetto ai diritti dell'interessato;
j. collaborare per la mappatura dei trattamenti, per il censimento delle banche dati e dei trattamenti dei dati esternalizzati, limitatamente a quelli riferibili alla Struttura di propria competenza, ai fini dell'aggiornamento del Registro dei trattamenti;
k. garantire, per ciascun trattamento riferibile alla Struttura di propria competenza, che siano sempre rispettati i principi generali previsti dalla normativa vigente in materia e in particolare che i dati siano esatti, aggiornati e completi;
l. assicurare che tutti i dati da pubblicare sul sito istituzionale, siano conformi alla normativa vigente in materia;
m. valutare, insieme agli Amministratori di sistema e in coerenza con le policy stabilite dal Responsabile della Conservazione di Ateneo, i tempi di conservazione dei dati, ovvero, se non è possibile, i criteri utilizzati per determinare tale periodo;

Con riferimento alle misure di sicurezza dovranno:

n. individuare e censire i trattamenti soggetti a maggiori rischi di impatto rispetto alle libertà ed ai diritti degli interessati, comunicando i necessari aggiornamenti delle schede destinate ad alimentare il registro dei trattamenti;

o. informare, senza ingiustificato ritardo, secondo la policy di Ateneo in materia di sicurezza informatica, il Responsabile della Sicurezza Informatica di Ateneo e per conoscenza il Titolare e il Responsabile della protezione dei dati, dopo aver avuto notizia di qualsiasi violazione che potrebbe compromettere il corretto trattamento e la sicurezza dei dati (anomalie, furti, perdite accidentali o distruzioni dei dati) al fine di attivare, nel caso sia riscontrato un rischio grave per i diritti e le libertà delle persone fisiche, la procedura del Data Breach;
p. documentare, in un apposito registro interno, le eventuali violazioni dei dati personali riferibili alla Struttura di competenza, le loro conseguenze e i provvedimenti adottati per porvi rimedio;
q. rispettare e far rispettare le misure di sicurezza tecniche indicate e adottate dall'Area dei sistemi informativi e le misure di sicurezza organizzative previste dalle normative vigente e dai provvedimenti del Garante, nonché eventuali misure ritenute adeguate su proposta del Titolare, atte a preservare la disponibilità e integrità del dato;
r. verificare periodicamente, in collaborazione con le strutture di competenza (es. uffici che si occupano della videosorveglianza, ecc.), le modalità di accesso ai locali e le misure adottate per la protezione delle aree logistiche in termini di custodia ed accessibilità ai dati (ad esempio: supporti di videosorveglianza), al fine di garantire la sicurezza e la riservatezza degli archivi cartacei;

Con riferimento ai diritti degli interessati dovranno:

s. vigilare sulla redazione e/o aggiornamento dell'informativa di cui agli artt. 13 e 14 del Regolamento UE, da fornire agli interessati, secondo quanto disciplinato di seguito all'art. 19;
t. integrare l'informativa e i moduli di consenso, nel caso di trattamenti specifici, sentito il Titolare e il Responsabile della protezione dati;
u. gestire e riscontrare, nei termini previsti dalla normativa vigente, le istanze per l'esercizio dei diritti dell'interessato (diritto accesso, rettifica, cancellazione, limitazione al trattamento ecc.), in collaborazione con tutti gli uffici coinvolti nel trattamento del dato oggetto della richiesta.

Con riferimento ai progetti di ricerca, che prevedono il trattamento dei dati personali dei soggetti reclutati dovranno:

v. tenere conto degli atti di "soft law" di cui al precedente art. 2 comma 3 applicabili al settore della ricerca, della *Convenzione europea sui diritti dell'uomo e la bioetica*, della *Dichiarazione internazionale Unesco del 2003 sui trattamenti dei dati genetici umani*, della *Carta dei diritti fondamentali dell'Unione europea* del 7 dicembre 2000, delle indicazioni del Titolare fornite tramite guide operative predisposte allo scopo;
w. individuare per ogni attività o progetto di ricerca il Referente del trattamento dei dati per la ricerca di cui al successivo art. 16.

4. Il Designato al trattamento altresì:

a. deve provvedere all'espletamento di tutte le operazioni necessarie per il rispetto e la corretta applicazione della normativa vigente in materia; collaborare nelle fasi connesse alla valutazione di impatto sui trattamenti che possono presentare un rischio elevato per i diritti e le libertà delle persone, ai sensi dell'art. 35 del Regolamento UE;
b. deve collaborare con il Titolare e con il Responsabile della protezione dati in caso di ispezioni da parte dell'Autorità Garante o di altre Autorità di controllo;
c. è tenuto a partecipare alle specifiche iniziative formative proposte dall'Amministrazione.

5. Il ruolo di Designato del trattamento è strettamente correlato alla funzione organizzativa e non è delegabile. Tale ruolo non prevede alcuna remunerazione aggiuntiva.

Articolo 15. Autorizzati al trattamento

1. Gli autorizzati (o incaricati) al trattamento sono le persone fisiche incaricate a trattare i dati personali sotto l'autorità diretta del Titolare e/o del Designato del trattamento. Ossia l'Autorizzato al trattamento è colui che materialmente effettua le operazioni di trattamento di dati.

All'interno dell'Università degli Studi di Siena si individuano:

- nel personale Strutturato (personale tecnico amministrativo, collaboratori esperti linguistici, personale docente e ricercatori) assegnato ad un'unità organizzativa (area/divisione/ufficio/dipartimento/centro/biblioteche) deputato a compiere operazioni di trattamento sui dati personali in possesso dell'Ateneo;
- in 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 ad un'unità organizzativa deputata a compiere operazioni di trattamento sui dati personali trattati dall'Ateneo;

2. Gli autorizzati al trattamento ricevono opportuna formazione/informazione specifica in materia di trattamento dei dati.

3. Tutti coloro che trattano dati che competono all'unità organizzativa cui afferiscono, sono ritenuti autorizzati al trattamento dei dati per documentata preposizione ad unità organizzativa e pertanto sono tenuti a conformare le operazioni loro assegnate alla normativa in materia di protezione dei dati personali, al presente Regolamento e ad ogni istruzione specifica ricevuta sui trattamenti dei dati personali, facendo proprie le politiche di sicurezza informatica e le linee guida in materia di utilizzo degli strumenti informatici adottate dall'Università, pubblicate e periodicamente aggiornate nel sito dell'Ateneo.

4. Gli autorizzati sono tenuti:

a. a mantenere il segreto e il massimo riserbo sull'attività prestata e su tutte le informazioni di cui sia venuto a conoscenza durante l'attività prestata;
b. ad attivare ogni misura idonea a inibire l'accesso ai dati trattati da parte di chi non è a ciò autorizzato, in ogni fase dell'attività di trattamento, compreso l'eventuale trasferimento dei dati o la loro conservazione;
c. ad accertarsi dell'identità del diretto Interessato, prima di fornire informazioni circa i dati personali o il trattamento effettuato;
d. a verificare, prima di procedere alla raccolta dei dati, che gli Interessati abbiano ricevuto le necessarie informative, diversamente invitandoli a prenderne visione;
e. a collaborare alla tenuta e all'aggiornamento del Registro delle attività di trattamento dei dati personali, informando preventivamente il Designato del trattamento di proprio riferimento delle eventuali modifiche dei trattamenti esistenti o dell'esigenza di introdurne di nuove;
f. a segnalare con tempestività al Designato del trattamento e/o al proprio responsabile di ufficio, eventuali anomalie, incidenti, furti, perdite accidentali di dati;
g. a seguire le attività formative ed informative in materia di protezione dei dati personali.

5. L'Autorizzato al trattamento è informato e consapevole che l'accesso e la permanenza nei sistemi informatici aziendali per ragioni estranee e comunque diverse rispetto a quelle per le quali è stato abilitato per fini istituzionali e di servizio può configurare il reato di accesso abusivo ai sistemi informativi e può comportare sanzioni disciplinari, oltre che esporre l'amministrazione a danni reputazionali o di altra natura.

6. L'Autorizzato al trattamento che opera in ambito informatico è tenuto a collaborare proattivamente con il Dirigente dei sistemi informativi di Ateneo per la valutazione del rischio delle attività di trattamento e per l'individuazione di misure tecniche e organizzative volte a garantire, tenuto conto dello stato dell'arte e dell'evoluzione tecnologica, idonei livelli di protezione dei sistemi informatici. Restano inoltre valide, per l'Autorizzato al trattamento che opera in ambito informatico, le istruzioni specifiche ricevute con la nomina ad Amministratore di sistema, attribuite in base al D.Lgs. 196/2003 prenovellato e ai provvedimenti ad esso conseguenti, fino a nuove disposizioni del Designato del trattamento della struttura di afferenza.

7. Nel caso di trasferimento, anche temporaneo, ad altra struttura/ufficio, o nell'ipotesi di cessazione del rapporto di lavoro, il soggetto perde i privilegi di accesso ai dati personali riconosciuti all'ufficio di provenienza. Il Designato del trattamento della struttura di afferenza provvede affinché lo stesso non abbia

più accesso ai sistemi di gestione di dati personali o di documenti condivisi, procedendo alla immediata disattivazione o cambio delle credenziali d'accesso ai sistemi che siano state note al soggetto.
8. I trattamenti di dati personali per i quali manchi l'autorizzazione comporta la qualificazione del soggetto che li tratta quale Terzo rispetto all'Amministrazione universitaria, con l'addebito a suo carico delle eventuali conseguenze pregiudizievoli.

Articolo 16. Referenti del trattamento dei dati per la ricerca

1. La funzione di "referente del trattamento dei dati per la ricerca" è assegnata a personale che ricopre funzioni di particolare rilievo nelle attività di ricerca quali per esempio i responsabili scientifici dei progetti di ricerca.
2. Il Referente è nominato dal Designato per le attività di ricerca (di cui al precedente art. 14) e opera sotto la sua responsabilità.
3. Per ogni attività di ricerca deve:
   a. tenere conto degli atti di "soft law" di cui al precedente art. 2 comma 3 applicabili al settore della ricerca, della Convenzione Europea sui diritti dell'uomo e la bioetica (approvata ad Oviedo nel 1997 e ratificata con L.28 marzo 2001 n.145), della Dichiarazione internazionale Unesco del 2003 sui trattamenti dei dati genetici umani, della Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000 (adottata il 12 dicembre 2007) e delle indicazioni del Titolare fornite tramite guide operative predisposte allo scopo;
   b. compilare la "Scheda di valutazione del progetto di ricerca", resa disponibile nell'area riservata, per effettuare una valutazione dei rischi del trattamento prima dell'avvio di ogni progetto di ricerca. Qualora la valutazione evidenzi un rischio medio/alto, prima di procedere al trattamento dei dati personali, deve contattare il Responsabile per la protezione dei dati (RPD) e, con la collaborazione dell'Interlocutore per la privacy, effettuare la valutazione dell'impatto sulla protezione dei dati personali (*Data Protection Impact Assessment*) di cui al successivo art. 31.
      La scheda valutazione del rischio e, se necessaria la DPIA, insieme ad una copia del progetto di ricerca devono essere conservati, con la dovuta riservatezza, per 5 anni dalla conclusione programmata della ricerca;
   c. porre in essere gli adempimenti derivanti dalla normativa per la protezione dei dati personali (per esempio: informativa agli interessati; adozione di misure di sicurezza quali, ove possibile, la pseudonimizzazione o l'anonimizzazione dei dati; ecc.) anche avvalendosi del supporto degli Interlocutori per la privacy e del DPO;
   d. acquisire, se necessario, il consenso dell'interessato per ciascuna finalità del progetto. Il rilascio del consenso deve avvenire con modalità che evidenzino la sua acquisizione in maniera libera e informata e che consentano di rispettare l'esercizio del diritto di revoca, da parte dell'Interessato, con modalità semplificate.

Articolo 17. Interlocutori per la privacy

1. Gli Interlocutori per la privacy in materia di trattamento dei dati, sono figure di supporto al Titolare e al Responsabile per la protezione dei dati (RPD) e si adoperano per facilitare le relazioni con i Designati del trattamento di cui al precedente art. 14.
2. Gli Interlocutori per la privacy svolgono i compiti attribuiti in materia di trattamento dei dati senza vincoli di responsabilità, nel pieno esercizio delle ordinarie attività amministrativo/gestionali già assegnate.
3. Gli Interlocutori per la privacy svolgono il ruolo di facilitatori per esaminare e segnalare le criticità che emergono all'interno delle singole strutture di riferimento (area amministrativa, dipartimenti, centro di servizio) negli ambiti concernenti il trattamento e la protezione di dati. Assumono all'interno delle strutture di riferimento una posizione di raccordo sia nei rapporti con i colleghi e i collaboratori rispetto alle attività

prescritte in materia di trattamento dei dati personali, sia nei rapporti tra i Designati al trattamento ed il Responsabile per la protezione dei dati (RPD).
4. Gli Interlocutori per la privacy in materia di trattamento dei dati sono tenuti a svolgere i seguenti compiti:
- collaborare nel censimento dei trattamenti dei dati di competenza dell'area di afferenza e vigilare sulla corretta compilazione delle schede destinate ad alimentare il Registro dei trattamenti;
- collaborare all'aggiornamento del Registro dei trattamenti dei dati;
- individuare in collaborazione con gli uffici competenti della Struttura di afferenza, i rapporti contrattuali con i fornitori esterni, in linea con la normativa europea ed italiana relativa al trattamento dei dati (art. 28 Regolamento UE);
- in collaborazione con gli uffici competenti della Struttura, verificare l'esistenza delle nomine ai Responsabili del trattamento nei casi di esternalizzazioni dei servizi (art. 28 Regolamento UE), aggiornare e/o revisionare la documentazione presente, ovvero collaborare nella redazione delle stesse se mancanti;
- in collaborazione con gli uffici competenti della Struttura, verificare l'esistenza delle informative al trattamento dei dati ai sensi degli artt. 13 e 14 del Regolamento UE, aggiornare e/o revisionare la documentazione presente, ovvero collaborare nella redazione delle stesse se mancanti;
- supportare il Responsabile della protezione dei dati e i Designati del trattamento nella revisione e/o predisposizione di adeguate policy e sorvegliare sulla corretta applicazione delle stesse;
- informare in modo tempestivo il Responsabile della protezione dei dati e i Designati del trattamento qualora si verifichi qualsiasi evento che possa compromettere la sicurezza dei dati trattati: (anomalie, furti, distruzione, divulgazione/accessi non autorizzati, perdite accidentali di dati) al fine di attivare la procedura del Data Breach che prevede la notifica all'Autorità Garante entro 72 ore nei casi in cui la violazione comporti gravi rischi per i diritti e le libertà delle persone fisiche (artt. 33 e 34 del Regolamento UE);
5. Gli Interlocutori per la privacy sono tenuti a seguire corsi di formazione ed aggiornamento, a partecipare alle riunioni e/o incontri organizzati dal RPD e/o dal coordinatore del gruppo di lavoro, per i temi da trattare in materia di protezione dei dati e sicurezza dei dati.
6. Il ruolo di Interlocutore per la Privacy non comporta alcuna modifica della qualifica professionale o delle mansioni e non determina remunerazione aggiuntiva.
7. Ai fini di un efficace coordinamento può essere costituita una Rete di Interlocutori per la privacy o un Gruppo di lavoro interdisciplinare.
8. L'elenco degli Interlocutori per la privacy è pubblicato nel Portale di Ateneo.

Articolo 18. Sensibilizzazione e formazione

1. Ai fini della corretta e puntuale applicazione della disciplina in materia di protezione dei dati personali, l'Università sostiene e promuove, ogni strumento di sensibilizzazione finalizzato a consolidare la consapevolezza del valore della protezione dei dati personali. L'Università promuove l'attività formativa del personale universitario e l'attività informativa diretta a tutti coloro che hanno rapporti con l'Università.
2. L'Università predispone ogni anno, sentito il Responsabile per la protezione dei dati, un piano formativo in materia di trattamento dei dati personali e di prevenzione dei rischi di violazione, al fine di garantire una gestione delle attività di trattamento responsabile, informata ed aggiornata.
Tale formazione è preferibilmente integrata e coordinata con le attività pianificate in materia di etica e prevenzione della corruzione, di trasparenza amministrativa e di esercizio del diritto di accesso.
3. La frequenza delle attività di formazione è obbligatoria.

Articolo 19. Informativa sul trattamento dei dati personali

1. L'Università, prima di raccogliere i dati personali, fornisce all'Interessato adeguata informativa sul trattamento dei suoi dati personali.

2. L'informativa fornita all'interessato deve essere concisa, trasparente, intellegibile, facilmente accessibile e usare un linguaggio chiaro e semplice.
3. L'informativa deve contenere:
   a. i dati di contatto del Titolare;
   b. i dati di contatto del Responsabile della protezione dei dati personali;
   c. le finalità del trattamento;
   d. la base giuridica del trattamento;
   e. gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali e, nel caso in cui i dati personali non siano raccolti presso l'interessato, anche le categorie di dati trattati e le relative fonti di provenienza;
   f. l'eventuale volontà dell'Università di trasferire dati personali a un paese terzo o a un'organizzazione internazionale, l'esistenza di un fondamento giuridico alla base di tale trasferimento, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stai resi disponibili;
   g. il periodo di conservazione dei dati personali oppure, in alternativa, i criteri utilizzati per determinare tale periodo;
   h. i diritti che l'interessato può esercitare;
   i. la necessità di comunicare i dati personali in base a un obbligo legale o contrattuale nonché la natura obbligatoria o facoltativa del conferimento, nonché le possibili conseguenze della mancata comunicazione di tali dati;
   j. l'esistenza di un processo decisionale automatizzato, compresa la profilazione e le conseguenze previste da tale trattamento per l'interessato,
   k. nel caso in cui i dati non siano raccolti presso l'interessato, l'Università informa l'Interessato anche della fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.

4. Se i dati sono comunicati spontaneamente dall'Interessato, l'informativa deve essere fornita al momento del primo contatto utile, successivo alla ricezione dei dati medesimi, pena l'inutilizzabilità degli stessi.
5. Le informazioni sul trattamento così dichiarate definiscono il confine di liceità del trattamento stesso. Ogni utilizzo differente da quanto indicato nell'informativa costituisce una violazione dei princìpi di cui al precedente art. 5, per cui nel caso in cui i dati personali debbano essere trattati per una diversa finalità da quella per cui sono stati raccolti, l'Università fornisce all'Interessato nuove informazioni in merito alla diversa finalità dell'utilizzo.
Tale disposizione non si applica se e nella misura in cui l'interessato già dispone dell'informazione, ovvero quando comunicare una nuova informazione in merito alla diversa finalità, risulta impossibile o implicherebbe uno sforzo sproporzionato, in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fermo restando che l'ulteriore finalità del trattamento non sia incompatibile con le finalità iniziali in conformità all'art. 5 lett. b) e all'art. 89 del Regolamento UE. In tali casi l'Università adotta misure appropriate per tutelare, i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni.
6. L'Università pubblica le informative di rilevanza trasversale sul proprio sito istituzionale (www.unisi.it), mentre fornisce quelle relative a specifici trattamenti in occasione dell'effettuazione degli stessi.
7. L'aggiornamento delle informative rientra nei compiti di vigilanza del Designato del trattamento con il supporto degli interlocutori per la privacy.
8. La modulistica, sia cartacea che digitale, che prevede la raccolta di dati riferiti a una persona fisica deve contenere almeno le seguenti informazioni:
   a. la finalità per cui i dati sono raccolti e per la quale saranno usati;
   b. l'indicazione di chi tratterà i dati all'interno dell'Università e se essi saranno resi disponibili a terzi;
   c. l'espressione del consenso ove questo fosse una condizione di liceità del trattamento.

d. il link all'informativa di rilevanza trasversale pubblicata nel sito web istituzionale.

9. Il personale e chiunque operi sotto l'autorità dell'Università può trattare i dati personali solo per le specifiche finalità indicate nell'informativa fornita all'interessato al momento del conferimento dei dati o per ogni altra finalità prevista dalla legge.

Articolo 20. Diritti dell'interessato

1. L'Università opera nel rispetto dell'art. 12 del GDPR e garantisce il rispetto dei diritti degli Interessati, secondo le condizioni previste agli artt. 15 - 22 del Regolamento UE. In particolare l'interessato può nei confronti del Titolare del trattamento:

a. ottenere la conferma dell'esistenza o meno di trattamenti di dati personali che lo riguardano, e la comunicazione dei dati in forma intelligibile ("diritto di accesso");
b. ottenere la rettifica dei dati personali inesatti che lo riguardano e ottenere l'integrazione dei dati personali incompleti ("diritto di rettifica");
c. ottenere la cancellazione dei dati personali che lo riguardano, nonché esercitare il diritto all'oblio, chiedendo la cancellazione degli stessi qualora sussista almeno una delle condizioni indicate dall'art. 17 del Regolamento UE. L'Università informa della richiesta di cancellazione ogni altro titolare che tratta i dati personali cancellati, compresi qualsiasi collegamento, copia o riproduzione ("diritto alla cancellazione e diritto all'oblio");
d. esercitare il diritto alla limitazione del trattamento come previsto dall'art. 18 del Regolamento UE ("diritto di limitazione");
e. ottenere la portabilità dei dati forniti nei casi in cui è prevista l'applicazione ai sensi dell'art. 20 del Regolamento UE ("diritto alla portabilità"). Il diritto alla portabilità, applicabile ai soli trattamenti automatizzati, non può essere esercitato per i trattamenti di dati personali necessari per l'adempimento di un obbligo legale cui è soggetto il Titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
f. esercitare il diritto di opposizione come previsto dall'art. 21 del Regolamento UE ("diritto di opposizione");
g. esercitare il diritto di non essere sottoposto ad una decisione basato su un trattamento automatizzato, compresa la profilazione, secondo quanto previsto dall'art. 22 del Regolamento UE ("diritto a non essere sottoposto ad un processo decisionale automatizzato");
h. proporre reclamo all'Autorità di controllo, secondo quanto previsto dall'art. 77 del Regolamento UE ("diritto di reclamo").

2. Il Titolare, per mezzo dell'informativa, comunica all'Interessato le modalità per l'esercizio dei suoi diritti. Tali modalità sono pubblicate anche nel sito web istituzionale.

3. Il riscontro alla richiesta presentata dall'Interessato, previo accertamento della sua identità, viene fornito senza ingiustificato ritardo e comunque non oltre 30 giorni dalla data di acquisizione della richiesta stessa, anche nei casi di diniego. Per i casi di particolare e comprovata difficoltà il termine dei 30 giorni può essere prorogato per altri 2 mesi, non ulteriormente prorogabili. Di tale proroga deve essere data informazione motivata all'Interessato entro un mese dall'acquisizione della richiesta.

4. L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato.

5. Nel caso in cui le richieste siano manifestamente infondate, eccessive o di carattere ripetitivo, l'Università può addebitare un contributo spese ragionevole tenuto conto dei costi amministrativi sostenuti, oppure può rifiutare di soddisfare la richiesta, dimostrando il carattere manifestamente infondato o eccessivo della stessa.

6. Nelle comunicazioni all'interessato l'Università utilizza modalità di trasmissione, anche elettronica, che garantiscano la riservatezza e confidenzialità dei dati trasmessi.

7. Se le finalità per cui vengono trattati i dati personali non richiedono o non richiedono più l'identificazione dell'Interessato, non si devono conservare, acquisire o trattare ulteriori informazioni per identificare l'Interessato al solo fine di consentirgli l'esercizio dei diritti previsti dal Regolamento UE.

Articolo 21. Trattamento di "categorie particolari di dati" e di dati relativi a condanne penali e reati

1. I trattamenti delle categorie particolari di dati personali, di cui all'art. 3 lettera b) del presente Regolamento, necessari per motivi di interesse pubblico rilevante sono ammessi se previsti da norme dell'Unione europea, da disposizioni di legge in ambito nazionale o, nei casi previsti dalla legge, di regolamento e sempreché la finalità non possa essere raggiunta senza trattare tali dati. Nelle stesse norme devono essere rinvenibili i tipi di dati che possono essere trattati, le operazioni eseguibili, il motivo di interesse pubblico rilevante e le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dei soggetti cui si riferiscono.
2. Il trattamento di dati personali relativi a condanne penali, a reati o a connesse misure di sicurezza, deve avvenire solo se è autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, come disciplinato in particolare all'art. 2-octies del Codice privacy.
3. Qualora l'Università, nell'esercizio delle sue funzioni istituzionali, venga a conoscenza di dati personali non necessari allo svolgimento di tali attività, anche se trasmessi dall'interessato, questi non potranno essere utilizzati e dovranno essere eliminati, fatto salvo l'eventuale obbligo di conservazione, previsto dalla legge, dell'atto o del documento che li contiene.

Articolo 22. Trattamenti nell'ambito del rapporto di lavoro

1. L'Università effettua il trattamento dei dati personali dei dipendenti nell'ambito del rapporto di lavoro adottando garanzie appropriate per assicurare la protezione dei diritti e delle libertà fondamentali degli individui e nel rispetto della legge e dei contratti collettivi.
2. Il trattamento dei dati relativi ai dipendenti da parte dell'Università non richiede il consenso esplicito in quanto il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale.
3. Nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, l'informativa è fornita all'interessato al momento del primo contatto utile, successivo all'invio del curriculum stesso.

Art. 23. Studenti: trattamenti connessi alla gestione della carriera universitaria ed erogazione dei servizi

1. L'Università, in qualità di Titolare del trattamento, acquisisce i dati personali dello Studente in sede di registrazione, preimmatricolazione, immatricolazione o iscrizione, per la gestione della carriera dei soggetti interessati (studenti, laureati e iscritti a qualsiasi corso o attività formativa erogata dall'Ateneo) e di ogni altro servizio e adempimento ulteriore che si rende necessario in forza dell'esistenza di tale rapporto. Il trattamento dei dati è finalizzato esclusivamente allo svolgimento di tutte le attività connesse ai compiti istituzionali e di pubblico interesse di competenza dell'Università
2. L'Università non ricorre a processi decisionali automatizzati relativi ai diritti dell'interessato sulla base dei dati personali, compresa la profilazione, nel rispetto delle garanzie previste dall'art. 22 del Regolamento UE.
3. L'accesso alle piattaforme e ai servizi online messi a disposizione dall'Università avviene tramite credenziali istituzionali fornite dall'Università e protette dal sistema di controllo accessi centralizzato, utilizzando sempre la stessa coppia di credenziali (login e password) generata per la gestione della casella di posta di Ateneo (@student.unisi.it). Le credenziali degli utenti non sono accessibili, nemmeno in forma cifrata, dai fornitori dei servizi e dalle applicazioni web e mobile, in quanto il processo di identificazione avviene sempre all'interno del sistema di autenticazione dell'Università.

4. Esclusivamente ai fini dell'erogazione della didattica a distanza, l'Università si avvale di software e piattaforme online e altri strumenti innovativi dedicati all'e-learning. Le modalità di svolgimento e le tecnologie utilizzate sono pubblicate e costantemente aggiornate nell'*Informativa sul trattamento dei dati personali degli studenti nella didattica ed esami on line* pubblicata nel sito web dell'Ateneo – sezione privacy.
5. Nell'utilizzo di tali piattaforme, l'Università opera nel rispetto del principio di minimizzazione, trattando solo i dati personali strettamente necessari al perseguimento delle finalità didattiche, senza effettuare indagini sulla sfera privata dell'interessato.

Articolo 24. Accesso ai documenti amministrativi e accesso civico

1. I limiti per l'esercizio del diritto di accesso documentale ai sensi della legge 241/90) e dell'accesso civico ai sensi del D.Lgs. 33/2013 ad atti e documenti dell'Università contenenti dati personali sono disciplinati dalle rispettive normative di riferimento.
2. Quando le istanze di accesso riguardano categorie particolari di dati personali o dati relativi a condanne penali e reati, l'accesso è consentito esclusivamente se la situazione giuridicamente rilevante, che si intende tutelare con la richiesta di accesso, è di rango almeno pari ai diritti dell'Interessato al trattamento dei dati personali, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

Articolo 25. Comunicazione e diffusione dei dati personali

1. L'Università può comunicare ad altri Titolari i dati personali, purché diversi dai dati particolari e da quelli relativi a condanne penali e reati, per l'esecuzione di un compito di interesse pubblico e nei limiti delle proprie finalità istituzionali, solo se la comunicazione è prevista da una norma di legge o, nei casi previsti dalla legge, da un regolamento.
2. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli Interessati (art. 2-ter Codice privacy).
3. La comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste da una norma di legge o, nei casi previsti dalla legge, da un regolamento.
4. La diffusione di dati personali, anche tramite pubblicazione su un sito web, è ammessa unicamente se prevista da norma di legge o regolamento o, ove applicabile, con il consenso degli interessati.
5. La pubblicazione dei dati sui siti web, anche per obblighi derivanti dalla cd. "trasparenza amministrativa" o per l'albo online, deve avvenire nel rispetto del principio della minimizzazione dei dati, mediante la diffusione dei dati strettamente necessari al raggiungimento delle finalità per le quali sono pubblicati e per i soli tempi richiesti dalle stesse finalità o norme di legge. Quando sono stati raggiunti gli scopi per i quali essi sono stati resi pubblici e gli atti hanno prodotto i loro effetti, i dati personali devono essere oscurati, anche qualora l'obbligo di pubblicazione dell'atto non sia pervenuto a scadenza.
6. La pubblicazione dei nomi e dei dati di contatto dei referenti delle attività amministrative istituzionali sul sito istituzionale dell'Ateneo, o di altre strutture ad esso appartenenti, è effettuato in adempimento di obblighi di legge e al fine di fornire all'utente un punto di contatto con l'Ateneo. Tali dati possono essere utilizzati solo per il perseguimento di siffatto scopo.
7. L'Università, al fine di agevolare l'orientamento, le esperienze formative e professionali e l'eventuale collocazione nel mondo del lavoro, anche all'estero, può comunicare dati personali, diversi dai dati particolari [vedi lettera b), art, 3 del presente Regolamento] e giudiziari, riguardanti studenti, laureandi e laureati, specializzati, borsisti, dottorandi, assegnisti e altri profili formativi, nonché di soggetti che hanno superato l'esame di Stato.

La finalità del trattamento deve essere esplicitamente dichiarata nella richiesta pervenuta all'Università. Il soggetto che riceve i dati potrà utilizzati per le sole finalità per le quali vengono comunicati.
9. È vietato diffondere dati personali idonei a rivelare lo stato di salute o informazioni da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici. Analogo divieto sussiste per i dati personali idonei a rivelare altre informazioni di carattere particolare di cui al precedente art. 3 lettera b) o che rilevino situazioni di disagio economico o sociale.

Articolo 26. Diffusione delle valutazioni d'esame

1. La pubblicazione di valutazioni d'esame avviene, di norma, in aree riservate del sito web istituzionale, salve le normative di settore che regolino diversamente tempi e forme di pubblicità legale, avendo in tal caso cura di rispettare i princìpi di minimizzazione dei dati e di limitazione della conservazione di cui al precedente art. 4.
2. La pubblicazione dei dati sul sito web istituzionale è consentita unicamente mediante la diffusione del numero di matricola dello studente e del voto conseguito, nel rispetto dei diritti e delle libertà fondamentali, della dignità dell'interessato e del diritto alla protezione dei dati personali.
3. Le valutazioni sono rese disponibili per un periodo di tempo non superiore a tre mesi.

Articolo 27. Diffusione dei risultati di concorsi e selezioni

1. Salve le normative di settore che regolano tempi e forme di pubblicità legale, tutti gli atti delle procedure concorsuali e selettive sono pubblicati contemperando le esigenze di trasparenza amministrativa con quelle di protezione dei dati personali, nel rispetto dei principi di minimizzazione dei dati e di limitazione della conservazione di cui al precedente art. 4.
2. Il reclutamento di personale appartenente alle categorie protette avviene attraverso procedure concorsuali che prevedano la pseudonimizzazione dei candidati già in fase di predisposizione dei bandi di concorso, ciò al fine di proteggere la loro identità in ogni fase della procedura concorsuale, con particolare riguardo ad eventuali esigenze di pubblicazione dei dati ad essa connesse.

Articolo 28. Trattamento dei dati nelle sedute degli Organi Collegiali di Ateneo

1. Nelle sedute degli Organi Collegiali dell'Università il trattamento dei dati avviene in conformità al presente Regolamento e al solo fine delle attività istruttorie dei componenti degli Organi per le finalità deliberative di competenza degli stessi.

Articolo 29. Trasferimenti verso Paesi extra UE

1. Il trasferimento di dati personali verso Paesi non appartenenti allo Spazio economico europeo o verso organizzazioni internazionali o altri destinatari situati in Paesi terzi, deve avvenire assicurandosi che non sia compromesso il livello di tutela delle persone fisiche assicurato dalle normative europee e nazionali per la protezione dei dati personali, come richiesto dal Capo V del Regolamento UE.
2. Il trasferimento di dati personali, come ogni trattamento, deve essere innanzitutto conforme alle disposizioni generali inerenti alla protezione dei dati personali, in relazione alle finalità per cui viene effettuato, quindi deve essere:

a. fondato su una base giuridica tra quelle previste dall'art. 6, par. 1 del Regolamento UE;
b. eseguito nel pieno rispetto dei princìpi elencati all'art. 5 del Regolamento UE, riportate al precedente art. 4, e in generale di tutte le disposizioni pertinenti del Regolamento UE e delle altre normative applicabili ai trattamenti di dati personali;
c. inserito nel Registro dei trattamenti, riportando i paesi terzi o le organizzazioni internazionali a cui i dati personali sono stati o saranno comunicati, la valutazione del rischio effettuata e la descrizione delle garanzie attuate per il trasferimento, in relazione ai rischi valutati, affinché l'interessato

benefici di un adeguato livello di protezione dei suoi dati personali anche nell'eventuale ulteriore trasferimento da questi ad altro paese terzo, secondo le disposizioni al Capo V del regolamento UE;

d. inserito nell'informativa per l'interessato, riportando quali siano i Paesi terzi o le organizzazioni internazionali destinatarie e le motivazioni per cui ha luogo il trasferimento. Devono essere inoltre riportate le valutazioni del Titolare e del Designato del trattamento in merito alla scelta dello strumento di garanzia adottato, tra quelli previsti dal Regolamento UE, in caso di assenza di una decisione di adeguatezza.

3. La valutazione dell'adeguatezza della tutela offerta da un Paese terzo va considerata in funzione di tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti, che riguardano anche la modalità, la frequenza, la durata e il contesto del trasferimento.
4. Sia nella valutazione del rischio sia nelle garanzie attuabili, il Titolare e, in particolare, il Designato del trattamento, devono prestare attenzione anche ai trasferimenti che potrebbero subentrare tra l'importatore dei dati e un successivo sub-incaricato, in virtù di un subcontratto dell'importatore.
5. L'Università adotta e aggiorna una apposita scheda tematica per fornire indicazioni operative specifiche della disciplina.

Articolo 30. Trattamento a fini di ricerca scientifica

1. L'Università valorizza e promuove la ricerca scientifica e adotta misure tecniche e organizzative funzionali ad assicurare che i trattamenti di dati effettuati in tali ambiti avvengano nel rispetto dei diritti degli interessati e della normativa in materia. Speciale attenzione viene riservata alla ricerca medica, biomedica ed epidemiologica che prevede trattamenti di dati particolari la cui conoscibilità può incidere in maniera significativa sui diritti e le libertà degli interessati.
2. Il Titolo VII, Capo III del Codice privacy delimita le modalità del trattamento dei dati a fini statistici o di ricerca scientifica, i casi in cui non è necessario acquisire il consenso al trattamento dei dati personali da parte degli interessati e le materie oggetto di disposizioni particolari dell'Autorità garante per la protezione dei dati personali nell'ambito della ricerca scientifica.
3. La disciplina sul trattamento di dati personali nell'ambito della ricerca scientifica annovera, oltre al GDPR e al Codice privacy, anche fonti internazionali e atti di "soft law", cui ogni progetto di ricerca deve conformarsi. Alcuni esempi sono richiamati nell'art. 16, comma 3 del presente Regolamento.
4. L'Università, al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico, ai sensi dell'art. 100 del Codice privacy può, con autonome determinazioni, comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione delle categorie particolari di dati personali e dei dati personali relativi a condanne penali e reati.
5. Tutto il personale che si occupa di ricerca è tenuto a conoscere la normativa di settore. Al solo fine di facilitare la conoscibilità della complessa disciplina in materia, l'Ateneo può adottare e aggiornare periodicamente una "guida pratica sugli adempimenti" da porre in essere alla luce delle disposizioni di cui al comma 3, pubblicandola sul sito web istituzionale, favorendo altresì la formazione del personale

Articolo 31. Archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici

1. I documenti contenenti dati personali possono essere trattati a fini di archiviazione nel pubblico interesse o di ricerca storica, tenendo conto della loro natura e solo se pertinenti e indispensabili per il perseguimento di tali scopi; ove possibile e senza pregiudicare il raggiungimento delle finalità del trattamento, dovranno essere trattati con misure tecniche che non consentano più di identificare l'interessato.
2. Il trattamento dei dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato nel rispetto del principio della minimizzazione dei dati, delle autorizzazioni generali del Garante per la protezione dei dati personali e dei codici deontologici in materia.

3. La consultazione dei documenti di interesse storico conservati negli archivi dell'Università è disciplinata dal decreto legislativo 22 gennaio 2004, n. 42 (c.d. Codice dei beni culturali e del paesaggio).
4. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici può essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati (art. 99, comma 1, Codice privacy).
5. A fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici possono comunque essere conservati o ceduti ad altro titolare i dati personali dei quali, per qualsiasi causa, è cessato il trattamento, nel rispetto di quanto previsto dall'articolo 89, paragrafo 1, del GDPR (art. 99 comma 2 Codice privacy).

Articolo 32. Valutazione di impatto sulla protezione dei dati (DPIA)

1. Quando si intende intraprendere un tipo di trattamento di dati personali che può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, tenuto conto in particolare della natura dei dati, dell'ambito di applicazione, del contesto e delle finalità del trattamento, l'Università effettua, prima di procedere al trattamento, una valutazione dell'impatto sulla protezione dei dati personali.
2. Il rischio deve essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato, suscettibile di cagionare un danno fisico, materiale o immateriale agli interessati, in particolare nei seguenti scenari:

a. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente sulle suddette persone fisiche;
b. il trattamento, su larga scala, di categorie particolari di dati personali, quali quelli relativi all'origine razziale o etnica, alle opinioni politiche, alle convinzioni religiose o filosofiche, o all'appartenenza sindacale, nonché di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, dati relativi a condanne penali e a reati;
c. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (videosorveglianza) o l'introduzione di nuove tecnologie che comportano variazioni del rischio correlato all'attività di trattamento;
d. il trattamento dei dati particolari, specie se relativi alla salute a fini di ricerca scientifica in campo medico, biomedico o epidemiologico (art. 110 D.Lgs. 196/2003).

3. Qualora la valutazione, effettuata dal Designato del trattamento della struttura interessata o per le attività di ricerca dal Referente del trattamento per la ricerca, evidenzi un rischio medio/alto, prima di procedere al trattamento dei dati è necessario informare il Responsabile della protezione dei dati (RPD) per l'individuazione e l'adozione di opportune misure che ne attenuino i rischi.
4. Il Titolare rende disponibile un modello per effettuare e documentare la DPIA a supporto dell'esecuzione di tale adempimento nell'apposita sezione del sito web istituzionale.
5. Il Responsabile per la transizione al digitale e il Security specialist forniscono supporto agli autorizzati e collaborano con il RPD ai fini dello svolgimento della valutazione di impatto.
6. È possibile condurre una singola valutazione di impatto per un insieme di trattamenti simili, effettuati nello stesso contesto e che presentano analoghi rischi.
7. Se le risultanze della DPIA effettuata indicano l'esistenza di un rischio residuale elevato, il Titolare, per il tramite del Responsabile della protezione dei dati, consulta il Garante per la protezione dei dati personali prima di procedere al trattamento.

Articolo 33. Data Breach – Violazione di dati personali

1. Ai sensi degli artt. 33 e ss. e del considerando 87 del GDPR, il Titolare adotta la Procedura di comunicazione del Data Breach per consentire a chiunque la segnalazione di un evento che comporti,

accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la rivelazione o l'accesso non autorizzato ai dati personali trasmessi, memorizzati o comunque elaborati. La suddetta Procedura è pubblicata sul sito internet istituzionale.
2. Il Titolare predispone inoltre una procedura interna di gestione di tali segnalazioni e degli incidenti di sicurezza informatica, individuando le risorse organizzative alle quali, per le competenze possedute, sia possibile assegnare il compito di svolgere le attività richieste per la valutazione del rischio per i diritti e le libertà degli interessati, per la loro mitigazione nonché per la corretta e tempestiva gestione delle azioni complessive da intraprendere per far fronte alla violazione occorsa.
3. Compete alle stesse risorse organizzative, individuate nella procedura, la valutazione della necessità di procedere alla notifica all'Autorità garante per la protezione dei dati personali, di cui all'art. 33 del GDPR, senza ingiustificato ritardo e, ove possibile, entro 72 ore dall'avvenuta conoscenza della violazione, così come compete alle medesime risorse la valutazione della necessità di comunicare la violazione all'Interessato, nel rispetto delle previsioni di cui all'art. 34 del GDPR.
4. Il Titolare provvede alle notifiche di cui al precedente comma e documenta in un apposito Registro dei Data Breach qualsiasi violazione di dati personali, comprese le circostanze in cui si è verificata, le conseguenze e i provvedimenti adottati per attenuarne le conseguenze.

Articolo 34. Registro dei Data Breach

1. L'art. 33 del Regolamento UE prevede l'obbligo per il Titolare del trattamento di documentare tutti i Data Breach avvenuti. Il Titolare conserva, quindi, un registro dei Data Breach che deve essere tempestivamente aggiornato e contenere le seguenti informazioni:
   a. i dettagli relativi al Data Breach (e cioè la causa, il luogo dove è avvenuto e la tipologia di Dati personali violati);
   b. gli effetti e le conseguenze della violazione e il piano di intervento predisposto dal Titolare.
2. Oltre a quanto prevede il precedente comma, il Titolare deve anche motivare la ragione delle decisioni assunte a seguito del Data Breach con particolare riferimento ai seguenti casi:
   a. il Titolare ha deciso di non procedere alla notifica;
   b. il Titolare ha ritardato nella procedura di notifica;
   c. il Titolare ha deciso di non notificare il Data Breach agli Interessati.

Articolo 35. Videosorveglianza

1. Il trattamento dei dati personali effettuato mediante l'attivazione di impianti di videosorveglianza negli ambienti dell'Università si svolge nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale, garantendo altresì i diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento.
2. Le immagini e i dati raccolti tramite gli impianti di videosorveglianza non possono essere utilizzati per finalità diverse da quelle indicate nella regolamentazione di Ateneo in materia di videosorveglianza e non possono essere diffusi o comunicati a terzi, salvo in caso di indagini di polizia giudiziaria.

Articolo 36. Rifiuti di apparecchiature elettriche ed elettroniche (RAEE) contenenti dati personali

1. Il Titolare trattamento adotta appropriate misure organizzative e tecniche volte a garantire la sicurezza dei dati personali trattati e la loro protezione anche nei confronti di accessi non autorizzati che potrebbero verificarsi in occasione della dismissione di apparati elettrici ed elettronici suscettibili di memorizzare dati personali quali, ad esempio, personal computer, tablet, telefoni, pennette USB, ecc..
Le misure adottate devono garantire l'effettiva cancellazione o trasformazione in forma non intelligibile dei dati personali negli stessi contenute, sì da impedire a soggetti non autorizzati che abbiano a vario titolo la disponibilità materiale dei supporti di venirne a conoscenza non avendone diritto (si pensi, ad esempio, ai

dati personali memorizzati sul disco rigido dei *personal computer* o nelle cartelle di posta elettronica, oppure custoditi nelle rubriche dei terminali di comunicazione elettronica).
2. Qualora si proceda al riuso di AEE o al riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche o di loro componenti è fondamentale che le misure e gli accorgimenti volti a prevenire accessi non consentiti ai dati personali in esse contenuti assicurino l´effettiva cancellazione dei dati o garantiscano la loro non intelligibilità.
3. In caso di smaltimento di rifiuti elettrici ed elettronici, l´effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature elettriche ed elettroniche può anche risultare da procedure che, nel rispetto delle normative di settore, comportino la distruzione dei supporti di memorizzazione in modo da impedire l'acquisizione indebita di dati personali.

Articolo 37. Sanzioni per l'inosservanza delle norme

1. L'art. 83 del GDPR prevede sanzioni amministrative pecuniarie fino a 10.000.000 Euro, estendibili ulteriormente a 20.000.000 Euro in caso di violazione delle disposizioni relative ai principi base del trattamento, ai diritti degli Interessati o al trasferimento di dati a paesi terzi.
2. L'art. 166 del Codice privacy definisce i criteri di applicazione delle sanzioni amministrative pecuniarie e il procedimento per l'adozione dei provvedimenti correttivi e sanzionatori.
3. Gli artt. 167 - 172 del Codice privacy disciplinano gli illeciti penali derivanti dalle violazioni della normativa sulla protezione dei dati personali, dalla falsità di dichiarazioni rese all'Autorità garante o da azioni volte intenzionalmente a interrompere o turbare la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.
4. Le sanzioni disciplinari e amministrative a carico del personale in caso di violazione delle leggi e delle procedure in tema di protezione dei dati personali saranno definite dall'Università anche sulla base di quanto disposto dai CCNNLL, dal Codice etico e dal Codice di comportamento.

Articolo 38. Disposizioni finali

1. Dalla data di entrata in vigore del presente Regolamento, devono intendersi abrogate tutte le norme regolamentari e statutarie incompatibili in relazione a soggetti e materie interessate al trattamento.
2. Per quanto non espressamente previsto dal presente Regolamento si rinvia alle disposizioni del Regolamento UE 2016/679 e del D.Lgs. 196/2013 Codice per la protezione dei dati personali, oltre che a quanto previsto dalle Linee guida e di indirizzo e dalle Regole deontologiche adottate e approvate dal Garante.
3. La documentazione redatta dall'Università in materia di protezione dei dati personali è messa a disposizione sul sito web istituzionale dell'Ateneo o nell'area riservata del medesimo portale, è oggetto di periodico aggiornamento, costituisce parte integrante delle misure tecniche e organizzative di cui all'art. 6 del presente Regolamento.

Responsabile del trattamento

(art. 28 GDPR)

Soggetti esterni all'amministrazione che, a seguito di convenzione, contratto o provvedimento di nomina, trattano dati personali per conto dell'Università di Siena

Titolare del trattamento
Università degli Studi di Siena

Legalmente rappresentata dal Rettore pro-tempore

Contitolari

(art. 26 GDPR)

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento

Designati del trattamento

Sono soggetti interni all'amministrazione, si identificano con i responsabili delle strutture nell'ambito delle quali i dati personali sono gestiti per le finalità istituzionali, individuati sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono.

• Per le strutture amministrative: il direttore generale, per le attività di competenza della direzione generale; i dirigenti delle aree amministrative, per le attività di competenza della direzione e per gli uffici che non afferiscono ad una divisione; i responsabili di divisione; i direttori dei centri di servizio; i responsabili delle segreterie amministrative dei dipartimenti - relativamente ai dati personali trattati nella gestione amministrativa delle rispettive strutture.

• Per le attività di didattica e di ricerca: i direttori dei dipartimenti - relativamente ai dati personali trattati nello svolgimento delle attività didattiche (lezioni, esami, compilazioni dei registri, diari e syllabus) e nell'ambito delle attività di ricerca condotte dal dipartimento e dai centri di ricerca a questo afferenti.

Amministratori di sistema (AdS)

Soggetti preposti alla gestione e alla manutenzione di un impianto di elaborazione di dati o di sue componenti, notificano al Designato del trattamento e al RPD eventuali anomalie rischi di sicurezza, supportano i Designati del Trattamento e gli Autorizzati per gli aspetti di tipo tecnico informatico nelle normali attività operative

Interlocutori per la Privacy

Sono figure di supporto al Titolare e al Responsabile della protezione dei dati (RPD) e si adoperano per facilitare le relazioni con i Designati del trattamento e gli Autorizzati al trattamento

Responsabile della protezione dei dati (RPD) o Data Protection Officer (DPO)

(artt. 37, 38 e 39 GDPR)

Ha compiti di consulenza nei confronti del Titolare e dei Designati del trattamento e di sorveglianza sull'osservanza dell'applicazione del Regolamento UE.
Per lo svolgimento dei propri compiti il RPD è supportato dal Servizio Legale, dall'Area dei sistemi informativi, dai Designati del trattamento dei dati personali e da una rete di Interlocutori per privacy.

Si avvale della consulenza del Security Specialist.

Security Specialist

Esperto nella cyber security che collabora con il RPD

Referenti del trattamento dati per la ricerca

Soggetti che ricoprono funzioni di particolare rilievo nelle attività di ricerca quali per esempio i responsabili scientifici dei progetti di ricerca

Autorizzati (o incaricati) al trattamento

Sono i soggetti autorizzati a trattare i dati personali sotto l'autorità diretta e per le finalità del Titolare e/o del Designato al trattamento. Ossia tutti coloro che quotidianamente gestiscono i dati personali su supporto sia cartaceo che informatico.

Allegato 1