Regolamento sul trattamento, la comunicazione e la diffusione da parte dell'Università degli Studi di Parma dei dati personali, ivi compresi quelli sensibili e giudiziari, ai sensi del Regolamento UE 679/2016

Sommario

CAPO I[1]
Principi e definizioni

Articolo 1. Oggetto, ambito di applicazione e finalità

1. Il presente regolamento, in attuazione del regolamento UE 679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito GDPR) e del Dlgs. 30.06.2003, n. 196, "Codice in materia di protezione dei dati personali", e successive modificazioni, disciplina il trattamento, la comunicazione e la diffusione da parte dell'Università degli Studi di Parma dei dati personali, ivi compresi quelli sensibili e giudiziari, e garantisce che tale trattamento si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, da ottenersi attraverso l'attenzione, in particolare, ai principi di responsabilizzazione, semplificazione, correttezza e trasparenza alla base dei contenuti del presente documento.

2. Tutti i trattamenti dei dati personali, ivi compresi quelli sensibili e giudiziari, devono essere conformi alle disposizioni del presente regolamento. In esso sono disciplinati i ruoli e le responsabilità, nonché gli adempimenti da seguire in materia di protezione dei dati personali ai sensi della normativa applicabile.

3. L'accesso ai dati personali, ivi compresi quelli sensibili e giudiziari, per fini istituzionali dell'Ateneo, è garantito dalle prescrizioni del presente regolamento e dalla normativa vigente in materia.

Articolo 2. Principi di riferimento

1. Il GDPR detta i seguenti principi di riferimento:

a. correttezza e trasparenza: i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. Il trattamento deve sempre essere giustificato da una valida base giuridica.

b. finalità: i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modi compatibili con tali finalità. Il trattamento deve rientrare nelle finalità per cui l'interessato ha conferito i dati personali e/o il proprio consenso, espressamente indicate nell'Informativa.

c. necessità: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Ciò risponde prima di tutto alla richiesta di "minimizzazione" dei trattamenti che è

[1] Riferimenti Normativi
Decreto legislativo del 30 giugno 2003 n. 196, "Codice in materia di protezione dei dati personali" ("Codice privacy") integrato dal Dlgs.n. 101/2018;
Regolamento (UE) 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al Trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE ("GDPR");

principio fondamentale del GDPR. Devono essere oggetto di trattamento solo i dati personali strettamente necessari.

d. esattezza: i dati personali devono essere esatti e, se necessario, aggiornati. Devono essere adottate tutte le misure ragionevoli per cancellare/rettificare tempestivamente i dati inesatti rispetto alle finalità per cui sono trattati.

e. conservazione: i dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un tempo non superiore al conseguimento delle finalità per cui sono trattati. Una volta che vengono meno le finalità per cui i dati personali sono stati raccolti (o finalità compatibili), gli stessi devono essere distrutti o de-identificati (la *de-identificazione* è una forma di *anonimizzazione* dove i dati personali sono mantenuti intatti, ma i riferimenti ad essi o le specifiche informazioni di identificazione, come ad esempio i nomi, vengono sostituiti con identificatori anonimi).

f. integrità e sicurezza: i dati personali devono essere trattati in modo da garantire un'adeguata sicurezza degli stessi, compresa la protezione da trattamenti illeciti o non autorizzati e dalla perdita, distruzione, danni accidentali. Tenendo 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 per i diritti e le libertà degli interessati, sono adottate misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, in conformità con quanto previsto dalle indicazioni di settore. Ogni volta che sono effettuate operazioni di trattamento dei dati personali, occorre adottare la massima attenzione e la prudenza.

g. responsabilizzazione: tutti gli agenti a vario titolo coinvolti nella attività di trattamento dei dati personali, devono garantire il rispetto dei principi *privacy*, la corretta applicazione del presente regolamento e, più in generale, delle disposizioni applicabili in tema di trattamento dei dati personali. Non solo il titolare è responsabile per il rispetto della normativa sulla *privacy*. Al contrario, tutti gli attori della *privacy*, dai responsabili del trattamento, agli incaricati devono fare tutto quanto ragionevolmente possibile per l'effettivo rispetto del presente regolamento.

h. tutela dei diritti dell'interessato: l'Università di Parma in qualità di titolare del trattamento dei dati personali, adotta le misure appropriate per fornire all'interessato tutte le informazioni relative al trattamento dei suoi dati personali, nonché per tutelare i diritti dell'interessato, fermi restando i limiti previsti da altri strumenti normativi applicabili in materia. Le risposte ad eventuali richieste dell'interessato devono essere fornite in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, ponendo in essere le azioni opportune a soddisfare la richiesta. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici.

i. *privacy* by design e *privacy* by default. L'articolo 25 del GDPR stabilisce che il trattamento dei dati deve avvenire in modo che la protezione degli stessi dati sussista fin dalla progettazione e che essa avvenga

per impostazione predefinita (principio di "*privacy* by design"). Si devono adottare le misure tecniche e organizzative idonee a dare concreta attuazione a quelle che sono le disposizioni e i principi in materia di protezione dei dati e garantendo, in questo modo, i diritti degli interessati. La predisposizione delle misure necessarie deve partire dal momento in cui il titolare del trattamento determina i mezzi con i quali attuare il trattamento stesso e deve persistere fino a quello in cui pone in essere le vere e proprie operazioni di trattamento. Questo implica che il titolare non effettuerà un trattamento conforme al GDPR se applicherà delle misure standard e predeterminate per diverse tipologie di trattamento, ma dovrà sempre procedere ad un'analisi realistica e specifica del singolo contesto di riferimento. La protezione dei dati personali deve essere garantita "per impostazione predefinita" (principio di "*privacy* by default"). Tutte le valutazioni che il titolare del trattamento deve effettuare devono essere compiute a monte, prima di procedere al trattamento dei dati vero e proprio. Il titolare deve svolgere un'analisi preventiva della situazione complessiva e adottare un approccio pratico, eseguendo una serie di attività specifiche e dimostrabili.

Articolo 3. Definizioni, abbreviazioni ed acronimi

1. Si elencano le principali definizioni a cui si fa riferimento all'interno del presente regolamento:

a. **interessato al trattamento**: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

b. **titolare** del trattamento dei dati personali (o anche TITOLARE - *persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le* **finalità** *e i* **mezzi** *del trattamento di dati personali*" - art. 4. par. 1, n. 7 GDPR): Università degli Studi di Parma;

c. **responsabile del trattamento** dei dati personali (è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento - art. 4, par. 1, n. 8 GDPR): titolare della funzione attribuita per mettere in atto misure tecniche e organizzative adeguate a che ciascun trattamento soddisfi i requisiti in materia di protezione dei dati personali e garantisca la tutela dei diritti dell'interessato. Sono responsabili del trattamento i Dirigenti delle aree amministrative e i Direttori di Dipartimenti e Centri. Per particolari necessità, può essere nominato anche un responsabile esterno all'Ateneo;

d. **responsabile per la protezione dei dati personali** (o anche "*Data Protection Officer*" "DPO"): figura, prevista dal GDPR, nominata dal titolare cui sono affidate le funzioni di garanzia della conformità della circolazione e della protezione dei dati personali secondo quanto stabilito dal presente regolamento e, più in generale, dal GDPR. In particolare, i compiti in carico alla figura sono:

- informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che trattano i dati personali;

- sorvegliare l'osservanza della normativa comunitaria e nazionale nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento riguardanti anche "l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo";
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- cooperare con l'autorità Garante nazionale;
- fungere da punto di contatto per l'autorità Garante nazionale per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione

e. **incaricato** del (designato, autorizzato al) trattamento: ai fini del presente regolamento è la persona fisica, prevista dalle normative italiane ed europee, che, nell'adempimento delle proprie mansioni, compie operazioni di trattamento. Le mansioni sono indicate nel funzionigramma di Ateneo. In ogni caso, il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche espressamente designate che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta (art. 2 quaterdecies d.lgs 101/2018), laddove le mansioni non siano già oggetto di assegnazione attraverso il funzionigramma;

f. **amministratore di sistema** (rif. Provvedimento del Garante del 27 novembre 2008): la figura professionale prevista dalla normativa italiana in ambito informatico che mantiene, configura e gestisce un sistema centrale di elaborazione dati o sue componenti, ivi inclusi sistemi software complessi quali i sistemi gestionali e centralizzati, basi di dati o reti e apparati di telecomunicazioni;

g. **autorità di controllo**: l'autorità pubblica indipendente, prevista dal GDPR, istituita da uno Stato membro al fine di sorvegliare l'applicazione della normativa in materia di protezione dei dati personali ossia l'Autorità di Controllo istituita nel territorio italiano, ai sensi della normativa italiana: il Garante *privacy*;

h. **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 personale (es. codice identificativo dipendente), 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;

i. **categorie particolari di dati personali** (o anche dati sensibili): i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché

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;

j. **dato giudiziario**: il dato personale idoneo a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del Codice di Procedura Penale;

k. **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;

l. **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;

m. **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;

n. **dato anonimo**: la normativa europea e nazionale in materia di protezione dei dati personali non si applica alle informazioni "anonime", ossia quelle informazioni raccolte senza alcun riferimento ad una persona fisica identificata o identificabile a cui il dato potrebbe riferirsi;

o. **trattamento dei dati personali**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati ed applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

p. **trasferimento**: trasferimento di dati personali verso un Paese extra-UE o un'organizzazione internazionale;

q. **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 in materia di dati personali, 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;

r. **diffusione**: dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

s. **profilazione**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per

analizzare o prevedere aspetti riguardanti 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;

t. **diritti dell'interessato**: sono i diritti riconosciuti all'interessato in relazione alla conoscenza e trasparenza dei trattamenti di dati personali che lo riguardano, rispetto al diritto di accesso ai propri dati personali, al diritto di integrazione e di rettifica, al diritto alla cancellazione dei dati personali e al diritto all'oblio, al diritto alla portabilità dei dati personali e al diritto alla limitazione, seppur per brevi periodi, del trattamento;

u. **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, sul trattamento dei dati personali che lo riguardano in relazione ad una specifica attività;

v. **diritto all'oblio**: interesse di un singolo ad essere dimenticato; l'esercizio di tale diritto consiste nella possibilità di richiedere la cancellazione dei contenuti dalle varie pagine web e di precedenti informazioni (spesso pregiudizievoli come ad esempio precedenti penali) che non rappresentano più la vera identità dello stesso interessato;

w. **informativa**: insieme di informazioni fornite all'interessato dal titolare del trattamento circa il trattamento posto in essere da quest'ultimo.

x. **pseudonimizzazione**: il trattamento dei dati personali in modo tale che gli stessi 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 intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

y. **anonimizzazione**: misura di sicurezza tecnica volta a impedire irreversibilmente l'identificazione dell'interessato a cui i dati si riferiscono. A seconda della tecnica utilizzata e dalle misure di sicurezza definite all'interno di apposite policies, i dati anonimizzati potrebbero rientrare nell'ambito di applicazione della normativa di protezione dati personali;

z. **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.

aa. **registro delle attività di trattamento**: il documento, anche informatico, che ogni responsabile del trattamento per la propria area di competenza, deve compilare e mantenere aggiornato, contenente, tra l'altro, (i) indicazione delle finalità del trattamento, (ii) l'elenco delle categorie di dati e di interessati, (iii) indicazione dei destinatari e dei trasferimenti, incluse le garanzie adottate (iv) le misure di sicurezza adottate, (v) l'elenco dei responsabili del trattamento esterni. Congiuntamente considerati, tali registri andranno a costituire il registro delle attività di trattamento dell'Università di Parma (o registro consolidato);

bb. **reclamo**: ai fini del presente regolamento è qualsiasi comunicazione e/o trasmissione di notizie fatta con qualsiasi mezzo da parte di un interessato al titolare o all'Autorità di controllo in relazione ai fatti e alle circostanze che potrebbero ledere i propri dati;

cc. **valutazione d'impatto** sulla protezione dei dati (o anche "*data protection impact assessment*" o "***DPIA***"): valutazione dell'impatto e dei rischi per i diritti e le libertà delle persone fisiche relativi ai trattamenti di dati personali effettuati dal titolare in ragione delle tecnologie utilizzate e considerati la natura, l'oggetto, il contesto e le finalità dei singoli trattamenti;

dd. **violazione dei dati personali** (o anche "***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;

ee. **accountability**: principio di responsabilizzazione secondo cui il Responsabile dei trattamenti è, appunto, responsabile delle scelte di mezzi, operazioni, procedure, finalità, ecc. in materia di trattamento dei dati, ma deve anche essere in grado di "dare conto" delle valutazioni svolte alla base delle scelte poi operate.

Articolo 4. Ruoli e responsabilità delle funzioni di supporto

1. Vengono individuati, ai fini del presente regolamento, specifici ruoli a cui possono essere associate strutture dell'organizzazione dell'Ateneo, così da poter mantenere una nomenclatura coerente a fronte di cambiamenti organizzativi[2]:

a. funzione *compliance* - è preposta all'assistenza legale e giuridica agli Organi Accademici e alle Strutture di Ateneo, è quindi competente anche per le tematiche legali in materia di *privacy* e protezione dei dati personali. Svolge un ruolo di coordinamento all'interno del processo di *compliance*, definendo mediante il presente regolamento il corpo metodologico da utilizzare per lo svolgimento delle attività riguardanti la gestione dei dati personali, ivi comprese le attività di valutazione dei rischi per i diritti e le libertà degli interessati (*risk assessment, data protection impact assessment)*, monitoraggio e reporting;
b. funzione *ICT* - ha la responsabilità di indirizzare e controllare le attività relative al processo ICT e ha la responsabilità di (i) adottare le misure di sicurezza identificate, (ii) aggiornare le istruzioni agli incaricati e (iii) di designare gli Amministratori di Sistema;
c. funzione *security*: (i) definisce le misure di sicurezza da adottare, (ii) supporta la funzione ICT ai fini dell'azione delle misure di sicurezza, (iii) supporta il responsabile del trattamento per la determinazione del tempo di conservazione dei dati , (iv) per la Valutazione di Impatto (DPIA), (v) in caso di analisi ed eventuale denuncia di violazione, (vi) provvede al consolidamento delle informazioni

[2] Nell'allegato 1 sono identificate le attuali strutture dell'Ateneo competenti a svolgere le funzioni elencate nelle lettere a), b) e c) dell'art. 4, con riferimento al vigente funzionigramma. Le modifiche del contenuto dell'allegato 1 non comportano la modifica del Regolamento.

relative alla sicurezza nel registro dei trattamenti effettuati da ciascun responsabile del trattamento dell'Ateneo e (vii) diffonde in Ateneo la cultura della sicurezza e della protezione dei dati.

2. Tali funzioni si coordinano su base trimestrale in un comitato indetto dal DPO. Gli obiettivi del comitato sono:
   a. il monitoraggio dell'applicazione del regolamento e della normativa vigente in materia di protezione dei dati personali all'interno dell'Ateneo;
   b. l'analisi delle criticità segnalate dai Responsabili dei trattamenti, dagli Incaricati e da tutti i soggetti direttamente o indirettamente coinvolti dal trattamento dei dati personali;
   c. l'eventuale discussione e proposta di revisione del presente regolamento e/o degli strumenti, policy e linee guide ad esso eventualmente allegati;
   d. la formalizzazione di una sintesi ed una visione di insieme in relazione alle attività summenzionate per il Titolare.

In linea generale, il comitato si potrà avvalere del contributo di altre funzioni o strutture per l'analisi di tematiche di particolare complessità e la partecipazione sarà aperta ed estesa di volta in volta ai responsabili dei trattamenti. I temi relativi alla revisione del presente regolamento richiederanno obbligatoriamente la presenza e/o la consultazione delle figure apicali dell'Ateneo individuate nei Dirigenti d'area, di dipartimento e dei Centri.

Articolo 5. Ambito di applicazione materiale

1. Oggetto del presente regolamento è il trattamento, interamente o parzialmente automatizzato, di dati personali e il trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

2. Sono esclusi dall'ambito di applicazione i trattamenti dei dati personali effettuati da persone fisiche per fini esclusivamente personali e nei casi in cui tali dati non siano destinati ad una comunicazione sistematica o alla diffusione, anche se utilizzati ai fini di esigenze di lavoro (ad esempio, banca dati su *personal computer* accessibile ed utilizzata solo ed esclusivamente dall'utente/persona fisica, rubrica telefonica, foto personali, esiti di esami clinici/diagnostici, ecc.).

Articolo 6. Tipologia di dati trattati dall'Ateneo

1. L'Università effettua i trattamenti di dati personali, previsti da disposizioni legislative e regolamentari riguardanti, a titolo esemplificativo e non esaustivo:

a. dati, anche di natura particolare, 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 (in occasione ad esempio di: 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 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;

b. dati relativi a studenti intesi nell'accezione più ampia, per tutte le attività e modalità connesse alla qualità di studente e ai laureati (in occasione ad esempio di: 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 alla laurea- 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;

c. dati relativi alla didattica e alla ricerca (compresa la ricerca in ambito medico - sanitario);

d. dati relativi alle attività gestionali, conto terzi e/o connessi ad attività trasversali (quali ad esempio: 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*; erogazione federata di servizi; erogazione del servizio Eduroam; accesso a servizi federati; tracciamento di informazioni non primarie).

2. È vietato trattare dati personali atti a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento 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, fatti salvi i seguenti casi:

a. l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;

b. 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;

c. il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d. il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

e. il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;

f. il trattamento è necessario per motivi di interesse pubblico rilevante ai sensi dell'art. 2-sexies del Codice in materia di protezione dei dati personali.

3. I dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento solo in conformità alle misure di garanzia disposte e adottate con apposito provvedimento dal Garante per la protezione dei dati personali.

4. Il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza è consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, ai sensi dell'art. 2-octies del Codice in materia di protezione dei dati personali.

Articolo 7. Base giuridica dei trattamenti con finalità istituzionali

1.L'Università è una pubblica amministrazione ai sensi dell'art. 1, c. 2 del D. Lgs. 165/2001 e ss.mm., persegue finalità di interesse generale, opera in regime di diritto amministrativo ed esercita potestà pubbliche. Pertanto, il trattamento di dati personali nell'esercizio dei suoi compiti istituzionali trova il fondamento di liceità nella condizione prevista dall'art. 6, paragrafo 1 let. e) del Regolamento (UE). Il trattamento è lecito se è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

2. La base giuridica per il trattamento di dati personali effettuato 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, di Regolamento, secondo quanto previsto dall'art. 2-ter, c. 1 del Codice in materia di protezione dei dati personali.

3. Il trattamento deve sempre essere necessario al perseguimento dei fini per i quali viene lecitamente effettuato ("principio di necessità").

Articolo 8. 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 istituzionali.

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 alla loro specifica funzione, è consentito in via diretta e tracciato senza ulteriori formalità nella misura necessaria e al solo fine del perseguimento dell'interesse istituzionale, ferma restando 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 9. Comunicazione e diffusione dei dati

1. L'Università può comunicare a finanziatori di borse di dottorato e assegni, anche stranieri, dati comuni relativi a dottorandi e assegnisti che abbiano usufruito dei finanziamenti.

2. In considerazione del sistema di autovalutazione, accreditamento e valutazione periodica dei Corsi di studio definito dal MIUR, l'Università può elaborare e/o comunicare le opinioni degli studenti sulla didattica agli organismi deputati ad effettuare verifiche della qualità della didattica quali il Nucleo di Valutazione o il Presidio della Qualità. Tali dati sono trattati con lo scopo di definire azioni volte al miglioramento della qualità della didattica.

3. L'Università può comunicare, alle Aziende Ospedaliere in convenzione, dati inerenti al personale dell'Università che eserciti la propria attività nell'ambito della convenzione con tali Enti.

4. In ottemperanza ai principi di trasparenza cui l'Università si ispira e al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, è consentita la pubblicazione dei dati inerenti alle valutazioni d'esame anche sui siti web di Ateneo. La pubblicazione dei dati sui siti web 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. Le valutazioni sono rese disponibili per un periodo di tempo non superiore a tre mesi.

5. In ottemperanza ai principi di trasparenza cui l'Università si ispira, è consentita la pubblicazione di esiti di prove concorsuali e selettive, nonché delle relative graduatorie, anche sui siti web di Ateneo. La pubblicazione dei dati sui siti web è effettuata nel rispetto del principio della minimizzazione dei dati, mediante la diffusione dei dati strettamente necessari al raggiungimento delle finalità per le quali sono pubblicati. Nel caso di diffusione delle valutazioni sui siti web di Ateneo, tali informazioni sono pubblicate per un periodo di tempo non superiore a sei mesi.

6. I limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali e per l'esercizio dell'accesso civico restano disciplinati rispettivamente dalla legge 7 agosto 1990, n. 241 e successive modificazioni e dal decreto legislativo 14 marzo 2013, n. 33 e successive modificazioni e dai Regolamenti attuativi di Ateneo in materia. Quando il trattamento riguarda categorie particolari di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza, l'accesso è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

Articolo 10. Titolare del trattamento dei dati personali

1. Il titolare del trattamento dei dati personali è individuato nella persona giuridica che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento. Titolari del trattamento sono, pertanto,

l'Ateneo e, ove esistenti, ciascuna delle società partecipate che rientrano nell'ambito d'applicazione del presente regolamento.

2. Il titolare adempie, secondo quanto precisato nel presente regolamento, alle responsabilità di seguito elencate con il supporto e/o per il tramite del responsabile della protezione dei dati personali (DPO - *Data Protection Officer*), della funzione di *compliance* per quanto riguarda le tematiche di *compliance* normativa, della funzione ICT e della funzione *security* competente, ciascuna in relazione agli ambiti di rispettiva competenza, nonché dei responsabili del trattamento.

3. Le responsabilità attribuite al titolare sono:

a. coordinare il sistema di *compliance privacy* nel suo complesso, assicurandone l'efficacia, l'efficienza e la realizzazione con il supporto del DPO e della funzione di *compliance*;
b. designare i responsabili del trattamento interni e, se necessario, esterni;
c. nominare, revocare o ratificare il DPO;
d. rappresentare la società in relazione a tutte le questioni relative alla tutela dei dati personali innanzi all'Autorità di controllo, nominando eventualmente procuratori speciali e consulenti;
e. assicurare l'esecuzione delle valutazioni di impatto (Data Protection Impact Assessment, DPIA);
f. assicurare che le funzioni competenti definiscano le misure di sicurezza;
g. impartire le Istruzioni generali che i responsabili del trattamento e gli incaricati devono seguire per assicurare che i trattamenti avvengano in coerenza a tutto quanto previsto dalla normativa applicabile e dal presente regolamento.

4. È facoltà del titolare individuare un delegato, che eserciterà in concreto la titolarità del trattamento dei dati personali facenti capo ad ambiti (aree dirigenziali, dipartimenti, centri) che, per peculiarità e specificità delle tematiche trattate, richiedono una *governance* dei temi relativi alla protezione dei dati personali non scindibile dalla posizione apicale occupata. Il delegato del titolare, munito dei necessari poteri, ha la responsabilità di adempiere agli obblighi ed esercitare i diritti e le facoltà previste a carico del titolare, provvedendo ad adottare le misure organizzative atte a garantire la valutazione, la definizione e il coordinamento e la realizzazione delle iniziative di Ateneo in materia di protezione dei dati personali.

Articolo 11. Responsabile per la protezione dei dati personali (DPO - Data Protection Officer)

1. Il DPO è nominato, dal titolare del trattamento e svolge le sue funzioni nell'interesse dello stesso.

2. Il DPO svolge una funzione di garanzia della conformità della circolazione e della protezione dei dati personali secondo quanto stabilito dal presente regolamento e, più in generale, dal GDPR.

3. Le responsabilità attribuite al DPO sono, a titolo esemplificativo e non esaustivo:

– informare e fornire consulenza in materia di tutela dei dati personali al titolare e ai responsabili del trattamento, nonché direttamente agli incaricati che eseguono i trattamenti;

- garantire, in coordinamento con le competenti funzioni di *compliance* l'osservanza del regolamento ovvero, più in generale, delle previsioni del GDPR e delle altre disposizioni, anche regolamentari, e provvedimenti dell'Autorità di controllo applicabili in tema di protezione dei dati personali;
- cooperare all'eventuale redazione di codici di condotta ovvero cooperare con gli organismi di certificazione all'uopo autorizzati;
- cooperare con l'Autorità di controllo per tutte le questioni rilevanti quali consultazioni preventive, ispezioni/procedimenti, reclami e/o segnalazioni;
- fornire supporto, per quanto di competenza, nella gestione dei reclami e/o segnalazioni di violazione dei dati personali, cooperando con il titolare per l'eventuale presentazione delle notifiche obbligatorie di violazione dei dati personali ai sensi del GDPR e attraverso l'assistenza specialistica delle funzioni Security e ICT e, laddove necessario, della funzione eventualmente deputate ad eseguire *Internal Audit*;
- vigilare sul corretto funzionamento ed applicazione della valutazione d'impatto sulla protezione dei dati (*Data Protection Impact Assessment*).

Articolo 12. Responsabile del trattamento dei dati personali

1. I responsabili del trattamento sono designati dal titolare, nelle persone dei dirigenti di aree amministrative e dei direttori di dipartimenti e centri, queste posizioni organizzative presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che ciascun trattamento soddisfi i requisiti in materia di protezione dei dati personali e garantisca la tutela dei diritti dell'interessato. In particolare, i responsabili sono così individuati:

- per le attività di competenza del Rettorato: il Rettore o un suo delegato espressamente designato;
- per le strutture amministrative e gestionali: il Direttore generale per le attività di competenza della Direzione generale e i Dirigenti per le rispettive attività di competenza;
- per le attività di didattica e di ricerca: i Direttori dei Dipartimenti e dei Centri, i Presidenti delle Scuole, i Responsabili di altre tipologie di strutture.

2. Inoltre, nello svolgimento delle attività di competenza, i responsabili del trattamento possono avvalersi del supporto operativo di funzioni/unità/referenti appartenenti alla propria struttura, in virtù del coinvolgimento diretto e prevalente nel trattamento, ferma restando la responsabilità di vigilanza.

3. Ciascun responsabile del trattamento, relativamente ai trattamenti rientranti nella propria area di competenza, ha i seguenti principali compiti:

a. agire sulla base delle indicazioni ricevute dal titolare e di eventuali indicazioni del DPO;

b. sovrintendere continuativamente a tutti gli aspetti relativi alla *compliance privacy* di ciascun trattamento quali, a titolo esemplificativo e non esaustivo: (i) l'Informativa agli interessati; (ii) le Istruzioni agli incaricati e il rispetto delle stesse; (iii) le misure di sicurezza; (iv) i tempi di conservazione dei dati e le

modalità di *data portability*, (v) lo svolgimento - quando e se necessario - della valutazione d'impatto (DPIA), etc. Inoltre, il responsabile del trattamento, avvalendosi del supporto della funzione ICT e della funzione *security*, ciascuno per gli ambiti di propria competenza, mette in atto tutte le azioni possibili per individuare ogni violazione dei dati personali, nonché l'eventuale perdita o distruzione di dati, ovvero l'accesso non autorizzato ai database da parte di terzi, oppure il mancato funzionamento delle misure di sicurezza predisposte dal titolare; il responsabile informa senza indugio di tali evenienze il DPO e il titolare, comunque, facendo in modo che siano garantite le tempistiche previste dalla normativa in relazione alle notifiche ricevute dal Garante in merito alle predette violazione, per il tramite della funzione di *compliance*;

c. provvedere a fornire idoneo e puntuale riscontro ad ogni richiesta ricevuta dagli interessati circa l'esercizio dei propri diritti in materia di *privacy* con il supporto, ove necessario, del DPO e della funzione di *compliance*;

d. assicurare la compilazione e l'aggiornamento dei registri delle attività di trattamento;

e. designare, uno o più amministratori di sistema quando necessario ai sensi di quanto previsto al successivo articolo 11;

f. fornire alla funzione di *compliance* e al DPO ogni supporto utile al processo di monitoraggio relativo alla corretta implementazione del presente regolamento e a tutte le tematiche rilevanti in tema di *privacy* e protezione dei dati, in particolare attraverso la redazione di specifica attestazione/reportistica annuale, laddove concordato preventivamente, e qualora fossero in essere trattamenti con profili di rischio elevato;

g. fornire alla struttura competente per la formazione e benessere organizzativo e al DPO ogni supporto utile a promuovere e realizzare piani di formazione in materia di *privacy* e protezione dei dati.

4. In casi del tutto eccezionali, qualora il responsabile del trattamento fosse effettivamente impossibilitato ad adempiere ai compiti sopra indicati, lo stesso dovrà informare tempestivamente il titolare, che potrà assumere la responsabilità del trattamento limitatamente all'esecuzione degli atti urgenti non postergabili e comunque nei soli casi in cui l'impedimento non sia prolungato nel tempo.

Articolo 13. Responsabile del trattamento dati esterno

1. In ipotesi di attività affidata a soggetti terzi, che comportino il trattamento di dati personali la cui titolarità è dell'Ateneo, il responsabile del trattamento di tali dati, che sottoscrive il contratto di affidamento, nomina l'affidatario quale responsabile esterno del trattamento dei dati. La predetta nomina deve prevedere, tra l'altro, l'impegno del responsabile esterno al rispetto dei criteri, delle finalità e delle modalità di trattamento dei dati personali previsti dalla normativa vigente e da eventuali istruzioni impartite dall'Ateneo o da una sua struttura, nonché controlli e vigilanza specifica sulle attività del responsabile del trattamento esterno.

2. L'elenco dei responsabili del trattamento esterno è contenuto in apposita sezione del Registro delle attività di trattamento.

Articolo 14. Incaricati del trattamento dati personali

1. Le persone che effettuano trattamenti di dati personali nello svolgimento delle attività di propria competenza assumono la qualità di incaricato del trattamento.

2. L'incaricato effettua le operazioni di trattamento afferenti all'attività lavorativa di sua competenza, attenendosi alle Istruzioni impartite dal titolate/responsabile del trattamento, nonché dal presente regolamento. Il titolare/responsabile è individuato in quello, di volta in volta, competente per lo specifico trattamento a cui si riferiscono le operazioni medesime.

3. Attraverso il presente regolamento, pertanto, tutti coloro (dipendenti, collaboratori, studenti etc.) che, a qualsiasi titolo, nell'ambito delle proprie prestazioni lavorative, svolgano operazioni in relazione ad uno o più trattamenti di dati, sono di fatto incaricati in relazione a tali trattamenti.

4. L'autorizzato 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.

5. L'autorizzato si impegna a osservare le istruzioni, le politiche e i regolamenti in materia di sicurezza informatica e logica adottate dall'Università.

6. L'incarico relativo al trattamento non comporta responsabilità e oneri aggiuntivi, rispetto alle funzioni e mansioni esercitate, se non quelli del rispetto delle indicazioni su menzionate.

Articolo 15. Amministratore di sistema

1. La designazione delle funzioni di amministratore di sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto da designare, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

2. A tale riguardo possono essere designati quali amministratori di sistema i soggetti in possesso dei seguenti requisiti:

a. competenza in ambito informatico, anche in relazione a tematiche inerenti al profilo della sicurezza, ad esempio in considerazione del percorso formativo e/o dell'esperienza professionale maturata;

b. conoscenza approfondita del contesto in cui si trovano ad operare.

3. Gli amministratori di sistema sono tenuti all'osservanza delle disposizioni normative e di Ateneo in materia di trattamento di dati personali.

4. Laddove il trattamento dei dati personali lo preveda, l'amministratore di sistema è designato individualmente dal responsabile del trattamento competente nella cui area di riferimento sono svolte direttamente attività di amministrazione di sistemi informatici che implicano il trattamento di dati personali.

5. Per i sistemi gestiti dalla funzione ICT, l'amministratore di sistema è di norma centralizzato nella stessa funzione ICT. Il responsabile del trattamento verifica e documenta la sussistenza dei requisiti indicati nel presente articolo.

6. Ai fini delle presenti istruzioni si considerano come potenziali amministratori di sistema eventuali collaboratori autonomi esterni.

Articolo 16. Funzione di compliance in materia di privacy e protezione dei dati personali

1. La funzione di *compliance* è responsabile di fornire assistenza specialistica in materia di *privacy* e protezione dei dati a tutti gli agenti (ivi inclusi i responsabili del trattamento e gli incaricati), di volta in volta, interessati dell'Ateneo e delle eventuali società partecipate.

2. In particolare, a titolo esemplificativo, la funzione di *compliance*:

a. fornisce consulenza e assistenza specialistica in materia di *legal compliance* in relazione alle normative sulla *privacy* e *data protection*, incluse le evoluzioni normative e giurisprudenziali a livello europeo e, per gli aspetti di maggior rilievo, extraeuropeo, supportando l'Ateneo e le eventuali società partecipate affinché si dotino di un assetto organizzativo e di processi conforme alle normative, incluse le linee guida e le raccomandazioni delle Autorità di Controllo, in materia di tutela dei dati personali; garantendo assistenza nello sviluppo complessivo di attività e/o progetti che presentino questioni rilevanti in materia di tutela dei dati personali; supportando le funzioni di Ateneo interessate su questioni specifiche in materia di tutela dei dati personali;

b. svolge il ruolo di segreteria tecnica del DPO provvedendo alla gestione dei flussi informativi e/o di altra natura fra il DPO e le funzioni di Ateneo, di volta in volta, interessate e/o i terzi.

c. contribuisce alle campagne e alle iniziative di formazione, ai training specifici, di concerto con le strutture competenti alla formazione, alla comunicazione e alla *security*, per le attività di comunicazione e formazione al fine di promuovere e diffondere la cultura in materia di *privacy* e *data protection* e garantire la conoscenza e la sensibilità del personale dell'Ateneo verso la normativa di riferimento;

d. di concerto con il DPO, riesamina periodicamente l'efficacia del presente regolamento anche sulla base delle risultanze delle attività di *risk assessment*, monitoraggio e delle *best practice* di riferimento e di eventuali gap o criticità riscontrati, e assume le conseguenti opportune iniziative.

CAPO II
Linee guida per la conformità in materia di tutela dei dati personali

Articolo 17. Garanzie del trattamento

1. L'Ateneo garantisce che il trattamento dei dati personali avvenga in modo lecito e secondo correttezza e comunque in base a regole specifiche che possono essere adottate al fine di prevenire i rischi relativi alla violazione dei dati personali, inclusi a titolo esemplificativo e non esaustivo quelli concernenti le seguenti macro-categorie di attività a rischio:

a) i rapporti con gli studenti ed in generale a tutti gli individui che prendono parte alle iniziative dell'Ateneo;

b) i rapporti con i dipendenti e i soggetti ad essi assimilabili;

c) i rapporti con i fornitori;

d) i rapporti con fruitori di servizi forniti dall'Ateneo e dalle sue strutture;

e) i rapporti con altre Pubbliche Amministrazioni e Istituzioni;

f) i rapporti con soggetti giuridici partecipati a vario titolo.

2. Il livello di rischio associato alle succitate macro-categorie e ai trattamenti da esse scaturenti viene individuato sulla base dell'analisi del contesto, delle eventuali indicazioni di carattere legale comunicate dalla funzione di *compliance* e di *security*. Inoltre, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi rilevanti per gli interessati, le operazioni di trattamento sono eseguite in modo da garantire il rispetto della normativa applicabile e i principi di riferimento riportati nel presente regolamento. In particolare, nell'ambito di qualsiasi iniziativa, i sistemi informativi utilizzati e i processi adottati devono soddisfare i principi della protezione dei dati fin dalla progettazione (c.d. *privacy by design*) e per impostazione predefinita (c.d. *privacy by default*).

3. Il presente capo riporta linee guida e indicazioni generali finalizzate a esplicitare gli elementi essenziali della *compliance* in materia di *privacy* e data protection e della sua declinazione nell'Ateneo.

Articolo 18. Linee guida in materia di privacy by design e by default. Aspetti generali

1. Il regolamento GDPR stabilisce che la *privacy* e la protezione dei dati debba essere considerata nelle valutazioni preliminari di ogni nuova attività, progetto e/o servizio avviato dall'Ateneo o dalle partecipate (*privacy* by design), a prescindere dalle modalità di esecuzione dei trattamenti sottesi (es: cartacea, informatica). In un'ottica di *privacy* by design il responsabile di nuovo progetto/iniziativa o attività (di seguito, "attività") deve verificare, con il supporto del DPO e della funzione di *compliance*, se la nuova attività comporti un trattamento di dati personali a rischio per la tutela dei diritti degli interessati. In tal caso, è

necessario presidiare il trattamento dei dati personali con l'adozione di idonee misure di sicurezza individuate dalla funzione *security* e con le funzioni o aree dell'Ateneo eventualmente coinvolte (es: U.O. vigilanza).

2. Il principio di privacy by default (protezione per impostazione predefinita) prevede, appunto, che si vadano a trattare solo i dati personali nella misura **necessaria** e **sufficiente** per le finalità previste e per il periodo strettamente necessario a tali fini. Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti. in modo che l'interessato riceva un alto livello di protezione anche se non si attiva per limitare la raccolta dei dati

3. I principi che sottendono al concetto di privacy by design sono i seguenti:
    a. prevenire non correggere, cioè i problemi vanno valutati nella fase di progettazione, e il trattamento deve prevenire il verificarsi dei rischi per i diritti e le libertà degli interessati;
    b. privacy come impostazione di default (ad esempio, non deve essere obbligatorio richiedere un dato il cui conferimento di dati è facoltativo o non necessario ai fini del trattamento);
    c. privacy incorporata nel progetto (ad esempio, l'utilizzo di tecniche di pseudonimizzazione o minimizzazione dei dati);
    d. sicurezza durante tutto il ciclo del trattamento;
    e. visibilità e trasparenza del trattamento, cioè tutte le fasi operative devono essere trasparenti in modo che sia verificabile la tutela dei dati;
    f. centralità dell'utente, quindi rispetto dei diritti, tempestive e chiare risposte alle sue richieste di accesso.

Articolo 19. Analisi preventiva delle attività con potenziali impatti in materia di *privacy* e *data protection*

1. Le funzioni di *compliance*, di *security* ed il DPO devono essere consultati, già nella fase di ideazione/pianificazione e in ogni caso prima della realizzazione, in merito ad attività che prevedano il trattamento di dati personali, nonché nella successiva fase di realizzazione/esecuzione, qualora l'attività possa comportare, anche potenzialmente, un trattamento dei dati personali a rischio per la tutela dei diritti degli interessati e qualora vengano apportate modifiche sostanziali a quanto pianificato.

2. Le attività dovranno essere preventivamente sottoposte dal responsabile della specifica attività (di seguito, richiedente) mediante nota (anche via email) alla funzione di *compliance* e di *security*, e per conoscenza, al responsabile del trattamento eventualmente competente (se diverso dal richiedente) al fine di esaminarne la rilevanza e la compatibilità con la normativa in materia di *privacy* e *data protection*. Le informazioni da fornire sulle caratteristiche delle attività sono:

a. un inquadramento generale delle finalità dell'attività;

b. una descrizione specifica delle attività che prevedono la necessità di effettuare un trattamento di dati personali;

c. ogni altra informazione disponibile in merito a trattamento che si intenderebbe svolgere (tipologia di interessati; natura e caratteristiche dei dati; modalità tecniche previste per il trattamento; flussi di dati);

d. le principali questioni e criticità che, ad un'analisi preliminare effettuata anche sulla base del presente regolamento, appaiano rilevanti;

e. qualsiasi altra informazione che possa essere rilevante al fine delle analisi prescritte dal presente regolamento.

3. La funzione di *compliance* e di *security*, unitamente al DPO, valutano le informazioni ricevute e:

a. se l'attività non dà luogo ad un nuovo trattamento di dati personali e/o ad una modifica di un trattamento già presente nel Registro dei trattamenti, invia una comunicazione al Richiedente e, se diverso da quest'ultimo, anche al responsabile del trattamento;

b. se l'attività dà luogo ad un nuovo trattamento di dati personali e/o ad una modifica di un trattamento già presente nel Registro dei trattamenti, invia una comunicazione al responsabile del trattamento e, se diverso da quest'ultimo, anche al richiedente, indicando, ove necessario, le azioni da porre in essere per assicurare la conformità al presente regolamento, ivi inclusa la necessità di effettuare un'analisi di impatto (*data protection impact assessment*) e/o l'opportunità di consultare il DPO.

4. Il responsabile del trattamento di cui trattasi:
   a. tiene conto delle Indicazioni anche ai fini dell'annotazione nel Registro dei trattamenti di un nuovo trattamento e/o dell'aggiornamento di un trattamento già presente;
   b. fornisce alla funzione di compliance un riscontro in merito all'avvenuta iscrizione e/o aggiornamento del Registro dei trattamenti, nonché sulle Informative, Istruzioni e Misure di Sicurezza, etc., effettivamente adottate.

Articolo 20. Linee guida in materia di conservazione (c.d. *Data Retention*), sicurezza del dato e valutazione dei rischi.

1. I dati personali sono conservati dall'Ateneo in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono raccolti e trattati. Al venire meno delle finalità per i cui dati sono raccolti e trattati, di norma questi stessi devono essere distrutti e/o de-identificati; tuttavia i dati personali possono essere conservati per periodi più lunghi a condizione che vi sia il consenso espresso dell'interessato, ovvero ciò sia consentito da una norma di legge e/o di regolamento, ovvero siano conservati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

2. Il responsabile del trattamento, con il supporto della funzione di *compliance* e della funzione ICT competente e della funzione *security* stabilisce, rendendolo noto nelle Istruzioni, il tempo di conservazione dei dati in relazione alle finalità di ciascun trattamento di cui è responsabile. La valutazione deve essere fatta

considerando le normative applicabili al caso specifico (es: difesa in sede giudiziale, archiviazione dei dati contabili, dati della carriera studentesca, ecc).

3. la funzione di *compliance* fornisce uno schema tipo di documento per la conservazione dei dati.

Articolo 21. Misure di sicurezza

1. Tenendo 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 degli interessati, i responsabili del trattamento, ciascuno per i trattamenti rientranti nel proprio ambito di competenza, con il supporto della funzione di *compliance*, della funzione ICT e della funzione *security*, mettono in atto misure adeguate per garantire un livello di sicurezza proporzionato al rischio per le libertà ed i diritti degli interessati, che comprendono, tra le altre:

   a. la *pseudonimizzazione*, l'*anonimizzazione* e la *crittografia* dei dati personali, ove applicabile;

   b. l'utilizzo di mezzi e modalità di comunicazione idonei ai dati trasmessi;

   c. la protezione delle informazioni dell'Ateneo trattate al di fuori delle applicazioni informatiche;

   d. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

   e. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

   f. modalità operative per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, il responsabile del trattamento tiene conto dei rischi derivanti dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, di dati personali trasmessi, conservati o comunque trattati.

Articolo 22. Valutazione d'impatto (data protection impact assessment o DPIA)

1. I responsabili del trattamento, ciascuno per i trattamenti di propria competenza, con il supporto della funzione di *compliance*, della funzione ICT e, quando necessario, della funzione *security*, sentito il DPO, procedono alla Valutazione d'Impatto qualora ricorrano **almeno due condizioni** fra quelle indicate nelle seguenti casistiche:

   a. trattamenti valutativi o di *scoring*, compresa la profilazione e le attività che consentano di prevedere il comportamento, tenuto conto in particolare di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

b. decisioni automatizzate che producono significativi effetti giuridici o di analoga natura (è il caso dei trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici o incidono su di essi);

c. monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico (Ai sensi delle linee guida WP29 per "sistematico" si intende "ciò che avviene per sistema, predeterminato, organizzato o metodico; che ha luogo nell'ambito di un progetto complessivo di raccolta di dati; svolto nell'ambito di una strategia. L'espressione "area accessibile al pubblico" definisce un luogo aperto alla generalità delle persone, per esempio una piazza, una strada, una stazione di rifornimento di benzina);

d. trattamento di dati sensibili o di dati di natura estremamente personale;

e. trattamenti di dati su larga scala, ovvero: (i) che coinvolgono un numero significativo di interessati, in termini numerici o di percentuale rispetto alla popolazione di riferimento, quest'ultima intesa come bacino dei potenziali interessati dal trattamento (es: gli studenti, i dipendenti); (ii) per volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; (iii) per durata e/o persistenza, dell'attività di trattamento; (iv) per ambito geografico dell'attività di trattamento;

f. combinazione o raffronto di insiemi di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

g. dati relativi a interessati vulnerabili (la categoria degli interessati vulnerabili comprende i minori, i soggetti che non siano in grado di opporsi o di prestare consenso, in modo consapevole e ragionato al trattamento dei propri dati personali);

h. utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative, come l'associazione fra tecniche con utilizzo di impronte digitali e riconoscimento del volto per migliorare il controllo degli accessi fisici;

i. tutti quei trattamenti che, di per sé, impediscono agli interessati di avvalersi di un servizio o di un contratto e/o accordo (si tratta in particolare di valutazioni interne di natura discrezionale sugli interessati, che comportano la limitazione all'accesso a taluni servizi).

2. La Valutazione d'Impatto contiene quanto meno:

a. una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare;

b. una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c. una valutazione dei rischi per i diritti degli interessati;

d. le misure di sicurezza previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

3. Laddove il risultato della valutazione d'impatto indichi che il trattamento possa presentare un rischio elevato, il titolare, in accordo con il responsabile del trattamento e in cooperazione con il DPO, valuterà se:

a. iniziare il trattamento dopo aver adottato le misure correttive idonee a mitigare sufficientemente il rischio;

b. procedere alla consultazione preventiva dell'Autorità di controllo, per ottenere indicazioni su come gestire l'eventuale rischio residuale (residuo rispetto alle misure correttive già individuate).

4. Nell'ambito della consultazione preventiva, il titolare comunica all'Autorità di controllo:

a. le rispettive responsabilità all'interno dell'organizzazione interna del titolare del trattamento nonché le forme di contitolarità;

b. le finalità e i mezzi del trattamento oggetto di consultazione;

c. le misure correttive e le garanzie previste per proteggere i diritti e le libertà degli interessati;

d. i dati di contatto del DPO e del titolare;

e. la valutazione d'impatto effettuata;

f. ogni altra informazione richiesta dall'Autorità di controllo.

Articolo 23. Denuncia di Violazione dei Dati personali – (*data breach*)

1. Tutte le persone che operano, a qualsiasi titolo nell'Ateneo devono prestare attenzione - nel rispetto del presente regolamento e delle istruzioni ad accedere - ai dati oggetto dei trattamenti; ciò, esclusivamente per quanto funzionale ad adempiere alle proprie funzioni. Un accesso ai dati al di fuori di quanto funzionale ad adempiere alle proprie funzioni e/o comunque non conforme alle Istruzioni deve essere considerato una Violazione dei dati personali ai fini del presente regolamento e potrà conseguentemente essere fonte di responsabilità per l'attore.

2. Il personale dell'Ateneo deve agire con la massima diligenza al fine di prevenire episodi di violazione dei dati personali, ossia accessi non autorizzati -da parte di altre persone dell'Ateneo e/o terzi- ai dati oggetto dei trattamenti facenti capo all'Ateneo o comunque incidenti al corretto svolgimento dei trattamenti medesimi.

3. Chiunque venga a conoscenza, direttamente e/o indirettamente (su indicazione di un incaricato, di un dipendente dell'Ateneo e/o di un terzo) di una possibile violazione di dati personali (anche solo sospetta) - quale che sia la possibile fonte/origine di tale violazione (terzi, personale dell'Ateneo, fonte non identificata, evento accidentale) - deve comunicare immediatamente, tramite l'indirizzo email databreach@unipr.it, al

DPO, alla funzione *security*, al responsabile del trattamento competente, ove noto, e, in ogni caso, alla funzione di *compliance* tale possibile violazione.

4. A seguito della ricezione della segnalazione di una possibile violazione di dati personali, l'unità di *compliance* coinvolge, a seconda del caso, ciascuna per gli aspetti di competenza, la funzione ICT, la funzione di gestione del personale e la funzione vigilanza.

5. Le funzioni come sopra identificate, a seguito di tempestiva consultazione, valuteranno congiuntamente se ricorrono effettivamente i presupposti per considerare l'evento come violazione di dati personali e, ove possibile, quale ne sia la portata e le caratteristiche, ponendo particolare attenzione ai rischi per i diritti e le libertà degli interessati i cui dati siano stati oggetto della violazione. In particolare, si valuterà se ricorrano o meno le circostanze che, in coerenza con la normativa applicabile, rendono necessario o opportuno informare dell'avvenuta violazione l'Autorità di controllo e/o gli interessati i cui dati siano stati oggetto della violazione.

6. Sarà cura della funzione di *security* trasmettere, per tramite di una comunicazione email secondo quanto di seguito precisato, le conclusioni di tali valutazioni, contenute in una breve relazione. In particolare:

a. qualora non sia stata accertata una violazione dei dati personali, la relazione sarà inviata al responsabile del trattamento segnalante e/o al responsabile del trattamento competente, nonché alle funzioni coinvolte;

b. qualora sia stata accertata una violazione dei dati personali, la relazione sarà inviata al titolare, al DPO, nonché al responsabile del trattamento segnalante e al responsabile del trattamento competente nonché alle funzioni coinvolte.

7. Il titolare, sulla base di quanto indicato nella Relazione, provvederà, con il supporto della funzione di *compliance*, alla notifica della Violazione all'Autorità di Controllo e, se del caso, agli interessati di cui sopra.

Articolo 24. Linee guida in materia di Informativa agli interessati, consenso e diritti degli interessati.

1. Per ogni tipologia di trattamento dei dati l'Ateneo fornisce l'informativa all'interessato, ai sensi degli artt. 13 e 14 del Regolamento (UE). L'informativa fornita all'interessato deve essere concisa, trasparente, intelligibile, facilmente accessibile e deve essere usato un linguaggio chiaro e semplice.

2. L'informativa contiene, di fatto, tutte le informazioni necessarie a garantire che l'interessato sia consapevole dei contenuti del trattamento relativo ai suoi dati. Fondamentale è l'indicazione, nell'informativa, delle finalità del trattamento, delle modalità dello stesso, delle categorie di soggetti interni ed esterni all'Ateneo che avranno accesso ai dati dell'interessato, del tempo per la cui durata i dati sono conservati, degli estremi identificativi dell'Ateneo, o delle partecipate, quale titolare del trattamento, dei dati di contatto del DPO, dell'eventualità che i dati siano trasferiti oltre il territorio UE, del fatto che venga effettuata una profilazione con i dati dell'interessato, del diritto di revocare il consenso prestato, nei casi in

cui il trattamento è svolto sulla base del consenso dell'interessato (v. sotto), nonché di ogni altro Diritto dell'interessato.

3. L'informativa deve essere fornita prima dell'inizio dell'attività di trattamento se i dati sono raccolti direttamente presso l'interessato e prima dell'espressione del consenso (se e quando richiesto) ovvero al primo contatto utile con l'interessato, se i dati sono raccolti presso terzi.

4. Nel caso in cui i dati personali già raccolti devono essere trattati ulteriormente per una finalità diversa da quella per cui sono stati ottenuti, l'Università, prima di attivare l'ulteriore trattamento, fornisce all'interessato informazioni in merito alla diversa finalità. 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.

5. Sono rilasciate specifiche informative:

a. ai dipendenti all'atto dell'assunzione, a cura delle competenti funzioni dell'Area personale e organizzazione;

b. ai soggetti che, a qualunque titolo, collaborano con l'Ateneo, prima dell'inizio dell'attività, a cura delle funzioni competenti;

c. ai terzi fornitori, all'atto della richiesta di offerta, a cura delle funzioni competenti in merito agli approvvigionamenti;

d. ai richiedenti dei servizi, al momento della raccolta dei dati personali (es. sottoscrizione del contratto) a cura delle unità/funzioni competenti;

e. a tutti gli altri soggetti terzi non rientranti nelle categorie sopra riportate per i quali sia necessario raccogliere e trattare dati personali che li riguardino, alla prima occasione disponibile di contatto con l'Ateneo, a cura della funzione incaricata di gestire tale contatto (ad esempio, componenti degli Organi e degli Organismi di Ateneo;

f. a tutti gli utenti dei siti Internet gestiti dall'Ateneo e dalle partecipate, anche in relazione al trattamento dei dati tramite cookie e altri strumenti di profilazione, a cura della funzione competente per la gestione del sito e in collaborazione con le altre competenti funzioni dell'Ateneo, quali ICT e/o Comunicazione.

6. L'Ateneo presta la massima attenzione affinché le operazioni di trattamento siano svolte nel rispetto a quanto previsto nell'informativa ed a tal fine i responsabili del trattamento assicurano piena coerenza e continuità logica tra informativa e istruzioni.

7. La funzione di *compliance* fornisce uno schema tipo di informativa. In ogni caso, l'informativa deve contenere:

- l'identità e i dati di contatto dell'Università;
- i dati di contatto del Responsabile della Protezione dei Dati personali;
- le finalità del trattamento;
- la base giuridica del trattamento ai sensi dell'art. 6 del Regolamento (UE);
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- l'indicazione dell'eventuale trasferimento dei dati personali a un paese terzo o a un'organizzazione internazionale, l'esistenza di una decisione di adeguatezza alla base del trasferimento, ovvero il riferimento alle garanzie adeguate, i mezzi per ottenere una copia di tali dati ed il luogo dove sono stati resi disponibili;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- i diritti che l'interessato può esercitare, quali: l'accesso ai dati personali, la rettifica, la cancellazione, la limitazione del trattamento, l'opposizione al trattamento, la portabilità dei dati, il diritto di proporre reclamo al Garante per la protezione dei dati personali e in generale tutti i diritti previsti dagli artt. da 15 a 22 del Regolamento (UE);
- la necessità di comunicare i dati personali in base a un obbligo legale o contrattuale, la natura obbligatoria o facoltativa del conferimento con l'indicazione delle possibili conseguenze in caso di mancato conferimento di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e le conseguenze previste da tale trattamento per l'interessato.

8. Nel caso in cui i dati non siano raccolti presso l'interessato, l'informativa deve contenere oltre che gli elementi suindicati anche le categorie di dati trattati e le relative fonti di provenienza. In questa ipotesi l'informativa deve essere fornita:

- entro un termine ragionevole dall'ottenimento dei dati personali, e comunque non oltre un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
- non oltre la prima comunicazione all'interessato, se i dati personali sono destinati alla comunicazione stessa;

- non oltre la prima comunicazione dei dati personali, se è prevista la comunicazione ad altro destinatario.

Articolo 25. Consenso preventivo dell'interessato e casi in cui il consenso non è necessario.

1. Tra i presupposti giuridici che legittimano il trattamento di dati personali rientra il consenso espresso da ciascun interessato al trattamento dei propri dati personali.
2. Tale consenso deve essere libero (non condizionato da situazioni che potrebbero obbligare l'interessato a fornirlo), espresso (fornito in maniera inequivocabile), informato (fornito a seguito dell'informativa) e modulare (riferito alle singole e specifiche modalità e finalità del trattamento per cui la legge impone la richiesta del consenso[3]).
3. La normativa autorizza il titolare a trattare i dati degli interessati senza il loro espresso consenso per specifiche casistiche fra le quali quelle in cui:
   a. il trattamento è necessario per adempiere a un obbligo contrattuale ovvero ad un obbligo di legge e/o regolamentare;
   b. sussiste un legittimo interesse del titolare;
   c. sussiste il diritto di difesa in giudizio o nelle fasi di pre-contenzioso;
   d. i dati sono pubblici e/o liberamente accessibili, ma solo purché siano utilizzati dal titolare per gli stessi scopi per cui sono stati pubblicati.
4. La funzione di *compliance* fornisce uno schema tipo di consenso.

Articolo 26. Diritti dell'interessato

1. L'Ateneo assicura il rispetto dei diritti dell'interessato di cui agli artt. da 15 a 22 del Regolamento (UE), ponendo in essere le iniziative utili ad un effettivo ed agevole esercizio di tali diritti a tutti gli interessati.
2. Qualora un interessato proceda a esercitare i propri diritti, la funzione di Ateneo cui fa capo il trattamento a cui si riferiscono i reclami dell'interessato deve, nella persona del responsabile del trattamento, attivarsi prontamente per dare seguito agli stessi. A tal fine, ove opportuno, il responsabile del trattamento potrà richiedere delucidazioni al DPO e supporto operativo alle funzioni ICT e di *compliance* nel caso di dubbi sull'effettiva portata dei diritti medesimi.
3. Ulteriori precisazioni sulle modalità di gestione dei diritti dell'interessato inclusi i reclami sono fornite nelle istruzioni agli incaricati, unitamente ai relativi riferimenti normativi.
4. 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 loro comunicazione in forma intelligibile ("diritto di accesso");

[3] Trasferimento a terzi per finalità diverse da quelle dell'informativa; profilazione; comunicazione a terzi autonomi titolari del trattamento oltre all'Ateneo.

b. ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa ("diritto di rettifica");
c. ottenere la cancellazione dei dati personali che lo riguardano, raccolti in forma cartacea o digitale, senza ingiustificato ritardo nonché esercitare il diritto all'oblio in ipotesi di indicizzazione dei dati, chiedendo la cancellazione degli stessi qualora sussista almeno una delle seguenti condizioni indicate dall'art. 17 del Regolamento (UE):
    i. l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento (es: la possibilità e/o necessità dell'Ateneo di potersi difendere in giudizio);
    ii. i dati personali sono trattati illecitamente;
    iii. i dati sono trattati per l'adempimento ad un obbligo legale (es: i dati sul profitto scolastico, ecc.);
    iv. i dati sono stati raccolti relativamente all'offerta di servizi della società dell'informazione e riguardano minori.

    L'Ateneo 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");
f. esercitare il diritto di opposizione ("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").

5. L'interessato può esercitare i suoi diritti con richiesta indirizzata al Responsabile della struttura competente alla gestione dei dati personali oggetto della richiesta o, in alternativa, al Responsabile interno della Struttura stessa o suo Referente, secondo i dati di contatto indicato nelle informative di riferimento.

6. Il riscontro alla richiesta presentata dall'interessato viene fornito dal destinatario della richiesta, come indicato nel comma precedente, in riferimento alla Struttura che ha la gestione del dato di cui si tratta,

senza ingiustificato ritardo e comunque entro 30 giorni dalla data di acquisizione della richiesta al Protocollo, 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 al Protocollo.

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

8. 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.

9. I Responsabili dei trattamenti devono adottare soluzioni organizzative per la gestione delle istanze e possono avvalersi, nei casi più complessi, del supporto del Responsabile della protezione dati. La modulistica per la presentazione delle istanze è disponibile sul sito nazionale dell'autorità Garante.

10. Le richieste di esercizio di diritti da parte degli interessati devono essere tracciate entro e non oltre 30 giorni dalla data di conclusione del procedimento. La gestione è affidata ad ogni struttura per le richieste di rispettiva competenza e non richiede l'utilizzo di strumenti specificamente identificati.

11. Nei casi di trattamenti di dati esternalizzati, il Responsabile esterno, come stabilito nell'ambito dell'atto di nomina, è tenuto a collaborare con l'Università in sede di riscontro delle istanze di esercizio dei diritti presentate dall'interessato e segnalare le stesse con tempestività.

Articolo 27. Istruzioni agli incaricati

1. Le istruzioni definiscono -per ciascun trattamento o insieme di trattamenti- le regole che il responsabile del trattamento e gli incaricati devono seguire per assicurare che tale trattamento sia svolto in conformità a tutto quanto previsto dalle normative applicabili e nel presente regolamento, ossia in modo tale da proteggere la sicurezza e riservatezza dei dati e consentendo agli interessati l'effettivo esercizio dei loro diritti.

2. Le istruzioni si distinguono in generali e specifiche. Le istruzioni generali sono rese disponibili dal titolare a tutti i responsabili del trattamento e agli incaricati; è obbligo, pertanto, di tutti i soggetti precedentemente descritti operare nel rispetto delle medesime.

3. Le istruzioni generali possono essere integrate con istruzioni specifiche (riferite cioè al trattamento per aree specifiche o su tematiche specifiche) dai responsabili del trattamento - con il supporto, ove necessario, della funzione organizzazione competente, delle funzioni di *compliance*, *ICT* e *security*, per gli aspetti di propria competenza – in relazione a ciascun singolo trattamento o insieme di trattamenti che presentino sufficienti elementi di omogeneità, ogni volta che ciò risulti opportuno. Le istruzioni specifiche, in coerenza con le istruzioni generali, sono pubblicate nella intranet di Ateneo o diffuse con altre modalità che ne garantiscano la conoscenza tra tutti i soggetti che, a qualunque titolo, prestano attività nell'Ateneo.

Ognuno di tali soggetti ha la responsabilità di condurre i trattamenti nel rispetto delle istruzioni ricevute. A titolo esemplificativo possono essere considerati omogenei quei trattamenti che prevedono l'utilizzo di strumenti simili per raccogliere le stesse tipologie di dati per le identiche finalità, ad esempio ai sistemi di videosorveglianza installati presso ambienti analoghi (es: uffici, sedi didattiche, data center) oppure trattamenti dei dati dei dipendenti su specifici applicativi, trattamenti dei dati degli studenti, etc.).

4. Il presente regolamento è da considerarsi come insieme di indicazioni di carattere generale con funzione prescrittiva.

Articolo 28. Linee guida per l'elaborazione dei Registri delle attività di trattamento.

1. L'Ateneo detiene più Registri delle attività di trattamento, che vengono redatti e aggiornati da ogni responsabile del trattamento e contengono informazioni relative:
   a. all'elenco dei trattamenti eseguiti nell'area di competenza;
   b. alle finalità del trattamento;
   c. alle categorie di interessati e di dati personali;
   d. ai destinatari a cui i dati sono o saranno comunicati;
   e. ad eventuali trasferimenti, insieme all'indicazione delle garanzie adeguate;
   f. ai responsabili esterni del trattamento nominati;
   g. ai termini ultimi previsti per la cancellazione delle diverse categorie di dati oppure, ove non possibile, ai criteri per determinare tali termini;
   h. alle misure di sicurezza.
2. Le informazioni inserite dai responsabili del trattamento confluiranno in un registro consolidato a cura della funzione *security* che lo renderà disponibile al titolare, al DPO e all'Autorità competente ove ne faccia richiesta.
3. I responsabili del trattamento devono in ogni caso mantenere aggiornati i registri delle attività di trattamento di propria competenza durante tutto l'anno.
4. Al fine di garantire il necessario collegamento ed omogeneità tra i responsabili del trattamento appartenenti alle diverse strutture dell'Ateneo, le competenti funzioni *ICT* e *security* con il supporto dell'unità di *compliance*, si occupano di:
   a. istituire e mantenere un applicativo finalizzato alla redazione e all'aggiornamento dei Registri delle attività di trattamento;
   b. supportare i responsabili del trattamento ai fini del censimento degli archivi elettronici delle diverse aree di competenza.

Articolo 29. Linee guida in materia di Reportistica *privacy*. Reportistica a cura del responsabile del trattamento dati

1. Con cadenza annuale, il responsabile del trattamento dei dati personali invia alle funzioni di *compliance, di security* e al titolare, una attestazione/reportistica contenente indicazioni in merito almeno ai seguenti argomenti:
   a. nuovi trattamenti;
   b. interventi di modifica/aggiornamento delle Istruzioni o la redazione di nuove istruzioni;
   c. elenco dei progetti sottoposti a Data Protection Impact Assessment ricadenti nella sua sfera di operatività attivati nel corso dell'anno di riferimento;
   d. elenco delle iniziative formative in materia di *privacy* alle quali ha preso parte come docente e/o come discente;
   e. elenco delle Violazioni ricadenti nella sua sfera di operatività occorse nell'anno di riferimento e/o degli episodi di sospetta Violazione;
   f. interventi di modifica sostanziali delle misure di sicurezza;
   g. elenco del numero di richieste/Reclami da parte di interessati e ricadenti nella sua sfera di operatività.
2. Nel compilare l'attestazione/reportistica, il responsabile del trattamento si avvale del supporto, ove necessario, della funzione di *compliance* e/o della funzione *security*. È possibile fare diretto riferimento al registro dei trattamenti, con le dovute integrazioni a completamento degli aspetti summenzionati laddove non già riportate nel registro stesso.
3. Copia della documentazione a supporto dell'attestazione/reportistica deve essere archiviata e conservata a cura di ciascun responsabile del trattamento.

Articolo 30. Reportistica a cura del DPO

1. Il DPO riferisce al titolare attraverso la redazione di una relazione annuale sulle attività svolte e sulle questioni in merito alle quali è stato coinvolto.

Articolo 31. Trasferimento dati all'estero

1. Il trasferimento di dati verso Paesi extra UE è consentito solo in presenza di specifiche garanzie in merito al rispetto dei diritti dell'interessato.
2. Ogni volta che l'Ateneo o una partecipata, in qualità di titolare autonomo del trattamento, intenda effettuare un trasferimento di dati personali dall'Unione Europea verso un Paese extra-UE, è necessario verificare se il trasferimento rientri una delle seguenti ipotesi di deroga al divieto:

a. il trasferimento di dati personali è diretto verso un Paese ricompreso nell'elenco dei Paesi che, ai sensi di una decisione di adeguatezza della Commissione Europea, presenta un livello di protezione adeguato tale da fornire idonee garanzie per i diritti dell'interessato[4].

b. il trasferimento di dati personali è disciplinato a livello contrattuale tra le parti tramite l'inserimento di apposite clausole standard adottate dalla Commissione Europea i cui contenuti di dettaglio sono descritti in un allegato del presente regolamento;

c. il trasferimento dei dati è diretto verso gli USA, laddove l'ente importatore abbia aderito formalmente al c.d. *privacy* Shield[5].

3. Il responsabile del trattamento dei dati oggetto di trasferimento dovrà, pertanto, consultare l'unita *compliance* già nella fase di ideazione/pianificazione e, in ogni caso, prima della realizzazione delle attività che prevedano il trasferimento.

Articolo 32. Formazione

1. Al fine di garantire la diffusione, all'interno dell'Ateneo, di una cultura della *privacy* e fornire gli strumenti adeguati per assicurare il rispetto della normativa in materia di dati personali, la funzione di *compliance* competente per le attività di comunicazione e formazione, sviluppa, in coordinamento con le altre funzioni competenti nell'ambito della formazione, campagne di formazione e iniziative specifiche sui temi principali e più rilevanti in materia di *privacy* e *data protection*.

2. L'Università predispone ogni anno, sentito il DPO 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, sentito il RPCT, è integrata e coordinata con la formazione in materia di prevenzione della corruzione nonché con la formazione in tema di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza, accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera l'Università. Ogni sessione formativa prevede, nell'ottica della responsabilizzazione, una prova finale di apprendimento.

[4] Al momento della pubblicazione del presente regolamento, la Commissione Europea ha emanato decisioni di adeguatezza rispetto ai seguenti Paesi: Andorra, Argentina, Canada, Faer Oer, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera, Uruguay. L'elenco aggiornato dei Paesi che forniscono adeguato livello di protezione dei Dati personali è sempre consultabile al link: *http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi;*

[5] Si tratta dell'accordo che regolamenta il trasferimento di dati tra Unione Europea e USA recepito dalla Commissione Europea nel 2016. È possibile verificare lo status di iscrizione dei partecipanti al *Privacy Shield* sul seguente sito web: https://www.*privacy*shield.gov/list.

3. La frequenza delle attività di formazione è obbligatoria e viene considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale.

Articolo 33. Monitoraggio e miglioramenti

1. Il DPO, di intesa con la funzione di *compliance*, effettuerà le attività di monitoraggio in ambito *privacy*, nel rispetto degli strumenti normativi applicabili e delle metodologie e tempistiche ivi individuate.

2. Nel caso in cui sia identificata una violazione dei dati - *data breach* – il Titolare, con il supporto del DPO, dell'unità di *compliance* e della funzione *security,* valuterà se eventuali revisioni del presente regolamento o miglioramenti degli altri strumenti normativi potrebbero prevenire il ripetersi della violazione.

3. Ogni partecipata deve rispondere adeguatamente al fine di rimediare a qualunque criticità emerga nell'ambito della gestione delle proprie attività.

CAPO III
Linee guida per i trattamenti nelle aree di specifico interesse dell'Ateneo

Articolo 34. Trattamento di categorie particolari di dati personali

1. È vietato trattare ai sensi dell'art. 9 del Regolamento (UE) dati personali atti a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento 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, fatti salvi i seguenti casi:
   a. l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali, per una o più finalità specifiche;
   b. 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, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo;
   c. il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
   d. il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
   e. il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
   f. il trattamento è necessario per motivi di interesse pubblico rilevante che deve essere proporzionato alla finalità perseguita;
   g. il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali conformemente alla normativa nazionale in materia o ad un contratto con un professionista della sanità;
   h. il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria nel rispetto dei diritti e delle libertà dell'interessato;
   i. il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità con l'art. 89, paragrafo 1, 2 del Regolamento (UE).

Le misure di garanzia sui dati genetici, biometrici e relativi alla salute, sono definite con apposito provvedimento dal Garante per la protezione dei dati personali, secondo quanto previsto dal Codice in materia di protezione dei dati personali.

Articolo 35. Trattamento di dati personali relativi a condanne penali e reati

1. Il trattamento di dati personali relativi a condanne penali, a reati o a connesse misure di sicurezza, deve avvenire solo sotto il controllo dell'autorità pubblica, se è autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento.

Articolo 36. Accesso civico e trasparenza amministrativa.

1. L'accesso del pubblico ai documenti ufficiali è un trattamento considerato di interesse pubblico e i dati personali, contenuti in documenti conservati presso l'Ateneo, possono essere comunicati nei casi previsti dalla legge al fine di conciliare in riferimento al singolo caso concreto l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi dell'art. 86 del Regolamento (UE).

2. Per i presupposti, le modalità e i limiti relativi all'esercizio del diritto di accesso si richiamano le disposizioni vigenti in materia di Trasparenza amministrativa oltre alle considerazioni incluse negli allegati al presente regolamento e a quanto indicato nell'art. 8.

Articolo 37. Considerazioni relative a comunicazione e diffusione dei dati personali

1. L'Ateneo può comunicare ad altre pubbliche amministrazioni e diffondere, anche sui propri siti web: i nominativi del proprio personale e dei collaboratori, informazioni sul ruolo ricoperto, i recapiti telefonici e gli indirizzi telematici istituzionali.

2. Fermo restando le norme vigenti in materia di accesso ai documenti amministrativi, e le norme vigenti in materia di scambio di dati tra enti pubblici, la comunicazione di dati è sempre ammessa per i fini istituzionali ove prevista da norma di legge o, nei casi previsti dalla legge, di regolamento, ai sensi dell'art. 2-ter del Codice in materia di protezione dei dati personali, ovvero, in mancanza, quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali.

3. L'Ateneo, al fine di agevolare l'orientamento, le esperienze formative e professionali e l'eventuale collocazione nel mondo del lavoro, anche all'estero, può, su richiesta degli interessati, comunicare o diffondere, anche a privati e per via telematica: dati relativi agli esiti formativi, intermedi e finali degli studenti e altri dati personali diversi da quelli previsti dagli artt. 9 e 10 del Regolamento UE, dati ed elenchi riguardanti studenti, diplomati, laureandi e laureati, specializzati, borsisti, dottorandi, assegnisti, e altri profili formativi, nonché di soggetti che hanno superato l'esame di stato.

4. L'Ateneo può comunicare altresì, a finanziatori di borse di dottorato e assegni, anche stranieri, dati comuni relativi a dottorandi e assegnisti che abbiano usufruito dei finanziamenti.

5. In considerazione del sistema di autovalutazione, accreditamento e valutazione periodica dei Corsi di studio definito dal MIUR, l'Ateneo può elaborare e/o comunicare le opinioni degli studenti sulla didattica agli organismi deputati ad effettuare verifiche della qualità della didattica. Tali dati sono trattati con lo scopo di definire azioni volte al miglioramento della qualità della didattica.

Articolo 38. Trattamento nell'ambito del rapporto di lavoro

1. 1. L'Ateneo 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. L'Ateneo garantisce ai dipendenti l'esercizio dei diritti previsti dagli articoli da 12 a 22 del Regolamento (UE).
3. L'Ateneo adotta misure tecniche e organizzative atte a garantire la tutela delle prerogative individuali e sindacali come disposte dalla normativa italiana, in particolare dallo Statuto dei lavoratori e dalle norme che lo richiamano, oltre che dalle regole deontologiche promosse dal Garante per la protezione dei dati personali.
4. L'Ateneo può comunicare a soggetti pubblici e privati dati comuni del personale che, in ragione di una qualità professionale specifica, usufruisce di corsi di formazione forniti in accordo con altri Enti pubblici, con lo scopo di migliorarne la fruibilità e di garantire la qualità e l'efficacia della formazione sul territorio nazionale.
5. 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.
6. Non è dovuto il consenso da parte dell'interessato al trattamento dei dati personali presenti nei curricula spontaneamente trasmessi, quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.

Articolo 39. Comunicazione e diffusione dei dati relativi ad attività di studio e ricerca

1. Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico l'Ateneo può, ai sensi dell'art.100 del Codice in materia di protezione dei dati personali, 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 dei trattamenti di categorie particolari di dati personali e dei trattamenti dei dati personali relativi a condanne penali e reati .
2. I dati relativi ad attività di studio e di ricerca non costituiscono documenti amministrativi ai sensi della legge 7 agosto 1990, n. 241 e possono essere trattati per i soli scopi in base ai quali sono comunicati o diffusi.
3. L'Ateneo può comunicare eventuali informazioni inerenti produttività scientifica, i riconoscimenti e i fondi acquisiti da singoli, da gruppi o da specifici settori scientifico-disciplinari, anche nell'ambito di procedure di valutazione di richieste di finanziamento o di progetti di ricerca, al fine di:
    a. promuovere modelli di programmazione delle attività di ricerca e di allocazione delle risorse secondo meccanismi che consentano di garantire trasparenza nella definizione delle priorità,

di valorizzare adeguatamente le capacità dei singoli e dei gruppi e di rispettare i principi di trasparenza ed equità di trattamento;

b. favorire la cooperazione tra singoli e gruppi mediante una precisa conoscenza dei risultati conseguiti, allo scopo di migliorare la capacità di attrarre finanziamenti esterni o di istituire forme di collaborazione strutturata con soggetti terzi;

c. fornire orientamento e sostegno per lo sviluppo di modelli organizzativi di supporto alla ricerca, anche tramite la realizzazione di analisi comparative e la condivisione di buone pratiche.

4. L'Ateneo può comunicare dati personali a soggetti pubblici che abbiano erogato dei finanziamenti per la ricerca, ai fini di rendicontazione e per consentire elaborazioni statistiche.

Articolo 40. Diffusione delle valutazioni d'esame

1. In ottemperanza ai principi di trasparenza cui l'Ateneo si ispira e al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, è consentita la pubblicazione dei dati inerenti alle valutazioni d'esame anche sui siti web di Ateneo.

2. La pubblicazione dei dati di cui al comma precedente sui siti web 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. I tempi di pubblicazione sono definiti dal corpo normativo dell'Ateneo nel rispetto della normativa vigente.

Articolo 41. Diffusione dei risultati di concorsi e selezioni

1. In ottemperanza ai principi di trasparenza cui l'Ateneo si ispira, è consentita la pubblicazione di esiti di prove concorsuali e selettive, nonché delle relative graduatorie, anche sui siti web di Ateneo.

2. La pubblicazione dei dati sui siti web è effettuata nel rispetto del principio della minimizzazione dei dati, mediante la diffusione dei dati strettamente necessari al raggiungimento delle finalità per le quali sono pubblicati.

3. Nel caso di diffusione delle valutazioni sui siti web di Ateneo, tali informazioni sono pubblicate per un periodo di tempo non superiore a quello che consente l'impugnazione della graduatoria (120 gg. dalla pubblicazione).

Articolo 42. Trattamento ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a ai fini statistici

1. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato garantendo il rispetto dei diritti e delle libertà dell'interessato in applicazione del principio della

minimizzazione dei dati, delle relative autorizzazioni generali del Garante e dei relativi codici deontologici in materia.

2. I dati dovranno essere trattati con misure tecniche e organizzative adeguate che non consentano di identificare l'interessato, al solo scopo di perseguire le finalità di archiviazione nel pubblico interesse o di ricerca storica.

3. La consultazione dei documenti di interesse storico conservati negli archivi dell'Ateneo è disciplinata dal decreto legislativo 22 gennaio 2004, n. 42, dalle relative regole deontologiche e dal corpo normativo di Ateneo in materia.

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 di dati sono stati in precedenza raccolti o trattati, secondo quanto previsto dall'art. 99 del Codice in materia di protezione dei dati personali.

5. Per il raggiungimento di tali finalità, possono 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'art. 89 paragrafo 1 del Regolamento (UE).

Articolo 43. Trattamento ai fini di ricerca medica, biomedica ed epidemiologica

1. Non è necessario il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea, ivi incluso il caso in cui la ricerca rientri in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del d.lgs. 30 dicembre 1992, n. 502, e sia condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento (UE).

2. Il consenso non è altresì necessario quando, a causa di particolari ragioni, informare gli interessati risulti impossibile o implichi uno sforzo sproporzionato, oppure vi sia un rischio reale di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il Responsabile scientifico della ricerca adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato. Il progetto di ricerca deve essere sottoposto a preventiva consultazione del Garante per la protezione dei dati personali.

3. In caso di esercizio del diritto di rettifica e integrazione dei dati personali da parte dell'interessato, la rettifica e l'integrazione dei dati sono annotate senza modificare questi ultimi, quando il risultato di tali operazioni non produca effetti significativi sul risultato della ricerca.

4. Ai fini del trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici, si applica quanto disposto dall'art. 110-bis del Codice in materia di protezione dei dati personali.

Articolo 44. Videosorveglianza

1. L'Ateneo può utilizzare, in qualità di ente pubblico, gli impianti di videosorveglianza per finalità istituzionali, di didattica e di ricerca. L'Ateneo può utilizzare tali impianti ai sensi e nel rispetto di quanto stabilito all'art. 4, c. 1 e 2, della L. 300/1970 e ss.mm. (cd. "Statuto dei lavoratori"). Gli impianti di videosorveglianza possono essere utilizzati altresì per esigenze organizzative, per la sicurezza del lavoro e per la tutela del patrimonio dell'ente
2. Il trattamento effettuato tramite i sistemi di videosorveglianza dovrà, in ogni caso, rispettare i principi elencati all'art. 5 del Regolamento (UE), così come quanto stabilito nel provvedimento del Garante sulla videosorveglianza del 10 aprile 2010 ed eventuali successive modifiche, nonché le norme indicate nella regolamentazione di Ateneo di riferimento.
3. Il trattamento di dati personali connesso agli impianti di videosorveglianza deve essere effettuato altresì nel rispetto:
    a. del principio di proporzionalità, nella scelta delle modalità di ripresa e dislocazione, nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite;
    b. del principio di necessità, il quale comporta un obbligo di attenta configurazione di sistemi informativi e di programmi informatici per ridurre al minimo l'utilizzazione di dati personali.
4. Le strutture, nel rispetto del principio di *accountability*, sono tenute a individuare, documentare e verificare la necessità, le finalità e le caratteristiche dell'installazione delle telecamere.
5. Le strutture comunicano, con congruo preavviso, la creazione, la modifica o la dismissione degli impianti di videosorveglianza alla Dirigenza dell'Area Edilizia, Logistica e Sostenibilità, che ha il compito di censimento, gestione e manutenzione dei suddetti impianti, di monitoraggio compreso quello di audit della relativa cartellonistica e informativa. La Direzione Edilizia, Logistica e Sostenibilità, in sinergia con la Dirigenza dell'Area Sistemi Informativi, Portale, E-Learning, verificano l'adeguatezza delle misure di sicurezza tecniche dell'impianto e il relativo aggiornamento. Le sopra citate Dirigenze di Area adottano e aggiornano le relative policy in materia.
6. I dati personali raccolti tramite il sistema di videosorveglianza potranno essere comunicati in caso di indagini alla polizia giudiziaria o altra autorità competente.
7. I soggetti autorizzati al trattamento di dati personali connessi ai sistemi di videosorveglianza, sono tenuti a partecipare alle iniziative di informazione e ai corsi di formazione in materia, in armonia con quanto previsto dalla normativa vigente in tema di protezione dei dati personali.

8. 8. Solo il personale autorizzato può avere accesso alle immagini ed è sottoposto a tutti i vincoli di riservatezza previsti dall'atto di nomina che ha ricevuto nonché ad applicare scrupolosamente e diligentemente le istruzioni fornite.

9. La conservazione delle immagini deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o servizi, in ogni caso non superiori alla settimana nel rispetto delle indicazioni del Garante. Solo in alcuni casi, per peculiari esigenze tecniche o per la particolare rischiosità dell'attività svolta dal titolare del trattamento, nonché su richieste delle competenti autorità, può ritenersi ammesso un tempo più ampio di conservazione dei dati.

10. Resta ferma la necessità di effettuare una valutazione di impatto (DPIA), nei casi previsti dalla normativa e dalle Linee guida dei Garanti europei e nazionale, ai sensi dell'art. 30, comma 3, lettera c) del Regolamento (UE), ogni qualvolta vengano installate apparecchiature di videosorveglianza in ambienti o zone accessibili al pubblico.

Articolo 45. Trattamento dei dati nelle sedute degli organi collegiali di ateneo

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

2. Per la trattazione di argomenti inerenti sviluppo strategico dell'Ateneo, rapporti con gli operatori economici e altri soggetti privati e la tutela della riservatezza dei dati personali, è esclusa, in applicazione del regolamento europeo sulla protezione dei dati personali, la diffusione in qualsiasi forma, ivi compreso lo streaming e le videoriprese, ferma restando l'informazione sulle decisioni degli Organi.

3. Il Presidente dell'Organo Collegiale può avvalersi della consulenza del Responsabile della Protezione dei Dati.

Articolo 46. Sanzioni amministrative

1. Fermo restando quanto previsto dagli artt. 58, 82, 83 e 84 del Regolamento (UE) e dall'art. 166 del Codice in materia di protezione dei dati personali, 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'Ateneo anche sulla base di quanto disposto dai CCNL, dal Codice etico e dai Codici di comportamento.

Articolo 47. Informative e liberatorie per l'utilizzo di materiale audio/video/fotografico

1. In considerazione della natura particolare dei dati personali rappresentati da riprese fotografiche, video e di cattura di registrazioni audio che rendano facilmente identificabile gli interessati, a prescindere dalla finalità del trattamento, è richiesta la raccolta del consenso al trattamento.

2. Il trattamento, che può successivamente prevedere la diffusione e pubblicazione del materiale per specifiche finalità e con specifiche modalità, dovrà quindi prevedere la somministrazione di una informativa redatta secondo i principi elencati nel presente Regolamento, accompagnata dalla raccolta del consenso (c.d. liberatoria).

3. L'interessato autorizzerà il trattamento, oltre che per le finalità indicate nell'informativa, a titolo gratuito, senza limiti di tempo, anche ai sensi degli artt. 10 e 320 cod. civ. e degli artt. 96 e 97 legge 22.4.1941, n. 633, Legge sul diritto d'autore. Inoltre, l'interessato dichiarerà di non aver nulla a pretendere in ragione di quanto indicato e di rinunciare irrevocabilmente ad ogni diritto, azione o pretesa derivante da quanto autorizzato.

4. Il conferimento del consenso al trattamento dei dati personali è facoltativo se non strettamente correlato al funzionamento dell'attività o al servizio proposto. In qualsiasi momento è possibile esercitare tutti i diritti indicati degli artt. 15 a 22 e dell'art. 34 del GDPR, in particolare la cancellazione, la rettifica o l'integrazione dei dati.

5. Qualora l'organizzazione di eventi che prevedono l'acquisizione di materiale audio/foto/video renda difficoltosa o particolarmente onerosa la raccolta dei consensi firmati, considerando la portata del trattamento e le condizioni specifiche del contesto, può essere sufficiente informare in modo adeguato ed inequivocabile i partecipanti relativamente alle operazioni di registrazione in atto

   a. con opportuni avvisi ben visibili ed apposti ad ogni punto di ingresso nei locali adibiti all'evento, riportando fra le altre informazioni anche i diritti degli interessati
   b. informando i partecipanti al momento dell'inizio dell'evento, e
   c. riservando spazi opportunamente indicati che si avrà cura di non sottoporre a registrazione.

L'utilizzo di questo approccio richiede in modo tassativo la raccolta di evidenze relative agli adempimenti messi in atto secondo i punti summenzionati.

6. La funzione di *compliance* mette a disposizione delle strutture e funzioni preposte alla comunicazione di Ateneo uno schema tipo per l'informazione e la raccolta del consenso all'utilizzo di materiale audio//video/fotografico.

CAPO IV
Disposizioni finali ed attuazione

Articolo 48. Disposizioni finali

1. Per quanto non espressamente previsto dal presente Regolamento si rinvia alle disposizioni del Regolamento UE e del Codice per la protezione dei dati personali, oltre che a quanto previsto dalle Linee guida e di indirizzo, dalle policy di Ateneo e dalle Regole deontologiche adottate e approvate dal Garante per la protezione dei dati personali.
2. Costituiscono parte integrante e sostanziale del presente Regolamento tutti gli allegati che ad esso si riferiscono in quanto connessi ad ambiti specifici in esso contenuti, anche redatti successivamente alla sua emanazione.

Articolo 49. Norma di attuazione

1. L' allegato 1 al presente regolamento individua le attuali strutture dell'Ateneo competenti a svolgere le funzioni elencate nelle lettere a), b) e c) dell'art. 4, con riferimento al vigente funzionigramma.
2. Le modifiche del contenuto dell'allegato 1 non comportano la modifica del Regolamento.
3. Il presente regolamento, emanato con decreto rettorale, entra in vigore il giorno successivo alla data di pubblicazione sul sito informatico dell'Università.

ALLEGATO 1

Elenco strutture competenti a svolgere le funzioni di cui all'art. 4, comma 1:

a. l'Unità Organizzativa Legale per la funzione *compliance*
b. l'Area Sistemi Informatici (ASI) per la funzione *ICT*
c. l'Unità Organizzativa Sicurezza e Processi IT afferente all'ASI per la funzione security