Università degli Studi di Perugia

Regolamento sul trattamento dei dati personali

in attuazione del R.UE. 679/2016 e del D.lgs. 196/2003

<pagina lasciata intenzionalmente bianca>

Sommario

Art. 1. Ambito di applicazione

1. L'Università degli Studi di Perugia adotta il presente Regolamento quale misura organizzativa necessaria a dare attuazione alla protezione dei dati di carattere personale trattati nell'Ateneo, direttamente o indirettamente riconducibili a persone fisiche, secondo le previsioni del Regolamento (UE) 27 aprile 2016, n. 679 e del D. Lgs. n. 196/2003, come novellato dal D. Lgs. n. 101/2018.
2. La delicatezza e la complessità della materia richiedono una particolare attenzione da parte del personale dell'Ateneo in ciascun contesto della propria attività, data la diversità delle modalità e delle finalità con cui i dati personali, siano essi comuni o particolari (*cd* "sensibili" nella previgente normativa), vengono trattati nell'ambito universitario.
3. L'Università considera una propria azione prioritaria il trattamento dei dati personali in modo lecito, corretto e trasparente nei confronti di ciascun soggetto interessato.
4. Tutti coloro che trattano dati personali all'interno dell'Università, per l'espletamento dei propri compiti o perché espressamente a ciò autorizzati, devono effettuare il trattamento secondo quanto stabilito dalla normativa in materia, di cui al successivo articolo 2, e dal presente Regolamento.
5. Ogni persona ha la responsabilità dei dati personali, dei quali effettua trattamenti nell'ambito dell'espletamento dell'attività lavorativa, e della loro protezione, per assicurare il rispetto dei diritti e delle libertà fondamentali, della dignità dell'Interessato e del diritto alla protezione dei dati personali.

Art. 2. Contesto normativo

1. L'attuale normativa in materia di protezione dei dati personali si articola in disposizioni di fonte europea e di matrice nazionale, di rango legislativo e sub-legislativo.
2. Le disposizioni generali attualmente vigenti e non derogabili sono rappresentate da:
   a) Regolamento Europeo 679/2016 (cd. GDPR): normativa direttamente efficace e vincolante per gli Stati Membri e per tutti i cittadini. Ha rango superiore rispetto alla legge, pertanto, in caso di conflitto tra le due tipologie di fonti, va disapplicata la legge nazionale contrastante e applicata quella dell'Unione;
   b) D.lgs. 196/03 Codice in materia di protezione dei dati personali (cd. Codice privacy), entrato in vigore nel 2003 e tuttora vigente, come integrato dalle modifiche introdotte dal D.lgs. 101/2018, che lo ha adeguato alla disciplina europea.
3. Integrano la disciplina normativa di rango normativo in materia di protezione dei dati personali i cosiddetti atti di "soft law". Consistono nel complesso di strumenti e documenti operativi che, sebbene privi di forza legale vincolante, nondimeno hanno efficacia giuridica pratica in virtù dei poteri e compiti assegnati dal GDPR e dal Codice privacy agli organismi che li emettono:
   a) Le linee guida del Comitato europeo per la protezione dei dati (EDPB) e i pareri del Comitato ex art. 29 (cd. WP29);
   b) Le Autorizzazioni generali, le Regole deontologiche e le linee guida del Garante per la protezione dati personali;
   c) I Provvedimenti del Garante per la Protezione dei dati personali, emanati nell'esercizio dei poteri ed in esecuzione dei compiti e poteri attribuiti all'Autorità garante dagli artt. 57 e 58 GDPR, 154 - 154 ter del D.Lgs. 196/2003.

Art. 3. Definizioni

Si intende per:

a) **Dato personale**: l'informazione che identifica o rende identificabile, direttamente o indirettamente, una persona fisica. La nozione ricomprende anche i dati che possono fornire informazioni sulle sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, culturale o sociale, la sua ubicazione, gli identificativi o in generale gli elementi caratteristici della sua identità on line, le sue fotografie, video e tracce audio.

b) **Categorie particolari di dati**: i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, dati biometrici atti a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale;

c) **Dati genetici**: i dati personali relative alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

d) **Dati biometrici**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

e) **Dati relativi alla salute**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

f) **Dati giudiziari**: dati relativi a condanne penali e a reati (cd. giudiziari) di una persona direttamente o indirettamente identificabile, anch'essi soggetti ad un regime particolare di trattamento;

g) **Dato anonimo**: informazioni raccolte senza alcun riferimento ad una persona fisica identificata o identificabile a cui il dato potrebbe riferirsi, cui non si applica la normativa europea e nazionale in materia di protezione dei dati personali;

h) **Trattamento**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali (ad es. raccolta, registrazione, conservazione, estrazione, consultazione, uso, comunicazione, trasmissione, raffronto e interconnessione, diffusione, cancellazione, distruzione);

i) **Comunicazione**: tipo di trattamento consistente nel dare conoscenza dei dati personali a uno o piu' 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 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 (comma 4 art. 2-ter Codice privacy);

j) **Diffusione**: è un tipo di trattamento consistente nel dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione o pubblicazione su sito internet;

k) **Confidenzialità**: termine che indica la protezione dei dati e delle informazioni scambiate tra un mittente e uno o più destinatari nei confronti di terze parti;

l) **Anonimizzazione**: procedimento che ha lo scopo di impedire irreversibilmente l'identificazione dell'Interessato a partire dai dati trattati. E' una misura di sicurezza tecnica applicabile al trattamento dei dati;

m) **Pseudonimizzazione**: il trattamento dei dati personali finalizzato ad ottenere che i dati

personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative volte a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile. Proprio perché tale attribuzione resta possibile, i dati pseudonimizzati devono essere trattati come informazioni relative a una persona fisica identificabile, seppure in via indiretta, diversamente dai dati anonimi;

n) **Profilazione**: qualsiasi forma di trattamento automatizzato di dati personali che utilizzi tali dati personali per valutare determinati aspetti personali relativi ad una persona fisica, in particolare per analizzare o prevedere aspetti inerenti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
o) **Interessato**: la persona fisica identificata o identificabile attraverso i dati o le informazioni;
p) **Titolare**: è la persona fisica o giuridica, l'autorità pubblica o altro organismo che assume le decisioni in ordine alle finalità e ai mezzi del trattamento dei dati personali, ivi compreso il profilo della sicurezza dei trattamenti;
q) **Responsabile del Trattamento**: ai sensi del GDPR, è la persona fisica o giuridica, diversa dal Titolare del Trattamento, che tratta dati personali per conto di quest'ultimo. Il Responsabile si colloca al di fuori dell'organizzazione presieduta dal Titolare (cd. Responsabile esterno del trattamento);
r) **RPD o DPO**: è il Responsabile della protezione dati che, tra le altre attività previste all'art. 39 GDPR, fornisce consulenza al Titolare e al personale, vigila sull'osservanza del GDPR e funge da punto di contatto con il Garante per la protezione dei dati personali e con gli Interessati;
s) **Destinatario**: la persona fisica o giuridica, il servizio o un altro organismo o autorità pubblica che riceve comunicazione dei dati personali, che si tratti o meno di terzi;
t) **Terzo**: è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'Interessato, il Titolare del trattamento, il Responsabile del trattamento e gli Autorizzati al trattamento;
u) **Informativa**: informazioni che, ai sensi degli artt. 13 e 14 GDPR, il Titolare del trattamento deve fornire all'Interessato per comunicargli come i suoi dati verranno trattati, per quale finalità, con quali mezzi, per quanto tempo, da chi e come l'Interessato potrà far valere i suoi diritti;
v) **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 indubitabile, a che i dati personali che lo riguardano siano oggetto di trattamento;
w) **Misure tecniche e organizzative**: misure che il Titolare del trattamento deve porre in essere al fine di garantire, ed essere in grado di dimostrare, che il trattamento è effettuato in conformità alla normativa sul trattamento dei dati personali, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche;
x) **Valutazione d'impatto sulla protezione dei dati (DPIA)**: procedura atta a descrivere l'attività di trattamento, valutarne la particolare probabilità e gravità del rischio tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio. La valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio assicurando la protezione dei dati personali e dimostrando la conformità dell'attività di trattamento alla normativa in materia di protezione dei dati personali;

y) **Data Breach**: violazione dei dati personali che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali memorizzati, trasmessi o comunque elaborati.

Art. 4. Principi Generali

1. Il trattamento dei dati personali viene effettuato dall'Università in applicazione dei principi previsti dall'art. 5 del GDPR:

   a) Liceità, Correttezza e Trasparenza: i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato. Il trattamento è lecito se sussiste almeno una base giuridica, come indicato nel successivo paragrafo.

   b) Limitazione della finalità: i dati devono essere raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità. L'ulteriore trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici risulta compatibile con le finalità iniziali.

   c) Minimizzazione dei dati: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Non bisogna acquisire dati non strettamente necessari alle finalità dichiarate all'Interessato né trattarli per un periodo di tempo superiore al raggiungimento delle stesse finalità.

   d) Esattezza: i dati personali devono essere esatti e, se necessario, aggiornati, con conseguente obbligo di cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

   e) Limitazione della conservazione nel tempo: i dati personali trattati devono essere conservati in una forma che consenta l'identificazione degli Interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono stati raccolti. È ammessa una conservazione più lunga a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici e fatta salva l'adozione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà, richieste dal Regolamento UE 679/2016.

   f) Integrità e riservatezza: i dati personali devono essere trattati in modo da garantire ad essi un'adeguata sicurezza e la protezione dai trattamenti illeciti o non autorizzati, dalla perdita, dalla distruzione o dal danno accidentali, mediante l'adozione di misure tecniche e organizzative adeguate.

2. L'Università assicura, nell'operato del proprio personale, che siano trattati per impostazione predefinita solo i dati necessari per ogni specifica attività di trattamento, con riguardo alla quantità dei dati personali raccolti, alla portata del trattamento, ai tempi di conservazione e all'accessibilità, nonché alla conoscibilità derivante da obblighi di legge o richiesta dall'azione amministrativa.

3. Il principio della libera circolazione delle informazioni, in funzione del raggiungimento delle finalità istituzionali, ispira la disciplina dell'accesso e dell'utilizzo dei dati all'interno delle strutture da parte del personale universitario, in un'ottica di bilanciamento tra i diritti e le libertà dell'interessato e l'interesse pubblico all'espletamento delle attività istituzionali. Il trattamento dei dati personali, connesso con lo svolgimento dell'attività inerente alla propria specifica funzione, è consentito nella misura necessaria e al solo fine del perseguimento dell'interesse istituzionale. Resta ferma, nella comunicazione tra strutture e persone, la responsabilità del richiedente derivante dall'utilizzo improprio dei dati.

Art. 5. Base giuridica del trattamento

1. L'Università degli Studi di Perugia è un'istituzione pubblica di alta cultura, che opera in conformità ai principi della Costituzione e agli impegni internazionali assunti dall'Italia in materia di ricerca scientifica e di formazione universitaria. I fini primari dell'Università sono la ricerca scientifica, il trasferimento dei suoi risultati e la formazione superiore.
2. I trattamenti effettuati per il raggiungimento dei propri fini istituzionali trovano fondamento principalmente nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare (art. 6 par.1 lettera e) GDPR). Diversamente, possono essere effettuati per adempiere un obbligo legale cui è soggetto il titolare (art. 6 par.1 lettera c) o perché necessari all'esecuzione di un contratto di cui l'interessato è parte o per l'esecuzione di misure precontrattuali adottate su richiesta dell'interessato (art. 6 par.1 lettera b). In tali casi non necessitano del consenso dell'interessato.
3. 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 (art. 2 ter d.lgs. 196/03).
4. Le finalità di interesse pubblico rilevante relativo a trattamenti effettuati nell'esercizio di pubblici poteri o nello svolgimento di compiti di interesse pubblico sono quelle riportate all'art. 2-sexies comma 2 del Codice privacy.
5. Gli ulteriori trattamenti di dati sono leciti solo se sussiste una base giuridica alternativa che, ai sensi dall'art. 6, lett. a), d) ed f) del GDPR può consistere rispettivamente nella manifestazione del consenso, salvaguardia di interessi vitali dell'interessato o di un terzo o legittimo interesse del Titolare.
6. Il consenso e il legittimo interesse non possono essere applicati, come base giuridica, al trattamento di dati personali effettuato dall'Università nell'esecuzione dei suoi compiti istituzionali.
7. L'eventuale consenso al trattamento deve essere libero, specifico, informato e inequivocabile; non è ammesso il consenso tacito o presunto e deve poter essere revocabile in qualsiasi momento con la stessa facilità con cui è stato prestato. In caso di minore età il consenso deve essere prestato dagli esercenti la responsabilità genitoriale.
8. Il trattamento deve sempre essere necessario al perseguimento dei fini per i quali viene lecitamente effettuato ("principio di necessità").
9. Il legittimo interesse richiede un'attenta valutazione del bilanciamento tra l'interesse perseguito dal Titolare e gli interessi o i diritti e le libertà fondamentali dell'interessato, specie se minore d'età.
10. Per le ulteriori condizioni di liceità richieste per il trattamento dei dati particolari si rinvia agli artt. 20 e seguenti del presente Regolamento.

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

1. L'Università di Perugia dà attuazione alla normativa in materia di trattamento dei dati personali attraverso l'adozione di misure tecniche e organizzative adeguate a garantire la conformità del trattamento al GDPR e al Codice privacy, tenendo conto della natura, dell'ambito di applicazione, del contesto, della base giuridica e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

   Le suddette misure sono periodicamente riesaminate e aggiornate, tenuto conto dello stato dell'arte e dell'evoluzione tecnologica.

2. La valutazione di adeguatezza del livello di sicurezza, che le misure tecniche e organizzative possono garantire, presuppone l'effettuazione dell'analisi dei rischi che il trattamento presenta e che possono derivare, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai dati personali trasmessi, conservati o comunque trattati.
3. Le misure tecniche possono comprendere appositi Regolamenti, guide tematiche o schede tecniche, tra cui la Procedura per l'effettuazione della Data Protection Impact Assessment (DPIA), approvate dagli organi di governo dell'Ateneo e aggiornate periodicamente.
4. Le misure organizzative sono volte ad attuare in maniera efficace i principi di protezione dei dati personali, anche attraverso la formazione continua del personale, la procedura di gestione delle violazioni di dati ed ogni altra documentazione volta a fornire indicazioni operative, nelle varie e specifiche attività di trattamento dei dati personali e particolari nel contesto universitario.
5. I documenti che integrano le misure tecniche e organizzative per la protezione dei dati personali o che forniscono istruzioni per il trattamento dei dati personali, ai sensi dell'art. 29 GDPR, sono pubblicati sul sito istituzionale dell'Ateneo, all'interno delle aree riservate o, se di portata generale, nel portale d'ateneo www.unipg.it.
6. L'Università, ai sensi dell'art. 2-*quaterdecies* d.lgs. 196/03*,* attribuisce funzioni e compiti in materia di trattamenti di dati personali attraverso la nomina dei soggetti di cui agli articoli successivi, promuove la collaborazione tra questi, il Responsabile della prevenzione della corruzione e della trasparenza, il Responsabile della protezione dati personali e il Responsabile per la transizione al digitale per creare, a livello istituzionale, una sinergia tra i processi e le direttive relative alla gestione del trattamento dei dati personali e l'adozione di misure di sicurezza dei sistemi informatici.

Art. 7. Tipologie di dati personali e Registro delle attività di trattamento

1. L'Università, in qualità di Titolare (di cui al successivo art. 8), effettua numerosi trattamenti di dati personali per lo svolgimento delle proprie finalità istituzionali, come individuate da disposizioni di legge, statutarie e regolamentari, nei limiti posti dalla normativa in materia. L'Università tratta, a titolo esemplificativo e non esaustivo, le seguenti tipologie di dati.
    a) I dati personali comuni: dati anagrafici, codice fiscale, documento di identità, dati di contatto, dati economico-finanziari, reddituali, curriculum vitae, dati di carriera universitaria, credenziali e informazioni d'accesso a servizi informatici;
    b) I dati particolari: dati relativi allo stato di salute, dati idonei a rivelare l'appartenenza a partiti politici, sindacati, associazioni/organizzazioni a carattere religioso o assistenziale, dati che rivelino situazioni di disagio psichico o sociale, dati biologici, biometrici e genetici, questi ultimi in prevalenza per le attività di ricerca;
    c) I dati giudiziari: dati in materia di casellario giudiziale o relativi a misure di sicurezza o alla qualità di imputato o di indagato; dati inerenti procedure di conciliazione, procedimenti civili, penali, amministrativi, di carattere disciplinare.
2. Le suddette categorie di dati personali e le attività di trattamento che li hanno ad oggetto sono documentate e costantemente aggiornate dall'Università, ai sensi dell'art. 30 GDPR nel:
    a) Registro del Titolare, con riferimento alle attività di trattamento di cui l'Università definisce i mezzi e le finalità (art. 30, par. 1 GDPR),
    b) Registro del Responsabile, con riferimento alle attività di trattamento che l'Università effettua

per conto di un soggetto terzo (art 30, par. 2 GDPR).

3. I Registri descrivono il trattamento fornendo le informazioni previste dall'art. 30 GDPR e quelle ritenute utili dal Titolare in accordo con il Responsabile della protezione dati personali di cui al successivo art. 11.
4. Il Registro rappresenta sia una misura tecnico-organizzativa che permette al Titolare di monitorare le attività di trattamento e di verificare che le stesse siano conformi alla normativa in materia, sia uno strumento indispensabile per l'analisi del rischio per gli interessati.
5. È onere di ogni Struttura, attraverso i soggetti espressamente a ciò incaricati, tenere aggiornato il Registro secondo le istruzioni, le modalità e la periodicità espressamente indicate dal Titolare, prestando particolare attenzione alla caratterizzazione dei trattamenti e delle modalità analogiche o informatiche con cui essi vengono effettuati, nonché degli archivi in cui viene effettuata la conservazione dei dati.

Art. 8. Titolare del trattamento dei dati

1. Il Titolare del trattamento dei dati è l'Università nel suo complesso, nella persona del Rettore, rappresentante legale pro tempore.
2. Tenuto conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Titolare adotta misure tecniche e organizzative atte a comprovare di essersi adeguato alla normativa sulla protezione dei dati personali ("principio di responsabilizzazione del Titolare").
3. Il Titolare è tenuto, altresì, alla redazione e aggiornamento dei Registri delle attività di trattamento di dati personali di cui al precedente art. 7, alla effettuazione della valutazione dei rischi che queste possono determinare sui diritti e le libertà degli Interessati e, ove necessario, alla Valutazione d'impatto o DPIA (art. 16).
4. Il Titolare promuove ogni opportuno strumento di informazione e sensibilizzazione per consolidare la consapevolezza del valore della protezione dei dati personali e predispone ogni anno, sentito il Responsabile per la protezione dati, un piano formativo in materia di trattamento dei dati personali e di prevenzione dei rischi di violazione, al fine di garantire una gestione delle attività di trattamento informata, responsabile ed aggiornata. Tale formazione è integrata e coordinata con le attività pianificate in materia di prevenzione della corruzione nonché in tema di trasparenza e di accesso agli atti, ai documenti, ai dati ed alle informazioni. La frequenza è obbligatoria per tutti coloro che trattano dati personali.
5. Nel caso di trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, l'Università assicura che non sia pregiudicato il livello di protezione delle persone fisiche provvedendo all'adozione delle garanzie adeguate che permettano all'interessato diritti azionabili e mezzi di ricorso effettivi, previste al Capo V del GDPR.
6. Il Titolare coopera con il Garante per la protezione dei dati personali, con il supporto del Responsabile della protezione dati (art. 11).

Art. 9. Contitolare del trattamento dei dati

1. Quando uno o più Titolari del trattamento determinano congiuntamente con l'Università le finalità e i mezzi del trattamento, essi sono Contitolari del trattamento.

2. I Contitolari del trattamento determinano in modo trasparente, mediante un accordo formale, i rispettivi obblighi in merito all'osservanza del GDPR, con particolare riguardo alla collaborazione per l'esercizio dei diritti dell'Interessato e alle rispettive funzioni nella comunicazione delle informazioni a lui dovute, salvo che tali aspetti non siano già definiti dal diritto europeo o nazionale.
3. L'accordo riflette adeguatamente i rispettivi ruoli relativamente alle attività svolte e alle responsabilità assunte nel trattamento dei dati personali, con riguardo anche ai rapporti tra i Contitolari e gli Interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'Interessato.
4. L'Interessato può esercitare i propri diritti nei confronti di ciascun Contitolare del trattamento.

Art. 10. Responsabile del trattamento

1. Il Responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento, secondo quanto disciplinato all'art. 28 GDPR.
2. I trattamenti effettuati da un Responsabile del trattamento sono disciplinati da un contratto o altro atto giuridico che vincoli il Responsabile del trattamento al Titolare del trattamento in ordine alla materia disciplinata e che riporti la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare, nonché quanto specificato all'art. 28 paragrafo 3 GDPR. Non può pertanto ricoprire il ruolo di Responsabile ex art. 28 GDPR un soggetto che agisca sotto l'autorità del Titolare.
3. L'Università, nell'affidare servizi che richiedano il trattamento di dati personali di cui è Titolare, ricorre a Responsabili del trattamento che presentino garanzie sufficienti perché i trattamenti soddisfino i requisiti del GDPR e i diritti degli interessati.
4. In alcuni casi l'Università, svolgendo attività di trattamento di dati personali per conto di altri titolari, viene da questi nominata Responsabile del trattamento.
5. Gli atti di nomina, sia redatti in qualità di Titolare sia ricevuti in veste di Responsabile del trattamento, vanno sottoposti all'attenzione del RPD (di cui all'art. seguente) prima della sottoscrizione da parte del rappresentante legale dell'Ateneo.
6. Le attività di trattamento effettuate dall'Università in qualità di Responsabile del trattamento devono essere segnalate al RPD per essere inserite nell'apposito Registro delle Attività di trattamento.

Art. 11. Responsabile della protezione dei dati personali (RPD) o Data Protection Officer (DPO)

1. L'Università nomina, ai sensi dell'art. 37 del GDPR, un Responsabile della protezione dei dati o RPD. La posizione del RPD è normata dall'art. 38 del GDPR.
2. Il RPD è figura di supporto al Titolare in materia di trattamento dati personali e svolge la funzione di raccordo con il Garante per la protezione dei dati personali e di garante per i soggetti interessati.
3. Ha, nello specifico, i seguenti compiti:
   a) sensibilizzare il Titolare e i suoi dipendenti in materia di protezione dei dati personali;
   b) fornire consulenza al Titolare e al Responsabile del trattamento di cui all'art. 10, così come ai dipendenti dell'Ateneo, in merito agli adempimenti scaturenti dalla normativa sulla protezione dei dati, vigilando sull'osservanza sia delle norme di cui all'art. 2 sia delle politiche del Titolare;

c) cooperare con il Titolare in merito alla:

   i. definizione delle istruzioni da fornire ai soggetti coinvolti nel trattamento dei dati personali;

   ii. scelta delle modalità con cui provvedere alla tenuta e all'aggiornamento del Registro dei trattamenti;

   iii. individuazione delle esigenze di informazione e di formazione del personale dell'Ateneo, anche conseguenti all'introduzione di novità normative sulla protezione dei dati;

   iv. osservanza della normativa e delle misure adottate dal Titolare sulla protezione dati, indicando le eventuali azioni da porre in essere a tale scopo;

   v. gestione delle violazioni dei dati personali.

d) fornire, se richiesto, un parere in merito alla necessità di effettuare una Valutazione di impatto e, nel caso, collaborare allo svolgimento della stessa, in particolare per l'introduzione e l'impiego nell'Università di particolari innovazioni tecnologiche;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto con lo stesso, per risolvere ogni questione connessa al trattamento dei dati, tra cui l'effettuazione di eventuali consultazioni preventive ai sensi dell'art. 36 del GDPR.

4. L'Università mette a disposizione del RPD risorse necessarie e adeguate per mantenere la sua conoscenza specialistica e per garantirgli lo svolgimento ottimale dei suoi compiti, consentendogli di avvalersi delle competenze e della collaborazione delle strutture universitarie e adoperandosi affinché sia coinvolto nelle attività che impattano sul trattamento dei dati, fin dalla fase di progettazione delle stesse.

5. L'adeguamento al Regolamento UE e la redazione degli atti conseguenti sono posti a carico di tutte le Strutture, a seconda dell'ambito di competenza e sulla base delle istruzioni impartite dal Titolare nei rispettivi atti di nomina di cui ai successivi artt. 12 - 14, con la consulenza del RPD e il supporto dei Referenti per la protezione dei dati di cui all'art.13.

6. Il RPD redige periodicamente una relazione in merito all'attività svolta, tenuto conto di questioni che impattano con priorità ed urgenza sul trattamento dei dati e riferisce almeno una volta all'anno agli Organi di governo.

Art. 12. Designato

1. Il Titolare, considerata l'alta complessità dell'organizzazione universitaria, si avvale della possibilità riconosciuta dall'art. 2-quaterdecies d.lgs. 196/03, di attribuire funzioni e compiti in materia di trattamenti di dati personali a persone fisiche che operano nell'ambito del suo assetto organizzativo, con specifico atto di nomina a Designati.

2. I Designati sono responsabili della conformità delle attività di trattamento dei dati personali, svolte sulla base delle competenze attribuite o nell'ambito dell'incarico ricoperto, alla normativa in materia di protezione dati personali di cui all'art.2 e alle misure tecniche e organizzative adottate dal Titolare, in collaborazione con il RPD. Sono a tal fine opportunamente formati e tenuti a partecipare personalmente alle iniziative formative organizzate dall'Amministrazione sul tema della protezione dei dati.

3. I Designati, in particolare, hanno il compito di:

   A. Con riferimento alle attività di trattamento dei dati:

a) richiedere obbligatoriamente, nell'acquisizione di software o nello sviluppo interno di software o altri dispositivi, l'applicazione di policy di sicurezza nello sviluppo delle applicazioni, con particolare riguardo a misure di protezione dei dati, per impostazione predefinita, fin dalla progettazione delle applicazioni;

b) aggiornare il Registro delle attività di trattamento (di cui all'art.7) della propria Struttura secondo le indicazioni del Titolare e dell'RPD, verificandone la completezza dei contenuti anche in relazione ad eventuali mutamenti organizzativi o tecnici (p.e. acquisizione di nuove banche dati e/o applicativi, passaggi del trattamento da modalità analogiche a digitali) e comunicando le variazioni all'RPD;

c) avere cura di trattare solo i dati personali necessari per ogni specifica finalità adottando misure atte a garantirne le caratteristiche di riservatezza, integrità e disponibilità; valutare i tempi di conservazione dei dati, ovvero, se non è possibile, i criteri utilizzati per determinare tale periodo, vigilando sulla cancellazione dei dati al termine della scadenza;

d) effettuare la preventiva valutazione d'impatto nei casi che lo richiedano, ai sensi del successivo art. 16 e consultare l'RPD, nei casi previsti dall'art. 36 del GDPR, quando tale valutazione d'impatto indichi che il trattamento presenta un rischio elevato; predisporre la documentazione necessaria per la consultazione preventiva al Garante, qualora risultasse necessaria agli esiti del confronto con l'RPD;

e) assicurare che i documenti e i dati da pubblicare sul sito web istituzionale, per le parti di competenza, siano conformi alla normativa vigente in materia, contemperando gli obblighi derivanti dalla trasparenza e pubblicità legale con quelli della protezione dei dati personali anche in relazione ai tempi di pubblicazione e alla possibile indicizzazione nei motori di ricerca;

f) verificare periodicamente, anche in collaborazione con gli Uffici tecnici competenti, le modalità di accesso ai locali e le misure adottate per la corretta custodia dei documenti ed accessibilità dei dati, al fine di garantire la sicurezza e la riservatezza degli archivi cartacei ed informatici;

g) adottare le opportune misure tecniche e organizzative per garantire la protezione dei dati personali qualora tali dati dovessero essere trattati dal personale di competenza al di fuori degli archivi cartacei ed informatizzati, dei server e dei sistemi informatici gestiti in maniera centralizzata dall'Ateneo (p.e. tramite dispositivi amovibili quali chiavi usb o hard disk esterni o fascicoli cartacei tra strutture), dettagliando questa evenienza nel Registro dei trattamenti;

h) coinvolgere tempestivamente l'RPD nelle questioni riguardanti i dati personali, collaborando con lui nelle attività di audit o nelle verifiche richieste dall'Autorità garante e garantire il rispetto di quanto stabilito dalla "Procedura di Data Breach"(di cui all'art. 17), assicurando l'immediata notifica di eventuali violazioni di dati personali all'RPD, nonché la fattiva collaborazione per gli adempimenti conseguenti.

B. Con riferimento ai diritti degli Interessati:

   a) vigilare sulla redazione e/o aggiornamento delle informative relative al trattamento dei dati personali nel rispetto degli artt. 13 e 14 del GDPR e, nel caso di trattamenti specifici, della modulistica relativa alla richiesta di manifestazione di consenso, sentito il RPD;

   b) adoperarsi per garantire che l'informativa stessa sia resa all'interessato al momento della raccolta o del primo trattamento dei suoi dati, anche nei casi in cui tali attività avvengano tramite servizi "on line";

   c) garantire agli interessati l'esercizio dei diritti previsti dalla normativa e provvedere a dare riscontro alle istanze degli interessati, (diritto accesso, rettifica, cancellazione, limitazione al

trattamento etc..), in collaborazione con tutti gli uffici coinvolti nel trattamento del dato oggetto della richiesta e comunicandola tempestivamente all'RPD;

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

   a) vigilare affinché questi operino nel rispetto della normativa in materia di protezione dati personali, del presente Regolamento e delle istruzioni loro impartite per il corretto trattamento dei dati nonché di ogni documentazione resa disponibile nel sito d'ateneo o diversamente diffusa;

   b) garantire la formazione e l'aggiornamento del personale, assicurando la partecipazione a corsi ed eventi formativi in materia di protezione dei dati personali;

   c) autorizzare espressamente i soggetti, anche esterni, che svolgono attività di trattamento di dati personali non ricompresi nell'attività ordinaria, fornendo loro specifiche istruzioni, se del caso anche nello stesso atto di costituzione di una commissione, di un gruppo di lavoro, di un gruppo di progetto o nell'affidamento di una collaborazione;

   d) individuare e nominare, in base alla complessità della struttura ed all'eterogeneità delle attività di trattamento dei dati personali, uno o più Referenti per la protezione dati per la propria struttura (di cui all'art. 13). I nominativi devono essere comunicati al RPD.

D. Con riferimento ai fornitori:

   a) verificare che la società fornitrice dei servizi garantisca il rispetto della normativa europea e nazionale in tema di protezione dati personali e si conformi alle disposizioni del Capo V del GDPR nel caso di trattamenti di dati effettuati verso, o da, Paesi terzi, in particolare per i servizi utilizzati in cloud;

   b) provvedere alla nomina dei fornitori di servizi quali "Responsabile del trattamento", secondo le modalità previste all'art. 28 paragrafo 3 GDPR, qualora le attività loro affidate comportino il trattamento di dati personali;

   c) segnalare all'RPD eventuali inadempimenti o violazioni imputabili ai suddetti Responsabili.

E. Con riferimento ai progetti di ricerca, che prevedano il trattamento dei dati personali dei soggetti reclutati:

   a) tenere conto degli atti di "soft law" di cui al precedente art. 2 comma 3 applicabili al settore della ricerca, della Convenzione Europea sui diritti dell'uomo e la bioetica (approvata ad Oviedo nel 1997 e ratificata con L.28 marzo 2001 n.145), della Dichiarazione internazionale Unesco del 2003 sui trattamenti dei dati genetici umani, della Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000 (adottata il 12 dicembre 2007) e delle indicazioni del Titolare fornite tramite guide operative predisposte allo scopo;

   b) compilare la "Scheda di valutazione del progetto di ricerca", resa disponibile nell'area riservata, per effettuare una valutazione dei rischi del trattamento prima dell'avvio di ogni progetto di ricerca, consegnandone una copia al Referente privacy della propria struttura unitamente ad una copia del progetto di ricerca perché provveda, come richiesto dalla normativa, a conservarli entrambi con la dovuta riservatezza per 5 anni dalla conclusione programmata della ricerca;

   c) porre in essere gli adempimenti derivanti dalla normativa per la protezione dati (informativa agli interessati, adozione di misure di sicurezza quali, ove possibile, la pseudonimizzazione o l'anonimizzazione dei dati,..);

   d) predisporre, se necessario, la modulistica relativa alla richiesta di manifestazione di consenso

affinché lo stesso sia specifico per ciascuna finalità del progetto, sia acquisito in maniera libera e informata e consenta di rispettare l'esercizio del diritto di revoca, da parte dell'Interessato, con modalità semplificate.

4. I Designati per la protezione dei dati, ove ciò sia reso necessario dalla dimensione della struttura e/o dalla complessità dei trattamenti di competenza, possono nominare, nell'ambito del personale strutturato afferente alla struttura medesima, incaricati per la protezione dei dati cui delegare compiti e responsabilità loro proprie, con riguardo a singole categorie di procedimenti o a singole attività di ricerca. Agli incaricati è fatto divieto di delegare ulteriormente. L'atto di delega, da redigersi per iscritto, dovrà essere comunicato al RPD.

Art. 13. Referente per la protezione dati (Referente privacy)

1. Il Referente per la protezione di dati personali è individuato e nominato dal Designato della struttura presso cui presta l'attività lavorativa quale supporto alle attività del Designato di cui all'art. 12, comma 3, lettere A, B, D ed E;
2. Coadiuva il RPD nel monitoraggio dell'attuazione della normativa e nel facilitare la diffusione della cultura in materia di protezione e sicurezza dei dati personali. In particolare, nell'operare con il massimo riserbo:
   a) svolge un ruolo di raccordo tra i colleghi e i collaboratori della sua struttura e tra questi e il Designato ed il RPD, anche al fine di facilitare la rilevazione e la segnalazione delle criticità collegate al trattamento dei dati personali, favorire la conformità normativa dei trattamenti in essere e formulare proposte sulle attività di formazione del personale;
   b) coopera per assicurare l'immediata notifica di eventuali violazioni di dati personali all'RPD e per gli adempimenti conseguenti, nonché per facilitare il riscontro alle istanze degli interessati;
   c) partecipa proattivamente alle riunioni e/o incontri organizzati su attività di trattamento di dati personali dal Titolare, dal Designato o dall'RPD, ricevendo una formazione specifica in materia.
3. Il Designato assicura la massima collaborazione del personale, che opera sotto la sua responsabilità, ai Referenti privacy nominati nella sua struttura.
4. In caso di trasferimento o cessazione dall'attività lavorativa del soggetto nominato, il Designato provvede alla revoca delle autorizzazioni eventualmente ad egli concesse ed alla nomina tempestiva di un nuovo Referente, comunicando la variazione al RPD.

Art. 14. Autorizzato o Incaricato al trattamento

1. Le operazioni di trattamento possono essere effettuate solo da incaricati espressamente autorizzati dal Titolare, direttamente o per il tramite del Designato della struttura di appartenenza, attenendosi alle istruzioni impartite.
2. La designazione o autorizzazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito, anche con riferimento alle attività svolte dall'unità organizzativa cui la persona è assegnata o dell'attività cui partecipa.
3. E' possibile autorizzare, con uno stesso atto, una pluralità di soggetti aventi compiti e funzioni omogenee in relazione alle attività di trattamento dei dati che sono riportate nel Registro di cui all'art. 7.
4. Le autorizzazioni devono essere conferite anche ai soggetti, eventualmente esterni all'Ateneo,

incaricati di specifici compiti e funzioni connessi al trattamento dei dati personali di titolarità dell'Università, come nel caso di progetti di ricerca o convenzioni, gruppi di lavoro o attività finalizzate a un risultato peculiare.

5. Gli Autorizzati sono tenuti a conformare le operazioni loro assegnate alla normativa in materia di protezione dei dati personali, al presente Regolamento e ad ogni istruzione specifica ricevuta sui trattamenti dei dati personali, facendo proprie le politiche di sicurezza informatica e le linee guida in materia di utilizzo degli strumenti informatici adottate dall'Università, pubblicate e periodicamente aggiornate nel sito dell'Ateneo.
6. Ogni Autorizzato, in particolare, è tenuto:
   a) a mantenere il segreto e il massimo riserbo su tutte le informazioni o dati appresi in relazione a fatti e circostanze di cui sia venuto a conoscenza nella propria qualità di autorizzato;
   b) ad attivare ogni misura idonea a inibire l'accesso ai dati trattati da parte di chi non è a ciò autorizzato, in ogni fase dell'attività di trattamento, compreso l'eventuale trasferimento dei dati o la loro conservazione;
   c) ad accertarsi dell'identità del diretto Interessato, prima di fornire informazioni circa i dati personali o il trattamento effettuato;
   d) a verificare, prima di procedere alla raccolta dei dati, che gli Interessati abbiano ricevuto le necessarie informative, diversamente invitandoli a prenderne visione;
   e) a collaborare alla tenuta e all'aggiornamento del Registro delle attività di trattamento, informando preventivamente il Designato di eventuali modifiche dei trattamenti esistenti o dell'esigenza di introdurne di nuovi;
   f) a segnalare con tempestività, al Referente privacy della sua struttura o al RPD, eventuali anomalie, incidenti, furti, perdite accidentali di dati;
   g) a frequentare i corsi di formazione organizzati dal Titolare in materia di protezione dati personali.
7. L'autorizzato è informato e consapevole che l'accesso e la permanenza nei sistemi informatici per ragioni estranee e comunque diverse rispetto a quelle per le quali è stato abilitato per fini istituzionali e di servizio può, nei casi previsti dalla legge, integrare il reato di accesso abusivo ai sistemi informativi e può comportare sanzioni disciplinari, oltre che esporre l'Amministrazione a danni patrimoniali e reputazionali.
8. Nel caso di trasferimento, anche temporaneo, ad altra struttura/ufficio, o nell'ipotesi di cessazione del rapporto di lavoro, il soggetto perde i privilegi di accesso ai dati personali riconosciuti all'ufficio di provenienza. Il Designato della struttura di afferenza provvede affinché lo stesso non abbia più accesso ai sistemi di gestione di dati personali o di documenti condivisi, procedendo alla immediata disattivazione o cambio delle credenziali d'accesso ai sistemi che siano state note al soggetto.
9. I trattamenti di dati personali per i quali manchi l'autorizzazione comporta la qualificazione del soggetto che li tratta quale Terzo rispetto all'Amministrazione universitaria, con l'addebito a suo carico delle eventuali conseguenze pregiudizievoli.

Art. 15. Autorizzati o Incaricati in ambito informatico

1. Il Titolare, direttamente o per il tramite del Designato della struttura di appartenenza, fornisce

specifiche autorizzazioni e istruzioni in ambito informatico alla persona fisica che si occupa della gestione e manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali oppure dello sviluppo di sistemi o servizi software.

2. L'autorizzato è tenuto a conformare il proprio operato sia alle prescrizioni rivolte a tutto il personale autorizzato al trattamento dei dati personali di cui al precedente art. 14 sia, nei limiti dei compiti assegnati e del ruolo o della qualifica ricoperti all'interno dell'unità organizzativa cui afferisce e/o delle attività cui partecipa, al rispetto dei princìpi di protezione dei dati fin dalla progettazione e per impostazione predefinita di cui all'art. 25 GDPR.
3. Egli è tenuto a collaborare proattivamente con il Dirigente dei sistemi informativi di Ateneo per la valutazione del rischio delle attività di trattamento e per l'individuazione di misure tecniche e organizzative volte a garantire, tenuto conto dello stato dell'arte e dell'evoluzione tecnologica, idonei livelli di protezione dei sistemi informatici.
4. Restano inoltre valide per l'autorizzato le istruzioni specifiche, ricevute con le lettere di incarico o di nomina ad Amministratore di sistema, attribuite in base al D. Lgs. 196/2003 ante riforma e ai provvedimenti ad esso conseguenti, fino a nuova disposizione del Designato della struttura di afferenza.
5. Nel caso di trasferimento, anche temporaneo, ad altra struttura/ufficio, o nell'ipotesi di cessazione del rapporto di lavoro, il soggetto perde i privilegi di accesso ai dati personali riconosciuti all'ufficio di provenienza. Il Designato della struttura di afferenza provvede affinché lo stesso non abbia più accesso ai sistemi, procedendo alla immediata disattivazione o cambio delle credenziali d'accesso ai sistemi che siano state note al soggetto e aggiornando, se del caso, le nomine ad amministratore di sistema.

Art. 16. Valutazione di impatto sulla protezione dei dati (DPIA)

1. Quando si intende intraprendere un tipo di trattamento di dati personali dovrebbero essere determinate la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato con riguardo alla natura dei dati, all'ambito di applicazione, al contesto e alle finalità del trattamento.
2. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato, suscettibile di cagionare un danno fisico, materiale o immateriale agli interessati, in particolare nei seguenti scenari:
   a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente sulle suddette persone fisiche;
   b) il trattamento, su larga scala, di categorie particolari di dati personali quali: 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, dati relativi a condanne penali e a reati;
   c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (videosorveglianza) o l'introduzione di nuove tecnologie che comportano variazioni del rischio correlato all' attività di trattamento;
   d) il trattamento dei dati particolari, specie se relativi alla salute o di natura estremamente personale quale l'opinione politica, anche a fini di ricerca scientifica in campo medico, biomedico o epidemiologico (art. 110 D.Lgs. 196/2003).
3. Qualora la valutazione evidenzi un rischio medio/alto, il Designato della struttura interessata, previa consultazione con l'RPD e in collaborazione con il Referente privacy individuato per la stessa struttura,

effettua la valutazione dell'impatto sulla protezione dei dati personali (Data Protection Impact Assessment) prima di procedere al trattamento, come previsto all'art. 35 GDPR.

4. Il Titolare rende disponibile un modello per effettuare e documentare la DPIA a supporto dell'esecuzione di tale adempimento, che è obbligatorio nei casi indicati dall'Autorità garante nell'apposita sezione del suo sito.
5. Il Responsabile per la transizione al digitale fornisce supporto ai Designati e collabora con il RPD ai fini dello svolgimento della valutazione di impatto.
6. È possibile condurre una singola valutazione di impatto per un insieme di trattamenti simili, effettuati nello stesso contesto e che presentano analoghi rischi.
7. Il Titolare, per il tramite dell'RPD, consulta il Garante per la Protezione dei dati personali prima di procedere al trattamento se le risultanze della DPIA effettuata indicano l'esistenza di un rischio residuale elevato.

Art. 17. Data Breach – Violazione di dati personali

1. Ai sensi degli artt. 33 e ss. del GDPR e del Considerando 87, il Titolare adotta la Procedura di comunicazione del Data Breach per consentire a chiunque la segnalazione di un evento che comporti, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la rivelazione o l'accesso non autorizzato ai dati personali trasmessi, memorizzati o comunque elaborati. La suddetta Procedura è pubblicata sul sito internet istituzionale.

2. Il Titolare predispone inoltre una procedura interna di gestione di tali segnalazioni e degli incidenti di sicurezza informatica, individuando le risorse organizzative alle quali, per le competenze possedute, sia possibile assegnare le attività richieste per la valutazione del rischio per i diritti e le libertà degli interessati, per la loro mitigazione nonché per la corretta e tempestiva gestione delle azioni complessive da intraprendere per far fronte alla violazione occorsa.

3. Compete alle stesse risorse organizzative, individuate nella procedura, la valutazione della necessità di procedere alla notifica all'Autorità garante per la protezione dei dati personali, di cui all'art. 33 del GDPR, senza ingiustificato ritardo e, ove possibile, entro 72 ore dall'avvenuta conoscenza della violazione, come pure la valutazione della necessità di comunicare la violazione all'Interessato, nel rispetto delle previsioni di cui all'art. 34 del GDPR.

4. Il Titolare provvede alle notifiche di cui al precedente comma e documenta in un apposito "Registro degli incidenti" qualsiasi violazione di dati personali, comprese le circostanze in cui si è verificata, le conseguenze e i provvedimenti adottati per attenuarne le conseguenze.

Art. 18. Informativa sul trattamento dei dati personali

1. L'Università, prima di raccogliere i dati personali, fornisce all'interessato le informazioni inerenti i dati di contatto del Titolare e dell'RPD, le finalità, le basi giuridiche, la durata e le modalità del trattamento, l'obbligatorietà o la facoltatività del conferimento dei dati e i diritti che questi può esercitare, secondo quanto previsto agli artt. 13 e 14 del GDPR.

2. Se i dati sono comunicati spontaneamente dall'Interessato, l'informativa deve essere fornita al momento del primo contatto utile, successivo alla ricezione dei dati medesimi, pena l'inutilizzabilità degli stessi.

3. Le informazioni sul trattamento così dichiarate definiscono il confine di liceità del trattamento stesso. Ogni utilizzo differente da quanto indicato nell'informativa costituisce una violazione dei princìpi di cui al precedente art. 4, a meno che non siano previamente fornite all'Interessato le aggiuntive, opportune

e necessarie informazioni in merito a tali ulteriori utilizzi.

4. Laddove vengano trattati dati personali che non sono stati raccolti presso l'Interessato, il Titolare fornisce all'Interessato l'informativa di cui all'art. 14 del GDPR.
5. Il Titolare rende disponibile un modello per redigere l'informativa, a supporto dell'esecuzione di tale adempimento, nell'area riservata del sito istituzionale di ateneo. L'informativa deve essere sottoposta al preventivo parere del RPD.
6. Il Titolare pubblica le informative di rilevanza trasversale sul proprio sito istituzionale (www.unipg.it), mentre fornisce quelle relative a specifici trattamenti in occasione dell'effettuazione degli stessi.

Art. 19. Diritti dell'Interessato

1. Il Titolare opera nel rispetto dell'art. 12 del GDPR e garantisce il rispetto dei diritti degli Interessati, secondo le condizioni previste agli artt. 15 - 22 del GDPR.
2. Il Titolare, per mezzo dell'informativa, comunica all'Interessato i diritti che può esercitare in relazione alle specifiche attività di trattamento cui si riferisce l'informativa e pubblica, sul sito istituzionale, nella sezione "Privacy e protezione dati personali", la Procedura e i Modelli per l'esercizio degli stessi.
3. Il riscontro alla richiesta presentata dall'Interessato viene fornito senza ingiustificato ritardo e comunque non oltre 30 giorni dalla data di acquisizione della richiesta stessa, anche nei casi di diniego, sempreché sia previamente accertata l'identità dell'interessato. Per i casi di particolare e comprovata difficoltà il termine dei 30 giorni può essere prorogato per altri 2 mesi, non ulteriormente prorogabili. Di tale proroga deve essere data informazione motivata all'Interessato entro un mese dall'acquisizione della richiesta.
4. 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.
5. Il diritto alla portabilità, applicabile ai soli trattamenti automatizzati, non può essere esercitato per i trattamenti di dati personali necessari per l'adempimento di un obbligo legale cui è soggetto il Titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.
6. Nelle comunicazioni all'interessato, specie se contenenti dati particolari o giudiziari, l'Università utilizza modalità di trasmissione, anche elettronica, che garantiscano la riservatezza e confidenzialità dei dati trasmessi.
7. Se le finalità per cui vengono trattati i dati personali non richiedono o non richiedono più l'identificazione dell'Interessato, non si devono conservare, acquisire o trattare ulteriori informazioni per identificare l'Interessato al solo fine di consentirgli l'esercizio dei diritti previsti dal GDPR.

Art. 20. Trattamenti in ambito universitario

1. L'Università, nell'espletamento della propria attività istituzionale, considera il diritto alla protezione dei dati personali nella sua funzione sociale, contemperandolo con gli altri diritti fondamentali, disciplinati dalle fonti normative sovranazionali e nazionali, nel rispetto del principio di proporzionalità.
2. I trattamenti delle categorie particolari di dati personali, di cui all'art. 3 lettera b), necessari per motivi di interesse pubblico rilevante sono ammessi se previsti da norme dell'Unione europea, da disposizioni

di legge in ambito nazionale o, nei casi previsti dalla legge, di regolamento e sempreché la finalità non possa essere raggiunta senza trattare tali dati. Nelle stesse norme devono essere rinvenibili i tipi di dati che possono essere trattati, le operazioni eseguibili, il motivo di interesse pubblico rilevante e le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dei soggetti cui si riferiscono.

3. Il trattamento di dati personali relativi a condanne penali, a reati o a connesse misure di sicurezza, deve avvenire solo se è autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, come disciplinato in particolare all'art. 2-octies del Codice privacy.
4. Qualora l'Università, nell'esercizio delle sue funzioni istituzionali, venga a conoscenza di dati personali non necessari allo svolgimento di tale attività, anche se trasmessi dall'interessato, questi non potranno essere utilizzati e dovranno essere eliminati, fatto salvo l'eventuale obbligo di conservazione, previsto dalla legge, dell'atto o del documento che li contiene.
5. L'Università può adottare eventuali linee guide o schede tematiche per fornire indicazioni aggiuntive e specifiche in relazione ai trattamenti di dati personali ea particolari categorie di trattamenti dei dati personali. Il personale è tenuto a prenderne visione in Area riservata o alla pagina del sito d'ateneo "Privacy e protezione dati personali" e a verificare periodicamente la presenza di aggiornamenti.

Art. 21. Comunicazione e diffusione dei dati personali

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

7. Su richiesta degli Interessati, l'Università può comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali degli studenti di ogni livello di istruzione universitaria e altri dati personali diversi dai dati particolari o giudiziari, al fine di agevolarne l'orientamento, la formazione e l'inserimento professionale, anche all'estero. I dati devono essere pertinenti in relazione a tali finalità, espressamente indicate dall'Interessato nella sua richiesta. I dati possono essere successivamente trattati esclusivamente per le stesse finalità.
8. La pubblicazione di valutazioni d'esame o di esiti di prove concorsuali e selettive, nonché delle relative graduatorie, avviene in aree riservate del sito istituzionale, salve le normative di settore che regolino diversamente tempi e forme di pubblicità legale, avendo in tal caso cura di rispettare i princìpi di minimizzazione dei dati e di limitazione della conservazione di cui al precedente art. 5.
9. Il reclutamento di personale appartenente alle categorie protette avviene attraverso procedure concorsuali che prevedano la pseudonimizzazione dei candidati già in fase di predisposizione dei bandi di concorso, ciò al fine di proteggere la loro identità in ogni fase della procedura concorsuale, con particolare riguardo ad eventuali esigenze di pubblicazione dei dati ad essa connesse.
10. E' vietato diffondere dati personali idonei a rivelare lo stato di salute o informazioni da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici. Analogo divieto sussiste per i dati personali idonei a rivelare altre informazioni di carattere particolare di cui al precedente art. 3 lettera b) o che rilevino situazioni di disagio economico o sociale.

Art. 22. Trasferimenti verso Paesi extra UE

1. Il trasferimento di dati personali verso paesi al di fuori dell'Unione o organizzazioni internazionali o altri destinatari in paesi terzi, deve avvenire assicurandosi che non sia compromesso il livello di tutela delle persone fisiche assicurato dalle normative europee e nazionali per la protezione dei dati personali, come richiesto al Capo V del GDPR.
2. Il trasferimento di dati personali, come ogni trattamento, deve essere innanzitutto conforme alle disposizioni generali inerenti la protezione dei dati personali, in relazione alle finalità per cui viene effettuato, quindi deve essere:
   a) fondato su una base giuridica tra quelle previste all'art. 6 del GDPR;
   b) eseguito nel pieno rispetto dei princìpi elencati all'art.5 del GDPR, riportate al precedente art. 4, e in generale di tutte le disposizioni pertinenti del GDPR e delle altre normative applicabili ai trattamenti di dati personali;
   c) inserito nel Registro dei trattamenti, riportando i paesi terzi o le organizzazioni internazionali a cui i dati personali sono stati o saranno comunicati, la valutazione del rischio effettuata e la descrizione delle garanzie attuate per il trasferimento, in relazione ai rischi valutati, affinché l'interessato benefici di un adeguato livello di protezione dei suoi dati personali anche nell'eventuale ulteriore trasferimento da questi ad altro paese terzo, secondo le disposizioni al Capo V del GDPR;
   d) inserito nell'informativa per l'interessato, riportando quali siano i paesi terzi o le organizzazioni internazionali destinatarie e le motivazioni per cui ha luogo il trasferimento. Devono essere inoltre riportate le valutazioni del Titolare in merito alla scelta dello strumento di garanzia adottato, tra quelli previsti dal GDPR, in caso di assenza di una decisione di adeguatezza.
3. La valutazione dell'adeguatezza della tutela offerta da un paese terzo va considerata in funzione di tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti, che riguardano

anche la modalità, la frequenza, la durata e il contesto del trasferimento.

4. Sia nella valutazione del rischio sia nelle garanzie attuabili, il Titolare deve prestare attenzione anche ai trasferimenti che potrebbero subentrare tra l'importatore dei dati e un successivo sub-incaricato, in virtù di un subcontratto dell'importatore.
5. L'Università adotta e aggiorna una apposita scheda tematica per fornire indicazioni operative specifiche della disciplina.

Art. 23. Archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici

1. I documenti contenenti dati personali possono essere trattati a fini di archiviazione nel pubblico interesse o di ricerca storica, tenendo conto della loro natura e solo se pertinenti e indispensabili per il perseguimento di tali scopi; ove possibile e senza pregiudicare il raggiungimento delle finalità del trattamento, dovranno essere trattati con misure tecniche che non consentano più di identificare l'interessato.
2. Il trattamento dei dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato nel rispetto del principio della minimizzazione dei dati, delle autorizzazioni generali del Garante per la protezione dei dati personali e dei codici deontologici in materia.
3. La consultazione dei documenti di interesse storico conservati negli archivi dell'Università è disciplinata dal decreto legislativo 22 gennaio 2004, n. 42 (c.d. Codice dei beni culturali e del paesaggio).
4. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici può essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati (art. 99 comma 1 Codice privacy).
5. A fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici possono comunque essere conservati o ceduti ad altro titolare i dati personali dei quali, per qualsiasi causa, è cessato il trattamento, nel rispetto di quanto previsto dall'articolo 89, paragrafo 1, del GDPR (art. 99 comma 2 Codice privacy).

Art. 24. Trattamento ai fini di ricerca scientifica

1. L'Università valorizza e promuove la ricerca scientifica e adotta misure tecniche e organizzative funzionali ad assicurare che i trattamenti di dati effettuati in tali ambiti avvengano nel rispetto dei diritti degli interessati e della normativa in materia. Speciale attenzione viene riservata alla ricerca medica, biomedica ed epidemiologica che prevede trattamenti di dati particolari la cui conoscibilità può incidere in maniera significativa sui diritti e le libertà degli interessati.
2. Il Capo III del Codice privacy delimita le modalità del trattamento dei dati a fini statistici o di ricerca scientifica, i casi in cui non è necessario acquisire il consenso al trattamento dei dati personali da parte degli interessati e le materie oggetto di disposizioni particolari dell'Autorità garante per la protezione dei dati personali nell'ambito della ricerca scientifica.
3. La disciplina sul trattamento di dati personali nell'ambito della ricerca scientifica annovera, oltre al GDPR e al Codice privacy, anche gli atti di "soft law" di cui all'art. 2 comma 3, cui ogni progetto di ricerca deve conformarsi, alcuni richiamati all'art.12 comma E lettera a).
4. L'Università, al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e

tecnologico, ai sensi dell'art. 100 del Codice privacy può, con autonome determinazioni, comunicare e diffondere anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione dei trattamenti di categorie particolari di dati personali e dei trattamenti dei dati personali relativi a condanne penali e reati.

5. Tutto il personale che si occupa di ricerca è tenuto a conoscere la normativa di settore. Al solo fine di facilitare la conoscibilità della complessa disciplina in materia, l'Ateneo può adottare e aggiornare periodicamente una guida pratica sugli adempimenti da porre in essere alla luce delle disposizioni di cui al comma 3, pubblicandola sul sito istituzionale, favorendo altresì la formazione del personale docente e ricercatore in materia di protezione dei dati personali.

Art. 25. Videosorveglianza

1. L'Università effettua trattamenti di dati personali mediante l'attivazione di impianti di videosorveglianza negli ambienti dell'Università nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche.
2. L'Università adotta il Regolamento dell'attività di videosorveglianza delle strutture dell'Università degli Studi di Perugia, sulla base del quale fornisce disposizioni attuative per il rispetto del Regolamento e la corretta tenuta dei sistemi di videosorveglianza attivati nelle sedi universitarie. Il Regolamento è pubblicato sul sito internet dell'Ateneo.

Art. 26. Sanzioni per inosservanza delle norme

1. Gli artt. 82, 83 e 84 del GDPR prevedono sanzioni amministrative pecuniarie fino a 10.000.000 Euro, estendibili ulteriormente a 20.000.000 Euro in caso di violazione delle disposizioni relative ai principi base del trattamento, ai diritti degli Interessati o al trasferimento di dati a paesi terzi.
2. L'art. 166 a 172 del Codice privacy definisce i criteri di applicazione delle sanzioni pecuniarie e il procedimento per l'adozione dei provvedimenti correttivi e sanzionatori.
3. Gli artt. da 167 a 172 del Codice privacy introducono le modalità di applicazione dei periodi di reclusione per gli illeciti penali derivanti dalle violazioni della normativa sulla protezione dei dati personali, dalla falsità di dichiarazioni rese all'Autorità garante o da azioni volte intenzionalmente a interrompere o turbare la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.
4. L'Università può prevedere, in aggiunta a quanto previsto ai commi precedenti, sanzioni a carico del personale in caso di violazione delle leggi e delle procedure in tema di protezione dei dati personali.

Art. 27. Efficacia temporale e pubblicità

1. Il presente Regolamento entra in vigore il quindicesimo giorno successivo alla data di pubblicazione sull'albo on line di Ateneo.
2. In attuazione delle previsioni di cui all'art. 6 e conformemente all'art. 8, comma 1 il Rettore provvede, entro 60 giorni dall'entrata in vigore del presente Regolamento, alla nomina dei soggetti di cui all'art. 12 e, eventualmente per il tramite dei Designati, dei soggetti di cui agli artt. 14 e 15. Gli atti di nomina possono riguardare una pluralità di soggetti aventi compiti e funzioni omogenee.
3. L'Università provvede a dare pubblicità al presente Regolamento ed alle successive modifiche ed

integrazioni mediante pubblicazione sul sito istituzionale di Ateneo.

4. La documentazione redatta dall'Università in materia di protezione dei dati personali è messa a disposizione sul sito istituzionale dell'Ateneo, nella sezione Privacy e protezione dati personali o nell'Area riservata del medesimo portale; è oggetto di periodico aggiornamento e costituisce parte integrante delle misure tecniche e organizzative di cui all'art. 6 del presente Regolamento.