REGOLAMENTO DELL'UNIVERSITÀ IUAV DI VENEZIA PER IL TRATTAMENTO E LA PROTEZIONE DEI DATI PERSONALI
(emanato con decreto rettorale 3 dicembre 2021 n. 700)

INDICE

TORNA ALL'INDICE

Capo I – Oggetto, definizioni e basi giuridiche

Articolo 1
(Oggetto e ambito di applicazione)

1. Il presente Regolamento contiene disposizioni atte ad assicurare la conformità del trattamento dei dati personali da parte dell'Università Iuav di Venezia ("Università") nell'ambito del perseguimento delle proprie finalità istituzionali e dei compiti ad esse connesse, a quanto previsto dal Regolamento UE 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali ("Regolamento UE" o "GDPR"), dal Decreto Legislativo n. 196 del 30 giugno 2003, "Codice in materia di protezione dei dati personali" ("Codice Privacy"), come modificato e integrato dal Decreto Legislativo n. 101 del 10 agosto 2018.

Articolo 2
(Definizioni e rinvio)

1. Ai fini del trattamento dei dati personali si intende per:
- "dato personale", qualsiasi informazione riguardante una persona fisica identificata o identificabile ("Interessato/i"), direttamente o indirettamente, con particolare riferimento a un identificativo - come il nome, un numero di identificazione, dati relativi all'ubicazione e un identificativo online - o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- "trattamento", qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la 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;
- "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;
- "archivio", qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- "consenso dell'interessato", qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- "violazione dei dati personali" ("Data breach"), la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- "pseudonimizzazione", il trattamento dei dati personali in modo tale 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 intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'Interessato;
- "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

TORNA ALL'INDICE

2. Per le ulteriori definizioni relative al trattamento dati, si rinvia a quanto stabilito dall'articolo 4 del Regolamento UE.

Articolo 3
(Base giuridica del trattamento dei dati personali)

1. Ogni trattamento di dati personali da parte dell'Università, fermo restando in ogni caso l'obbligo di fornire l'informativa agli Interessati secondo quanto previsto all'articolo 20 del presente Regolamento, deve trovare fondamento in un'idonea base giuridica. Pertanto, il trattamento è lecito solo se ricorre almeno una delle seguenti condizioni di cui all'articolo 6 del Regolamento UE:
a) consenso dell'interessato: il consenso deve essere libero, specifico, informato e inequivocabile, non essendo ammesso il consenso tacito o presunto e, se il trattamento persegue più finalità, il consenso deve essere espresso specificamente con riguardo a ciascuna di esse; l'Università deve sempre essere in grado di dimostrare che l'Interessato ha prestato il proprio consenso, inoltre, per i dati "particolari" di cui all'articolo 9 del Regolamento UE e per le decisioni basate su trattamenti automatizzati (compresa la profilazione) esso deve essere anche "esplicito";
b) trattamento necessario per l'adempimento di un contratto, di cui l'Interessato è parte o per l'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) trattamento necessario per l'adempimento di obblighi di legge cui è soggetta l'Università;
d) trattamento necessario per la salvaguardia degli interessi vitali della persona interessata o di terzi, utilizzabile però come presupposto solo se nessuna delle altre condizioni di liceità può trovare concreta applicazione;
e) trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

Capo II - Modello organizzativo Iuav - soggetti individuati e compiti

Articolo 4
(Soggetti coinvolti)

1. Il GDPR individua, quali figure deputate a gestire e garantire la sicurezza dei dati personali:
- il Titolare del trattamento ("Titolare"): la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che determina le finalità e i mezzi del trattamento di dati personali da solo ovvero congiuntamente ad altro soggetto ("Contitolari");
- il Responsabile Esterno del trattamento ("Responsabile Esterno"): la persona fisica o giuridica, l'Autorità pubblica, il servizio o l'organismo che tratta i dati personali per conto del Titolare;
- gli Autorizzati del trattamento ("Autorizzati"): chiunque, nel trattamento dei dati personali, agisca sotto l'autorità del Titolare e secondo le istruzioni impartite da quest'ultimo;
- il Responsabile della Protezione dei Dati ("DPO"): il soggetto che fornisce consulenza al Titolare e agli Autorizzati in merito agli obblighi derivanti dal GDPR, supporta nel processo di adeguamento alla normativa in materia di protezione dei dati, sorveglia l'osservanza delle prescrizioni del Regolamento EU e del Codice privacy nonché funge da punto di contatto per l'Autorità di controllo (Garante per la protezione dei dati personali – "Garante").
2. L'Università, nel rispetto del GDPR, ai fini di una propria organizzazione funzionale alla protezione dei dati personali che consenta una chiara suddivisione dei compiti e dei ruoli, adotta un proprio modello organizzativo che individua quali soggetti coinvolti nella protezione dei dati personali trattati dall'Università Iuav di Venezia, le seguenti figure: il Titolare; il DPO; il Responsabile Interno che coadiuva il Titolare, garantendo il rispetto della normativa in materia di protezione dei dati ("Responsabile/i Interno/i"); i Referenti per

TORNA ALL'INDICE

la protezione dei dati personali (“Referente/i”); gli Autorizzati; gli Amministratori di sistema (“ADS”).
3. L’Università ha, inoltre, costituito il Comitato Etico per la Ricerca dell’Università: per ogni progetto di ricerca avviato dall’Università, o al quale quest’ultima partecipa, che presenti problematiche di natura etica, è obbligatorio il parere del Comitato Etico per la Ricerca. Qualora il progetto di ricerca comporti trattamento dei dati personali, il parere del Comitato Etico per la Ricerca è obbligatorio qualora sia previsto dalle regole di finanziamento del progetto stesso.

Articolo 5
(Titolare del trattamento)

1. L’Università, nella persona del Rettore pro tempore, è Titolare di tutti i dati personali trattati nell’ambito delle proprie attività istituzionali.
2. All’Università competono quindi le decisioni in ordine alle finalità, alle modalità di trattamento dei dati e agli strumenti utilizzati, nonché le scelte in merito alla sicurezza. In particolare, l’Università deve:
a) mettere in atto tutte le misure tecniche e organizzative adeguate ed efficaci per garantire, ed essere in grado di dimostrare, che ogni trattamento è effettuato conformemente alle norme vigenti, al Regolamento UE e al Codice privacy;
b) mettere in atto misure tecniche ed organizzative adeguate per garantire che, per impostazione predefinita, siano trattati solo i dati personali necessari per ogni specifica finalità di trattamento e sia assicurato che i dati personali non siano resi accessibili a un numero indefinito di persone fisiche, senza che sia necessario l'intervento di un operatore;
c) provvedere alla nomina:
- previa individuazione da parte del Consiglio di Amministrazione, del DPO di cui all’articolo 7 del presente Regolamento;
- dei Responsabili Interni di cui all’articolo 8 del presente Regolamento, con l’indicazione dei compiti e delle responsabilità loro affidate in relazione a quanto disposto dalle normative vigenti; nel provvedimento di designazione, l’Università autorizza il Responsabile Interno a nominare a sua volta uno o più Referenti di cui all’articolo 9 del presente Regolamento;
- degli ADS di cui all’articolo 11 del presente Regolamento;
- dei Responsabili Esterni, di cui all’articolo 12 del presente Regolamento;
d) tenere i Registri delle attività di trattamento effettuate sia in qualità di Titolare che di Responsabile Esterno per conto di altri Titolari, secondo quanto previsto dall’articolo 16 del presente Regolamento;
e) inoltre, avvalendosi del DPO:
- accertare periodicamente la puntuale osservanza della normativa vigente e delle istruzioni impartite;
- effettuare, previa consultazione del DPO e con il suo supporto, la valutazione di impatto sulla protezione dei dati (“DPIA”) di cui all’articolo 35 del Regolamento UE, adempiendo a quanto previsto all’articolo 18 del presente Regolamento e notificando al Garante le violazioni di dati personali, ai sensi del successivo articolo 22 del presente Regolamento;
- definire le istruzioni operative di cui all’articolo 17 del presente Regolamento, dandone opportuna diffusione anche mediante l’organizzazione di appositi momenti formativi, al fine di garantire la sicurezza dei dati oggetto di trattamento;
f) dare seguito alle richieste di esercizio dei diritti degli Interessati di cui all’articolo 19 del presente Regolamento;
g) valutare se procedere alla comunicazione agli Interessati delle eventuali violazioni di dati personali accertate, ai sensi dell’articolo 36 del GDPR;
h) sentito il DPO, predisporre con i servizi competenti, un piano formativo annuale 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;

TORNA ALL'INDICE

i) favorire l'adesione ai codici di condotta elaborati dalle Associazioni e dagli Organismi rappresentativi di categoria, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione della normativa europea e per dimostrarne il concreto rispetto da parte dell'Università.

Articolo 6
(Contitolari del trattamento)

1. Qualora l'Università determini le finalità e i mezzi del trattamento di dati personali congiuntamente ad un altro soggetto, quest'ultimo assume il ruolo di Contitolare. Rapporti, obblighi e responsabilità dei Contitolari vengono definiti in un apposito accordo scritto il cui contenuto essenziale viene reso noto all'Interessato, che potrà esercitare i propri diritti nei confronti di ciascun Contitolare.

Articolo 7
(Responsabile della Protezione dei Dati - DPO)

1. Il DPO viene individuato dal Consiglio di Amministrazione dell'Università e nominato dal Rettore con proprio decreto; il DPO può essere individuato tra i soggetti interni o esterni all'Università, in funzione delle conoscenze tecniche e delle qualità professionali in materia di protezione dei dati nonché delle capacità di assolvere ai propri compiti.
2. La nomina del DPO viene comunicata a cura dell'Università al Garante.
3. Al DPO spettano le seguenti funzioni:
a) informare e fornire consulenza all'Università, ai Responsabili Interni e agli Autorizzati, in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati;
b) vigilare sull'osservanza da parte dell'Università della normativa in materia di protezione dei dati, delle politiche di attuazione, comprensive delle attività di sensibilizzazione, formazione e controllo poste in essere dall'Università stessa;
c) fornire pareri e supporto in merito alla DPIA e sorvegliarne l'osservanza;
d) tenere i Registri delle attività di trattamento che l'Università svolge sia in qualità di Titolare che di Responsabile Esterno per conto di altri Titolari. I predetti Registri sono predisposti e aggiornati sulla base delle informazioni fornite dai Responsabili Interni e dai Referenti delle varie Aree/Divisioni dell'Università che trattano dati personali;
e) cooperare e fungere da punto di contatto per il Garante in merito alle questioni connesse al trattamento dei dati, effettuando, se del caso, consultazioni preventive di cui all'articolo 36 del Regolamento UE;
f) fornire pareri in merito alla DPIA, su indicazioni del Comitato Etico per la Ricerca, per ogni progetto di ricerca sottoposto allo stesso.
4. Si applicano al DPO le disposizioni vigenti in materia di conflitto di interessi.
5. L'Università assicura che il DPO sia tempestivamente coinvolto in tutte le questioni riguardanti il trattamento dei dati fornendogli a tal fine tutte le informazioni necessarie all'adempimento dei propri compiti.
6. Nello svolgimento delle suddette attività, il DPO deve debitamente considerare i rischi inerenti ai trattamenti, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità dei medesimi. In tal senso, quest'ultimo:
a) procede, con il supporto dei Responsabili Interni e dei Referenti, ad una mappatura dei trattamenti di dati personali, valutandone il grado di rischio per i diritti e le libertà degli Interessati;
b) definisce un piano annuale delle attività da svolgere, secondo le priorità stabilite in base alle Aree/Divisioni valutate come maggiormente rischiose nell'ambito della normativa sulla protezione dei dati;
c) redige e consegna all'Università una relazione annuale dell'attività svolta.
7. Il DPO opera in posizione di autonomia e indipendenza: non riceve alcuna istruzione per l'esecuzione dei propri compiti e riferisce direttamente all'Università nella persona del Rettore.

TORNA ALL'INDICE

8. Il provvedimento di nomina del DPO può indicare ulteriori e più specifici compiti.
9. I dati di contatto del DPO sono pubblicati all'interno della sezione privacy presente sul sito dell'Università e comunicati al Garante in base alla procedura informatizzata predisposta dallo stesso.
10. Il DPO, ferme restando le proprie responsabilità, può essere supportato da un ufficio o gruppo di lavoro appositamente nominato.

Articolo 8
(Responsabili Interni)

1. I Responsabili Interni sono individuati all'interno dell'Università tra soggetti che, per esperienza e capacità, forniscano idonea garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali e sono individuati come segue:
− per le Aree dei Servizi tecnico-amministrativi, ciascun dirigente per la propria Area di competenza;
− per le divisioni e i servizi in staff alla Direzione Generale e al Rettorato, il Direttore Generale;
− per il Dipartimento, il Direttore del Dipartimento;
− per la Scuola di dottorato, il Direttore;
− per la Scuola di specializzazione, il Direttore.
2. La nomina dei Responsabili Interni individuati avviene con decreto rettorale dell'Università con cui vengono impartite tutte le istruzioni necessarie a garantire la conformità alla normativa vigente, autorizzando quest'ultimi alla nomina dei Referenti di cui all'articolo 9 del presente Regolamento.
3. I Responsabili Interni coadiuvano l'Università nella definizione delle finalità, delle modalità di trattamento nonché dei mezzi atti a garantire l'osservanza della normativa vigente in materia di protezione dei dati personali; i Responsabili Interni devono altresì assicurare il rispetto della predetta normativa in relazione ai trattamenti svolti nell'ambito della propria struttura di riferimento e di quanto più precisamente identificato nei Registri delle attività di trattamento di cui all'articolo 16 del presente Regolamento. In particolare, i Responsabili Interni sono tenuti, interfacciandosi con il DPO, a:
a) verificare che il trattamento dei dati personali sia effettuato dai propri collaboratori secondo le norme vigenti e le istruzioni operative impartite dall'Università;
b) adottare le opportune misure di sicurezza necessarie a garantire la protezione dei dati personali, quando tali dati vengano raccolti in autonomia dalle Aree di propria competenza e al di fuori degli archivi cartacei e informatizzati o dei server gestiti in maniera centralizzata dall'Università (es. devono essere trattati per impostazione predefinita solo i dati personali necessari per ogni specifica finalità del trattamento, applicando il principio di minimizzazione con riferimento sia alla quantità degli stessi, sia ai tempi di conservazione, ai livelli di accessibilità e alle finalità perseguite).
c) predisporre le informative relative al trattamento dei dati personali, nel rispetto degli articoli 13 e 14 del Regolamento UE, nonché effettuare ogni adempimento organizzativo necessario per garantire agli Interessati l'esercizio dei diritti previsti dalla normativa;
d) individuare e nominare per iscritto, qualora lo ritengano necessario, all'interno della propria Area/Divisione, collaboratori a cui assegnare il ruolo di Referenti, impartendo loro istruzioni specifiche per lo svolgimento dei compiti delegati. La suddetta nomina e l'eventuale cessazione dovranno essere comunicate all'Università e al DPO;
e) provvedere a dare riscontro alle istanze degli Interessati inerenti all'esercizio dei diritti previsti dalla normativa, con il supporto del DPO;
f) fornire al DPO tutte le informazioni necessarie alla predisposizione e all'aggiornamento dei Registri delle attività di trattamento, di cui all'articolo 16 del presente Regolamento, per la parte di propria competenza;
g) raccogliere ogni segnalazione di violazione di dati personali da parte di dipendenti, collaboratori e/o interessati e comunicarla tempestivamente al DPO, all'Università e nel

TORNA ALL'INDICE

caso in cui la violazione abbia ad oggetto dati personali trattati in formato elettronico, all'Ufficio IT. La segnalazione deve avvenire nel rispetto delle istruzioni operative e della procedura di notifica di violazione dei dati personali, consultabile nella sezione privacy del sito dell'Università;
h) comunicare all'Università e al DPO eventuali nuovi trattamenti prima di avviarli, la cessazione di trattamenti in corso, l'acquisizione di nuove tecnologie che prevedano il trattamento di dati personali;
i) collaborare con l'Università e con il DPO al fine di determinare se il trattamento di cui al punto h) che precede può presentare rischi elevati che necessitano di una DPIA di cui all'articolo 18 del presente Regolamento.

Articolo 9
(Referenti)

1.Il Referente, ove ritenuto necessario, è nominato per iscritto dal Responsabile Interno che gli impartisce tutte le istruzioni necessarie allo svolgimento dei propri compiti; la sua nomina, così come la sua eventuale cessazione, deve essere comunicata all'Università e al DPO.
2. Il Referente ha il compito di supportare il Responsabile Interno in tutti gli adempimenti prescritti dalla normativa in materia di trattamento dei dati personali, rapportandosi anche con il DPO.
3. Tutti i Responsabili Scientifici dei progetti di ricerca, di cui l'Università è titolare, sono nominati Referenti Scientifici nell'ambito del singolo progetto. La nomina dei Referenti Scientifici avviene con decreto rettorale dell'Università con cui vengono impartite tutte le istruzioni necessarie a garantire la conformità alla normativa vigente.
I Referenti Scientifici dei progetti di ricerca dell'Università sono tenuti, tra l'altro, a:
a) conformare la propria attività alle "Regole Deontologiche per trattamenti a fini statistici o di ricerca scientifica" ("Regole Deontologiche") emanate dal Garante e alle relative istruzioni impartite dall'Università;
b) adempiere ai compiti di cui all'articolo 8 comma 3, per quanto compatibili. Prima dell'avvio di ogni progetto di ricerca, i Referenti Scientifici compilano la "Scheda di analisi dei rischi dei progetti di ricerca" utilizzando il modello pubblicato alla pagina del sito dell'Università dedicata al Comitato Etico. La suindicata Scheda verrà sottoposta al parere preventivo del Comitato Etico e, qualora quest'ultimo ritenga che la ricerca in oggetto possa comportare rischi per i diritti e le libertà degli interessati, dovrà essere tempestivamente trasmessa al DPO e all'Università unitamente al parere del Comitato Etico e alla ulteriore documentazione a supporto per i conseguenti adempimenti.

Articolo 10
(Autorizzati)

1. Gli Autorizzati al trattamento dei dati sono tutti coloro che sono legati da un rapporto di dipendenza o di collaborazione all'Università e gestiscono dati personali, sia su supporto cartaceo che informatico (personale tecnico amministrativo, docenti, ricercatori, assegnisti, borsisti, stagisti, studenti collaboratori 150 ore ecc.). Sono nominati con decreto rettorale dell'Università con cui vengono impartite tutte le istruzioni atte a garantire che il trattamento dei dati sia effettuato conformemente alle prescrizioni del GDPR.
2. Nello specifico, l'Autorizzato è tenuto:
a) a trattare i dati personali ai quali ha accesso, esclusivamente per lo svolgimento dei trattamenti indicati nei Registri delle attività di trattamento per la propria specifica Area/Divisione, attenendosi alle istruzioni fornite dall'Università o dai Responsabili Interni;
b) a mantenere il segreto e il massimo riserbo sull'attività prestata e su tutte le informazioni di cui sia venuto a conoscenza durante lo svolgimento della stessa;

TORNA ALL'INDICE

c) a segnalare con tempestività - al proprio Referente o, in mancanza, al proprio Responsabile Interno e, nel caso in cui la violazione abbia oggetto dati personali trattati in formato elettronico, al servizio ICT di ateneo - eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare, ove sussista un rischio grave per i diritti e le libertà delle persone fisiche, le procedure di notifica delle violazioni di dati al Garante e di comunicazione ai soggetti Interessati. La segnalazione deve avvenire nel rispetto delle istruzioni operative e della procedura di notifica di violazione dei dati personali, consultabile nella sezione privacy del sito dell'Università.

Articolo 11
(Amministratori di sistema)

1. Possono essere nominati ADS solo i soggetti interni o esterni all'organizzazione in possesso delle necessarie conoscenze e competenze professionali; per i soggetti interni è richiesta, altresì, la congruenza del profilo di servizio unita a una anzianità nel medesimo profilo, almeno annuale; per i soggetti esterni sono, invece, richieste adeguate qualificazioni e certificazioni professionali unite ad esperienza, almeno annuale, ovvero, nel caso di soggetti alle dipendenze di altre organizzazioni, la congruenza del profilo di servizio unita ad una anzianità nel medesimo profilo almeno annuale.
2. Il Dirigente dell'Area Tecnica individua i soggetti che dovranno essere nominati ADS con provvedimento assunto dall'Università; il provvedimento è sempre individuale, reca l'elencazione analitica degli ambiti di operatività consentiti ed è soggetto ad accettazione da parte del nominato. L'anagrafica degli ADS e delle relative attribuzioni è riportata a cura dell'Università, in persona del Dirigente dell'Area Tecnica, in un elenco periodicamente aggiornato e disponibile per gli accertamenti di Legge.
3. L'Università, in persona del Dirigente dell'Area Tecnica, redige annualmente l'inventario degli asset degli impianti di elaborazione (e loro componenti) che sono utilizzati dall'organizzazione (direttamente o in outsourcing) per la gestione di dati personali e che necessitano di amministrazione professionale. Ciascun impianto/componente viene funzionalmente associato ad una articolazione organizzativa o a un progetto di ricerca. Per ciascuno degli impianti/componenti inseriti nell'inventario deve essere individuato e nominato il relativo ADS.
4. Gli ADS svolgono professionalmente le funzioni di gestione e manutenzione di un impianto di elaborazione di dati o di sue autonome componenti (quali ad esempio, in via esemplificativa e non esaustiva componenti software complessi, basi di dati, apparati di sicurezza, apparati di rete ecc.) con cui vengono effettuati trattamenti di dati personali. Gli ADS sono responsabili del proprio operato, caratterizzato da discrezionalità tecnica, e delle conseguenze derivanti da malfunzionamenti a loro imputabili.
5. L'operato degli ADS è oggetto, con cadenza almeno annuale, di verifica da parte dell'Università finalizzata al controllo della rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.
6. Gli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli ADS devono essere registrati; le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità, devono permettere la verifica della loro integrità, al fine di garantire il raggiungimento dello scopo di verifica per cui sono richieste, e devono essere conservate per un periodo non inferiore a sei mesi, salvo diverse indicazioni di legge.

Articolo 12
(Responsabile Esterno del Trattamento)

1. È Responsabile Esterno del trattamento qualunque soggetto esterno che esegue, in base a un contratto, una convenzione o altro atto giuridico, trattamenti di dati personali per conto dell'Università.

TORNA ALL'INDICE

2. Il Responsabile Esterno del trattamento è nominato con atto giuridico conforme a quanto richiesto dall'articolo 28 del Regolamento UE e può a sua volta nominare altri responsabili, ove espressamente previsto nell'atto di nomina ("Sub-responsabili"). In tal caso il Responsabile Esterno vincola il Sub-responsabile con un contratto che contenga gli stessi obblighi previsti nel contratto tra il Responsabile Esterno e l'Università.
3. Nell'ambito delle rispettive competenze in materia di stipulazione dei contratti, all'Università e ai Responsabili Interni può essere delegato il potere di stipulare, con i soggetti esterni che collaborano con l'Università per l'esercizio delle funzioni istituzionali, gli atti negoziali per la gestione dei trattamenti.
4. Il Responsabile Esterno del Trattamento risponde nei confronti dell'Università del proprio inadempimento nonché di quello degli eventuali Sub-responsabili, anche ai fini del risarcimento di eventuali danni causati dal trattamento.

Capo III - Modalità per il trattamento dei dati

Articolo 13
(Dati personali - Criteri)

1. Ciascun Autorizzato che tratta dati personali per conto dell'Università deve assicurarsi che il trattamento dei dati di propria competenza avvenga secondo i criteri di seguito indicati. I dati dovranno essere:
a) trattati in modo lecito- in presenza di una delle basi giuridiche di cui all'articolo 3 del presente Regolamento - corretto e trasparente;
b) raccolti per scopi determinati, espliciti e legittimi;
c) riportati in maniera esatta e, quando necessario, aggiornati tempestivamente;
d) adeguati, pertinenti, completi e non eccedenti le finalità per le quali sono raccolti o successivamente trattati;
e) conservati in una forma che consenta l'identificazione degli Interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
f) trattati in modo da garantire un'adeguata sicurezza, mediante l'adozione di misure tecniche e organizzative, impedire trattamenti non autorizzati o illeciti ovvero perdite, distruzioni o danni accidentali.

Articolo 14
(Trattamento di categorie particolari di dati personali)

1. Il trattamento di dati che rivelino l'origine etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché il trattamento di dati genetici, di dati biometrici intesi a identificare in modo univoco una persona fisica, di dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona è consentito solo nei limiti e alle condizioni di cui all'articolo 9, paragrafi 2 e 3 del Regolamento UE e in presenza di una delle basi giuridiche previste all'articolo 3 del presente Regolamento.

Articolo 15
(Trattamento di dati a fini di ricerca scientifica o a fini statistici)

1. Il trattamento di dati personali a fini di ricerca scientifica o a fini statistici deve essere effettuato conformemente alle Regole Deontologiche nonché alle Istruzioni operative fornite dall'Università.
2. Si potrà procedere al trattamento di dati personali per il perseguimento delle finalità di cui al punto che precede solo ove siano osservati i seguenti adempimenti:
a) la ricerca sia effettuata in conformità agli standard metodologici del pertinente settore disciplinare con redazione della "Scheda di analisi dei rischi dei progetti di ricerca" utilizzando il modello pubblicato alla pagina del sito dell'Università dedicata al Comitato Etico dove sia indicato il Referente Scientifico per lo specifico progetto di ricerca e precisate le misure adottate al fine di garantire il rispetto delle Regole Deontologiche e, in

TORNA ALL'INDICE

generale, della normativa privacy con allegata dichiarazione di impegno da parte dello stesso a conformarsi a tali regole (analoga dichiarazione deve essere sottoscritta anche dai soggetti - ricercatori, responsabili e Autorizzati - coinvolti nella ricerca);
b) sia redatta e resa agli Interessati l'informativa ai sensi degli articoli 13 e/o 14 del GDPR;
c) ove nell'ambito del progetto di ricerca siano trattati dati particolari ex articoli 9 e 10 del GDPR sia raccolto il consenso dell'Interessato, come previsto dall'articolo 7, comma 2 lettera a) delle Regole Deontologiche;
d) la documentazione sopra indicata sia depositata presso la struttura amministrativa competente e presentata al Comitato Etico;
e) la DPIA, ove risultata necessaria ai sensi dell'articolo 8 comma 3 del presente Regolamento, non rilevi rischi elevati per i diritti e le libertà degli Interessati;
f) il Comitato Etico esprima parere positivo sul progetto di ricerca;
g) le attività di ricerca siano svolte secondo quanto indicato nel progetto presentato al Comitato Etico e delle eventuali indicazioni risultanti dalla DPIA.
3. I dati personali possono essere conservati per scopi statistici o scientifici anche oltre il periodo necessario per il raggiungimento degli scopi per i quali sono stati raccolti o successivamente trattati, in conformità all'articolo 5, comma 1, lettera e) del Regolamento UE.

Articolo 16
(Registri delle attività di trattamento)

1. L'Università, in qualità di Titolare, istituisce ed aggiorna il Registro delle attività di trattamento dei dati personali, nel quale sono individuati i trattamenti effettuati da ogni Area/Divisione per lo svolgimento dei compiti istituzionali dell'Università. La tenuta del Registro è affidata al DPO che dovrà essere supportato dai Responsabili Interni e dai Referenti, secondo quanto previsto dagli articoli 7 e 9 comma 2.
Il Registro contiene almeno le seguenti informazioni:
a) nome e dati di contatto del Titolare, degli eventuali Contitolari nonché del DPO;
b) le finalità del trattamento;
c) la descrizione delle categorie degli Interessati e delle categorie di dati personali trattati;
d) le categorie di destinatari a cui i dati personali sono o saranno comunicati;
e) la descrizione generale delle misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza del trattamento secondo quanto previsto dall'articolo 32, comma 1, del Regolamento UE;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati, o i criteri per determinare il periodo di conservazione degli stessi;
g) i trasferimenti di dati personali verso un Paese Terzo o un'organizzazione internazionale con la loro identificazione nominativa nonché delle misure adottate ai sensi del capo V del Regolamento UE.
2. L'Università istituisce e aggiorna il Registro delle attività di trattamento, in qualità di Responsabile Esterno, nel quale sono descritte le attività di trattamento svolte per conto di altri Titolari. Il registro contiene almeno le informazioni di cui all'articolo 30, comma 2 del Regolamento UE e precisamente:
a) nomi e dati di contatto dell'Università, del Titolare per conto del quale il trattamento è svolto, di eventuali Sub-Responsabili del trattamento e dei relativi DPO;
b) le categorie di trattamenti effettuati per conto di ogni Titolare;
c) l'eventuale trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale con la loro identificazione nominativa nonché delle misure adottate ai sensi del Capo V del Regolamento UE;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative adottate per garantire la sicurezza del trattamento secondo quanto previsto dall'articolo 32, comma 1, del Regolamento UE.

TORNA ALL'INDICE

3. I Registri di cui ai commi 1 e 2 sono tenuti in formato elettronico e aggiornati periodicamente. La tenuta dei predetti Registri, unica per tutta l'Università, è affidata al DPO, il quale coordina le attività di implementazione e aggiornamento sistematico degli stessi a opera dei singoli Responsabili Interni e/o Referenti. A quest'ultimi spetta la responsabilità sulla completezza e adeguatezza dei dati e delle misure di sicurezza indicate per la parte di loro competenza.

Articolo 17
(Procedure e istruzioni operative)

1. Al fine di garantire l'effettivo rispetto della normativa in materia di protezione dei dati personali, l'Università adotta procedure e istruzioni operative.
2. Le procedure definiscono le regole e le misure organizzative da osservare a garanzia dell'efficacia di determinati adempimenti prescritti dal Regolamento UE. La redazione delle procedure è affidata al DPO in collaborazione con i Responsabili Interni, i Referenti di ciascuna Area/Divisione competente, il Comitato Etico per la Ricerca. L'Università ha adottato:
- la procedura di richiesta di accesso ai diritti degli interessati;
- la procedura per l'analisi del rischio e DPIA;
- la procedura di notifica di violazione dei dati personali;
- la procedura per il trasferimento dei dati personali verso Paesi extra UE e Organizzazioni internazionali.

L'Università ha, inoltre, adottato il "Regolamento per l'accesso e l'utilizzo del servizio internet e del servizio di posta elettronica".
3. Le istruzioni operative sono adottate dall'Università e aggiornate periodicamente. Tuttavia, ciascun Responsabile Interno e/o Referente può maggiormente dettagliare le istruzioni predisposte dall'Università, al fine di garantire maggiore operatività delle stesse rispetto alla mansione svolta e/o ai compiti delegati all'Autorizzato operante nella propria Area/Divisione.
4. L'Università, il Responsabile Interno o il Referente, contestualmente alla nomina degli Autorizzati, forniscono le istruzioni operative che quest'ultimi sono tenuti a rispettare a garanzia della conformità delle attività di trattamento dei dati personali al GDPR, ivi inclusa la componente della sicurezza delle informazioni secondo quanto disposto dagli articoli 7 - 10 del presente Regolamento.

Articolo 18
(Valutazione di impatto - DPIA)

1. L'Università, quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, tenuto conto della natura, dell'oggetto, del contesto, delle finalità del trattamento e dell'utilizzo di nuove tecnologie, effettua, ai sensi dell'articolo 35 del GDPR, una DPIA. Una singola DPIA può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi. L'Università, con la collaborazione dei Responsabili Interni e/o dei Referenti delle Aree/Divisioni interessate, del Comitato Etico per la Ricerca, del DPO, determina i casi in cui è necessario svolgere una DPIA nel rispetto di quanto previsto dalle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Gruppo di lavoro Articolo 29 il 4 aprile 2017 e modificate il 4 ottobre 2017, nonché il provvedimento n. 467 dell'11 ottobre 2018 (doc. web. 9058979) del Garante.
2. La DPIA è obbligatoria nei seguenti casi:
− 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 su dette persone fisiche;

TORNA ALL'INDICE

− trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, comma 1 del GDPR, o di dati relativi a condanne penali e a reati;
− sorveglianza sistematica su larga scala di una zona accessibile al pubblico (videosorveglianza).
3. L'Università, il Responsabile Interno o il Referente delle Aree/Divisioni interessate si consultano con il DPO sulla necessità o meno di effettuare la DPIA, nel rispetto di quanto previsto al precedente comma 1; tale consultazione e le conseguenti decisioni assunte devono essere documentate. L'Università può, documentandone le motivazioni, adottare condotte difformi da quelle raccomandate dal DPO. I Responsabili Interni e i Referenti competenti sono tenuti a collaborare nella conduzione della DPIA, fornendo ogni informazione e documentazione necessaria. Il Responsabile per la transizione al digitale di cui all'articolo 17 del decreto legislativo 82/2005 fornisce supporto ai Responsabili Interni, ai Referenti e al DPO per lo svolgimento della DPIA. L'Università, in collaborazione con il DPO, consulta il Garante nel caso in cui le risultanze della DPIA condotta indichino l'esistenza di un rischio residuale elevato.

Capo IV - Diritti dell'interessato e misure di sicurezza

Articolo 19
(Diritti dell'Interessato)

1. All'Interessato sono riconosciuti i diritti di cui agli articoli da 15 a 22 e 77 del Regolamento UE e, più precisamente, il diritto di:
a) accesso ai dati personali: il diritto di ottenere dall'Università la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali e alle informazioni di cui all'articolo 15 del GDPR;
b) rettifica: il diritto di ottenere dall'Università, senza ingiustificato ritardo, la rettifica dei dati personali inesatti che lo riguardano e l'integrazione dei dati incompleti;
c) cancellazione («diritto all'oblio»): il diritto di ottenere dall'Università la cancellazione dei dati personali che lo riguardano, senza ingiustificato ritardo, salvo nei casi previsti dall'articolo 17, comma 3, del Regolamento UE;
d) limitazione al trattamento, nelle ipotesi previste dall'articolo 18 del Regolamento UE;
e) portabilità dei dati: il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti all'Università e il diritto di trasmettere tali dati ad un altro Titolare senza impedimenti da parte dell'Università, nelle ipotesi di cui all'articolo 20 del Regolamento UE;
f) opposizione: il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, comma 1, lettere e) o f), del GDPR, compresa la profilazione. In questo caso l'Università si astiene dal trattare ulteriormente i dati personali salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'Interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
g) a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato relativo alle persone fisiche, compresa la profilazione, che produca effetti giuridici nei confronti dell'Interessato stesso o che incida in modo analogo significativamente sulla propria persona, fatti salvi i casi in cui ciò è previsto dalla legge.
h) proporre reclamo al Garante.
2. L'Università fornisce riscontro all'Interessato riguardo le richieste di cui al comma 1 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Se l'Università non è in grado di ottemperare alle richieste dell'Interessato nei termini previsti, informa quest'ultimo senza ritardo, al più tardi entro un mese dal ricevimento della richiesta. Tale comunicazione

TORNA ALL'INDICE

dovrà indicare i motivi dell'inottemperanza, la possibilità di proporre reclamo al Garante ovvero ricorrere all'Autorità giudiziaria.

Articolo 20
(Informativa)

1. Prima di procedere alla raccolta e/o al trattamento di dati personali, l'Università deve fornire all'Interessato idonea informativa, ai sensi degli articoli 13 e 14 del Regolamento UE. L'informativa deve essere concisa, trasparente, intelligibile, facilmente accessibile e redatta con un linguaggio chiaro e semplice.
2. Qualora i dati siano raccolti presso l'Interessato, l'informativa deve essere resa nel momento in cui i dati personali sono ottenuti, e deve contenere:
a) l'identità e i dati di contatto dell'Università;
b) i dati di contatto del DPO;
c) le finalità e le modalità del trattamento nonché la base giuridica del trattamento di cui all'articolo 3 del presente Regolamento, precisando la natura obbligatoria o facoltativa del conferimento con l'indicazione delle possibili conseguenze in caso di mancato conferimento di tali dati;
d) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
e) l'indicazione dell'eventuale trasferimento dei dati personali a un Paese Terzo o a un'organizzazione internazionale, e, in caso affermativo, gli strumenti utilizzati ai sensi del Capo V del GDPR;
f) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
g) 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 e, in generale, tutti i diritti previsti dagli articoli da 15 a 22 del Regolamento UE;
h) la necessità di comunicare i dati personali in base a un obbligo legale o contrattuale,
i) l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le conseguenze previste da tale trattamento per l'Interessato.
3. Nel caso in cui i dati personali già raccolti debbano essere trattati per una finalità diversa da quella per cui sono stati ottenuti, l'Università, prima di procedere con l'ulteriore trattamento, deve fornire 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'articolo 5, lettera b) e all'articolo 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.
4. L'Università deve rendere l'informativa ogni qualvolta intenda procedere con un nuovo trattamento.
5. Nel caso in cui i dati non siano raccolti presso l'Interessato, ma presso terzi, l'informativa deve essere fornita entro un termine ragionevole, e comunque non oltre un mese dalla raccolta dei dati ovvero al momento della prima comunicazione di quest'ultimi a terzi. L'informativa deve contenere oltre che gli elementi suindicati anche le categorie di dati trattati e le relative fonti di provenienza.
6. L'aggiornamento o la redazione delle informative rientra nei compiti di vigilanza del Responsabile Interno e/o del Referente competente.
7. Le informative redatte dall'Università sono pubblicate sul sito di Ateneo.

TORNA ALL'INDICE

Articolo 21

(Sicurezza dei dati personali)

1. Al fine di garantire la sicurezza dei dati personali, l'Università, i Responsabili Interni e i Referenti nelle Aree/Divisioni di propria competenza, adottano misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio connesso al trattamento. Tali misure sono finalizzate a ridurre al minimo il rischio di distruzione, perdita, modifica, divulgazione o accesso non autorizzato, accidentale o volontario, ai dati personali trasmessi, conservati o comunque trattati dall'Università.
2. I Responsabili Interni e i Referenti adottano le misure di cui al comma 1 sulla base e nell'ambito delle indicazioni fornite dall'Università.
3. Le misure tecniche e organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento sono, tra le altre, la minimizzazione e la cifratura dei dati personali, la capacità di assicurare la continua riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali nonché la capacità di ripristinare tempestivamente l'accesso e la disponibilità dei dati in caso di incidente fisico o tecnico.

Articolo 22

(Notifica al Garante di violazione dei dati personali - procedura di "data breach")

1. In caso di violazione di dati personali, che comporti - 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 dall'Università, i Responsabili Interni e/o i Referenti, mediante l'apposito modello disponibile sul sito dell'Ateneo, ne danno tempestiva comunicazione al Titolare e al DPO.
2. Le violazioni di dati personali sono gestite dal Titolare o da un suo delegato, sotto la supervisione del DPO, secondo la procedura di cui al documento "Procedura di notifica di violazione dei dati personali" pubblicata nella sezione privacy del sito di Ateneo.

Articolo 23

(Dati personali concernenti persone decedute)

1. Ai sensi dell'articolo 2 terdecies del Codice Privacy, i diritti relativi ai dati personali dei defunti possono essere esercitati da chi ha un interesse proprio, oppure agisce a tutela del defunto quale mandatario o per ragioni familiari meritevoli di protezione.
2. L'esercizio dei diritti di cui al comma 1 non è ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della società dell'informazione, l'Interessato lo ha espressamente vietato con dichiarazione scritta inequivocabile presentata al Titolare o a quest'ultimo comunicata.
3. L'Università, tuttavia, non potrà rifiutare al terzo l'accesso ai dati del defunto qualora quest'ultimo agisca a tutela dei propri diritti patrimoniali che derivano dalla morte dell'Interessato o per far valere in giudizio i propri interessi.

Articolo 24

(Norme di rinvio)

1 Le norme del presente Regolamento trovano applicazione in conformità e a integrazione del Regolamento UE, del Codice Privacy, come modificato e integrato dal Decreto Legislativo n. 101 del 10 agosto 2018, dal Modello Organizzativo approvato dal Consiglio di Amministrazione dell'Università e periodicamente aggiornato nonché, per quanto compatibili, dei Regolamenti interni dell'Università, in particolare del Regolamento per l'accesso e l'utilizzo del servizio internet e del servizio di posta elettronica, del Regolamento sul diritto di accesso agli atti, di accesso civico semplice e di accesso generalizzato dell'Università.